Bürgerrechte & Polizei

Cilip 85
Nr. 3/2006

Hilfloser Datenschutz

Polizei und Geheimdienste gegen Amokläufer und „Terrorismusverdächtige"
Polizeirecht durch die Bremer Dunkelbrille

Inhalt

Hilfloser Datenschutz

Redaktionsmitteilung

Im September 2001, kurz nach den Anschlägen in den USA, räsonierte der damalige Bundesinnenminister Otto Schily darüber, dass man es hierzulande „vielleicht … im Datenschutz etwas übertrieben" hätte. Der Minister beließ es bekanntlich nicht bei der Nachdenklichkeit, sondern präsentierte in Windeseile ein Paket von Gesetzesänderungen. Der „Otto-Katalog" trat Anfang Januar 2002 als Gesetz zur Bekämpfung des internationalen Terrorismus in Kraft. Die darin auf fünf Jahre befristeten Befugnisse der Geheimdienste hat der Bundestag am 1. Dezember 2006 verlängert und erweitert. Am selben Tag verabschiedete er auch ein Gesetz über gemeinsame Dateien von Polizei und Geheimdiensten.

Was der Ex-Minister, der heute auch als Berater einer Biometriefirma tätig ist, in etwas feiner ziselierten Worten ausdrückte, ist nichts anderes als das alte Stammtisch-Motto vom Datenschutz als „Täterschutz". Es durchzieht die Diskussion um polizeiliche und geheimdienstliche Methoden und Instrumente seit den 70er Jahren. Und es erweist sich in seiner ganzen Banalität als äußerst wirksam.

Der Datenschutz scheint die letzte Verteidigungslinie der Bürgerrechte gegen die Angriffe der Kriminalitäts- und Unsicherheitsbekämpferlnnen zu sein. Der Hoffnungsträger steht jedoch auf einem hoffnungslosen Posten, bei dem er durch die permanent ratternde Gesetzgebungsmaschinerie regelmäßig übertönt wird. Fortsetzungen zu diesem Thema sind deshalb auch in der Zukunft sicher.

***

Bürgerrechte & Polizei/CILIP wird sich im Schwerpunkt der nächsten Ausgabe mit dem Thema „Polizei und Prävention" befassen.

Hilfloser Datenschutz

Verrechtlichung, Individualisierung, Entpolitisierung

von Heiner Busch

Die Verrechtlichungsspirale dreht sich unaufhörlich und füllt Polizei- und Geheimdienstgesetze mit datenschutzrechtlicher Poesie. Entpolitisiert droht der Datenschutz zum legitimatorischen Beiwerk zu verkommen.

Privacy International (PI) ist eine in London ansässige internationale Datenschutzorganisation. Sie hat die „Big Brother Awards", jene Negativpreise für die besten Schnüffler, erfunden, die Bürgerrechts- und Datenschutzorganisationen mittlerweile in vielen europäischen Ländern jährlich vergeben. Anfang Oktober 2006 veröffentlichte PI ihren diesjährigen „International Privacy Survey", der im Unterschied zu den Big Brother Awards durchaus nicht ironisch gemeint ist.[1] Die Bundesrepublik Deutschland hat dabei nicht nur im Vergleich zu den anderen europäischen Staaten, sondern weltweit die besten Noten für ihren Datenschutz erhalten. Selbst im Bereich „Law enforcement" erzielte sie einen Spitzenplatz. Wir gratulieren.

Aber wundern müssen wir uns doch ein wenig. Sicher: die Zahl der Videokameras im öffentlichen Raum ist in Britannien erheblich höher als etwa in Deutschland, und auch was die Quote der in der polizeilichen DNA-Datei erfassten Personen anbetrifft, reicht keine Polizei des Kontinents an die der Insel heran. Die Datenschutzbeauftragten haben in Deutschland ihren festen Platz, das Recht auf informationelle Selbstbestimmung gilt seit dem Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983 als ein Grundrecht, als Teil des allgemeinen Persönlichkeitsrechtes.[2] Kaum ein Gesetz dieses Landes kommt ohne

1 www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269

2 BVerfG: Volkszählungsurteil v. 15.12.1983, in: Neue Juristische Wochenschrift (NJW) 1984, H. 8, S. 419-428

Datenschutzbestimmungen aus. Und das gilt in besonderem Maße für Polizei- und Geheimdienstgesetze, in denen teilweise über die Hälfte der Paragrafen daten- und datenschutzrechtliche Regelungen sind. So gesehen, hat sich der Datenschutz hierzulande durchgesetzt.

Spirale der Verrechtlichung

Kein Zweifel, das Volkszählungsurteil hat deutlich gemacht, dass die neue Informationstechnologie – insbesondere in den Händen von Polizei und Geheimdiensten – auch neue Gefahren für die Freiheit der BürgerInnen mit sich bringt. Die Gegenmittel dazu schienen Transparenz, d.h. Rechte auf Auskunft und daran anknüpfend auf die Berichtigung und Löschung falscher und nicht (mehr) erforderlicher Daten, sowie die Forderung nach Zweckbindung, die zu dem zentralen Bestandteil des Datenschutzrechtes wurde. Indem das Gericht das „Recht auf informationelle Selbstbestimmung" formulierte, machte es den staatlichen Umgang mit Informationen zu einem Grundrechtseingriff. Und das bedeutete auch, dass sämtliche Formen der Erhebung, Verarbeitung und Weitergabe nun einer förmlichen gesetzlichen Grundlage bedurften.

Die erste Welle der neuen datenschutzrechtlich motivierten Gesetzgebung setzte unmittelbar nach dem Urteil ein und dauerte bis etwa 1990. In diese Periode fallen u.a. der Musterentwurf eines einheitlichen Polizeigesetzes (1986) und die darauf aufbauenden Gesetze der Länder, eine erste Änderung der Strafprozessordnung (§ 163d, Schleppnetzfahndung), die Einführung maschinenlesbarer Pässe und Personalausweise sowie die Geheimdienstgesetze, für die ab 1986 ständig neue Pakete von Entwürfen präsentiert wurden, die sich nur in den Formulierungen, aber nicht im Inhalt unterschieden. Sie gingen im Dezember 1990 unter dem Titel „Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes" über die parlamentarische Bühne.[3] Sieht man von den neuen (und heute alten) Pässen und Personalausweisen ab, so ging es in dieser ersten Welle von Gesetzen nach dem Volkszählungsurteil vor allem darum, die im Jahrzehnt zuvor aufgebaute polizeiliche und geheimdienstliche Datenverarbeitung und das bestehende Set von Methoden abzusichern. Diese wurden nun in Datenerhebungsregeln und in Bestimmungen umgegossen, die die Weiternutzung zu anderen Zwecken

3 Bundesgesetzblatt I Nr. 73 v. 29.12.1990, S. 2954-2981

gestatteten – für polizeiliche Aufgaben im „Vorfeld“, die z.T. rechtlich erst erfunden werden mussten (typisch: vorbeugende Bekämpfung von Straftaten, Vorsorge für die Gefahrenabwehr oder die zukünftige Strafverfolgung etc.). Ergebnis dessen waren unbestimmte, häufig auch sprachlich nicht mehr nachvollziehbare Befugnisnormen -gebunden an ellenlange Kataloge von Anlassstraftaten oder an einen unwirksamen Anordnungsvorbehalt des Behördenleiters, der Staatsanwaltschaft oder eines Ermittlungsrichters.

Auch nach 1990 drehte sich die Verrechtlichungsspirale weiter – und zwar meist nach dem selben Muster: Die Polizei oder die Geheimdienste „entdecken“ eine neue Technik oder Ermittlungsmethode oder dehnen den Anwendungsbereich bereits eingeführter Methoden aus. Sie tun das zunächst unter Berufung auf den Fundus der bereits bestehenden Eingriffsnormen. Der rechtliche Rahmen wird gedehnt bzw. überdehnt, bis Betroffene dagegen klagen und die Gerichte – vor allem die Verfassungsgerichte – das Fehlen oder die Mangelhaftigkeit der gesetzlichen Grundlage rügen. Der Gesetzgeber begibt sich an die Arbeit und schiebt eine Regelung nach. Am Ende ist alles mehr oder weniger sauber geregelt. Und gerade weil dies der Fall ist, kann die legalisierte neue Technik nun zur Routine werden. Sie wird unter Umständen viel häufiger angewandt, als das vor der gesetzlichen Regelung der Fall war. Herausgekommen ist bestenfalls eine Standardisierung der neuen Methoden, die allzu skandalöse Auswüchse verhindert.

Nur in zwei Fällen ist diese rechtsstaatliche Absicherung nicht erfolgt: So hat der Gesetzgeber zwar bereits 1992 mit dem Gesetz zur Bekämpfung des illegalen Drogenhandels und anderer Formen der organisierten Kriminalität (OrgKG) den Einsatz Verdeckter Ermittler, nicht aber den von V-Leuten im Strafprozess geregelt. Für diese nebenamtlichen Spitzel finden sich gesetzliche Bestimmungen nur im Polizeirecht der Länder. Im Falle der Ortung durch Peilsender, die durch ihre Verbindung mit dem Global Positioning System ständig den genauen Standort eines observierten Fahrzeuges anzeigen, war es das Bundesverfassungsgericht selbst, das eine Verrechtlichung dieser seit Ende der 90er Jahre angewandten Methode für unnötig und die Überdehnung des § 100c Abs. 1 StPO (Einsatz technischer Mittel bei Observationen) für rechtmäßig erklärte.[4] Dass eine Verrechtlichung in diesen Fällen jedoch

4 Urteil v. 12.4.2005, Az.: 2 BvR 581/01

mehr gebracht hätte als die Bestätigung der bestehenden Praxis, ist kaum zu erwarten. Auch ein Gesetz macht aus einem Spitzel keine vertrauenswürdige Person.

Die kontinuierliche Legalisierung neuer Techniken und Methoden der Polizei und der Geheimdienste verengt aber auch den Rahmen, der den Datenschutzbeauftragten für ihre Tätigkeit zur Verfügung steht. Ihre kritischen Stellungnahmen vor der Verabschiedung von Gesetzen gehören mittlerweile genauso zum Ritual der Verrechtlichung wie die Tatsache, dass sich die jeweilige parlamentarische Mehrheit keinen Deut um diese Kritik schert. Sobald das Parlament seinen rechtlichen Segen erteilt hat, können die Datenschutzbeauftragten nur noch den *Missbrauch* eines neuen Instruments zu privaten/kriminellen Zwecken oder den Übereifer einzelner MitarbeiterInnen von Polizei oder Geheimdiensten beanstanden. Sie treffen dabei mit ihren Rügen durchaus auf das Wohlwollen der Behörden. Der *Gebrauch* zu den im Gesetz vorgesehenen Zwecken ist der Kritik entzogen – zumindest solange das Bundesverfassungsgericht nicht erneut Grenzen setzt.

Individualisierung

Das hat es in seinen Urteilen zum Großen Lauschangriff (2004) und zur präventiven Telefonüberwachung (2005) getan, indem es festhielt, dass der „Kernbereich privater Lebensgestaltung" die definitive Grenze für polizeiliche und geheimdienstliche Überwachungsmaßnahmen sei.[5] Die Gesetzgeber in Bund und Ländern tun sich schwer mit den Urteilen, und es ist durchaus wahrscheinlich, dass das eine oder andere Gesetz, das die Vorgaben aus Karlsruhe umsetzen soll, erneut dort landet. Die beiden Entscheidungen lösten in Datenschutzkreisen eine ähnliche Euphorie aus wie seinerzeit das Volkszählungsurteil.

Aber das ist nur die eine Seite. So begrüßenswert es ist, dass das Verfassungsgericht den LauscherInnen eine Grenze gezogen hat, so offensichtlich ist aber auch, dass der überwachungsfreie „Kernbereich" eine Rückzugsposition darstellt – überspitzt formuliert: eine Art Schlafzimmer-Datenschutz. Geschützt ist eben nur noch das engste intime Umfeld des Individuums, nicht aber sein soziales oder politisches Handeln, das sich in der Öffentlichkeit abspielt. Bezeichnenderweise erging

5 BVerfG: Urteil v. 27.7.2005, in: NJW 2005, H. 36, S. 2603-2612; Urteil v. 3.3.2004, in: NJW 2004, H. 14, S. 999-1020

das zitierte GPS-Urteil des Verfassungsgerichts im selben Zeitraum und erklärte alle möglichen Überwachungsmethoden, die in diesem Fall kumuliert und außerhalb des Kernbereichs angewandt wurden, für rechtens und verfassungsmäßig.

Diese Tendenz zur Individualisierung war bereits im Volkszählungsurteil angelegt. Das Recht auf informationelle Selbstbestimmung erscheint dort als ein Recht auf den Besitz der eigenen privaten Daten, der Bürger als eine Art Daten-Besitzbürger. Konsequenterweise forderte das Gericht damals, dass der Gesetzgeber eine Güterabwägung zwischen den (nur) privaten Interessen der BürgerInnen an ihren Daten und dem öffentlichen Interesse, verkörpert durch den Staat, vorzunehmen habe – eine Abwägung, bei der die „privaten" Rechte zwangsläufig als zu leicht befunden werden: „Der einzelne hat nicht ein Recht im Sinne einer absoluten Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Das Grundgesetz hat ... die Spannung Individuum – Gemeinschaft im Sinne einer Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden ... Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen."[6]

Immerhin hatte das Gericht 1983 nicht nur die Intimsphäre, sondern ein gesellschaftlich und politisch aktives Individuum vor Augen: „Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten." Die „Risiken der modernen Datenverarbeitung", auf die sich das Bundesverfassungsgericht hier bezog, waren die Gefahren einer politischen Überwachung, deren Folgen im Zeitalter der Berufsverbote auf der Hand lagen.

Veraltet und unpolitisch

Was 1983 als „moderne" Datenverarbeitung galt, mutet dagegen heute fast schon steinzeitlich an. Zur Erinnerung: 1983 sorgten die Aussagen eines ehemaligen Mitarbeiters des Bundeskriminalamts (BKA) gegenüber dem „Spiegel" für helle Aufregung: Im Rahmen der „Aktion Paddy"

6 BVerfG: Volkszählungsurteil a.a.O. (Fn. 2)

hatte das BKA zwei Jahre zuvor dreizehn „Hochleistungskameras“ in und um Heidelberg aufgebaut, um die Zufahrtswege zum Nato-Hauptquartier zu überwachen und vor Anschlägen der RAF zu schützen. Die Übertragung der Bilder in die polizeiliche Zentrale war seinerzeit nur unter größtem Aufwand möglich.[7] Heute ist die Übertragung von Kamera-Bildern rund um die Welt ein zweifelhafter Spaß, den sich jede Privatperson und die Polizei sowieso problemlos leisten kann. Die lückenlose Überwachung öffentlicher Räume (CCTV), in britischen und vielen französischen Städten längst realisiert, ist in Deutschland nur vorerst abgewehrt. Das traditionelle Datenschutzrecht mit seiner Unterteilung in Erhebung, Verarbeitung und Weitergabe von Daten war auf Eingriffe gegen Einzelne ausgerichtet. Angesichts dieser alltäglichen Massenüberwachung erscheint seine Logik hoffnungslos veraltet – umso mehr als der Betrieb solcher Anlagen im Joint Venture zwischen Privaten und Staat auch eine Trennung von Verantwortlichkeiten für Erhebung, Verarbeitung und Weitergabe fiktiv werden lässt.

Ähnliches gilt für das Recht der Telefonüberwachung, das auf die traditionelle Festnetztelefonie gemünzt war, aber bruchlos auf die neuen Formen der Telekommunikation übertragen wurde. So erscheint der Zugriff auf Verkehrsdaten immer noch als ein im Vergleich zum Belauschen des Kommunikationsinhalts harmloser Eingriff, obwohl eine Vielzahl neuer Methoden wie der räumlichen Ortung von Handys gerade auf diese Daten aufbaut. Die Möglichkeiten der Kontrolle digitalisierter Kommunikation dürften noch in den Anfängen stecken. Erkennbar ist aber schon jetzt eine Tendenz zur Automatisierung der Überwachung. Der Datenschutz und sein Recht drohen von der technischen Entwicklung überrollt zu werden.

Er steht aber auch vor der Gefahr der Entpolitisierung: Noch vor wenigen Jahren diente die Biometrie vor allem dazu, den Zutritt zu den allerheiligsten Innenräumen von Banken auf die wenigen „Befugten“ zu begrenzen. Das jetzt im Aufbau befindliche Visa-Informationssystem (VIS) der EU dürfte innerhalb von wenigen Jahren hundert Millionen Datensätze umfassen und (vorläufig) die weltweit größte biometrische Datenbank werden. Die Biometrie ermöglicht nun die „Zutrittskontrolle“ zur Festung Europa und die Identifizierung von „Unbefugten“ in ihrem Innern. Eine Kritik, die das VIS als Datenschutzproblem diskutiert

7 Meyer-Larsen, W.: Der Orwell-Staat 1984, Reinbek 1983 (zuerst im „Spiegel“)

und Missbräuche verhindern will, geht daher an der politischen Realität vorbei.

Dasselbe gilt für die verdeckten Methoden von Polizei und Geheimdiensten, die rechtlich als „besondere Formen der Datenerhebung" verhandelt werden, als ginge es bloß um das Abgreifen einer Datenspur, die die Betroffenen unachtsam gelegt haben und nicht um gewöhnliche Spitzelei und geheimpolizeiliche Methoden mit all den Widerlichkeiten, die damit verbunden sind. Wo beginnt hier der Missbrauch und was ist mit dem Gebrauch? Die Zerstörung von Vertrauen und die Zersetzung sozialer Zusammenhänge, die eine solche Infiltration bewirkt und oftmals auch bezweckt, lässt sich nicht datenschutzrechtlich erfassen.

Das Gegenteil von „gut" ist „gut gemeint"

Zurück zum Ausgangspunkt: Deutschland konnte bei dem „Survey" von „Privacy International" deshalb gut abschneiden, weil die durchaus ehrenwerte Organisation nach Datenschutzgesetzen und -institutionen Ausschau hielt. Vor dem Hintergrund der britischen und US-amerikanischen Deregulierung mögen diese Bewertungskriterien nachvollziehbar sein. Das deutsche Beispiel zeigt allerdings, dass die Verrechtlichung eben keine politische Perspektive ergibt.

Das heißt nicht, dass der Kampf um Rechtspositionen, um Normenklarheit und Berechenbarkeit aufzugeben wäre. Er ist aber von vornherein verloren, wenn der Ausstieg aus der Bekämpfungslogik, die die rechtliche Entwicklung im „Sicherheitsbereich" in den letzten zwei Jahrzehnten bestimmt hat, nicht gelingt. Wer die Zielvorgaben der „Bekämpfung" des Terrorismus, der Organisierten Kriminalität, der „illegalen Einwanderung", der Jugendgewalt etc. akzeptiert, wird zwangsläufig zum Opfer der „Bedürfnisse der Praxis" und kann polizeilich-geheimdienstlichen Überwachungswünschen keine grundsätzlichen Alternativen mehr entgegensetzen. Ebenso unausweichlich wird dann die Reduktion des Datenschutzes auf unpolitische „Kernbereiche".

Wenn der Datenschutz nicht zur Legitimation polizeilicher Praxis verkommen soll, bedarf es daher einer Repolitisierung des Kontextes in dem der polizeiliche Umgang mit Daten stattfindet: der politischen Ziele, die mit technischen Mitteln erreicht werden sollen, und vor allem des polizeilichen Apparats selbst.

Datenschutz im Sicherheitsbereich

Möglichkeiten und Grenzen

von Thilo Weichert

Anders als die ständige Ausweitung polizeilicher und geheimdienstlicher Befugnisse erwarten lässt, kann der Datenschutz auch im Sicherheitsbereich durchaus etwas ausrichten. Dazu hat nicht nur die Rechtsprechung des Bundesverfassungsgerichts beigetragen. Dreißig Jahre nach den Anfängen stellen vernünftige VertreterInnen von Polizei und Geheimdiensten die Geltung des Datenschutzes nicht mehr in Frage.

Wer das Verhältnis von Sicherheitsbehörden zum Datenschutz in den letzten dreißig Jahren Revue passieren lässt, erinnert sich an die Auseinandersetzungen des ersten Bundesbeauftragten für den Datenschutz, Hans-Peter Bull, mit dem Bundesamt für Verfassungsschutz und dem Bundeskriminalamt über NADIS, INPOL und die Richtlinien über kriminalpolizeiliche Sammlungen (KpS-Richtlinien), hat die Konflikte seiner spitzzüngigen baden-württembergischen Kollegin Ruth Leuze mit ihrem Gegenspieler Alfred Stümper vor Augen und denkt an die Terrorismushetze und die Rasterfahndung des BKA-Präsidenten Horst Herold, an den Lauschangriff seit 1975 gegen Klaus Traube oder an die Stammheimaffäre, die auch eine Abhöraffäre war.

Der historische Beobachter könnte den oberflächlichen Eindruck haben, dass sich seitdem wenig geändert hat, außer dass sehr viele Eingriffsbefugnisse für die Sicherheitsbehörden dazugekommen sind und technische Möglichkeiten real wurden, von denen Horst Herold viel träumte und redete.[1] Die RAF-Rasterfahndung aus den 70ern, bei der es um bar bezahlte Stromrechnungen in anonymen Hochhäusern ging,[2]

1 „Weisungs- und politikfrei im Selbstlauf". Interview mit Dr. Horst Herold, in: Bürgerrechte & Polizei/CILIP 16 (3/1983), S. 63-71 (Teil 1), und 18 (2/1984), S. 30-46 (Teil 2)

2 Busch, H. u.a.: Die Polizei in der Bundesrepublik, Frankfurt/M. 1985, S. 139 ff.

scheint ihre natürliche Fortsetzung in der Suche nach islamistischen Schläfern nach dem 11. September 2001 gefunden zu haben.[3] Und das Trennungsgebot, seit der Abnabelung des polizeilichen Staatsschutzes vom Informationssystem der Nachrichtendienste (NADIS) Anfang der 90er informationell einigermaßen umgesetzt, wird mit der Anti-Terror-Datei 2006 wieder ignoriert.

Damals schon gab es die Parole vom „Datenschutz als Tatenschutz" oder als „... Täterschutz". Damals schon wurde darüber fabuliert, Opferschutz ginge über Datenschutz. Und damals schon hielten BürgerrechtlerInnen dem entgegen, dass Freiheit mit Sicherheit sterbe und dass wir auf dem Weg in den Überwachungsstaat seien, den George Orwell ins Jahr 1984 legte und mit dem Spruch kennzeichnete: „Big Brother is watching you."

Indes hat sich seitdem viel verändert. Da ist zum einen die lange Liste von Verfassungsgerichtsentscheidungen, die mit dem Volkszählungsurteil von 1983 als Paukenschlag ihren Auftakt hatte[4] und mit den Entscheidungen zur präventiven Telekommunikationsüberwachung von 2005[5] und zur Rasterfahndung von 2006[6] sicherlich noch lange nicht ihr Ende. Geändert hat sich die Normendichte in diesem Bereich, die eine direkte Reaktion auf den 1983 vom Bundesverfassungsgericht (BVerfG) eingeführten Gesetzesvorbehalt bei informationellen Eingriffen war, und mit der versucht wurde und wird, das bisher unzulässig Praktizierte zulässig zu machen. Geändert hat sich auch die Wahrnehmung der Normenflut der Legalisierungsbestrebungen, deren Verfassungsgemäßheit spätestens seit dem Lauschurteil des BVerfG von 2004[7] allgemein anerkannt in Frage gestellt werden darf und muss. Geändert hat sich insbesondere auch das Verhältnis der verschiedenen sicherheitsbehördlichen Player gegenüber dem Datenschutz.

---

3 Busch, H.: Rasterfahndung – eine Halbjahresbilanz, in: Bürgerrechte & Polizei/CILIP 71 (1/2002), S. 69-75; Köppen, H.: Studierende versus Rasterfahndung, in: Datenschutz-Nachrichten (DANA) 2002, H. 1, S. 10-12; Sauer, T.: Chronologie der Rasterfahndung in Hessen, in: DANA 2002, H. 1, S. 28 f.

4 Volkszählungsurteil v. 15.12.1983: in: BVerfG-Entscheidungen, Bd. 65, S. 1 ff. = Neue Juristische Wochenschrift (NJW) 1984, H. 8, S. 419-428

5 BVerfG: Urteil v. 27.7.2005, in: NJW 2005, H. 36, S. 2603-2612

6 BVerfG: Urteil v. 4.4.2006, in: NJW 2006, H. 27, S. 1939-1949

7 BVerfG: Urteil v. 3.3.2004, in: NJW 2004, H. 14, S. 999-1020.; dazu Roggan, F.: Lauschangriffe nach dem Verfassungsgerichtsurteil, in: Bürgerrechte & Polizei/CILIP 77 (1/2004), S. 65-70

Rahmenbedingungen

Um die Rezeption des Datenschutzes durch die Sicherheitsbehörden zu verstehen, bedarf es einer genaueren Beleuchtung der gesellschaftlichen und technischen Rahmenbedingungen. Wenig geändert hat sich – entgegen allen Behauptungen von Sicherheitsseite – die Kriminalität bzw. die Bedrohung. Sie war schon in den 70ern international und terroristisch, was sie – nach einer Zeit der Entspannung – heute unter den Vorzeichen der islamistischen Gewalt wieder ist. Massiv geändert hat sich die verfügbare und eingesetzte Technik: Biometrie, allgegenwärtige Telekommunikation, die Möglichkeit riesiger Vorratsdatenspeicherungen, Mustererkennung wie z.B. beim Kfz-Datenabgleich, Online-Abfragemöglichkeiten in vielen Behördendateien, die Digitalisierung unseres Lebensalltags – all dies eröffnet bisher ungeahnte Ermittlungsansätze. Zugleich kennzeichnen diese neuen Techniken – jenseits sicherheitsbehördlicher Tätigkeit – Realitäten, die im Interesse der Wahrung informationeller Selbstbestimmung für ArbeitnehmerInnen, KundInnen oder BürgerInnen eines ausgeklügelten rechtlichen, organisatorischen und technischen Schutzes bedürfen.

Dieser objektive Befund findet seinen Niederschlag im Bewusstsein der Betroffenen und Beteiligten. Dabei ist es klar, dass von den direkt Beteiligten oft nicht die Metasicht engagierter BürgerrechtlerInnen geteilt wird: Der Internet-Provider ist gegen die Vorratsdatenspeicherung für die Sicherheitsbehörden, findet aber wenig Anstößiges an der kommerziellen Nutzung solcher Daten für Werbezwecke. Der Bankier geißelt den Verstoß gegen das Bankgeheimnis durch die sicherheitsbehördliche Online-Abfragemöglichkeit von Kontobestandsdaten, hat aber keine Probleme, genau diese Daten mit den konzernangehörigen Unternehmen auszutauschen. Mancher Polizist hat sich schon gegen sein Fotografieren durch die Presse wegen Verletzung seines Rechts am eigenen Bild zu wehren gewusst, während er zugleich ungeniert auch noch die friedlichste Demonstration videografierte. Diese Betriebsblindheit zeigen auch die BürgerInnen, die sich zugleich an Seelenentkleidungsshows im Fernsehen ergötzen oder gar daran teilnehmen und zugleich gegenüber den Nachbarn die Vorhänge zuziehen. So meinen viele von diesen BürgerInnen, was Ihnen auch von den Medien suggeriert wird, sie hätten angesichts neuer sicherheitsbehördlicher Befugnisse „nichts zu verbergen“. Dies gilt freilich nur, bis etwa eine Hartz-IV-Ermittlungstruppe zu Besuch kommt, um die häuslichen Verhältnisse festzustellen.

Unbestritten ist aber die Geltung des Rechts auf informationelle Selbstbestimmung als Grund- und Bürgerrecht und als eine grundlegende Stütze einer freiheitlichen und demokratischen Informationsgesellschaft. Kein einigermaßen vernünftiger Vertreter der Sicherheitsbehörden käme heute noch auf die Idee, die Geltung des Datenschutzes für sich selbst oder für die Gesellschaft in Frage zu stellen. Das Problem besteht in der mangelnden Vorstellungskraft von Vertretern dieser Behörden sowie ihrer politischen Protagonisten, dass sie selbst bzw. ihresgleichen durch ihre informationellen Eingriffe eine Gefahr für dieses Grundrecht darstellen könnten. Diese mangelnde Phantasie – eine Art professioneller Deformation – ist nichts Außergewöhnliches: Es ist nun mal Aufgabe von Sicherheitsbehörden, personenbezogene Daten im größtmöglichen Umfang zur Aufgabenerfüllung zu sammeln. Und da ist der Versuch, die eigenen Kompetenzen auszuweiten, das Normalste der Welt und zunächst einmal Ausdruck besonderen professionellen Engagements. Es muss aber von diesen InteressenvertreterInnen als ebenso normal akzeptiert werden, dass sich ihren Begehrlichkeiten Betroffene, Bürgerrechtsgruppen, PolitikerInnen, Datenschutzbeauftragte und Verfassungsgerichte widersetzen und dass diese die Ausweitung der Befugnisse hinterfragen, kritisieren und verhindern.

Rolle des Datenschutzes im Sicherheitsbereich

Inzwischen ist unter aufgeklärten Vertretern der Sicherheitsbehörden anerkannt, dass der Schutz informationeller Selbstbestimmung für sie selbst eine zentrale Funktion erfüllt, auch wenn sich dieser Schutz gegen konkrete eigene Ermittlungsmaßnahmen richtet. So ist wohl vermittelbar, dass dieser Schutz ein Bestandteil unserer rechtlichen Ordnung ist, den zu schützen gerade auch die Aufgabe der Sicherheitsbehörden ist. Dies wird dort zunehmend anerkannt, wo die Behörden zur Ermittlung von Datenschutzverstößen eingesetzt werden, auch wenn diese Verstöße noch weitgehend als Kavaliersdelikte wahrgenommen werden. Schwer tun sich die Behörden selbstverständlich, wenn sie gegen ihresgleichen ermitteln müssen. Doch auch hier weicht alter Corpsgeist zunehmend einem rationaleren Verständnis: Vorsätzliche Verletzer des Datenschutzes aus den eigenen Reihen werden eher als Nestbeschmutzer, denn als heldenhafte Verteidiger professioneller Privilegien wahrgenommen.

Der zentrale Grund für die Akzeptanz des Datenschutzes durch die Sicherheitsbehörden ist der Erkenntnis geschuldet, dass bekannt wer-

dende Datenschutzverstöße gewaltige Akzeptanz- und Imageprobleme verursachen. Die Beachtung datenschutzrechtlicher Vorgaben ist – dank einer teilweise investigativ arbeitenden Presse – eine Bedingung für eine positive Berichterstattung. Massive Verstöße drohen früher oder später bekannt zu werden. Die Vermeidung von Negativmeldungen sind ein wichtiges Schmiermittel für öffentliche Akzeptanz. Natürlich geht es dabei weniger um die materielle Beachtung des Datenschutzes als um die mediale Wahrnehmung. Doch Wahrnehmung und Realität lassen sich in einer Demokratie nicht allzu weit voneinander entfernen. Dies ist auch ein Grund für das bestehende relativ enge Verhältnis der Datenschutzbehörden zu den Sicherheitsbehörden: Erstere sind die gesellschaftlich anerkannten Experten auf diesem Gebiet, sie sind die Datenschutzpolizei der Polizei. Positive Äußerungen werden gerne gesehen, negative sind zu vermeiden. So können Honig um den Mund der Datenschützer oder leere Versprechungen gegenüber diesen dazu führen, dass sich diese zu Akzeptanztrotteln der Sicherheitsbehörden machen. Trotz der Kurzlebigkeit von Politik und damit auch der Sicherheitspolitik haben solche Strategien aber langfristig keine nachhaltigen Effekte. Ausreichendes Bewusstsein bezüglich der eigenen Rolle als unabhängiger Datenschutzbeauftragter führt dazu, dass durch eine wohl reflektierte und rationale Verteilung von Lob und Tadel die Sicherheitsbehörden dazu gebracht werden, um die Sympathie und das Lob der Datenschutzbehörden zu buhlen.

Bisher kaum eine wahrnehmbare Rolle hat der Datenschutz bei der Sicherung der Ordnungsmäßigkeit der sicherheitsbehördlichen Datenverarbeitung (DV) gespielt. Tatsächlich liegt hierin aber eine gewaltige Chance für den Grundrechtsschutz: Nicht erst seit dem katastrophalen ersten Scheitern von INPOL-neu[8] sollte klar sein, dass die Funktionalität von polizeilicher oder sonstiger sicherheitsbehördlicher DV von deren Ordnungsgemäßheit abhängt. Ordnungsgemäßheit ist aber auch eine zentrale Grundvoraussetzung für Grundrechtskonformität personenbezogener DV. Datenschützer können und müssen sich profilieren als Experten für ordnungsgemäße DV, als Experten für Datensicherheit und Datenverarbeitungsmanagement. Sicherheitsbehörden haben insofern oft wenig Expertise und sind den kommerziellen Anbietern von Soft- und Hardware dann restlos ausgeliefert. Hier können sich Datenschutz-

8 Busch, H.: INPOL-neu, in: Bürgerrechte & Polizei/CILIP 76 (3/2003), S. 12-19

beauftragte als ehrliche Makler betätigen und profilieren, die aber nicht nur auf die Funktionalität und die Abschottung der Systeme nach außen achten, sondern generell auf die Konformität mit dem Recht: Abschottung nach innen, Datensparsamkeit, Beachtung der Erforderlichkeit auch bei Löschroutinen und Archivierung, Zweckbindung, Sicherung der Authentizität und Revisionsfähigkeit – also generell Gesetzeskonformität in Sachen Datenschutz. Gutes Datenmanagement bedeutet weitgehend auch gutes Datenschutzmanagement.[9] Dem Realbetrieb muss eine saubere Dokumentation, eine vernünftige Erprobung und verantwortungsvolle Freigabe vorausgehen; dieser muss mit Pflege, mit regelmäßigen Evaluationen und Audits begleitet werden.

Rolle der Unabhängigen Datenschutzinstanzen

Tatsächlich waren die Datenschützer noch nie wirkliche Gegner der Sicherheitsbehörden, sondern allenfalls kritische und oft für die Behörden selbst nützliche Begleiter. Dies den Sicherheitsbehörden zu vermitteln ist ein schwieriges Unterfangen: Die tägliche Arbeit als Datenschützer zeigt, dass es kaum empfindlichere Datenverarbeiter gibt als solche bei den Sicherheitsbehörden. Fachliche Kritik wird oft als persönliche Kritik wahrgenommen, umso mehr, je mehr sich die Sicherheitsbehördler mit ihrer Arbeit identifizieren. Viele haben ein sehr positives Verständnis von ihrer Arbeit, das Bewusstsein „die Guten“ zu sein. Dies ist im Grunde nicht zu kritisieren, sondern zu fördern, solange die Realität damit korrespondiert. Datenschützer müssen die kommunikative Kompetenz aufbringen, unter Beachtung dieses Selbstverständnisses den Sicherheitsbehörden konstruktive Kritik entgegenzubringen. Dies bedeutet scharf und klar strukturelle und vorsätzliche Missstände zu kritisieren, verständnisvoll und helfend bei Nachlässigkeiten und mangelhafter Organisation zu mahnen, freundlich aufzuklären und zu informieren und bei gesetzeskonformem Vorgehen zu loben oder gar zu werben.

Die Grundlage jedes Verhältnisses zwischen Datenschutz und Sicherheitsbehörden ist die Wahrnehmung der Kontrollkompetenz und die ungeschminkte Berichterstattung in Prüfberichten gegenüber den verarbeitenden Stellen über festgestellte Missstände. Wird diesen nicht abgeholfen, so kann und muss der Datenschützer eskalierend den Dis-

9 Weichert, T.: Datenschutzmanagement, in: DANA 2006, H. 3, S. 113-118

kurs hierüber erzwingen. Da keine anderen Sanktionen zur Verfügung stehen als die Beanstandung, muss das Potenzial der förmlichen Beanstandung – eventuell unter Einbeziehung der Öffentlichkeit – voll ausgenutzt werden. Die klassischen Eskalationsstufen sind: Information der Rechts- und Fachaufsicht, Anrufung des Ministers, Information des Parlaments, Presseerklärung und Tätigkeitsbericht, bis hin zur skandalisierenden Anprangerung. In den meisten Fällen genügt das einfache Beanstanden, doch muss – um die Beanstandung zur vollen Wirksamkeit zu bringen – allen Beteiligten klar sein, dass das Ausschöpfen aller Eskalationsstufen nicht erwünscht, aber möglich ist.

Bei der klassischen Kommunikation von Datenschützern stellt sich die Frage: „Wo bleibt das Positive?“ Tatsächlich werden die Sicherheitsbehörden, wenn sie die Regeln der Datensicherheit und des Datenschutzes beachten, viel zu wenig gelobt. Dem liegt die falsche Annahme zugrunde, geordnete und rechtskonforme Zustände wären der Normalfall. Dies ist nicht so und wird – strukturell bedingt – auch längerfristig so bleiben. Daher ist schon die Feststellung „keine Beanstandung“ eine besondere Qualitätsauszeichnung. Dabei muss es aber nicht bleiben: In Schleswig-Holstein gab es schon Sondierungen zwischen dem Innenministerium und dem Unabhängigen Landeszentrum für Datenschutz (ULD), eine neu entwickelte Polizeisoftware datenschutzrechtlich zu auditieren. Zwar sind wir hiervon in der Realität noch weit entfernt. Doch hat dies eine reale Perspektive: Die Auditierung von Produkten und Verfahren der Polizei brächte allen Seiten Vorteile – der Polizei Rechtssicherheit und Akzeptanz, den BürgerInnen Vertrauen in eine rechtskonforme Polizei, den Datenschutzbeauftragten eine präventive Herangehensweise und eine Erleichterung bei der kontrollierenden Tätigkeit, der Politik – nicht zu unterschätzen – unter Umständen Imagegewinne in Sachen Bürgerfreundlichkeit und Grundrechtsorientierung.

Die interne Beziehung zwischen Datenschutz und Sicherheitsbehörden muss von dauernder Kommunikation geprägt sein. Dabei muss wieder die gesamte Bandbreite möglicher Kommunikation genutzt werden, informell, formell mündlich und schriftlich bis hin zum Austausch oder Schlagabtausch über die Öffentlichkeit und die öffentlichen Medien. Als eine wichtige Kommunikationsstruktur haben sich dabei die behördlichen Datenschutzbeauftragten bei den Sicherheitsbehörden erwiesen, die als Sprachmittler in beide Richtungen wirken. Es ist inzwischen gute Praxis bei vielen Landesbeauftragten für den Datenschutz (LfDs), dass angehende behördliche Datenschutzbeauftragte bei den LfDs mehrmo-

natige Praktika durchlaufen, um die Grundlagen des Datenschutz, die Denk- und Arbeitsweise der LfDs wie auch diese selbst und deren Team kennen zu lernen.

Das Fundament jeder Zusammenarbeit ist, dass die gesetzliche Aufgabe des jeweils Anderen respektiert und gefördert wird. Wichtig für die Wertschätzung der Datenschützer durch die Polizei ist, dass sie neben ihren rechtlichen auch ihre technischen Kompetenzen einbringen. Hier können und sollten die Datenschützer für die Polizei „Freund und Helfer" sein. Dieses Potenzial wurde bisher – auch wegen unzureichender technisch-personeller Ausstattung – viel zu wenig genutzt. Es ist eine verblüffende praktische Erfahrung, dass die Sicherheitsbehörden beileibe nicht vorrangig darauf aus sind, immer mehr Befugnisse zu bekommen – sie wollen zu Recht adäquate Befugnisse und eine gute personelle und technische Ausstattung. Die Befugnisdiskussion wird oft nur symbolhaft von Politik und Behördenvertretern genutzt. Ein guter Beleg hierfür ist die von der Landesregierung Schleswig-Holstein betriebene Verschärfung des Polizeirechtes, die fast einhellig von der Polizei selbst abgelehnt wird, weil sie diese in vieler Hinsicht behindert: Sie führt zu zu hohen Erwartungen, zu offen formulierten unklaren Befugnissen und beeinträchtigt das öffentliche Vertrauen. So kritisierte zum Bespiel die Gewerkschaft der Polizei (GdP) die Novelle mit den Argumenten des BVerfG als verfassungswidrig, weil sie den Anspruch an sich selbst hat, verfassungskonform zu agieren. Dies ist bzw. war kein Lippenbekenntnis, sondern ein ernstes und ernst zu nehmendes Anliegen.

Kein Zuckerschlecken

Die bisherige Darstellung der Möglichkeiten und Grenzen des Datenschutzes bei Sicherheitsbehörden hat weitgehend die aktuelle Diskussion über den Terrorismus und die sich daraus ergebenden Konsequenzen ausgeblendet. Dies ist insofern akzeptabel, als der alltägliche Kontakt zwischen Datenschutz und Sicherheit von der Terrorismusdebatte – zumindest in Schleswig-Holstein – relativ unberührt geblieben ist. Der Alltag des ULD und der Polizei des Landes ist geprägt vom Umgang mit Alltagskriminalität und mit unpolitischer schwerer Kriminalität, vom Massengeschäft und von einzelnen Speziallagen wie etwa jüngst dem „Tag der deutschen Einheit" 2006 in Kiel. Dennoch hat natürlich die Terrorismusdebatte ihre direkten Auswirkungen auf den gelebten Datenschutz bei den Sicherheitsbehörden. So erachten es manche Politiker

als vorteilhaft, die Angst vor dem Terrorismus für eine publikumsträchtige und damit oft auch populäre Law-and-Order-Politik zu nutzen. Dabei macht es sich unter Umständen gut, gegen „den Datenschutz“ zu polemisieren. Diese zunächst symbolisch und ideologisch geprägte Politik ist nicht ohne reale Folgen. Sie ist geeignet, die Kommunikationskultur zwischen Sicherheit und Datenschutz bei den Handelnden wie in der öffentlichen Wahrnehmung zu beeinträchtigen. Sie unterminiert das Ansehen des Datenschutzes wie auch das Vertrauen in die Gesetzeskonformität der Polizei. Solche Imageprobleme können nur beschränkt durch das eigene öffentliche Agieren der Sicherheits- und Datenschutzbehörden kompensiert werden.

Gravierender sind die direkten realen Konsequenzen des Starker-Staat-Gehabes. Um in kein Glaubwürdigkeitsloch zu fallen, folgt der starken Rhetorik die starke politische Tat. Ein Betätigungsfeld ist hierbei die Gesetzgebung, über die verdeckte Datenerhebungsmethoden (z.B. der Telefon- und der Wohnraumüberwachung) sowie sogenannte Jedermannkontrollen erlaubt werden – von der Videoüberwachung, über die Schleierfahndung, das Kfz-Kennzeichen-Scanning, die Mautdatennutzung, die Funkzellenabfragen und Vorratsdatenspeicherung im Bereich der Telekommunikation (TK) bis hin zu, Gen-Massen-Screenings. Manche neue Befugnisse kommen gar nicht zur Anwendung.

So wurde von einigen Normen des sogenannten Otto-Kataloges bis heute überhaupt kein Gebrauch gemacht. Dies macht solche Schläfergesetze aber nicht ungefährlich, da sie jederzeit aktiviert werden können. Daneben gibt es symbolisch angelegte Gesetze, die auf Umsetzung drängen und deren Umsetzung den Überwachungsdruck in der Bevölkerung real erhöht. So folgt einem Kfz-Kennzeichen-Scan-Gesetz zwangsläufig die Beschaffung der Geräte und deren Einsatz. Derartige Maßnahmen mögen sicherheitspolitisch vollkommen ineffektiv und sogar schädlich sein, sie binden behördliche Energien und sind sehr teuer. Ein äußerst anschauliches Beispiel dafür war die Rasterfahndung 2002 in Deutschland. Nicht zu reden von dem Überwachungsdruck, der durch Gesetze und deren Umsetzung ausgeübt wird. Deren freiheitsbeschränkende Wirkung wurde vom BVerfG immer wieder hervorgehoben.[10] Die da-

10 z.B. grundlegend im Volkszählungsurteil a.a.O. (Fn. 4)

durch erfolgende informationelle Diskriminierung hat auf bestimmte gesellschaftliche Gruppen, z.B. MuslimInnen, schwerwiegende Folgen.[11]

Noch gravierender sind Gesetze, die strukturell die sicherheitsbehördliche Überwachung erhöhen, d.h. die Sicherheitsarchitektur in Deutschland, Europa und global nachhaltig verändern. Manche dieser Änderungen mögen notwendig und vernünftig sein, etwa eine verbesserte technische Kommunikation, neue Formen der Organisation oder die Nutzung neuer moderner Methoden der Datenerhebung und -auswertung. Viele Neuerungen sind aber einfach schädlich oder zumindest unverhältnismäßig. Dies gilt etwa für praktisch jede „Segnung", die über den Umweg USA nach Europa und Deutschland kam: Dazu gehört die Auswertung von Massendaten – von Flugpassagieren, Kunden des internationalen Bankverkehrs oder von Internet-Nutzenden. Dazu gehören im Verborgenen erfolgende internationale Kooperationen, wie sie derzeit massiv zwischen den USA und Europa ausgebaut werden. Dies gilt für manche europäische „Segnung" wie etwa den Ausbau des Schengener Informationssystems oder die geplante Vorratsspeicherung von TK-Verkehrsdaten[12] ohne spürbare öffentliche Debatte. Dies gilt aber auch für die nationale Ebene durch die Vergeheimdienstlichung der Polizei, wie sie jüngst durch die unsägliche sog. Anti-Terror-Datei vorangetrieben wird. Bei all diesen Entwicklungen geht die demokratische und justizielle Kontrollierbarkeit der Sicherheitsbehörden strukturell verloren. Von informationeller Selbstbestimmung kann in diesen Zusammenhängen nicht mehr die Rede sein.

Datenschutz auf verlorenem Posten?

Diese differenzierte Analyse lässt nicht den Schluss zu, der Datenschutz stünde auf verlorenem Posten. In der konkreten sicherheitsbehördlichen Arbeit hat ein kommunikativ angelegter Datenschutz eine gute Perspektive. So wie sich die Sicherheitsbehörden ändern, müssen sich auch die Datenschützer den neuen Herausforderungen stellen und adäquat reagieren. Angesichts des Umstandes, dass eine freiheitliche Informationsgesellschaft auf die Freiheit vor sicherheitsbehördlicher Überwachung

11 Weichert, T.: Der datentransparente Moslem, in: Der Schlepper Nr. 29/30 (Winter 2004), S. 46 f.

12 Holzberger, M.: Vorratsdatenspeicherung von Verbindungsdaten, in: Bürgerrechte & Polizei/CILIP 82 (3/2005), S. 59-69

angewiesen ist, und Freiheit nicht nur ein verfassungsrechtliches Muss, sondern auch ein individuelles Bedürfnis ist, muss einem nicht vollständig bange werden.

Bange machen können die angesprochenen strukturellen Veränderungen. Diese mögen teilweise umkehrbar sein, etwa durch die Rechtsprechung der Verfassungsgerichte. Doch gilt dies nicht für alle „Innovationen". So ist es unwahrscheinlich, dass die Milliarden-Euro-schwere Überwachungsinfrastruktur von Toll Collect auf deutschen Autobahnen aus Gründen des Datenschutzes wieder abgebaut wird.[13] Ebenso unwahrscheinlich ist es, dass eine Umsetzung der Vorratsspeicherung bei den TK-Verkehrsdaten vollständig rückabgewickelt werden könnte. Daher ist es notwendig, sich solchen – teilweise erst noch drohenden – Strukturveränderungen frühzeitig entgegenzusetzen.

Ist die Büchse der Pandora einmal geöffnet, so bleibt nur noch Schadensbegrenzung. Der Geist geht nicht mehr zurück in die Flasche. Die Mittel gegen den um sich greifenden Geist sind Transparenz und Kontrolle. Hierdurch kann die informationelle Fremdbestimmung zumindest teilweise und auf einer gesellschaftlichen und politischen Ebene wieder eingefangen und zur Selbstbestimmung gemacht werden. Diese Erkenntnis ist mit der Befristung einzelner Gesetze, der Pflicht zur Evaluation und der Verbesserung mancher Kontrollmechanismen im Grunde ins Bewusstsein der Gesetzgeber gelangt. Doch blieben die kleinen Pflänzchen noch vereinzelt und sind noch nicht überlebensfähig. Bezüglich der Kontrolle der Kontrolleure bzw. der Überwachung der Überwacher gibt es bisher erst eine einzige wirklich etablierte Institution: die unabhängigen Datenschutzbeauftragten. Weitere Institutionen warten noch auf ihre Etablierung: etwa die eigenständige Geheimdienstkontrolle, die generelle Evaluation von sicherheitsbehördlichen Kompetenzen oder der automatische Verfall von informationellen Eingriffsbefugnissen, die sich nicht bewähren.

13 Straßen-Totalüberwachungsvertrag mit Toll-Collect kündigen, in: DANA 2003, H. 4, S. 14-17

Grundrechtseingriffe auf Vorrat

Gesetzentwurf zur Vorratsdatenspeicherung

von Mark A. Zöller

Der Kampf um die Speicherung sog. Vorratsdaten über das Telekommunikationsverhalten der BürgerInnen und die Nutzung dieser Daten für die Strafverfolgung geht in die nächste Runde. Am 8. November 2006 stellte Bundesjustizministerin Brigitte Zypries einen Referentenentwurf vor, der u.a. die umstrittene EU-Richtlinie vom März dieses Jahres umsetzen soll.[1]

Die Möglichkeit, für Strafverfolgungszwecke auf Informationen über Telekommunikations-(TK)-Verbindungen zuzugreifen, lässt sich bis ins Jahr 1928 zurückverfolgen, als mit § 12 des damaligen Fernmeldeanlagengesetzes (FAG) eine entsprechende Befugnisnorm geschaffen wurde. Zu einem wichtigen Ermittlungswerkzeug wurden Daten über hergestellte Fernmeldeverbindungen allerdings erst, als die heutige Telekom 1989 begann, die bis dahin manuelle und elektromechanische durch digitale Vermittlungstechnik zu ersetzen. Seitdem wird für jede Kommunikationsbeziehung ein Datensatz erzeugt und digital auf den Servern der TK-Unternehmen abgelegt, um auf dieser Grundlage den KundInnen die in Anspruch genommenen Leistungen in Rechnung zu stellen.

Der sowohl technisch als auch rechtlich überholte § 12 FAG a.F. wurde im Jahre 2002 durch die §§ 100g und 100h der Strafprozessordnung (StPO) ersetzt. Diese ermöglichen es den Strafverfolgungsbehörden, bei bestehendem Anfangsverdacht in Bezug auf Straftaten von „erheblicher Bedeutung“ oder Straftaten, die mittels einer „Endeinrichtung“ begangen werden (z.B. beleidigende oder bedrohende Anrufe), von denjenigen, die geschäftsmäßig TK-Dienste erbringen oder daran

1 Richtlinie 2006/24/EG, in: Amtsblatt der EU L 105/54 v. 13.4.2006; s. Holzberger, M.: Aktenberge bis zum Mond, in: Bürgerrechte und Polizei/CILIP 82 (3/2005), S. 59-67; zu weiteren Inhalten des Entwurfs siehe den Artikel von N. Pütter in diesem Heft, S. 31-37

mitwirken, Auskunft über Verbindungsdaten zu verlangen. Sofern die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre, ist auch eine „Zielwahlsuche“ möglich. Dadurch können unbekannte Anschlussnummern ermittelt werden, von denen Verbindungen *zu* dem Anschluss des Beschuldigten hergestellt werden. Diese Maßnahme stellt schon deshalb einen intensiveren Grundrechtseingriff dar, weil dabei die Datensätze *aller* TeilnehmerInnen daraufhin gerastert werden, ob von ihren Anschlüssen aus Verbindungen zu dem „verdächtigen“ Anschluss hergestellt worden sind.

Als TK-Verbindungsdaten, über die Auskunft erteilt werden kann, nennt § 100g Abs. 3 StPO Berechtigungskennungen, Kartennummern, Standortkennung, Rufnummer oder Kennung des angerufenen Anschlusses oder der Endeinrichtung, sofern eine Verbindung zustande gekommen ist. Darüber hinaus werden auch Beginn und Ende der Verbindung nach Datum und Uhrzeit, die vom Kunden in Anspruch genommene TK-Dienstleistung, die Endpunkte festgeschalteter Verbindungen sowie ihr Beginn und Ende erfasst.

Damit die Auskunftsersuchen der Strafverfolgungsbehörden nicht ins Leere laufen, hat der Gesetzgeber durch TK-rechtliche Vorschriften die Erhebung und Bevorratung entsprechender Datensätze abgesichert. So dürfen die Diensteanbieter in Bezug auf ihre KundInnen auch „Verkehrsdaten“ i.S.d. § 96 des Telekommunikationsgesetzes (TKG) erheben und verwenden, die inhaltlich weitgehend dem Katalog des § 100g Abs. 3 StPO entsprechen. Der überwiegende Zweck der Erhebung besteht jedoch nach wie vor in der Rechnungslegung. Die Daten dürfen zwar bis zu sechs Monate nach Versendung der Rechnung gespeichert werden, allerdings können die KundInnen (nach § 97 Abs. 4 S. 1 Nr. 2 TKG) auch verlangen, dass die Zielnummer mit Versendung der Rechnung gelöscht wird. Da die meisten TK-Unternehmen monatliche Rechnungen stellen, bietet eine solche Vorgehensweise den Telefon- und InternetkundInnen die Möglichkeit, dass die sie betreffenden Verbindungsdaten nur ca. einen Monat lang in einer für die Strafverfolgungsbehörden interessanten, d.h. vollständigen Form vorrätig gehalten werden.

Umfassende Erhebungsbefugnis

Der nun vorgelegte Referentenentwurf, den das Kabinett im Frühjahr 2007 beraten soll, brächte weitreichende Änderungen der geltenden

Rechtslage und beruft sich dabei auf die Pflicht zur Umsetzung der EU-Richtlinie.[2] So schlägt das Bundesjustizministerium (BMJ) nunmehr die Schaffung einer umfassenden Befugnis zur Erhebung von Verkehrsdaten vor (§ 100g Abs. 1 S. 1 StPO-E).

In Anknüpfung an die Vorgaben von Art. 20 des Europarats-Übereinkommens zur Computerkriminalität[3] sollen Verkehrsdaten nun auch „in Echtzeit" erhoben werden können. Das Kommunikationsverhalten von Beschuldigten oder Personen, die diesen Nachrichten übermitteln oder ihren Anschluss überlassen, wäre damit live anhand der entstehenden Datenprotokolle auf dem Computerbildschirm mitzuverfolgen. Solche Ermittlungsmaßnahmen waren bislang nur auf der Grundlage der (inhaltlichen) TK-Überwachung nach den §§ 100a, 100b StPO möglich. Der bisherige § 100g StPO würde damit seinen Charakter als bloße gesetzliche Verankerung des behördlichen Auskunftsanspruchs verlieren.

Mit einer umfassenden Befugnisnorm zur Verkehrsdatenerhebung hält das BMJ eine eigenständige Regelung der Zielwahlsuche für überflüssig. Der Unterschied zwischen der „klassischen" Verbindungsdatenauskunft und der wesentlich eingriffsintensiveren Zielwahlsuche, bei der notwendigerweise alle vorhandenen Datensätze unverdächtiger Personen gerastert werden, würde damit nivelliert.

Objekte der vorgeschlagenen Ermittlungsbefugnisnorm sind nach dem Wortlaut des Entwurfs auch nicht mehr „Verbindungsdaten". Vielmehr knüpft nun auch das Strafprozessrecht an die Terminologie des § 96 Abs. 1 TKG an und spricht von „Verkehrsdaten", d.h. Daten, die bei der Erbringung eines TK-Dienstes erhoben, verarbeitet oder genutzt werden.[4] Dass diese Verkehrsdaten in Umsetzung von Art. 5 der EU-Richtlinie deutlich über den Katalog der bislang auskunftsfähigen Verbindungsdaten hinausreichen, dürfte kaum überraschen. Wann hätte schon jemals ein StPO-Gesetzgeber freiwillig, d.h. ohne klaren Auftrag aus Karlsruhe, auf Ermittlungskompetenzen verzichtet, mögen sie in der Praxis auch noch so überflüssig sein? Die vielleicht entscheidende Änderung folgt jedoch aus der Tatsache, dass die Verkehrsdaten nach § 110 a TKG-E nunmehr ohne Ausnahme sechs Monate lang zu speichern wären. Zwar folgt der Entwurf dem Votum des Bundestages und bewegt

2 Der Referentenentwurf v. 8.11.2006 ist abrufbar unter www.cilip.de/terror.
3 http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm
4 so die Legaldefinition in § 3 Nr. 30 TKG

sich mit dieser Speicherungsfrist am unteren Ende des in Art. 6 der Richtlinie vorgesehenen Rahmens (sechs Monate bis zwei Jahre).[5] Die KundInnen verlieren jedoch die Option, die Löschung der Daten nach Versendung der jeweiligen Rechnung zu verlangen. Die Sechsmonatsfrist wird unabänderbar.

Die Art der nach dem Referentenentwurf zu speichernden Verkehrsdaten dürfte insbesondere bei den Internet-Nutzern und den Datenschützern auf einen höchst sensiblen Nerv treffen. Dies lässt sich an folgenden drei Beispielen verdeutlichen: § 110 a Abs. 1 S. 1 TKG-E umschreibt den Kreis der zur Speicherung Verpflichteten mit den Worten: „wer Telekommunikationsdienste für die Öffentlichkeit erbringt oder daran mitwirkt". Von dieser Formulierung wären zwar nicht Universitäten oder die Administratoren unternehmensinterner Netze betroffen, wohl aber diejenigen, die einen Anonymisierungsdienst anbieten und hierbei die Ausgangskennung des Nutzers durch eine andere ersetzen (z.B. der vom Unabhängigen Landeszentrum für den Datenschutz Schleswig-Holstein, ULD, mit betriebene Dienst AN.ON). Die Verpflichtung zur Vorratsdatenspeicherung würde solche Dienste entwerten. Für User, die ihre Identität im Netz für sich behalten wollen, bleibt daher nur der Rückgriff auf Anonymisierungsdienste, die von Servern außerhalb der EU operieren.

Darüber hinaus deuten sich auch für das Datenaufkommen beim E-Mail-Verkehr drastische Änderungen an. Schließlich sollen die Anbieter von E-Mail-Diensten (z.B. GMX.de, Web.de oder Yahoo.com) nicht nur zur Erhebung von Verkehrsdaten, sondern über den nunmehr vorgeschlagenen § 111 TKG-E auch zur Erfassung von Kundendaten wie Name, Anschrift, Geburtsdatum oder der Kennung des elektronischen Postfachs verpflichtet sein. Damit dürfte die anonyme oder unter fremden Namen erfolgende Anmeldung eines E-Mail-Accounts – jedenfalls bei deutschen Webmail-Diensten – ausgeschlossen sein.

Von besonderer Brisanz ist im Übrigen die Tatsache, dass die Erfassung und Vorratsspeicherung von sog. Internet-Protokoll-Adressen (IP-Adressen) nunmehr ausdrücklich vorgeschrieben sein soll (§ 110a Abs. 2 Nr. 5, Abs. 3 Nr. 2 und Abs. 4 Nr. 1 TKG-E). Die Frage, ob Anbieter die verwendeten IP-Adressen überhaupt speichern dürfen, war in

5 vgl. die Beschlussempfehlung des Rechtsausschusses, BT-Drs. 16/690 v. 23.3.2006, und den entsprechenden Antrag der Koalitionsfraktionen, BT-Drs. 16/545 v. 7.2.2006

den letzten Jahren wiederholt Gegenstand (zivil-)gerichtlicher Entscheidungen. Zuletzt hatte das Landgericht (LG) Darmstadt in einem Urteil vom 7. Dezember 2005[6] entschieden, dass ein Kunde mit einem „Flatrate-Tarif“ gegenüber seinem Zugangs-Provider einen Anspruch auf Unterlassung der Erhebung und der Speicherung des bei der Internetnutzung übertragenen Datenvolumens und der (dynamischen, d.h. bei jedem Einwählvorgang an den Nutzer vergebenen) IP-Adresse hat, da diese Informationen weder für die Entgeltermittlung noch für die Entgeltabrechnung erforderlich sind. Im Zusammenspiel mit sog. „Logfiles“, in denen die Adressen der besuchten Internetseiten enthalten sind, ermöglichen aber gerade IP-Adressen auch eine inhaltliche Überwachung der Internetnutzung. Mit Beschluss vom 26. Oktober 2006 hat nun auch der 3. Zivilsenat des Bundesgerichtshofs[7] eine Beschwerde von T-Online gegen die Nichtzulassung der Revision als unzulässig verworfen, so dass das Darmstädter Urteil rechtskräftig ist. Der berühmte „Federstrich des Gesetzgebers“ soll nun dieses eindeutige Votum der Rechtsprechung gegen die Speicherung von IP-Adressen in sein Gegenteil verkehren.

Verkehrsdaten ohne Verbindung

Mit dem Verzicht auf die Formulierung „im Falle einer Verbindung“ in § 100g StPO will der Entwurf den Weg dafür frei machen, auch Daten über solche technischen Vorgänge zu erlangen, bei denen überhaupt keine (erfolgreiche) Kommunikationsverbindung zustande gekommen ist. Diese Neuerung ist nicht durch die EU-Richtlinie erzwungen, sondern entspricht offenbar einem Interesse der deutschen Ermittlungsbehörden. Was zunächst wie eine harmlose Klarstellung wirkt, hat für den Beschuldigten weit reichende Konsequenzen.

Es bedeutet, dass Verbindungsdaten nicht nur dann anfallen und in die Hände der Strafverfolgungsbehörden gelangen können, wenn ein Verbindungsversuch scheitert (z.B. weil sich der angerufene Mobiltelefonkunde gerade in einem „Funkloch“ befindet). Vielmehr würde gerade

6 LG Darmstadt, in: Datenschutz und Datensicherheit 2006, H. 3, S. 178-181; vgl. dazu Köcher, J.K.; Kaufmann, N.C.: Speicherung von Verkehrsdaten bei Internet-Access-Providern, in: Datenschutz und Datensicherheit 2006, H. 6, S. 360-364; generell gegen die Erforderlichkeit der IP-Adressen-Speicherung zur Entgeltermittlung: Wüstenberg, D.: Argumente gegen die Rechtmäßigkeit der Vorratsdatenspeicherung, in: Recht der Datenverarbeitung 2005, H. 3, S. 102-104

7 Aktenzeichen: 3 AZR 40/06; abrufbar unter www.bundesgerichtshof.de

durch die bei Mobilfunkteilnehmern zu erhebenden Standortdaten (§ 110a Abs. 2 Nr. 4c TKG-E) die Ortung eingeschalteter Handys in einer Funkzelle möglich. Auf diese Weise können nicht nur umfassende Bewegungsprofile erstellt werden. Zwar bleibt eine solche Standortbestimmung je nach Größe der Funkzelle ungenau. Angesichts der bereits beschriebenen Überwachung in Echtzeit würde das mitgeführte Handy zu einer Art ungewolltem Peilsender, der bis zu einem gewissen Grad die Ortung des Anschlussnutzers mit anderen technischen Methoden wie dem Global-Positioning-System (GPS) ersetzt.

Damit wäre zugleich die Diskussion darüber, ob und auf welcher rechtlichen Grundlage die Strafverfolgungsbehörden zur Lokalisierung eines Beschuldigten eine „stille SMS" (Stealth-Ping-Verfahren) an dessen Mobiltelefon senden dürfen, erledigt und auch diese technische Ermittlungsmethode still und heimlich legalisiert.[8] Zwar sieht der Referentenentwurf (§ 100g Abs. 1 S. 3 StPO-E) die Erhebung von Standortdaten nur für schwere Straftaten i.S. des § 100a Abs. 2 StPO vor.[9] Allerdings zeigt ein Blick auf die zahlreichen dort genannten Vergehenstatbestände, dass durch diese Einschränkung lediglich Erscheinungsformen der leichten Kriminalität ausgeklammert wären. Kaum beruhigen kann da der beschwichtigende Hinweis, dass die Behörden nur dann auf Daten über „erfolglose Anrufversuche" nach § 110 a Abs. 5 TKG-E zugreifen können, wenn der Anbieter sie ohnehin zu eigenen Zwecken speichert oder protokolliert.[10] Schließlich sind die Mobilfunkanbieter längst dazu übergegangen, ihren KundInnen erfolglose Anrufversuche per SMS mitzuteilen, so dass § 110a Abs. 5 weitgehend leer laufen dürfte.

Schließlich ist unter der Vielzahl der Änderungen noch auf § 100g Abs. 3 StPO-E hinzuweisen. Diese Bestimmung legt fest, dass sich die Erhebung von Verkehrsdaten, die sich nicht im Gewahrsam eines TK-Diensteanbieters befinden, nach den „allgemeinen Vorschriften" bestimmt. Hinter diesem unscheinbaren Verweis steckt eine praktisch bedeutsame Weichenstellung. So wurde in der Vergangenheit verstärkt diskutiert, ob z.B. für ein Auslesen der Ruflisten aus einem im Zuge einer Durchsuchung aufgefundenen und sichergestellten Mobiltelefon die Regelung der §§ 100g, 100h StPO anwendbar ist. Insofern spricht

8 s. dazu Gercke, B.: Telekommunikationsüberwachung, in: Roggan, F.; Kutscha, M. (Hg.): Handbuch zum Recht der Inneren Sicherheit, Berlin 2006, S. 145-182 (157 f.) m.w.N.

9 zur geplanten Änderung des § 100a siehe den Artikel von N. Pütter in diesem Heft

10 vgl. die Begründung zu § 110a Abs. 5 TKG-E auf S. 147 des Referentenentwurfs

sich der Referentenentwurf in Anlehnung an die jüngste verfassungsgerichtliche Stellungnahme zu dieser Problematik[11] dafür aus, dass die Auswertung solcher Informationen (z.B. auch bei vorgefundenen Verbindungsnachweisen in Papierform) für Polizei und Staatsanwaltschaft schon auf der Grundlage der Beschlagnahmevorschriften (§§ 94 ff. StPO) zulässig sein sollen.

Geeignet, erforderlich, angemessen?

Dass die Neuregelung zur Vorratsdatenspeicherung nunmehr in ein umfangreiches Reformpaket verpackt wird, das auch positive und längst überfällige Reformen (z.B. Berücksichtigung von Zeugnisverweigerungsrechten, Datenkennzeichnungs- und Benachrichtigungspflichten) enthält, vermag über ihre Schwächen nicht hinwegzutäuschen. Schon eine formale Berufung auf die durch die bis zum 15. Juli 2007 umzusetzende EG-Richtlinie kann nur bedingt überzeugen. Schließlich soll sie gemäß Art. 1 Abs. 1 sicherstellen, dass unionsweit Kommunikationsdaten „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten“ zur Verfügung stehen. Damit geht es der Sache nach nicht um Fragen der Verwirklichung des EG-Binnenmarkts, die im Rahmen der Ersten Säule der Europäischen Union anzusiedeln wären. Vielmehr ist das Strafrecht und folglich die Dritte Säule betroffen[12]. In seinem Urteil vom 30. Mai 2006[13] zur Rechtmäßigkeit der Übermittlung europäischer Fluggastdaten an die USA hat der Europäische Gerichtshof (EuGH) bereits darauf hingewiesen, dass aus der Tatsache, dass Daten von privaten Wirtschaftsteilnehmern erhoben werden, noch nicht die Anwendbarkeit des Gemeinschaftsrechts folgt, wenn deren anschließende Übermittlung in einem von staatlichen Stellen geschaffenen Rahmen stattfindet und primär der öffentlichen Sicherheit dient. Insofern ist zu erwarten, dass der EuGH im Verfahren über die von Irland und der Slo-

11 BVerfG, in: Neue Juristische Wochenschrift 2006, H. 15, S. 976-978

12 Auch der Rat hatte sich vor Erlass der Richtlinie zunächst auf die Kompetenz für einen Rahmenbeschluss nach Art. 31 Abs. 1 Buchstabe c und Art. 34 Abs. 2 Buchstabe b des EU-Vertrags berufen; vgl. Alvaro, A.: Positionspapier zur Einführung einer Vorratsspeicherung von Daten, in: Recht der Datenverarbeitung 2005, H. 2, S. 47-50 (48).

13 EuGH, in: Europäische Zeitschrift für Wirtschaftsrecht 2006, H. 13, S. 403-406 (405) m. Anm. Westphal, ebd., S. 406-408 sowie Ehricke, U.; Becker, T.; Walzel, D.: Übermittlung von Fluggastdaten, in: Recht der Datenverarbeitung 2006, H. 4, S. 149-156

wakei mittlerweile erhobenen Nichtigkeitsklage[14] auch die Richtlinie 2006/24/EG – ungeachtet etwaiger Eingriffe in die Garantien des Art. 8 EMRK – schon mangels gemeinschaftsrechtlicher Kompetenzgrundlage für ihren Erlass für nichtig erklären wird.

Aber auch auf nationaler Rechtsumsetzungs-Ebene lässt sich die Verhältnismäßigkeit der nun im Referentenentwurf vorgeschlagenen Regelungen bezweifeln. Schließlich stellt die Übermittlung von Verkehrsdaten an die Strafverfolgungsbehörden einen Eingriff in das durch Art. 10 Abs. 1 GG gewährleistete Fernmeldegeheimnis bzw. – in Bezug auf bloße Positionsmeldungen aktiv geschalteter Mobiltelefone (sog. Stand-by-Daten) – das Recht auf informationelle Selbstbestimmung dar.[15] Die Zweifel betreffen vor diesem Hintergrund bereits die *Geeignetheit* der geplanten Maßnahmen. Zwar lässt sich nicht bestreiten, dass Auskünfte über Verkehrsdaten ein wichtiges Werkzeug für die Strafverfolgung darstellen. Sie zeigen auf, zwischen welchen Anschlüssen wann, wie lange und auf welche Weise kommuniziert worden ist bzw. noch kommuniziert wird. Daraus lassen sich wiederum Rückschlüsse auf das Verhalten, das soziale Umfeld oder den Aufenthaltsort der überwachten Person ziehen. Gerade TeilnehmerInnen aus dem Umfeld schwerer Kriminalitätsbereiche wie Terrorismus und Organisierter Kriminalität dürften die Verfolgbarkeit ihrer Daten leicht zu verhindern wissen – durch den Erwerb von Telefonkarten durch Strohmänner, den wechselnden Einsatz von Mobiltelefonen ausländischer Anbieter, die Nutzung von öffentlichen Telefonzellen und Internetcafés, die Veränderung von E-Mail- und IP-Adressen oder die Nutzung von Internet -Service-Providern außerhalb der EU.[16] Insofern dürften von den Speicherungen der TK-Diensteanbieter allenfalls Beteiligte an leichter bis mittelschwerer Kriminalität, vor allem aber unbescholtene Bürger betroffen sein.

Auch unter dem Blickwinkel der *Erforderlichkeit* sind die Pläne des BMJ fragwürdig. Gleichermaßen geeignete, aber in Bezug auf Grundrechtseingriffe mildere Mittel wurden vernachlässigt. Zum einen ist bislang weder auf EU- noch auf nationaler Ebene schlüssig dargelegt worden, dass kürzere Aufbewahrungsfristen für Verkehrsdaten den Be-

14 Aktenzeichen: Rs. C-301/06

15 näher dazu Zöller, M.A.: Die Jagd nach den Verbindungsdaten, in: Wolter, J.; Schenke, W.-R.; Rieß, P.; Zöller, M.A. (Hg.): Datenübermittlungen und Vorermittlungen, Heidelberg 2003, S. 291-323 (307 ff.)

16 Alvaro a.a.O. (Fn. 12), S. 48

dürfnissen der Strafverfolgungspraxis nicht gerecht würden. Der Wissenschaftliche Dienst des Bundestages verwies in einem Gutachten vom August 2006 auf Analysen britischer und schwedischer Stellen, wonach sich die Datenabfragen der dortigen Behörden zu 80 bis 85 Prozent auf den Zeitraum der letzten *drei* Monate beziehen.[17] Zum anderen käme als milderes Mittel die in den USA praktizierte „Data Preservation" in Betracht, bei der die Verkehrsdaten einer verdächtigen Person erst ab einem bestimmten Zeitpunkt auf richterliche Anordnung hin gespeichert werden („Data Freeze"). Dies könnte geschehen beim Verdacht auf Straftaten von erheblicher Bedeutung oder auf mittels Telekommunikation begangener Straftaten – in jenen Fällen also, die der Referentenentwurf jetzt als Voraussetzung einer umfassenden Erhebung auflistet. Eine solche anlassbezogene Datenspeicherung ist nicht nur in Art. 16 Abs. 2 des Europaratsübereinkommens über Computerkriminalität vorgesehen, sondern würde auch die Belastungen für die Anbieter durch eine Absenkung des Datenvolumens verringern.

Die im Referentenentwurf vorgesehenen Eingriffsmöglichkeiten sind im Übrigen auch nicht *angemessen*. Mit der Verpflichtung zur Erhebung und Speicherung von personenbezogenen Daten in erheblichem Umfang und für erhebliche Zeit werden alle Nutzer von TK-Dienstleistungen, de facto also nahezu alle EinwohnerInnen der EU, unter Generalverdacht gestellt. Zwar werden die BürgerInnen, deren Verkehrsdaten erfasst werden, formal weder als Beschuldigte geschweige denn bereits als Schuldige behandelt. Ein schaler Nachgeschmack bleibt dennoch – umso mehr, als in Zukunft auch die Nachrichtendienste mit ihren Zugriffsmöglichkeiten von den erweiterten TK-Datenbeständen profitieren.[18] Das BVerfG hat bereits in seinem Volkszählungsurteil auf die Gefahr hingewiesen, dass Personen, die damit rechnen, dass ihre Verhaltensweisen behördlich registriert werden und ihnen dadurch Risiken entstehen können, möglicherweise vollends auf eine Ausübung ihrer Grund-

17 Bundestag, Wissenschaftlicher Dienst: Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht, Berlin 2006, S. 12 f.; allgemeine rechtsvergleichende Angaben bei Büllingen, F.: Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, in: Datenschutz und Datensicherheit 2005, H. 6, S. 349-353

18 Die Nachrichtendienste (Verfassungsschutz, BND, MAD) können über § 8 Abs. 8 S. 3 Bundesverfassungsschutzgesetz, § 8 Abs. 3a S. 3 Bundesnachrichtendienstgesetz und § 10 Abs. 3 MAD-Gesetz nicht nur Auskünfte über Telekommunikationsverbindungsdaten, sondern auch über Teledienstenutzungsdaten erlangen.

rechte verzichten.[19] Aber nicht einmal dieser traurige Ausweg bleibt den um ihre Privatheit besorgten Personen in einer modernen Industriegesellschaft, die ohne Telefon und Internet kaum noch lebensfähig erscheint. Hinzu kommt, dass die Leistungssteigerung im Bereich der Strafverfolgung durch eine Abwälzung der Kosten auf private Unternehmen erreicht wird, die die Kapazitäten ihrer EDV-Systeme entsprechend ausbauen müssen, ohne dafür von Seiten des Bundes oder der Länder eine Entschädigung für Investitionen oder gesteigerte Betriebskosten zu erhalten. Der Bundesverband der Deutschen Industrie geht bei größeren Festnetz- und Mobilfunkunternehmen zusammen allein von Investitionskosten in dreistelliger Millionenhöhe und zusätzlichen Betriebskosten von mindestens 50 Mio. Euro pro Jahr aus.[20] Dennoch soll lediglich die schon bislang geltende Entschädigungspflicht nach § 23 des Justizvergütungs- und Entschädigungsgesetzes (JVEG) beibehalten werden, die pro Auskunftsersuchen eine Bearbeitungszeit von einer Stunde bei einem maximalen Stundensatz von 17 Euro vorsieht. Alle darüber hinausgehenden Kosten für weitere Server oder zusätzlich benötigtes Personal werden die Anbieter also notgedrungen an ihre KundInnen weitergeben müssen. Diese müssen letztlich für ihre eigene Bespitzelung auch noch einen Aufpreis in Kauf nehmen. Auf diese Weise bietet die nationale Entschädigungsregelung, die in den EU-Staaten unterschiedlich ausgestaltet werden kann, zugleich die Gefahr von Wettbewerbsverzerrungen innerhalb des Binnenmarkts.

Auch der nun vorgelegte Gesetzentwurf konnte der Versuchung nicht widerstehen, unter dem Deckmantel eines (tatsächlich oder vermeintlich) bestehenden gesetzlichen Reformbedarfs en passant auch noch weitere, damit inhaltlich nur bedingt zusammenhängende Wünsche der Sicherheitsbehörden nach Ausweitung der Überwachungsbefugnisse zu befriedigen. Das ist nicht nur unehrlich und der Schaffung bereichsspezifischer und normenklarer Datenschutzregelungen abträglich. Es verlagert einmal mehr die Last auf den Einzelnen, vor nationalen und europäischen Gerichten, insbesondere dem Bundesverfassungsgericht, dem Europäischen Gerichtshof und dem Europäischen Gerichtshof für Menschenrechte für die notwendigen Korrekturen zu sorgen.

19 BVerfG-Entscheidungen Bd. 65, S. 1 (43)

20 BDI-Position zur Vorratsdatenspeicherung, in: Datenschutz und Datensicherheit 2004, H. 10, S. 606-608

Verdeckte Methoden im Strafprozess

Zum Entwurf der aktuellen StPO-Novellierung

von Norbert Pütter

Bereits seit Jahren angekündigt, legte das Bundesjustizministerium im November 2006 einen Gesetzentwurf vor, der die Bestimmungen der Strafprozessordnung (StPO) über verdeckte Ermittlungsmethoden reformieren soll.[1] Indem der Entwurf versucht, ein rechtsstaatlich einwandfreies Fundament für geheime Polizeiarbeit zu liefern, wird er zu deren Ausweitung beitragen.

Nach eigenem Bekunden ist die Novelle aus drei Gründen erforderlich: Erstens verlangten technischer Fortschritt und praktische Schwierigkeiten der Strafverfolgung nach neuen und übersichtlicheren Regelungen für verdeckte Ermittlungsmethoden. Zweitens müsse der Gesetzgeber Entscheidungen des Bundesverfassungsgerichts (BVerfG) aus der jüngeren Vergangenheit Rechnung tragen – namentlich den Urteilen zum Großen Lauschangriff, zur Erhebung von Verkehrsdaten der Telekommunikation (TK) sowie den in verschiedenen Entscheidungen formulierten Maßstäben für Rechts- und Datenschutz bei verdeckten Ermittlungen. Drittens ergäben sich die Änderungen aus den Vorgaben der Cybercrime-Konvention des Europarats, die demnächst ratifiziert werde, sowie aus der EU-Richtlinie zur Vorratsspeicherung von TK-Verkehrsdaten.

Es ist kein Zufall, dass in dieser Motivliste die politische Diskussion um den massenhaften Einsatz verdeckter Polizeimethoden und insbesondere das ungebremste Wachstum der Telekommunikationsüberwachungen (TKÜ) fehlt. Vielmehr liegt dem Entwurf die Überzeugung zugrunde, dass die Strafverfolgung grundsätzlich über alle Instrumente verfügen müsse, um die „Ermittlung des wahren Sachverhalts“ zu errei-

1 s. www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/de-recht/RefE Teil1neu.pdf

chen. Dabei gehe es nicht allein um das „Interesse an einer umfassenden Wahrheitsermittlung und die Aufklärung von schweren Straftaten“, die „wesentlicher Auftrag des Rechtsstaates“ seien. Es gehe auch „um die Möglichkeit des Beschuldigten, einen gegen ihn erhobenen Verdacht auszuräumen“. Diese Chance werde beschnitten, wenn der Polizei nicht alle Methoden zur Verfügung stünden.[2] Im Klartext bedeutet das: Alle rechtschaffenen BürgerInnen müssen die verdeckten Methoden begrüßen, denn wer nichts zu verbergen hat ... So wird aus der liberalen Idee, dass die BürgerInnen in demokratischen Staaten frei von staatlicher Kontrolle leben sollen, eine Rechtfertigung umfassender staatlicher Überwachung. In dieser Logik kann es nur darum gehen, geheime Polizeiarbeit rechtlich abzusichern – genau das versucht der Entwurf.

Die wichtigsten Neuerungen

Das Bundesjustizministerium will mit der Novelle „die verfahrensrechtlichen Voraussetzungen und grundrechtssichernden Ausgestaltungen der verdeckten strafprozessualen Ermittlungsmaßnahmen harmonisieren“. Zu diesem Zweck fasst der Entwurf die Verfahrensvorschriften für „eingriffsintensivere“ Methoden in einer gemeinsamen Vorschrift zusammen. § 101 StPO-neu betrifft die Rasterfahndung, Postbeschlagnahme, TKÜ, technische Überwachungen, Verkehrsdatenerhebung, längerfristige Observationen, Verdeckte Ermittler, Schleppnetzfahndung und polizeiliche Beobachtung. Eingeführt werden sollen

- die Pflicht zur Kennzeichnung der verdeckt gewonnenen Daten
- die Pflicht zur nachträglichen Unterrichtung der betroffenen Personen: Festgelegt wird hier auch der zu benachrichtigende Personenkreis. Die Zurückstellung der Benachrichtigung wird an die Zustimmung des Gerichts gebunden
- die Möglichkeit nachträglichen Rechtsschutzes für Betroffene und
- die Pflicht zur Löschung der verdeckt gewonnenen Daten.

Der Verfahrensschutz soll weiterhin dadurch verbessert werden, dass die gerichtliche Anordnungskompetenz an den Sitz der ermittelnden Staatsanwaltschaft gebunden wird, die Anordnungskompetenzen vereinheitlicht und die Anordnungsdauer verkürzt werden. So soll eine TKÜ nicht mehr drei Monate, sondern nur noch zwei dauern dürfen; freilich kann

2 Allgemeine Begründung, III.3.c, S. 53, s. www.humanistische-union.de/fileadmin/hu/upload/doku/vorratsdaten/de-recht/RefETeil2neu.pdf

sie um jeweils einen Monat verlängert werden. Nach einem halben Jahr muss das übergeordnete Gericht über die Fortsetzung entscheiden.

Bedeutsam für alle verdeckten Methoden ist die Neuformulierung des § 477 StPO: Verdeckt gewonnene Daten wären demnach nur noch dann in anderen Ermittlungsverfahren nutzbar, wenn diese Straftaten betreffen, zu deren Aufklärung die jeweilige Methode ebenfalls zulässig gewesen wäre. Neu geregelt wird ferner das Zeugnisverweigerungsrecht.

Darüber hinaus enthält der Entwurf einige spezifische Bestimmungen zur TKÜ: Der Katalog der Anlassstraftaten wird neu gestaltet. Der „Kernbereich privater Lebensgestaltung", der gemäß BVerfG nicht angetastet werden darf, soll auch bei einer TKÜ geschützt sein. Die jährlichen TKÜ-Statistiken erhalten eine Rechtsgrundlage in der StPO.

Insgesamt scheint der Entwurf tendenziell bürgerrechtsfreundlich zu sein. Aus diesem Rahmen fallen nur die aus dem Cybercrime-Abkommen resultierende Ausweitung des Zugriffs auf Datenträger sowie die Vorratsdatenspeicherung, zu der die EU-Richtlinie verpflichtet.[3]

Dauerbrenner TKÜ

Betrachtet man die scheinbar liberalen Vorschläge etwas genauer, so zeigt sich jedoch sehr schnell, dass unter der Fahne „grundrechtssichernder Ausgestaltung" nur das Minimum verfassungsgerichtlich definierter Standards realisiert werden soll, das nicht nur deutliche Leerstellen aufweist, sondern zudem durch Ausweitungen an anderer Stelle ausgeglichen wird. Die TKÜ ist das Paradebeispiel für diese Logik. Auf der einen Seite wird die Anordnungsdauer begrenzt, der Kernbereich wird geschützt und die Berichtsstatistik wird verpflichtend. Die Verkürzung der Überwachungsfrist war leichten Herzens möglich, weil – darauf weisen die Verfasser selbst hin – das Gutachten des Max-Planck-Instituts (MPI) festgestellt hat, dass Erkenntnisse in aller Regel in den ersten beiden Monaten der TKÜ anfallen.[4] Der Schutz des „Kernbereichs" ergab sich zwingend aus den Verfassungsgerichtsentscheidungen zum Großen Lauschangriff und zum Niedersächsischen Sicherheits- und Ordnungsgesetz. Immerhin erweitert der Entwurf die Berichtspflicht auf

3 s. hierzu den Beitrag von Mark A. Zöller in diesem Heft, S. 21-30

4 Albrecht, H.-J.; Dorsch, C.; Krüpe, C.: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg 2003

Angaben über „die Anzahl der Beteiligten der überwachten Telekommunikation“. Nimmt man dies wörtlich, so wäre zukünftig immerhin der genauere Umfang polizeilich-strafprozessualer TKÜ abschätzbar. In eckigen Klammern wird angeregt zu prüfen, ob die Statistik auch Aussagen über die Relevanz der TKÜ-Erkenntnisse für das Anlassstrafverfahren oder für andere Strafverfahren liefern soll. Da jedoch weder die Kriterien der Relevanz offen liegen, noch die entsprechende Bewertung überprüft werden kann, sind solche Angaben wenig hilfreich. Nimmt man die Befunde der MPI-Studie, so blieben rund die Hälfte aller Überwachungen ohne jeden Ertrag.[5] Die neuen Vorschriften werden an dieser Quote nichts ändern; die verkürzten Fristen werden allenfalls dafür sorgen, dass unnütze Überwachungen nicht noch länger dauern.

Besondere Sorgfalt widmet der Entwurf den Katalogtaten, zu deren Aufklärung eine TKÜ zulässig sein soll. Im Unterschied zur geltenden Fassung wird betont – auch hier den verfassungsgerichtlichen Vorgaben folgend –, dass es sich um eine im Einzelfall schwer wiegende Tat aus dem Spektrum des Katalogs handeln muss. Das historisch gewachsene Sammelsurium an Katalogtaten wird im Entwurf neu geordnet, von einigen Ladenhütern befreit, aber um neue Katalogtaten erweitert. Nicht mehr zulässig sein soll die TKÜ bei Anstiftung etc. zur Fahnenflucht, bei Straftaten gegen die NATO-Streitkräfte und bei fahrlässiger Begehung von Straftaten nach dem Waffengesetz. Demgegenüber wird der TKÜ-Katalog erweitert um:

- eine Reihe von Korruptionsdelikten (Abgeordnetenbestechung, bestimmte Fälle von Bestechung und Bestechlichkeit)
- weitere bandenmäßig begangene Delikte (Fälschung von Zahlungsmitteln, Urkundenfälschungen, Schmuggel, Steuerhinterziehung, Steuerhehlerei)
- Delikte im Bereich des sexuellen Missbrauchs von Kindern und Kinderpornographie
- alle Menschenhandelsdelikte des Strafgesetzbuchs
- Verbrechen gegen die Menschlichkeit und bestimmte Kriegsverbrechen sowie
- einige Betrugsdelikte (Computer-, Subventionsbetrug, Bankrott).

Diese Ausweitungen seien aus unterschiedlichen Gründen erforderlich: Zum Teil handele es sich um typische Erscheinungsformen organisierter

5 ebd., S. 344 f.

Kriminalität, zum Teil seien durch diese Delikte besonders geschützte Rechtsgüter bedroht und zum Teil müsse ein Delikt aus systematischen Gründen aufgenommen werden, weil es bislang bereits im Katalog der Wohnraumüberwachung enthalten sei und bei TKÜ nicht fehlen dürfe, da diese den „milderen" Eingriff darstelle. Die Katalogausweitung hat Folgen über die TKÜ hinaus, weil sie auch für den „Kleinen Lauschangriff" (Abhören außerhalb von Wohnungen), die Erhebung von Verkehrsdaten und den Einsatz des IMSI-Catchers gilt. Außerdem verweisen einige Landespolizeigesetze auf den § 100a StPO, wenn sie „Straftaten von erheblicher Bedeutung" genauer bestimmen, die wiederum das polizeirechtlich zulässige Spektrum verdeckter Methoden festlegen.

Angesichts des erheblich ausgeweiteten Katalogs der Vortaten relativiert sich auch die Bedeutung der vorgeschlagenen neuen §§ 161 Abs. 2 und 477 Abs. 2 StPO, die die Verwertung verdeckt gewonnener Daten begrenzen sollen. Denn je mehr Delikte im Katalog erfasst sind, desto größer ist die Chance, dass die verdeckt gewonnenen Zufallsfunde solche Delikte betreffen, die ebenfalls im Katalog stehen. In diesen Fällen sind zufällig verdeckt erlangte Informationen unmittelbar für Strafverfolgung und -prozess verwertbar. Die Verwertungsbeschränkungen beziehen sich zudem generell nur auf die Verwendung „zu Beweiszwecken in anderen Strafverfahren". An der bestehenden Rechtslage, derzufolge Zufallserkenntnisse mittelbar genutzt werden können, indem sie Anlass zu weiteren Ermittlungen geben, will der Gesetzentwurf ausdrücklich nichts ändern. Mit Ausnahme der aus dem Abhören von Wohnungen gewonnenen Daten bleiben Verwertungen zu anderen polizeilichen Zwecken weiterhin zulässig. Der neue § 477 schränkt zwar die Verwendung verdeckt gewonnener personenbezogener Informationen auf die „Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit" ein (im geltenden Recht fehlt der Bezug auf die „öffentliche Sicherheit"), aber auch in der neuen Version bleibt der § 481 StPO „unberührt". Dieser erlaubt der Polizei, Daten aus Strafverfahren nach Maßgabe ihres jeweiligen Polizeirechts zu verwenden, und ermächtigt die Strafverfolgungsbehörden personenbezogene Daten an die Polizeien weiterzugeben.

Schutz der Betroffenen

Zu den positiven Elementen des Entwurfs gehören die stärkere Beteiligung der Gerichte an der Anordnung und Kontrolle der verdeckten Methoden sowie die detaillierten nachträglichen Mitteilungspflichten, die

den nachträglichen Rechtsschutz verbessern sollen. Ein besserer Grundrechtsschutz soll auch dadurch erreicht werden, dass die Informationen aus TKÜs, die aufgrund staatsanwaltschaftlicher Eilanordnungen geschaltet wurden, nur dann verwertbar sind, wenn die Maßnahme durch ein Gericht bestätigt wird. Durch die Verkürzung der Überwachungsfristen, die erwartbare Zunahme des Umfangs der Überwachungen, die Ausweitung der Benachrichtigungspflichten und die „Entwertung" der staatsanwaltschaftlichen Eilanordnung wird die zeitliche Belastung für die Gerichte erheblich wachsen.

Die MPI-Studie zitiert einen Richter mit der Aussage, dass er und seine KollegInnen schon heute nur zwischen zehn und dreißig Minuten pro Überwachungsanordnung aufwenden.[6] Die wachsende Belastung ist deshalb kaum allein durch die Verlagerung der gerichtlichen Zuständigkeiten an den Sitz der Staatsanwaltschaften auszugleichen, von der sich der Entwurf eine Spezialisierung an den Gerichten erhofft. Wenn die neuen Regelungen nicht ins Leere laufen sollen, bedürfte es also dringend einer personellen Verstärkung der Gerichte. Ein solcher Ausbau, der nicht erwartbar ist, liefe jedoch nicht auf eine Begrenzung verdeckter Polizeiarbeit hinaus, sondern würde im Gegenteil ihren „rechtsstaatlichen Ausbau" vervollständigen.

Im neuen § 101 StPO wird für jede der verdeckten Methoden aufgelistet, welche Personen nachträglich informiert werden müssen. Zwar erlaubt auch die nun vorgeschlagene Regelung nach wie vor, unter bestimmten Bedingungen von der Benachrichtigungspflicht abzusehen, was allerdings gerichtlich bestätigt werden muss. Die eigentliche Neuerung des Entwurfs liegt in der erheblichen Ausweitung des zu benachrichtigenden Personenkreises: So sind von einer Rasterfahndung alle Personen zu informieren, gegen die „weitere Ermittlungen" geführt wurden. Über eine TKÜ oder Verkehrsdatenerhebung sind die „Beteiligten der überwachten (bzw. betroffenen) Telekommunikation" zu unterrichten. Bei „kleinen Lauschangriffen", Bildaufnahmen und technischen Überwachungen sowie beim Einsatz Verdeckter Ermittler gilt dies sowohl für die Zielpersonen als auch für die „erheblich mit betroffenen Personen". Polizei, Staatsanwaltschaft und Gericht werden entscheiden müssen, wann eine solche Mit-Betroffenheit gegeben ist. Damit ist eine zusätzliche Möglichkeit eröffnet, aus der Benachrichtigungspflicht eine

6 ebd., S. 258

Benachrichtigungsoption für die Behörden zu machen. Auch in dieser Frage entscheiden nicht gesetzliche Normen, sondern pragmatische Zwänge.

Leerstellen

Trotz der grundrechtsfreundlichen Rhetorik und trotz einiger begrüßenswerter Elemente ist der Entwurf weit davon entfernt, Schutz- und Kontrollniveau den Gefahren verdeckter Polizeiarbeit anzupassen. Der Gesetzgeber tut nur das Nötigste, um den Forderungen des Verfassungsgerichts nachzukommen. Nicht dass man – angesichts der Regelungen in den Polizeigesetzen – an einen StPO-Paragraphen über V-Personen zu hohe Erwartungen richten dürfte; auffallend bleibt aber, dass die V-Personen weiterhin ohne gesetzliche Grundlage an der Strafverfolgung mitwirken.

Wer der Verrechtlichungslogik folgt, muss auch andere Lücken im Entwurf entdecken. Nur ein Teil der verdeckten Maßnahmen sind an Straftatenkataloge gebunden. Andere (etwa die Rasterfahndung oder der Einsatz Verdeckter Ermittler) können bei bestimmten Straftatengruppen oder Begehungsformen („gewerbs- oder gewohnheitsmäßig“, „von einem Bandenmitglied“ etc.) eingesetzt werden. Letztere Variante ist erheblich behördenfreundlicher, weil das Kriterium weicher ist als das einer bestimmten Straftat. Warum aber der Einsatz eines Verdeckten Ermittlers weniger streng geregelt sein sollte als die technische Überwachung außerhalb von Wohnungen, ist nicht plausibel. Denn der Verdeckte Ermittler kann erheblich intensiver in das Leben und die Rechtsgüter von Ziel- und anderen Personen eingreifen als das durch Filmen oder Tonaufnahmen in der Öffentlichkeit geschehen kann. Hier wird deutlich, wie begrenzt die Perspektive ist, wenn die verdeckten Methoden allein unter dem Gesichtspunkt des „Datenschutzes“ legalisiert werden.

Bemerkenswert ist auch, dass die Berichtspflichten (welche selbst nur an spärliche Inhalte gebunden sind) keineswegs für alle verdeckten Methoden eingeführt werden: Die Behörden sollen weder über den Umfang des Einsatzes Verdeckter Ermittler noch über die Zahl der technischen Überwachungen außerhalb von Wohnungen, der längerfristigen Observationen oder der Postbeschlagnahmen berichten müssen. Für ein transparentes Strafverfolgungssystem wäre dies selbstverständlich.

Grüne TKÜ-Novelle

Abschied vom Straftatenkatalog als Alternative?

von Norbert Pütter

Während der Entwurf des Justizministeriums noch in den vorparlamentarischen Beratungen steckt, haben Bündnis 90/Die Grünen einen Gesetzentwurf zur „Reform der Telekommunikationsüberwachung" (TKÜ) in den Bundestag eingebracht.[1]

Der Entwurf weist im Hinblick auf Ziele und Mittel streckenweise erstaunliche Ähnlichkeiten mit der Regierungsvorlage auf: Er will die Anordnungsfristen auf zwei Monate verkürzen, die Qualität der gerichtlichen Anordnung bzw. Kontrolle verbessern, die Berichtspflichten gesetzlich verankern, der Kernbereich privater Lebensgestaltung vor der TKÜ schützen und das Zeugnisverweigerungsrecht stärken. In den Details unterscheiden sich die Entwürfe: Während die Grünen die Anschlüsse aller Zeugnisverweigerungsberechtigten von der TKÜ ausnehmen wollen (es sei denn, der Zeugnisverweigerungsberechtigte ist selbst Beschuldigter), differenziert der Regierungsentwurf zwischen Geistlichen, Verteidigern und Parlamentariern, die mehr geschützt werden sollen als die anderen in § 52 StPO genannten Gruppen. Die Anordnung soll nach den grünen Vorstellungen nur von einem auf Lebenszeit beamteten Richter getroffen werden (die Regierung will das zuständige Gericht damit befassen). Während das Bundesjustizministerium (BMJ) Vorschriften über den Inhalt der Anordnung macht, formulieren die Grünen die Angaben, die die „Begründung der Anordnung" enthalten muss. Die Vorschläge der Grünen sind dabei detaillierter als die der Regierung. Das gilt auch für die Berichtspflichten, die sich auf elf Angaben – gegenüber sechs im Regierungsentwurf – erstrecken soll.

1 BT-Drs. 16/3827 v. 13.12.2006

Jenseits der Abweichungen im Detail weisen die Vorschläge zwei grundlegende Unterschiede auf. Der erste betrifft das Motiv der Novellierung. Das Ziel des Grünen Entwurfs ist ausdrücklich, das Ausmaß der TKÜ „deutlich (zu) senken". Zentrales Instrument – das ist der zweite fundamentale Unterschied –, um dieses Ziel zu erreichen, ist der Verzicht auf den Katalog der Anlasstaten, zu deren Aufklärung eine TKÜ zulässig sein soll. Bliebe man bei der Regelung über einen abgeschlossenen Katalog, so die AutorInnen, dann sind immer neue Erweitungen zu erwarten – eine Behauptung, die durch den BMJ-Entwurf überzeugend bestätigt wird. Stattdessen schlagen die Grünen eine Umschreibung der TKÜ-Anlasstaten vor, die sicherstellen soll, dass die Maßnahme nur bei schweren Straftaten angewandt wird:

> „Straftaten im Sinne des Abs. 1 sind:
> 1. Verbrechen und vorsätzliche Vergehen, die mit Freiheitsstrafe von mindestens einem Jahr bedroht sind,
> wenn nicht bereits auf Grund der äußeren Umstände des Einzelfalls damit zu rechnen ist, dass wegen der Tat eine Strafe von weniger als einem Jahr Freiheitsstrafe verhängt wird, und
> 2. vorsätzliche Vergehen, die im Höchstmaß mit Freiheitsstrafe von fünf Jahren bedroht sind und bei denen auf Grund der äußeren Umstände der Tat eine Freiheitsstrafe von mindestens einem Jahr zu erwarten ist."

Im Unterschied zum Straftatenkatalog sind diese Kriterien entwicklungs- und interpretationsoffen. Ähnlich der Einsatzvoraussetzungen für Verdeckte Ermittler, über die es seit ihrer Einführung keine öffentliche Debatte gibt, würde der Verzicht auf einen Katalog den Gesetzgeber der Zukunft entlasten und die Interpretationsspielräume von Polizeien, Staatsanwaltschaften und Gerichten erhöhen. Durch eine Reihe verfahrensmäßiger Bestimmungen (Anordnungsbefugnisse, Kennzeichnung, Berichtspflicht, Verwertungsverbote – in allen Fragen jedoch nur leicht strenger als der Regierungsentwurf) versuchen die Grünen dies auszugleichen.

Dass auf diesem Wege die Zahl der TKÜs verringert würde, darf bezweifelt werden. Eine enge rechtliche Regelungslogik wird aufgegeben zugunsten einer Option auf verfahrensmäßige Kontrollen. Dass diese substantiell begrenzen werden, ist sehr unwahrscheinlich. Denn welche (zeitlichen und sonstigen) Möglichkeiten haben RichterInnen, den polizeilichen Erkenntnissen etwas entgegenzusetzen? So lange das Strafprozessrecht als Bekämpfungsrecht ausgestaltet wird – was der grüne Entwurf nicht in Frage stellt –, wird die richterliche Verweigerung die Ausnahme bleiben.

Kontakt-Extremismus

(K)ein Recht auf Auskunft beim Verfassungsschutz?

von Udo Kauß

Rolf Gössner sei kein „Linksextremist", sagt das Bundesamt für Verfassungsschutz (BfV). Dennoch hat es in 36 Jahren der „Beobachtung" eine Menge Daten über ihn zusammengetragen. Die eigentlich interessanten will das Amt dem Rechtsanwalt und Publizisten jedoch nicht offen legen.

Seit zehn Jahren streitet sich Rolf Gössner mit dem BfV darüber, wie weit sein Recht auf Auskunft geht und ob die Daten zu seiner Person zu Recht erfasst wurden. Der heute 58-jährige Rechtsanwalt hat über Jahre hinweg grüne Parlamentsfraktionen beraten, ist Autor zahlreicher Aufsätze und Sachbücher zu Themen der „inneren Sicherheit" und seit 2003 Präsident der Internationalen Liga für Menschenrechte.

1996 verlangte er erstmals Auskunft über seine Daten und fragte das BfV, ob er sich als damaliger Redakteur und Autor der Zeitschrift „Geheim" als amtlich geprüfter „Linksextremist" bezeichnen lassen müsse. Das Amt antwortete mit dem Hinweis auf Gössners Beiträge in als linksextremistisch eingestuften Publikationen. Die Liste beginnt 1970. Darüber hinaus seien auch personenbezogene Daten über seine „Kontakte zur Zusammenarbeit mit linksextremistischen bzw. linksextremistisch beeinflussten Personenzusammenhängen" gespeichert.

Auf Gössners Nachfrage ergänzte das Amt seine Auskunft: Vorhanden und in Dateien erfasst seien auch Informationen über politische Veranstaltungen und Autorenlesungen. Die angehängte Liste mit genauen Zeit- und Ortsangaben bezieht sich auf die 80er und 90er Jahre und nennt u.a. eine von der „Vereinigung der Verfolgten des Nazi-Regimes" (VVN) gemeinsam mit der Stadtbibliothek Bremen in deren Räumen organisierte Lesung aus Gössners Buch „Die vergessenen Justizopfer des Kalten Kriegs". Erfasst wurden aber auch Lesungen in Buchhandlungen, die der Verfassungsschutz dem DKP-Umfeld zurechnete.

Der von Gössner eingeschaltete Bundesdatenschutzbeauftragte (BfD) fand das Vorgehen des Amtes rechtlich nicht zu beanstanden und die Auskünfte auch nicht „unzureichend oder unzutreffend". Bei der Überprüfung habe er sich „im Interesse einer zügigen Durchführung" damit begnügt, sich die Meldungen von BfV-Mitarbeitern vorlesen zu lassen. Diese Verfahrensweise diene dem Schutz der Quellen, sprich: der V-Leute des Verfassungsschutzes. Auf eine persönliche Einsichtnahme in deren Meldungen und Beurteilungen hat der BfD verzichtet. Aus Gründen des Geheimschutzes könne er keine weiteren Auskünfte erteilen.

Im Juni 1997 machte die Bundestagsfraktion von Bündnis 90/Die Grünen Gössners Erfassung durch den Inlandsgeheimdienst und dessen mangelhafte Auskunftserteilung zum Gegenstand einer Anfrage. Die Antwort der Bundesregierung beschränkte sich im Wesentlichen auf die Erklärung, die Überwachung Gössners habe sich nach Recht und Gesetz gerichtet und sei daher rechtmäßig.[1] Nur von begrenztem Erfolg blieb auch der offene Brief, mit dem u.a. prominente Schriftsteller des Deutschen PEN-Zentrums, die IG Medien und die Bürgerrechtsorganisationen im Juli 1997 gegen die Erfassung Gössners protestierten und die Offenlegung aller Daten sowie das Ende der Überwachung forderten.

Auf mehrfache erneute Anfragen hat das BfV seine Auskünfte bis zum Sommer 2005 fortgeschrieben und eine umfängliche Auflistung von Gössners eigenen Artikeln, vor allem aber von Veröffentlichungen Dritter über ihn – jeweils mit Titel, Publikationsorgan und Zeitpunkt des Erscheinens – vorgelegt. Von 2000 bis Mitte 2005 ergibt das allein 49 Einträge. Eigens betont das Amt, dass es keine Daten über Gössners berufliche und ehrenamtliche Aktivitäten auf nationaler und internationaler Ebene erfasse, und versichert, „keine Quelle gezielt gegen Ihre Person" eingesetzt zu haben.

Die Speicherung Gössners wird damit begründet, dass tatsächliche Anhaltspunkte dafür vorlägen, dass er extremistische Bestrebungen von Personenzusammenschlüssen nachdrücklich unterstütze (§ 4 Abs. 1 S. 2 BVerfSchG). Wörtlich:

> „Insbesondere Ihre regelmäßigen Veröffentlichungen in Presseerzeugnissen linksextremistischer bzw. linksextremistisch beeinflusster Publikationsorgane sowie Ihre über Jahrzehnte hinweg bestehenden regelmäßigen und intensiven Kontakte zur DKP und ihren Vorfeldorganisationen (im

1 BT-Drs. 13/8003 v. 19.6.1997

letztgenannten Zusammenhang vgl. die früheren Auskünfte des BfV) bieten tatsächliche Anhaltspunkte dafür, dass Sie mit den entsprechenden Personenzusammenschlüssen in einer Weise zusammenarbeiten, dass diese hierdurch in den von ihnen ausgehenden linksextremistischen Bestrebungen nachdrücklich unterstützt werden. In diesem Zusammenhang von einer sich (lediglich) auf berufliche Berührungspunkte gründenden Kontaktschuld zu sprechen, geht insofern an der Sache vorbei."

Über die Kontakte Gössners zu angeblich linksextremistischen bzw. linksextremistisch beeinflussten Organisationen verweigert das Amt jegliche weitere Auskunft.

Journalistische und anwaltliche Tätigkeit nicht tangiert?

Die bisher erteilten Auskünfte zeigen die bestehende Begriffsverwirrung: Nahezu alle Daten, die das BfV bisher herausrückte, haben einen Zusammenhang mit der publizistisch-journalistischen, fach-juristischen oder anwaltlichen Tätigkeit Gössners. Auch im Prozess vor dem Verwaltungsgericht (VG) Köln, bei dem Gössner im Oktober 2005 Klage gegen die Auskunftsverweigerung erhob, hat das Bundesamt seine Auffassung beibehalten, dass die „regelmäßigen Veröffentlichungen in Presseerzeugnissen linksextremistischer bzw. linksextremistisch beeinflusster Publikationsorgane" sowie die „über Jahrzehnte hinweg bestehenden regelmäßigen und intensiven Kontakte zur DKP und ihren Vorfeldorganisationen ... Anhaltspunkte für eine nachdrückliche Unterstützung links-extremistischer Bestrebungen" lieferten. Trotz der nun seit 36 Jahren dauernden Überwachung reichen die Erkenntnisse des Verfassungsschutzes offenbar weiterhin nur zu der Bewertung, dass bei Gössner lediglich „Anhaltspunkte" für die Unterstützung linksextremistischer Bestrebungen vorlägen. Die Auffassung des Verfassungsschutzes läuft auf eine Erfassungsbefugnis allein wegen des bestehenden Kontakts hinaus, und schafft die neue Kategorie eines „Kontakt-Extremismus". Das hat System.

Mit seiner Klage will Gössner das Bundesamt dazu zwingen, auch über nicht bereits veröffentlichte Informationen Auskunft zu geben. Dabei geht es insbesondere um Daten, die von „Quellen" zusammengetragen wurden, deren Einsatz sich vorgeblich gegen andere Personen, Träger „linksextremistischer Bestrebungen", richtete, mit denen Gössner in beruflichem Kontakt stand bzw. steht. Durch den Einsatz solcher „nachrichtendienstlicher Mittel" hat sich das Bundesamt in ein erhebliches Dilemma gebracht: Zu dieser Problematik hat das Bundesverfas-

sungsgericht (BVerfG) in seiner Entscheidung zum Großen Lauschangriff vom 3. März 2004 dargelegt, dass das Auskunftsrecht gegenüber allen von einer Überwachungsmaßnahme Betroffenen gilt, nicht nur gegenüber der ausdrücklich ins Visier genommenen „Zielperson".[2] Auch insoweit Unbeteiligte sind von dem Eingriff zu unterrichten, auch wenn diese Tatsache gegenüber den Zielpersonen nochmals zusätzlich belastend wirke. Personen, die gleichsam zufällig aufgrund der Überwachung Dritter zum Gegenstand geheimdienstlicher Erfassung geworden sind, verlieren ihren Auskunftsanspruch auch dann nicht, wenn sie durch die Auskunftserteilung Kenntnis davon erhielten, dass ihr Gegenüber als eigentliche Zielperson geheimdienstlicher „Beobachtung" unterliegt.

Ein solches Auskunftsrecht, so wird in der Klage argumentiert, muss erst recht dann bestehen, wenn die Geheimdienste, wie sie das qua Aufgabendefinition regelmäßig tun, im „Vorfeld von Gefahren" tätig werden. Gerade im Vorfeldbereich mit dem dort immanenten erhöhten Risiko der Fehlprognose erfordert der Grundsatz des effektiven Rechtsschutzes eine weitestgehende Unterrichtung. Das BVerfG hat für die vorbeugende Telefonüberwachung im für verfassungswidrig erklärten Niedersächsischen Polizeigesetz ausgeführt, dass nicht einmal die nach einer Unterrichtung der Betroffenen möglicherweise nicht mehr gegebene Einsetzbarkeit eines Verdeckten Ermittlers eine absolute Grenze der Auskunftserteilung darstelle.[3]

Im November 2006 forderte Gössners Anwalt das Bundesamt auf, alle zur Person seines Mandanten gespeicherten Daten zu löschen bzw. zu sperren, weil deren Erhebung und Speicherung von Anfang an rechtswidrig gewesen sei. Keine einzige der mitgeteilten Informationen enthalte eine Aussage, die verfassungsfeindlichen bzw. linksextremistischen Inhalt aufweise, selbst Presseberichte in sicher nicht linksextremismusverdächtigen Organen wie „Die Woche" oder „Frankfurter Rundschau" seien gespeichert.

Dem Bundesamt wurde gleichzeitig die Empfehlung gegeben, Berichte über die wissenschaftliche, journalistische, anwaltliche Tätigkeit nicht in den Fach- und Amtsdateien für politischen Extremismus zu dokumentieren, sondern in seine Bibliothek zu überführen. Wenn schon

2 Az.: 1 BvR 2378/98, in: Neue Juristische Wochenschrift (NJW) 2004, H. 14, S. 999-1022 (1016)

3 BVerfG: Urteil v. 27.7.2005, Az.: 1 BvR 668/04, in: NJW 2005, H. 36, S. 2603-2612 (2611)

Gössners Äußerungen den fachlich interessierten MitarbeiterInnen des Amtes zur Verfügung stehen sollen, sei die Bibliothek der richtige Platz. Für seine Antwort hat sich das Bundesamt Bedenkzeit erbeten.

Kein Einzelfall

Der Verfassungsschutz speichert Personen, die er nicht wagt, als Verfassungsfeinde und Linksextremisten zu bezeichnen. Ihre Einstufung als „Träger linksextremistischer Bestrebungen" würde öffentlicher und gerichtlicher Kritik nicht standhalten. Diese Personen, von denen der Verfassungsschutz seine Hände ansonsten lassen müsste, werden über den Umweg von „Anhaltspunkten" oder angeblichen Unterstützungshandlungen für Linksextremisten zum Beobachtungsgegenstand gemacht.

Seit Jahren überwacht der Verfassungsschutz so auch den Berliner Politogen Peter Grottian, weil in dem von ihm mitinitiierten „Berliner Sozialforum" angeblich auch „richtige" Linksextremisten mitarbeiten würden. Das ist die Legitimation dafür, Spitzel oder im Fachausdruck „Quellen" einzusetzen und deren Kontakte, die „demokratischen, aber gefahrdummen Unterstützer" ebenfalls zu erfassen und Datensammlungen über sie anzulegen.[4]

Auch den PDS-Abgeordneten im Thüringischen Landtag Bodo Ramelow bezeichnet der Verfassungsschutz nicht als Linksextremisten, sondern als „Förderer linksextremistischer Bestrebungen", weil „insbesondere die Linkspartei.PDS als Partei insgesamt in ihren programmatischen Aussagen und in ihrer politischen Praxis tatsächliche Anhaltspunkte für linksextremistische Bestrebungen" im Sinne der §§ 3 und 4 des Bundesverfassungsschutzgesetzes biete."[5]

Alle drei „Förderer" bzw. „Kontakt-Extremisten" haben den juristischen Kampf vor den Verwaltungsgerichten auf volle Auskunft des Verfassungsschutzes zu den über sie gespeicherten Daten aufgenommen, um dieser unter dem Deckmantel der Extremismus-Bekämpfung betriebenen demokratie-feindlichen Überwachung des politischen Alltags den Riegel vorzuschieben. Fortsetzung folgt.

4 vgl. die Stellungnahme des Komitees für Grundrechte und Demokratie v. 20.6.2006
5 zit. aus den Einlassungen des BfV v. 11.5.2006 an das VG Köln

Böcke als Gärtner

Die EU-Polizeien erarbeiten sich einen Datenschutzrahmen

von Tony Bunyan

Die EU arbeitet derzeit an einem Rahmenbeschluss, der den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit regeln soll. Da die Diskussion jedoch in einem vom „Krieg gegen den Terror" bestimmten Klima stattfindet, werden die Rechte der BürgerInnen erneut den Bedürfnissen der Strafverfolgung untergeordnet.

Am 4. Oktober 2005 präsentierte die EU-Kommission ihren Vorschlag für einen Rahmenbeschluss „über den Schutz personenbezogener Daten, die bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden".[1] Der EU-Datenschutzbeauftragte nahm im Dezember 2005 dazu Stellung, und das Europäische Parlament (EP) verabschiedete im September 2006 einen Bericht, in dem es insgesamt sechzig Änderungen empfahl. Fragen der polizeilichen und strafrechtlichen Kooperation, der Dritten Säule der EU, sind ausschließliche Domäne des (Minister-)Rates. Das EP wird hier nur konsultiert. Seine Änderungswünsche kann der Rat theoretisch ignorieren – und das tut er auch in der Praxis regelmäßig.

Wie die Minister mit dem vorliegenden Rahmenbeschluss umzugehen gedachten, wurde deutlich, als sie die „Multidisziplinäre Gruppe Organisierte Kriminalität" (MDG) mit dessen Beratung beauftragten. Die Datenschutzarbeitsgruppe des Rates war bereits 2001 aufgelöst worden – just zu dem Zeitpunkt, als sie über die Notwendigkeit einer Datenschutzregelung für den Polizeibereich diskutierte. Die MDG repräsentiert die Interessen der Strafverfolgungsbehörden. Wie Lord Avebury am 3. Oktober 2006 im EU-Ausschuss des britischen Oberhauses festhielt, besteht ihre „primäre Aufgabe darin, den Kriminellen das Leben schwer

1 KOM(2005) 475 endg. v. 4.10.2005 (= Ratsdok. 13019/05 v. 11.10.2005)

zu machen und nicht, sich um den Datenschutz zu kümmern." Ganz in diesem Sinne machte sich die Gruppe daran, die Rechte der Betroffenen weiter auszuhöhlen. Weder dem gegenseitigen Zugriff der Mitgliedstaaten auf ihre nationalen Polizeidaten noch dem Austausch mit den Behörden befreundeter Staaten wie den USA sollten Hindernisse im Weg stehen.

Die Verhandlungen der MDG waren geheim. Ihre Dokumente waren nicht zugänglich, bis Statewatch sie im September 2006 veröffentlichte.[2] Der EU-Datenschutzbeauftragte sah sich daraufhin zu einer unüblichen – sehr kritischen – zweiten Stellungnahme veranlasst, und der Bürgerrechtsausschuss des EP forderte den Rückruf des Rahmenbeschlusses für eine zweite Konsultierung. All das mag am Ergebnis letztlich nicht viel ändern, aber immerhin zu einer öffentlichen Debatte führen, die andernfalls nicht stattfinden würde.

Es ist zwar zweifellos eine ernüchternde Diagnose über den Zustand der demokratischen Kultur der EU, wenn hinsichtlich der Persönlichkeitsrechte ihrer BewohnerInnen nichts besseres zu erwarten ist, als eine öffentliche Debatte mit wenig Effekt. Bei der Verabschiedung der Rechtsgrundlagen für das Schengener Informationssystem der zweiten Generation – zwei Verordnungen und ein Beschluss – ließ es die EU jedoch selbst an dieser minimalen Öffentlichkeit fehlen. Die Schlussfassungen der Texte wurden hinter verschlossenen Türen bei geheimen „Trialog"-Treffen zwischen VertreterInnen des Rates, der Kommission und des EP ausgehandelt und dann im Eilverfahren ohne Änderungsmöglichkeit angenommen.

Das Prinzip der Verfügbarkeit

Die Idee einer umfassenden Datenschutzregelung für die Dritte Säule stand seit Mitte der 90er Jahre schon mehrmals auf der Tagesordnung der EU. Die Datenschutzrichtlinie von 1995 gilt nicht für Polizei und Strafjustiz. In diesem Bereich hat die EU bisher nur Regelungen produziert, die sich auf die einzelnen gemeinsamen Datenbanken (SIS, Europol-Dateien etc.) beziehen. Der sonstige polizeiliche Datenaustausch stützt sich nach wie vor auf die nationalen Gesetze sowie die rudimentären Bestimmungen des Europaratsabkommens „über den Schutz des

2 sämtliche hier zitierten Texte unter www.statewatch.org/eu-dp.htm

Menschen bei der automatischen Verarbeitung personenbezogener Daten“ von 1981. Spätestens seit sich die Mitgliedstaaten im Haager Programm vom 5. November 2004, dem Fünfjahresplan der EU für die Innen- und Justizpolitik, darauf geeinigt haben, den Austausch von Polizeidaten ab 2008 nach dem „Prinzip der Verfügbarkeit“ zu organisieren, schien eine umfassende datenschutzrechtliche Regelung für den Polizeibereich unausweichlich.

Der Grundsatz beinhaltet, dass Daten, die für die Polizei- und Strafverfolgungsbehörden eines Mitgliedstaates „verfügbar“ sind, auch den Behörden der anderen EU-Länder unmittelbar zugänglich sein müssen. Für die Umsetzung dieses Prinzips, das vorgeblich der besseren Bekämpfung des Terrorismus dienen soll, liegen mittlerweile eine Reihe von Vorschlägen auf dem Tisch, die in einem ersten Schritt den gegenseitigen Online-Zugriff auf Fingerabdruck- und DNA-Profil-Dateien sowie Fahrzeugregister vorsehen.[3]

Die Kommission nimmt in ihrem Entwurf des Datenschutz-Rahmenbeschlusses auf das Prinzip der Verfügbarkeit in Art. 1.2 Bezug, indem sie von den Mitgliedstaaten verlangt, sicherzustellen, „dass die Offenlegung personenbezogener Daten gegenüber den zuständigen Behörden anderer Mitgliedstaaten nicht aus Gründen, die mit dem Schutz personenbezogener Daten gemäß diesem Rahmenbeschluss zusammenhängen, eingeschränkt oder untersagt wird.“ In der von der MDG produzierten Version des Rates bleibt diese Intention – allerdings mit einer drastischeren Formulierung – erhalten. Der Rat fordert schlicht und einfach, dass keine nationalen Datenschutzregelungen den Austausch personenbezogener Daten „einschränken oder untersagen“ dürfen.[4] Damit ist gleich von Anfang an sichergestellt, dass der Datenschutz eine zahnlose Angelegenheit bleibt.

Konsequenterweise geht der Vorschlag des Rates auf eine ganze Reihe zentraler Fragen gar nicht erst ein: Er behandelt nicht den automatisierten Zugriff auf Datenbanken in einem anderen EU-Staat. Er unterscheidet nicht zwischen „harten“ Daten wie z.B. Verurteilungen und weichen Informationen („intelligence“), die auf bloßen „Anhaltspunkten“ oder Spekulationen beruhen können. Daten über Unverdächtige, die

3 Das ist auch das Ziel des Vertrags von Prüm, den bisher acht EU-Staaten unterzeichnet haben, siehe m.w.N. Bunyan, T.: Freier Markt für Polizeidaten – das Prinzip der Verfügbarkeit, in: Bürgerrechte & Polizei/CILIP 84 (2/2006), S. 21-28

4 derzeit letzte Version: Ratsdok. 13246/5/06 v. 22.11.2006, Art. 1.4

ohne ihr Zutun in eine Ermittlung geraten (Familie, Freunde, ArbeitskollegInnen etc.), aber auch über Opfer von Straftaten erhalten keinen besonderen Schutz. Ein programmiertes Vergessen bei abgesessenen Strafen gibt es nicht, obwohl die nationalen Gesetze in dieser Frage stark voneinander abweichen. Der Rahmenbeschluss betrifft alle personenbezogenen Daten, wie geringfügig die jeweiligen Straftaten auch immer sein mögen.

Dass der Rahmenbeschluss nicht dem Datenschutz gilt, sondern im Gegenteil, der polizeilichen Datenverarbeitung und vor allem der Weitergabe von Daten über die nationalen Grenzen hinweg zu einer rechtlichen Grundlage verhelfen soll, zeigen die Vorschläge zu den einzelnen Bestimmungen:

- **Gegenstand:** Die Mitgliedstaaten streiten sich im Rat darüber, ob der Rahmenbeschluss nur den grenzüberschreitenden und internationalen Datenaustausch oder auch die nationale polizeiliche Datenverarbeitung betreffen soll. Gemäß Art. 1.4 soll es den Mitgliedstaaten erlaubt sein, auf nationaler Ebene Schutzvorkehrungen zu treffen, die über das Niveau des Rahmenbeschlusses hinausgehen. Solche Vorschriften dürften aber den Austausch zwischen den Mitgliedstaaten weder „einschränken" noch „untersagen". Die finnische Ratspräsidentschaft drückt das in einer Note so aus: „Die Mitgliedstaaten werden verpflichtet, ihre nationalen Datenschutzbestimmungen dem Rahmenbeschluss anzupassen."[5]
- **Datenaustausch mit Drittstaaten:** Umstritten ist ebenfalls, ob die Weitergabe von Daten an Drittstaaten und internationale Organisationen an die Voraussetzung gebunden sein soll, dass diese ein vergleichbares, angemessenes Datenschutzniveau bieten (Art. 15.d).[6] Fünf Staaten unterstützen diese Forderung – Finnland, Griechenland, Portugal, Tschechien sowie die an Schengen assoziierte Schweiz. Sieben Staaten sind dagegen: Britannien, Dänemark, Deutschland, Irland, Schweden und das ebenfalls nur assoziierte Norwegen.[7]

---

5 Ratsdok. 12924/06 v. 19.9.2006

6 Gemäß dem Kommissionsvorschlag soll dies die Weitergabe von solchen Daten an Drittstaaten betreffen, die ein EU-Staat von einem anderen Mitgliedstaat erhalten hat. Fünf Staaten unterstützen diese Position: die Niederlande, Polen, Tschechien, Spanien und die Schweiz. Belgien und Ungarn wollen das angemessene Datenschutzniveau auch dann fordern, wenn die Daten aus dem EU-Staat, in dem sie erhoben wurden, an Drittstaaten weitergereicht werden, Ratsdok. 12924/06 v. 19.9.2006.

7 Ratsdok. 11547/3/06 v. 13.7.2006

Die USA, die über „hochrangige“ Treffen mit EU-VertreterInnen an dieser Diskussion beteiligt sind, wehren sich gegen diese Forderung nach einem angemessenen Datenschutzniveau, weil sie über keine Datenschutzbestimmungen für Nicht-US-BürgerInnen verfügen. Art. 15 würde „die exzellenten informellen Kontakte beeinträchtigen, die die US-Strafverfolgungsbehörden mit ihren Partnern in den EU-Mitgliedstaaten entwickelt haben.“[8] Der Austausch von Daten, z.B. mit den USA, soll sich gemäß den Vorstellungen des Rates nach bilateralen Vereinbarungen richten, die keinen Datenschutz für EU-BürgerInnen beinhalten – weder hinsichtlich der Übermittlung noch in Bezug auf die weitere Verarbeitung der Informationen.

- **Nationale Sicherheit:** Gemäß der bereits zitierten Note der finnischen Präsidentschaft gibt es im Rat einen „breiten Konsens“ darüber, dass Daten „mit einer Verbindung zu Zwecken der nationalen Sicherheit“ nicht zum Gegenstand des Rahmenbeschlusses gehören sollen. Der Austausch zwischen den Staatsschutz- bzw. Inlandsgeheimdiensten müsste dann in einem zusätzlichen Beschluss oder Rahmenbeschluss geregelt werden.[9]
- **Weitere Verarbeitung bei den Empfängern:** Der Rahmenbeschluss-Entwurf erlaubt die weitere Verarbeitung auch zu Zwecken, die nichts mehr mit dem der Erhebung und auch nichts mit Strafverfolgung oder der Verhütung von Straftaten zu tun haben.
- **Besonders sensible Daten:** In Art. 6 Abs. 1 sah der Kommissionsentwurf folgende Formulierung vor: „Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie von Daten über Gesundheit oder Sexualleben.“ In Abs. 2 folgten die Ausnahmen, nämlich dass die Verarbeitung gesetzlich vorgeschrieben und unabdingbar für die „Verhütung, Aufdeckung, Untersuchung und Verfolgung“ von Straftaten sein müsse. Der Rat hat diese Regelung umgekehrt: Die Mitgliedstaaten sollen die Verarbeitung solcher Daten zulassen, „wenn dies unbedingt erforderlich ist.“ Die Ausnahme ist damit zur Regel geworden.

---

8 so die Ergebnisse eines hochrangigen Treffens zu justiz- und innenpolitischen Fragen am 18.7.2006 in Helsinki, Ratsdok. 12064/06 v. 27.7.2006

9 Ein ähnliches Verfahren hat die EU beim Visa-Informationssystem angewandt, siehe den Entwurf eines Ratsbeschlusses über den Zugang der „für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten“ zum VIS, KOM(2005) 600 endg. v. 24.11.2005.

- **Rechte der Betroffenen:** Der Kommissionsentwurf enthielt in den Art. 19 und 20 ein Recht, unaufgefordert über die Speicherung und Weitergabe von Daten informiert zu werden. In der MDG ist weiterhin umstritten, ob diese Regelung nicht generell zu streichen sei. „Viele Delegationen", so bemerkt die Präsidentschaft, „haben sich gefragt, ob ein Prinzip sinnvoll ist, das aufgrund der vielen Ausnahmen in kaum einem Fall angewandt worden wäre."[10] Hinsichtlich der eigentlich gefährlichen Informationen, die hinter dem Rücken der Betroffenen erhoben wurden, ist dieses Recht in der derzeit letzten Fassung zur Unkenntlichkeit geschrumpft. Informationen soll es nur geben, wenn die jeweilige polizeiliche „Aktivität" nicht mehr gefährdet und kein „unverhältnismäßiger Aufwand" zu erwarten ist.

Zusammengestrichen hat die MDG auch das Auskunftsrecht auf Antrag: Die Betroffenen sollen nur noch die „Bestätigung" erhalten, ob Daten zu ihrer Person vorhanden sind und an wen sie weitergegeben wurden, sowie eine „Mitteilung in verständlicher Form" über den Inhalt. Die Kommission hatte zusätzlich über Datenkategorien, Zwecke und Rechtsgrundlage der Speicherung sowie über die Herkunft der Daten informieren wollen. Solche „operativen Informationen" dürfe man im Rahmen des Datenschutzes nicht erteilen, entschied die MDG.[11]

Nach Art. 22 des Kommissionsentwurfs sollten die von den Betroffenen erstrittenen Berichtigungen, Sperrungen und Löschungen auch an die Stellen mitgeteilt werden, denen man zuvor die Daten übermittelt hatte. Die MDG hat hier ergänzt: „... sofern es sich nicht als unmöglich herausstellt oder mit einem unverhältnismäßigen Aufwand verbunden ist." Selbst wenn falsche Daten an einen EU- oder einen Drittstaat weitergegeben wurden, soll es keine Pflicht zur Korrektur geben.

- **Verhältnis zu internationalen Abkommen:** Der Rahmenbeschluss ist zwar auf Verträge und Vereinbarungen anwendbar, die EU-Staaten untereinander geschlossen haben. „Bi- und multilaterale Abkommen zwischen Mitgliedstaaten und Drittländern sind nicht vom Rahmenbeschluss betroffen, und für die Mitgliedstaaten gilt keine Verpflichtung, diese Abkommen zu ändern."

Sofern es um Abkommen geht, die die EU selbst mit Drittstaaten geschlossen hat, befürchtet der Rat, dass jede Änderung „die Glaubwür-

10 Ratsdok. 12925/06 v. 19.9.2006

11 Ratsdok. 11547/3/06 v. 13.9.2006, Fußnote 102

digkeit der Europäischen Union als Verhandlungspartnerin beeinträchtigen könnte". Dies sei umso mehr der Fall, „als die wenigen Vereinbarungen, die bisher auf der Grundlage von Art. 24/38 des Vertrags über die Europäische Union getroffen wurden, neueren Datums sind."[12] Der Rat ist offensichtlich weniger besorgt um seine Glaubwürdigkeit bei den EU-BürgerInnen, als um jene bei der US-Regierung, mit der er Verträge „neueren Datums" über den Datenaustausch mit Europol, über Rechtshilfe und Auslieferung und über die Weitergabe von Flugpassagierdaten geschlossen hat.

Schlussfolgerungen

Der Rahmenbeschluss wird erhebliche Auswirkungen haben – auf die nationalen Datenschutzgesetze in den EU-Staaten, auf den Datenaustausch zwischen den Polizei- und Strafverfolgungsbehörden in der EU, aber auch rund um den Globus. Er bildet die Grundlage für eine ganze Serie schon geplanter und zukünftiger Maßnahmen, die mit dem „Prinzip der Verfügbarkeit", dem gegenseitigen direkten Zugang der Polizeien der Mitgliedstaaten zu ihren Datenbeständen, auf die EU und ihre BewohnerInnen zukommen.

Schon hinter dem Kommissionsvorschlag stand die Überlegung, dass es für die Umsetzung dieses Prinzips eines datenschutzrechtlichen Gerüsts in der EU bedürfe. Bei all seinen Schwächen enthielt dieser erste Entwurf immerhin noch einige grundlegende Rechte für die Betroffenen. Die ausschließlich an den Interessen der Strafverfolgung orientierte Ratsarbeitsgruppe hat auch diese Reste beseitigt.

12 Ratsdok. 12924/06 v. 19.9.2006

Es wächst zusammen ...

Zum Gemeinsame-Dateien-Gesetz

von Heiner Busch

Siebzehn Jahre nach der Auskoppelung der Staatsschutzabteilung des Bundeskriminalamtes aus dem Nachrichtendienstlichen Informationssystem des Bundesamtes für Verfassungsschutz hat das Parlament die informationstechnische Wiedervereinigung von Polizei und Geheimdiensten beschlossen.

Am Ende konnte es der Bundesregierung und ihrer Großen Koalition nicht schnell genug gehen. Im Juni 2004 – kurz nach dem Anschlag in Madrid – hatte die Innenministerkonferenz (IMK) den Aufbau einer gemeinsamen Anti-Terror-Datei von Polizei und Geheimdiensten des Bundes und der Länder gefordert, um der angeblich so zerstückelten föderalistischen „Sicherheitsarchitektur" der Bundesrepublik informationstechnisch auf die Sprünge zu helfen. Die Parteien diskutierten, ob es sich um eine Volltext- oder „nur" um eine Indexdatei handeln sollte und ob man darin „nur" Daten zum Terrorismus oder gleich auch solche zum Extremismus zu speichern hätte. Dann kamen das Ende der rot-grünen Ehe, die Wahlen und der halbe Regierungswechsel.

Am 4. September 2006 erneuerte die IMK ihre Forderung, diesmal mit dem Rückenwind zweier nicht explodierter Kofferbomben in deutschen Regionalzügen. Keine drei Wochen später lag der Gesetzentwurf dem Bundesrat vor. Er sei „besonders eilbedürftig", mahnte die Bundeskanzlerin in ihrem Anschreiben. Die Ländervertretung hatte denn auch inhaltlich nichts auszusetzen und empfahl am 3. November, einerseits die „sunset"-Klausel, das Auslaufen eines Teils des Gesetzes nach fünf Jahren, zu streichen und andererseits gleich auch noch dafür zu sorgen, dass die bei der Erfassung der LKW-Maut auf den Autobahnen anfallenden Daten von ihrer lästigen Zweckbindung befreit würden. Der Bundestag überwies seinerseits den Entwurf im Oktober an die Ausschüsse. Bei der öffentlichen Anhörung des Innenausschusses am 1. November

durften die KritikerInnen noch einmal kurz auf das Trennungsgebot von Polizei und Geheimdiensten hinweisen. Am 1. Dezember lehnte das Plenum des Bundestages sämtliche Anträge der kleinen Oppositionsparteien ab und nahm das Gesetz ohne viel Federlesen an.[1] Das endgültige Plazet des Bundesrates am 15. Dezember war dann nur noch Formsache. Pünktlich zu Weihnachten war die Bescherung perfekt.

Terrorismus im Konjunktiv

Das zweifelhafte Geschenkpaket enthält fünf Artikel: Das Anti-Terror-Datei-Gesetz (ATDG) ist dabei nur der erste. Eingerichtet wird die Datenbank beim Bundeskriminalamt (BKA). Zugriff haben sollen zum einen die sechzehn Landeskriminalämter, die Bundespolizeidirektion, das Bundesamt (BfV) und die Landesämter für Verfassungsschutz, der Militärische Abschirmdienst, der Bundesnachrichtendienst (BND) und schließlich das Zollkriminalamt (ZKA). In der Errichtungsanordnung, also durch einen exekutiven Federstrich, können zum andern neben diesen 38 Ämtern und Diensten noch weitere Polizeibehörden beteiligt werden, „soweit diesen Aufgaben zur Bekämpfung des internationalen Terrorismus ... nicht nur im Einzelfall besonders zugewiesen sind“ (§ 1 Abs. 2). Laut Begründung des Entwurfs kommen hierfür „in erster Linie die Dienststellen des polizeilichen Staatsschutzes der Länder“ in Frage.

Die „beteiligten Behörden“ können nicht nur Daten abrufen, sondern sie müssen auch die ihnen vorliegenden einschlägigen „Erkenntnisse“ hier erfassen. „In der Antiterrordatei dürfen nur bereits erhobene Daten gespeichert werden“, beteuert die Bundesregierung in der Begründung. Das ist Augenwischerei, denn die Pflicht zur „unverzüglichen Speicherung“ betrifft nicht nur die heute vorliegenden „Erkenntnisse“, sondern auch die, die jeweils neu erhoben werden. Das Gesetz enthält zwar keine Befugnis, Daten eigens für die Speicherung in der neuen Datenbank zu erheben, aber eine Pflicht zur Doppelerfassung, und zwar in den eigenen Datensammlungen der jeweiligen Behörden und in der gemeinsamen Anti-Terror-Datei.

---

1 Bundesgesetzblatt I Nr. 66 v. 30.12.2006, S. 3409-3415; Entwurf: BT-Drs. 16/2950 v. 16.10.2006 = BR-Drs. 672/06 v. 22.9.2006; Stellungnahme des Bundesrates: BT-Drs. 16/3292 v. 8.11.2006; Beschlussempfehlung des Innenausschusses: BT-Drs. 16/3642 v. 29.11.2006

Dass die Datei „Vorfelderkenntnisse“ enthalten wird, wie die GesetzesmacherInnen in der Begründung eigens betonen, ergibt sich zunächst daraus, dass sich die geheimdienstliche Hälfte der beteiligten Behörden in aller Regel im Vorfeld von strafrechtlichen Ermittlungen tummelt. Wie weit ins Vorfeld die Erfassung reicht, zeigt der nur mit großer Mühe verstehbare § 2 ATDG, der festlegt, welche Personen, Organisationen etc. gespeichert werden müssen. Eine Übersetzung aus dem Behördendeutsch ergibt folgendes Bild: Zum einen legt der Paragraf vier Kategorien von Personen fest:

- Mitglieder oder UnterstützerInnen von terroristischen Vereinigungen (§§ 129a und b Strafgesetzbuch), die entweder im Inland agieren, aber einen Auslandsbezug haben, oder im Ausland tätig sind und eine Verbindung zu Deutschland aufweisen (Nr. 1a)
- Mitglieder oder UnterstützerInnen einer „Gruppierung“, die eine terroristische Vereinigung unterstützt, m.a.W. auch UnterstützerInnen der UnterstützerInnen, was immer das auch sein mag (Nr. 1b)
- Personen, die rechtswidrige politisch oder religiös motivierte Gewalt anwenden, aber auch solche, die eine Gewaltanwendung „unterstützen, vorbereiten, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen“. Mit letzterem seien insbesondere „Hassprediger“ gemeint, heißt es in der Begründung (Nr. 2)
- Kontaktpersonen: Darunter hat man Leute zu verstehen, über die „tatsächliche Anhaltspunkte vorliegen“, dass sie „in nicht nur flüchtigem oder zufälligem Kontakt“ zu den unter den Nrn. 1a und 2 genannten Hauptpersonen stehen und dass „durch sie Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus gewonnen werden können.“ Die Präzisierung „... nicht nur flüchtig oder zufällig ...“ ist dem Innenausschuss des Bundestages zu verdanken, der allerdings eine von den Grünen geforderte weitere Einengung auf Personen, die vom Terrorismusbezug der Hauptpersonen wissen, ablehnte (Nr. 3).

Hinzu kommen zwei weitere Kategorien: einerseits Vereinigungen, Gruppierungen, Stiftungen und Unternehmen (Nr. 4a), andererseits Sachen sowie Bank- und Kommunikationsverbindungen (Anschriften, Telekommunikationsanschlüsse, Internetseiten, E-Mail-Adressen). In beiden Fällen müssen „tatsächliche Anhaltspunkte“ für eine Verbindung zu einer Person aus den Nrn. 1a, b und 2 da sein.

Schon die Kategorien selbst sind uferlos. Der um sie herum gebaute Text lässt die Grenzen vollends verschwimmen: Er verpflichtet die be-

teiligten Behörden zur Speicherung von Daten, „wenn sie (die Behörden, d.Verf.) über polizeiliche oder nachrichtendienstliche Erkenntnisse verfügen, aus denen sich tatsächliche Anhaltspunkte ergeben, dass die Daten“ sich auf eine der genannten Kategorien „beziehen“. Anhaltspunkte für einen solchen Bezug sind laut der Begründung dann „tatsächlich“, wenn sie „nach nachrichtendienstlichen oder polizeilichen Erfahrungswerten die Einschätzung rechtfertigen, dass die Erkenntnisse ... zur Aufklärung oder Bekämpfung des internationalen Terrorismus beitragen.“ Es geht also nicht darum, ob eine Person konkret verdächtig ist, eine terroristische Vereinigung zu unterstützen oder rechtswidrige Gewalt zu befürworten (was ohnehin keine Straftat darstellt). Entscheidend ist vielmehr, dass Polizei oder Geheimdienste davon ausgehen, dass die Person eine UnterstützerIn oder BefürworterIn sein könnte. Unter den möglichen Voraussetzungen für eine Speicherung hat sich der Gesetzgeber damit die am weitesten gehende Formulierung ausgesucht. Die im selben Paragrafen enthaltene Forderung, dass die gespeicherten Daten für die Zwecke der „Aufklärung“ bzw. „Bekämpfung“ des Terrorismus „erforderlich“ sein müssten, erscheint vor diesem Hintergrund als groteske Datenschutzlyrik, weil es dann, wenn „Erfahrungswerte“ und „Einschätzungen“ die Erfassung bestimmen, nichts mehr gibt, woran die Erforderlichkeit oder Verhältnismäßigkeit zu messen wäre.

In den folgenden Paragrafen unterscheidet das Gesetz bei den zu erfassenden Personen zwischen „Grunddaten“ und „erweiterten Grunddaten“. Erstere sollen ausschließlich zur Identifikation der Betroffenen dienen, gehen aber bereits über das Übliche hinaus: Gespeichert werden sollen neben Personalien, Aliaspersonalien, Anschrift auch besondere körperliche Merkmale, die gesprochenen Dialekte, Fotos sowie die „Fallgruppe“, d.h. die Kategorie, der die Person nach § 2 zugeordnet wird. Bei der Abfrage zu einer Person erhalten die dazu berechtigten MitarbeiterInnen der beteiligten Behörden zunächst diese Grunddaten sowie die Angabe über die aktenführende Stelle.

Für einen Zugriff auf die „erweiterten Grunddaten“ bedarf es im Normalfall eines Ersuchens an die Behörde, die die Daten eingegeben hat. Im Eilfall, der bei Ermittlungen im Terrorismus-Umfeld leicht zu konstruieren ist, kann eine abfragende Stelle das Ersuchen nachreichen und sich sofort an diesen Informationen bedienen. Auch die „erweiterten Grunddaten“ dienen angeblich der Identifikation der Betroffenen und erlauben laut Begründung „eine fachliche Ersteinschätzung im Sinne einer zuverlässigen Gefährdungseinschätzung“. Die Religionszugehö-

rigkeit ist dabei nur ein Beispiel für hochsensible Daten. Weit gefährlicher ist die Zuordnung zu einer Organisation und die Angabe von „besuchten Orten oder Gebieten“. Hinzu kommen Daten über eigene oder benutzte fremde Telekommunikationsanschlüsse, E-Mail-Adressen, Bankverbindungen, Fahrzeuge etc., die auch eigenständig erfasst werden. Auch wenn hier keine Verknüpfungsmöglichkeit zwischen den verschiedenen Personen- und Sachdaten vorgesehen ist, ermöglicht die Kenntnis der „erweiterten Grunddaten“ einer Person eine weitreichende Recherche ihres Umfelds. Wie die beteiligten Ämter und Dienste das Freitextfeld für „zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen“ nutzen, ob sie dort nur drei Zeilen oder ganze Aktenteile hinterlassen, hängt weder vom Gesetz noch von der Technik, sondern nur von ihrem Mitteilungsbedürfnis ab.

Mit diesem Feld verlässt das Gesetz definitiv die ursprüngliche Konzeption der „Indexdatei“. Entstanden ist vielmehr ein umfängliches gemeinsames Register für polizeiliche und geheimdienstliche Informationen; umfänglich wegen der Zahl der beteiligten Behörden, hinsichtlich der Breite des Kreises der zu erfassenden Personen und schließlich der Tiefe der zu ihnen gespeicherten Daten.

Zusammenarbeitspflicht

Dass Polizei und Geheimdienste regelmäßig Informationen austauschen, ist nichts Neues. Mit den Geheimdienstgesetzen von 1990 hat die Pflicht zur Zusammenarbeit und zur Weitergabe von Daten, die seit den 50er Jahren in diversen Weisungen festgehalten war, erstmals eine gesetzliche Fassung erhalten.

Es ist auch nicht das erste Mal, dass der Datenaustausch zwischen beiden Seiten auf automatisierte Weise erfolgt. Als der polizeiliche Informationsverbund (INPOL) und das Nachrichtendienstliche Informationssystem (NADIS) des Verfassungsschutzes in den 70er Jahren aufgebaut wurden, erschien beiden Seiten der gegenseitige Online-Zugriff völlig selbstverständlich – und das nicht nur wegen des Terrorismus der RAF. Nach heftigen Auseinandersetzungen mit dem Bundesdatenschutzbeauftragten wurde diese umfassende Verbindung 1979 gekappt. Allerdings führte die BKA-Staatsschutzabteilung noch bis 1989 ihren Personenindex nicht nur in der eigenen PIOS-Arbeitsdatei, sondern auch

in NADIS.[2] Das Bundesverfassungsschutzgesetz (BVerfSchG) von 1990 setzte diese technische Abkoppelung auch rechtlich um. Es schreibt in § 6 vor, dass Bundesamt und Landesämter für Verfassungsschutz gemeinsame Dateien zur gegenseitigen Unterrichtung betreiben und ein automatisierter Abruf durch andere Stellen unzulässig ist.

Das ATDG macht diese Regelung zur Makulatur. Es behandelt BKA und Landeskriminalämter, Bundespolizei und ZKA sowie sämtliche Geheimdienste als gleichberechtigte Mitglieder der großen Familie von „Sicherheitsbehörden", die in trauter Eintracht gegen den Terrorismus und sein großes Um- und Vorfeld zusammenarbeitet. Das Gesetz ratifiziert gewissermaßen den seit langem anhaltenden Prozess der Angleichung beider Seiten – der Vergeheimdienstlichung der Polizei einerseits und der Verpolizeilichung der Dienste andererseits. Dass sowohl die Polizei als auch die Dienste im Vorfeld arbeiten, erscheint in diesem Gesetz als selbstverständlich. Worin der qualitative Unterschied zwischen polizeilichen und geheimdienstlichen Vorfelderkenntnissen bestehen könnte, ist nicht ersichtlich. Selbst die unterschiedlichen Aufgabennormen, für die aufgrund der Vorverlagerung polizeilicher Tätigkeiten bisher lange Umschreibungen notwendig waren, reduzieren sich nun auf zwei Worte: „Aufklärung" einerseits und „Bekämpfung" andererseits. Das lange Gerede um „Strafverfolgung", „Gefahrenabwehr", „Gefahrenvorsorge" und „vorbeugende Bekämpfung von Straftaten" hat ein Ende. Die Trennung von Polizei und Geheimdiensten ist zwar nicht aufgehoben, sie ist aber nur noch eine organisatorische, die gleichzeitig zur Zusammenarbeit verpflichtet.

Das jetzt verabschiedete Gesetz gibt dieser Zusammenarbeit technische Formen, deren eine die Anti-Terror-Datei darstellt. So wie die Registerdateien der Polizeien von Bund und Ländern im Rahmen von INPOL oder des Bundesamtes und der Landesämter für Verfassungsschutz in NADIS ermöglicht die Anti-Terror-Datei zum einen eine „erste fachliche Einschätzung" über die Grenze zwischen Polizeien und Geheimdiensten hinweg. Sie ist zugleich eine Einladung, mit der aktenführenden Stelle in direkten Kontakt zu treten und mehr zu erfahren. Der automatisierte Datenabruf findet nur da seine Grenze, wo der Quellenschutz, das Grundgesetz der geheimdienstlichen und der verdeckten

2 Busch, H.: Staatsschützerische Großbaustelle, in: Bürgerrechte & Polizei/CILIP 78 (2/2004), S. 14-28

polizeilichen Tätigkeit, es erfordert. § 4 ATDG ermöglicht deshalb die „beschränkte“ und die „verdeckte“ Speicherung. Bei letzterer werden der Behörde, die die Daten eingegeben hat, automatisch die Abfragedaten übermittelt. Sie hat dann „unverzüglich“ mit der anfragenden Stelle Kontakt aufzunehmen. Während der ursprüngliche Regierungsentwurf eine verdeckte oder beschränkte Speicherung nur bei „besonderen Geheimhaltungsinteressen“ zulassen wollte, hat der Innenausschuss des Bundestages die „besonders schützwürdigen Interessen des Betroffenen“ ergänzt. Das sieht schöner aus, ist aber nicht weiter von Belang.

Projekte und Projektdateien

Während die Anti-Terror-Datei den Austausch von Einzelinformationen automatisiert, regeln die Artikel 2-4 des Gemeinsame-Dateien-Gesetzes eine erheblich intensivere Kooperation zwischen Polizei und Geheimdiensten, die aber in der Öffentlichkeit kaum wahrgenommen wurde. Die Artikel ergänzen das BVerfSchG, das BND- und das BKA-Gesetz um nahezu gleichlautende Formulierungen, die dem BfV, dem BND und dem BKA die Führung von Projektdateien für den „Austausch und die gemeinsame Auswertung von polizeilichen und nachrichtendienstlichen Erkenntnissen“ erlauben.

An den Projekten können je nach Bedarf die gleichen Behörden beteiligt werden, die auch auf die Anti-Terror-Datei Zugriff haben: Polizeien des Bundes und der Länder, ZKA und sämtliche Geheimdienste. Eine derartige Zusammenarbeit an einem Themenkomplex gibt es schon seit einigen Jahren. Die Begründung nennt zwei Beispiele: ein Projekt zu „Netzwerken arabischer Mudjahedin“ – ab 2001 geführt beim BKA – und ein Nachfolgeprojekt „Ausbildungslager arabischer Mudjahedin“ beim BfV. Die bisherige Rechtslage (z.B. § 6 BVerfSchG) habe dazu gezwungen, Informationen, die allen Projektmitarbeiterinnen und -mitarbeitern bereits zur Verfügung stehen oder übermittelt werden dürfen, jeweils getrennt in mehrere inhaltlich gleiche Dateien (einzugeben) oder regelmäßig auf Datenträgern wie CD-ROMs an die übrigen teilnehmenden Behörden“ zu übermitteln. Die gemeinsamen Projektdateien, so lautet die Botschaft, seien nur eine kleine Arbeitserleichterung.

In der Tat begann der Sündenfall nicht erst mit dem technischen Mittel. Wo Personen aus verschiedenen Behörden in einer Arbeitsgruppe am gleichen Thema und mit denselben Informationen arbeiten, haben Bestimmungen, die für die Übermittlung einzelner Informationen ge-

dacht waren, ihren Sinn verloren. Die neue Regelung ermöglicht denn auch nicht nur die gemeinsamen Dateien, sondern legalisiert gleichzeitig die projektmäßige Zusammenarbeit als solche. Sie tut das in der üblichen Art, nämlich ohne wirkliche Grenzen zu setzen.

Der Inhalt der Projektdateien und damit auch der Gegenstand der Projekte ist nur durch bestimmte Aufgabenbereiche der Geheimdienste bzw. des BKA vage angedeutet. So fordert der neue § 22a BVerfSchG nur, dass die „projektbezogene Zusammenarbeit" sich beziehen soll auf die in § 3 Abs. 1 Nr. 1-4 BVerfSchG genannten „Schutzgüter" – von der freiheitlichen demokratischen Grundordnung über die „auswärtigen Belange der Bundesrepublik Deutschland" bis hin zum „Gedanken der Völkerverständigung", den das Terrorismusbekämpfungsgesetz von Januar 2002 in die Aufgabennorm des Verfassungsschutzes einfügte. Die einzige Einschränkung besteht darin, dass die aufzuklärenden „Bestrebungen" diese Schutzgüter „durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen" gefährden sollen.

Im neuen § 9a BKA-Gesetz begnügte sich der Gesetzgeber mit dem Hinweis, dass „polizeiliche oder nachrichtendienstliche Erkenntnisse zu Straftaten" aus einem Deliktkatalog auszuwerten seien (geheimdienstliche Agententätigkeit – § 99 StGB, terroristische Vereinigungen – §§ 129a und b StGB, „bedeutsame" Straftaten des Außenwirtschaftsgesetzes sowie damit jeweils „unmittelbar" zusammenhängende Delikte). Auf eine Unterscheidung zwischen Verdächtigen, möglichen Verdächtigen, Kontaktpersonen, ZeugInnen etc. wurde verzichtet. In der Begründung heißt es denn auch nur, dass in Projektdateien „umfassende Informationen zu relevanten Personen" ausgewertet und „verdichtet" werden sollen. Bei einer maximalen Projektdauer von vier Jahren (zwei Jahre plus zwei Verlängerungen um jeweils ein Jahr) bedeutet dies, dass der Geruch des Terrorismus ebenso lang an den Betroffenen kleben bleibt.

Um die Folgen dieser intensiven Zusammenarbeit hat sich der Gesetzgeber nicht geschert. Wie sollen gegebenenfalls geheimdienstliche Daten in Strafverfahren eingeführt werden? Wer steht dafür gerade, wer sagt aus? Welche Akten werden dem Gericht und der Verteidigung offengelegt, welche gesperrt? Was ist, wenn die Erkenntnisse von befreundeten Diensten kommen, die sie per Folter in Guantánamo oder in einem anderen geheimen Gefängnis an irgendeinem Ort der Welt erpresst haben? Nach der Umwandlung des bis zur Unkenntlichkeit verwaschenen Trennungsgebots in eines der arbeitsteiligen Kooperation droht die geheimdienstliche Verseuchung des Strafprozesses.

… was nicht zusammen gehört

Polizei und Geheimdienste kooperieren gegen Ausländer

von Mark Holzberger

Bei der Bekämpfung der unerlaubten Einwanderung bzw. „terrorverdächtiger" AusländerInnen arbeiten deutsche Polizeibehörden und Geheimdienste inzwischen eng zusammen.

Den ersten Schritt in diese Richtung unternahm das Bayerische Staatsministerium des Inneren (StMI), als es im Herbst 2004 die Arbeitsgruppe BIRGiT ins Leben rief.[1] BIRGiT steht für „beschleunigte Identifizierung und Rückführung von Gefährdern aus dem Bereich des islamistischen Terrorismus/Extremismus". Die Arbeitsgruppe trifft sich etwa alle zwei Wochen. Neben dem StMI gehören ihr zunächst die Ausländerbehörden der Städte München und Nürnberg sowie der Bezirksregierungen Oberbayern und Mittelfranken an. Bei denen hatte das StMI im Juli 2005 eigens die Zuständigkeiten für Ausweisungsverfügungen und Überwachungsmaßnahmen (§ 54a Aufenthaltsgesetz, AufenthG) konzentriert.[2] Weil „die meisten Gefährderfälle einen Asylbezug haben", ist auch das Bundesamt für Migration und Flüchtlinge (BAMF) beteiligt.[3] Mit von der Partie sind ferner VertreterInnen des Landeskriminalamts (LKA) und des Landesamts für Verfassungsschutz (LfV). Anlassbezogen werden auch die Landesanwaltschaft sowie andere bayerische Behörden und Kommunen hinzugezogen.

Hauptziel der AG BIRGiT ist es, sog. Gefährder unter Ausschöpfung aller rechtlichen Möglichkeiten zur Ausreise aus Deutschland zu bewegen. Wenn eine Ausreise rechtlich (noch) nicht möglich sein sollte, so

1 s.a. Bürgerrechte & Polizei/CILIP 81 (2/2005), S. 86

2 s. die Stellungnahme von Kempfler, K. (StMI) in: Bundesministerium des Innern: Bericht zur Evaluierung des Zuwanderungsgesetzes, Berlin Juli 2006, Anlagenband I, S. 60-63

3 Buggisch, W.; Knorz, W.: Terrorismusbekämpfung einmal anders – Die AG BIRGiT und das Ausländerrecht, in: Kriminalistik 2006, H. 4, S. 226-233 (231)

will die Arbeitsgruppe den Handlungsspielraum der betroffenen Person so weit wie möglich einschränken.

Sie kann sich dabei auf die verschärften Ausweisungs- und Überwachungsmöglichkeiten stützen, die mit dem Terrorismusbekämpfungsgesetz (2002) und dem Zuwanderungsgesetz (2005) eingeführt wurden:

- Gemäß § 54 Nr. 5 AufenthG werden AusländerInnen „in der Regel" ausgewiesen, wenn „Tatsachen die Schlussfolgerung rechtfertigen", dass sie einer terroristischen bzw. extremistischen Vereinigung angehören oder sie unterstützen. Ein strafrechtlicher Nachweis ist nicht erforderlich, Geheimdienstinformationen sind hingegen unmittelbar nutzbar.
- § 54 Nr. 6 AufenthG sieht eine „Regelausweisung" auch vor, wenn AusländerInnen bei einer sog. sicherheitsrechtlichen Befragung unvollständige Angaben machen.
- Aufgrund eines Vorschlags, den Bayern in die Verhandlungen um das Zuwanderungsgesetz eingespeist hatte, können schließlich nach § 54a AufenthG AusländerInnen, die zwar des Terrorismus/Extremismus verdächtigt werden, bei denen aber (menschen)rechtliche Abschiebehindernissen bestehen, mit Aufenthaltsbeschränkungen belegt oder Überwachungsmaßnahmen unterworfen werden.[4]

Die AG BIRGiT geht folgendermaßen vor: In einer Vorbereitungsphase werden mögliche „Gefährder" identifiziert und deren angebliches Gefährdungspotential analysiert. Dabei gilt das „Mündlichkeitsprinzip". In einer Fallbesprechung tauschen die beteiligten Behörden die Erkenntnisse aus und entscheiden, ob die Arbeitsgruppe den Fall behandeln soll. Wenn ja, wird aus den Informationen von LKA und LfV eine schriftliche „Erkenntnismitteilung" gefertigt, auf deren Grundlage die zuständige Ausländerbehörde dann eine Ausweisung verfügen soll. Wenn möglich, koordiniert die AG BIRGiT deren Sofortvollzug. Wenn Abschiebungshindernisse bestehen, stimmen die Behörden in der Arbeitsgruppe Aufenthaltsbeschränkungen und Überwachungsmaßnahmen ab. In regelmäßigen Abständen überprüft die AG die einzelnen Vorgänge und steuert gegebenenfalls nach.

---

4 zum Beispiel: Verpflichtung zum Umzug in einen anderen (ggf. weit entfernten) Bezirk und Beschränkung des Aufenthaltes auf diese Gemeinde; verschärfte Meldeauflagen; Verpflichtung, in einer (von der Polizei leicht zu kontrollierenden) Gemeinschaftsunterkunft zu wohnen; Beschränkung der Nutzung bestimmter Kommunikationsmittel

Das StMI ist hoch zufrieden: Bis März 2006 hat die AG BIRGiT über 60 Fälle bearbeitet und 48 Ausweisungsbescheide produziert. In 28 Fällen wurden die Betroffenen abgeschoben, in 14 Fällen Maßnahmen nach § 54a AufenthG angeordnet. Mit diesen Aufenthaltsbeschränkungen und Überwachungsmaßnahmen habe man in Bayern „positive Erfahrungen" gemacht. Der auf die Betroffenen ausgeübte Druck befördere deren Motivation zur „freiwilligen" Ausreise „ganz erheblich".[5]

Das enge und vernetzte Zusammenwirken der beteiligten Behörden habe sich bewährt: MitarbeiterInnen verschiedener Behörden an einen Tisch zu setzen, führe zu einer erheblichen Verfahrensbeschleunigung, zur Minimierung von Koordinationsproblemen und Informationsverlusten und damit letztlich zur Qualitätssteigerung der aufenthaltsrechtlichen Entscheidungen. Vor diesem Hintergrund preist Bayern seine Arbeitsgruppe als Modell für die gesamte Republik an.

AG Status

Der Ruf aus München wurde in Berlin erhört: Im Juni 2005 richtete das Bundesinnenministerium (BMI) im Gemeinsamen Terrorismusabwehrzentrum (GTAZ) eine Arbeitsgruppe „Statusrechtliche Begleitmaßnahmen" (AG Status) ein.[6] Ständig vertreten sind darin neben dem federführenden BAMF (mit mindestens drei MitarbeiterInnen), das Bundesamt für Verfassungsschutz (BfV) und das Bundeskriminalamt (BKA; mit jeweils mindestens zwei Personen). Anlassbezogen werden die Bundespolizei, die Bundesanwaltschaft, Landeskriminalämter und Landesämter für Verfassungsschutz sowie diverse Ausländerbehörden beteiligt. Bis März 2006 hatte die Gruppe ca. 80 Fälle bearbeitet.

- In 20 Fällen leitete das BAMF auf Empfehlung der AG ein Verfahren zum Widerruf bzw. zur Rücknahme einer Asyl-/Flüchtlingsanerkennung ein. Derzeit sind aber nur fünf dieser Widerrufe bestandskräftig. Nach Angaben der Bundesregierung wurde bisher keine der betroffenen Personen abgeschoben.[7]

---

5 Kempfler a.a.O. (Fn. 2), S. 62

6 Antwort auf eine Kleine Anfrage von Bündnis 90/Die Grünen, BT-Drs. 16/3429 v. 16.11.2006

7 Betroffen waren hiervon Staatsangehörige aus: Algerien (8), Irak (6), Ägypten (2), Jordanien, Libyen und Tunesien (jeweils 1) sowie ein staatenloser Palästinenser. Die Betroffenen erhielten eine Duldung.

- In 17 Fällen empfahl die Arbeitsgruppe Maßnahmen zur Aufenthaltsbeendigung. In weiteren 32 Fällen seien laut BMI-Auskunft die zuständigen Ausländerbehörden von sich aus aktiv geworden und hätten Ausweisungsverfügungen verhängt.
- Überwachungsmaßnahmen nach § 54a AufenthG hat die AG Status nur einmal empfohlen.
- In 11 Fällen initiierte sie eine Ausschreibung im Schengener Informationssystem zur Verhinderung der (Wieder-)Einreise.
- Maßnahmen zur Verhinderung oder Rücknahme einer Einbürgerung hat die AG Status bisher noch nicht angeregt.

In drei Bundesländern bestehen mittlerweile ähnliche Gremien: in Hamburg die Anti-Terrorismuskoordinierungsgruppe, in Rheinland-Pfalz die Arbeitsgruppe zur Rückführung ausländischer Gefährder und in Nordrhein-Westfalen die sog. Sicherheitskonferenz. Unklar ist, ob Geheimdienste – konkret: das jeweilige LfV – unmittelbar beteiligt sind.[8]

Irreguläre Migration, Terrorismus und die Geheimdienste

Auf EU-Ebene werden derzeit grenzpolizeiliche und nachrichtendienstliche Aktivitäten miteinander verschmolzen: Die europäische Grenzschutzagentur FRONTEX soll nicht nur Informationen nationaler Geheimdienste verarbeiten. Bei ihr findet auch eine – geheimdienstlich untersetzte – Verknüpfung von Grenzschutz und Terrorismusbekämpfung statt.[9]

Unter den deutschen Diensten befasst sich insbesondere der BND seit längerem mit Fragen der unerlaubten Zuwanderung – wenn auch mit teilweise veränderten Bewertungen. Auf einem Symposium 1999 sah der BND in der „illegalen Migration" ein „globales Phänomen, das die innere Stabilität zahlreicher Länder bedroht. Die Perspektiven sind ungünstiger denn je."[10] Zwei Jahre später erschien ihm die unerlaubte Zuwanderung vor allem als potentielle Bedrohung für Wohlstand, soziale

8 Am 1. Juni 2006 hat das BMI der Innenministerkonferenz übrigens die bislang unveröffentlichte Best-Practice-Analyse einer gemeinsamen Projektgruppe zur Zusammenarbeit von Sicherheits- und Ausländerbehörden vorgelegt.

9 vgl. Holzberger, M.: Europols kleine Schwester – Die Europäische Grenzschutzagentur Frontex, in: Bürgerrechte & Polizei/CILIP 84 (2/2006), S. 59-65

10 zit n. Kleine Anfrage der PDS-Fraktion, BT-Drs. 14/2054 v. 10.11.1999, vgl. auch BND (Hg.): Illegale Migration, Bonn 2000

Stabilität und die außenpolitische Handlungsfähigkeit.[11] Heute wiederum verkündet August Hanning, bis 2005 BND-Präsident und jetzt Staatssekretär im BMI: Irreguläre Migration sei „eine der gegenwärtig größten Herausforderungen für unsere Gesellschaft".[12]

Hannings Nachfolger beim BND, Ernst Uhrlau, hält die „Implikationen zwischen Terrorismus und der illegalen Migration" für „deutlich geringer als gemeinhin vermutet."[13] Insbesondere sieht er „keine erkennbare und zwingende Kausalität zwischen illegaler Migration und islamistisch motiviertem Terrorismus. Es handelt sich um prinzipiell verschiedene Phänomene." Allerdings gäbe es eine „relativ kleine, aber gefährliche Schnittmenge" in Form einer „gewissen Konvergenz beim Aufbau und der Vorgehensweise". Zudem hätten sich gegenseitige Geschäftskontakte (z.B. in der Fälschungsbranche) ergeben. Insofern könnte für den BND z.B. in der „gezielten Ausschaltung einschlägiger Dokumentenfälscher ein interessanter Ansatz zur Bekämpfung des Internationalen Terrorismus und der illegalen Migration liegen".

GASIM

Im Mai 2006 hat das BMI nun das „Gemeinsame Analyse- und Strategiezentrum illegale Migration" (GASIM) eingerichtet. GASIM ersetzte damit das „Gemeinsame Analyse- und Strategiezentrum Schleusungskriminalität" (GASS), das erst im November 2004 unter gemeinsamer Regie des BKA und des damaligen Bundesgrenzschutzes (BGS) seine Arbeit aufgenommen hatte. Das GASS sollte zwar Erkenntnisse von BKA und BGS mit denen des BND und des BfV „verknüpfen".[14] Eine feste Einbindung der Geheimdienste gab es jedoch noch nicht. Diese wurde erst mit der Einrichtung des neuen Zentrums realisiert. Bei GASIM arbeiten derzeit 33 BeamtInnen des BKA, der Bundespolizei, des BAMF, der Zollverwaltungen (Finanzkontrolle Schwarzarbeit), des BND und des BfV ohne Umwege zusammen.

---

11 vgl. Der Spiegel v. 30.4.2001

12 BMI-Pressemitteilung v. 17.7.2006

13 Rede des BND-Präsidenten Ernst Uhrlau auf der BKA-Herbsttagung am 15. November 2006, www.bka.de/kriminalwissenschaften/herbsttagung/2006/langfassung_uhrlau.pdf

14 so Ex-Innenminister Otto Schily am 15.7.2005 vor dem Visa-Untersuchungsausschuss, www.bmi.bund.de/cln_028/nn_210460/Internet/Content/Nachrichten/Archiv/Reden/2005/07/Schily_Eingangsstatement_Untersuchungsausschuss.html

In einer Presseerklärung vom 17. Juli 2006 erklärte das BMI, Ziel von GASIM sei es, der unerlaubten Zuwanderung im Rahmen einer „institutionalisierten, behördenübergreifenden Informations-, Koordinations- und Kooperationsplattform“ mit „operativ und mit strategisch ausgerichteten und konzeptionell fundierten Maßnahmen wirksam entgegenzutreten.“

Auf Nachfrage der Linksfraktion bestritt das BMI nur einen Monat später, dass das GASIM operative Maßnahmen tatsächlich durchführen würde.[15] Worin denn nun genau der operative Beitrag des Zentrums besteht, ließ das BMI offen. Gleiches gilt für die „anlass- und aufgabenbezogene Kooperation“ von GASIM und GTAZ, die das Ministerium vorher bestätigt hatte. Auch die Erklärung, „im GASIM als solchem werden keine Daten gespeichert“, ist zumindest fragwürdig: Denn die beteiligten Behörden führen in diesem Zentrum ihre jeweiligen Erkenntnisse zum Komplex der irregulären Migration zusammen und generieren dadurch teilweise ganz neue Daten bzw. ganze Analysedateien. Für die analoge „projektmäßige Zusammenarbeit“ und eigenständigen Projektdateien des GTAZ hat der Bundestag mit dem „Gemeinsame-Dateien-Gesetz“ am 1. Dezember 2006 eine Rechtsgrundlage geschaffen.[16] Warum das BMI eine solche Rechtsgrundlage für GASIM nicht für erforderlich hält, bleibt sein Geheimnis.

Kontrollfreier Raum

Es ist schon erstaunlich, mit welcher Kreativität unter – wenn auch nur mehr formaler – Aufrechterhaltung des Trennungsgebotes auf Dauer angelegte Formen der Zusammenarbeit von Polizei und Geheimdiensten institutionalisiert werden. Mit den neuen Instrumenten des Ausländerrechts wird diese Zusammenarbeit umso gefährlicher, als hier die korrigierende Funktion des Strafprozessrechts und der Verteidigung nicht mehr gegeben ist. Worin der konkrete Beitrag der Dienste zur Arbeit dieser Gremien besteht, wird man vorerst nicht erfahren. Denn eines ist klar: Die demokratische bzw. parlamentarische Kontrolle endet faktisch dort, wo die Geheimdienste auf den Plan treten.

---

15 Antwort der Bundesregierung auf die Kleine Anfrage der Linksfraktion, BT-Drs. 16/2420 v.16.8.2006

16 siehe den Beitrag von H. Busch in diesem Heft, S. 52-59

Geheimdienstrechtsergänzungsgesetz

Terrrorismusbekämpfung als Universallegitimation

von Heiner Busch

Die Geheimdienste dürfen weiterhin Auskünfte von Banken, Fluggesellschaften und Telekommunikationsfirmen verlangen. Am 1. Dezember 2006 verlängerte und erweiterte der Bundestag die Befugnisse, die er den Diensten vor fünf Jahren eingeräumt hatte.

Das jetzt beschlossene „Terrorismusbekämpfungsergänzungsgesetz" (TBEG) ist der deutliche Beweis dafür, dass die Befristung von Sicherheitsgesetzen eine Farce ist. Ende Dezember 2001 hatte das damals von Otto Schily geführte Bundesinnenministerium (BMI) das „Gesetz zur Bekämpfung des internationalen Terrorismus" über die parlamentarischen Hürden gepeitscht.[1] Als Zückerchen für den kleinen grünen Koalitionspartner hatte man die darin enthaltenen neuen Befugnisse der Geheimdienste auf fünf Jahre befristet. Vor Ablauf der Frist sollten sie „evaluiert" werden.

Spätestens der im Mai 2005 – noch unter Rot-grün – vorgelegte Evaluationsbericht[2] musste selbst Gutgläubigen klar machen, dass ein Auslaufen der Befugnisse zu keinem Zeitpunkt ernsthaft zur Debatte gestanden hatte. Seine Standardsätze, die in Variationen immer wieder auftauchten, lauteten: „Die Befugnis hat aufgabendienliche Erkenntnisse erbracht, ohne dass damit unangemessen breite Überwachungsfolgen verbunden wären. Sie sollte beibehalten werden." Der Bericht zeigte vor allem, dass die neuen Befugnisse für die Geheimdienste einigermaßen praktikabel waren. Die angefragten Banken, Telekommunikations- (TK-) oder Fluggesellschaften hatten die Auskunft nicht verweigert, obwohl sie das hätten tun können. Die Informationen waren den Geheimdiens-

1 Bundesgesetzblatt I, Nr. 3 v. 11.1.2002, S. 361-395

2 abrufbar unter www.cilip.de/terror/eval_tbg_11052005.pdf

ten nützlich und erleichterten ihnen die Identifikation von Personen und dem BMI das Verbot von Organisationen. Dass dadurch terroristische Anschläge verhindert wurden, mussten die LeserInnen glauben – oder eben nicht.

Sicher: die Geheimdienste haben das Mittel des Auskunftsersuchens über TK-Verbindungsdaten nicht annähernd so oft genutzt wie die Polizei. Auf die Überlegung, dass eine so selten in Anspruch genommene Befugnis vielleicht nicht notwendig sei, hatten sich die VerfasserInnen des Berichts erst gar nicht eingelassen.

Schnellere Verfahren

Das TBEG, dessen Entwurf Bundesinnenminister Wolfgang Schäuble just auf der Pressekonferenz zum Ende der Fußballweltmeisterschaft präsentierte, könnte die bisher vergleichsweise niedrige Zahl geheimdienstlicher Auskunftsersuchen schnell erhöhen. Aus den „Evaluationsergebnissen" zog das BMI nämlich die Konsequenz, dass das „für eine solche Anfrage sehr aufwändige Verfahren ... zu einer erheblichen Verfahrensdauer und eingeschränkter Praktikabilität" geführt habe. „Diese Mängel könnten durch differenzierte Verfahrensregelungen behoben werden, die für weniger schwerwiegende Eingriffe einen geringeren Verfahrensaufwand vorsehen."[3]

Diese „Differenzierung" findet sich nun im neuen § 8a des Bundesverfassungsschutzgesetzes (BVerfSchG). Bisher galt für alle Auskunftsersuchen des Verfassungsschutzes das gleiche Verfahren, nämlich jenes, das in § 15 Abs. 5 des G 10-Gesetzes für die geheimdienstliche TK-Überwachung vorgeschrieben ist: Der Präsident des Bundesamtes für Verfassungsschutz (BfV) oder sein Stellvertreter stellt den Antrag. Das „vom Bundeskanzler beauftragte Bundesministerium" ordnet an. Die G 10-Kommission wird monatlich über die Auskunftsersuchen unterrichtet und prüft deren Zulässigkeit – im Normalfall vor dem Vollzug, in dringlichen Fällen hinterher. Bei einem nachträglichen Nein der Kommission sind die Maßnahmen sofort zu stoppen, für die bereits erhaltenen Informationen gilt ein absolutes Nutzungsverbot. Das Parlamentarische Kontrollgremium für die Geheimdienste (PKGr) wird halbjährlich informiert und legt selbst einen jährlichen Bericht vor.

3 BMI: Fakten zur Evaluierung des Terrorismusbekämpfungsgesetzes, v. 11.5.2006, S. 6, abrufbar unter www.cilip.de/terror/eval_tbg_11052005_kurz.pdf

Die „differenzierten Verfahrensregeln“ des neuen § 8a BVerfSchG sehen nun Folgendes vor:

- Für Auskünfte über „Bestandsdaten“ von Post- und Telediensten (Telebanking; Internet-Zugang mit Ausnahme der privaten TK wie z.B. E-Mail etc.) gibt es neu keine besonderen Verfahrensregeln und keine besonderen Voraussetzungen (§ 8a Abs. 1). Das BfV – und nicht etwa nur sein Chef – darf die Informationen immer einholen, „soweit dies zur Erfüllung seiner Aufgaben erforderlich ist“. „Bestandsdaten“ beziehen sich auf die „Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses“ über Post- oder Teledienstleistungen. Darunter fallen Informationen darüber, ob eine Person ein Postfach hat, ob sie ihre Bankgeschäfte per Internet abwickelt oder einen „Verkaufsraum“ bei Ebay eingerichtet hat etc.
- Das Verfahren für Auskünfte bei Luftfahrtunternehmen hat der Gesetzgeber erst gar nicht festgelegt (§ 8a Abs. 2 S. 1 Nr. 1). Es soll in einer Dienstvorschrift mit Zustimmung des BMI geregelt werden. Erfragen kann das BfV hier Namen und Anschriften von KundInnen sowie Daten zur „Inanspruchnahme und den Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg“. Laut Begründung könnte das BfV auch ganze Passagierlisten verlangen, sofern „tatsächliche Anhaltspunkte“ vorlägen, dass z.B. ein namentlich noch nicht identifizierter Terrorist unter den Fluggästen sei.
- Anträge auf Konto-Anfragen (über InhaberInnen, Zeichnungsberechtigte, Kontostand, Aus- und Eingänge sowie deren Empfänger oder Sender) bei Banken, Kredit- und Finanzunternehmen (§ 8a Abs. 2 S. 1 Nr. 2) können nun nicht mehr nur der Präsident und der Vizepräsident des BfV stellen, sondern auch MitarbeiterInnen, die die Befähigung zum Richteramt haben. Die Anordnung trifft das Ministerium. Die G 10-Kommission hat hier nichts mehr zu sagen.
- Das bisherige G 10-Verfahren bleibt nur für Auskünfte über die „Umstände des Postverkehrs“, die Nutzungsdaten von Telediensten und die TK-Verkehrsdaten erhalten (§ 8a Abs. 2 S. 1 Nr. 3-5). Von solchen Anfragen können auch Dritte betroffen sein, sofern die eigentliche Zielperson ihren Anschluss benutzt oder sie Nachrichten oder Post für sie entgegennehmen. In den TK-Verkehrsdaten sind auch die Standortdaten von Mobiltelefonen eingeschlossen. Mit der unscheinbaren Formulierung „sonstige zum Aufbau und zur Auf-

rechterhaltung der Telekommunikation notwendigen Verkehrsdaten“ erfasst das Gesetz auch gleich sogenannte „stand-by-Daten“, durch die ein Handy auch dann geortet werden kann, wenn seinE BesitzerIn nicht telefoniert, und durch die auch Methoden wie die „stille SMS“ möglich werden. Die Erfassung dieser Daten habe man bereits 2001 intendiert, heißt es in der Begründung des Gesetzentwurfs. Generell werden die Geheimdienste auch von der EU-Richtlinie zur Vorratsdatenspeicherung und deren anstehender Umsetzung profitieren.[4] Hier wird bereits im nächsten Jahr mit einer „Anpassung“ auch der Geheimdienstbefugnisse an die neuen TK-rechtlichen Bedingungen zu rechnen sein.

Erhalten bleiben die Berichtspflichten an das und des PKGr.

Geringere Voraussetzungen

Damit aber nicht genug der „Differenzierung“. Mit dem TBEG senkt der Gesetzgeber auch die Voraussetzungen für Auskunftsersuchen ab – und das nicht nur für die Bestandsdaten von Post- und Telediensten in § 8a Abs. 1, die der Verfassungsschutz – siehe oben – in Zukunft für jede x-beliebige seiner ohnehin rechtlich kaum zu begrenzenden Aufgabenstellungen erfragen darf.

Der Zugriff auf Post-, Teledienst- und TK-Verkehrsdaten – so erklären die GesetzesmacherInnen in der Begründung – sei ein weit geringerer Eingriff als die Überwachung von kommunizierten Inhalten, für die das G 10-Gesetz eigentlich gedacht sei. Der Gesetzgeber streicht daher erstens den in der alten Regelung zu diesen Daten enthaltenen Verweis auf § 3 Abs. 1 des G 10-Gesetzes. In diesem Paragrafen findet sich ein langer Straftatenkatalog, der von den traditionellen politischen Delikten (Hochverrat etc.) bis hin zur terroristischen Vereinigung reicht. Gefordert werden „tatsächliche Anhaltspunkte für den Verdacht“, dass „jemand“ solche Straftaten „plant, begeht oder begangen hat.“ Mit der Streichung des Verweises auf § 3 Abs. 1 des G 10-Gesetzes entfällt bei der Verkehrsdaten-Auskunft selbst dieser nur sehr vage Bezug zum Strafrecht.

Für alle im neuen § 8a Abs. 2 genannten Informationen – von den Daten über Flugpassagiere und Kontenbewegungen bis hin zu den Ver-

4 siehe dazu den Artikel von Mark A. Zöller in diesem Heft, S. 21-30

kehrs- bzw. Nutzungsdaten von Post-, Tele- und TK-Diensten – erweitert das TBEG zweitens die Aufgaben, zu deren Erfüllung der Verfassungsschutz Auskünfte einholen kann. Nach der bisherigen Regelung war dies möglich zu Zwecken der Spionageabwehr (§ 3 Abs. 1 Nr. 2 BVerfSchG) sowie für die Aufklärung von „Ausländerextremismus“ (Nr. 3) und von Bestrebungen gegen den „Gedanken der Völkerverständigung“ (Nr. 4). Die neue Version bezieht nun auch die Beobachtung des (Inländer-)„Extremismus“ (§ 3 Abs. 1 Nr. 1) mit ein, soweit es dabei um „volksverhetzende“ oder „militante“ Bestrebungen geht. Im Gesetzestext liest sich diese Einschränkung folgendermaßen:

> „Im Falle des § 3 Abs. 1 Nr. 1 gilt dies nur für Bestrebungen, die bezwecken oder aufgrund ihrer Wirkungsweise geeignet sind,
> 1. zu Hass oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumden anzugreifen und dadurch die Bereitschaft zur Anwendung von Gewalt zu fördern und den öffentlichen Frieden zu stören oder
> 2. Gewalt anzuwenden oder vorzubereiten, einschließlich dem Befürworten, Hervorrufen oder Unterstützen von Gewaltanwendung, aber auch durch Unterstützung von Vereinigungen, die Anschläge gegen Personen veranlassen, befürworten oder androhen.“

Die „Menschenwürde“ von „Teilen der Bevölkerung“? „Bestrebungen, die ... aufgrund ihrer Wirkungsweise geeignet sind, ... Gewalt ... vorzubereiten“? Einzeln gelesen zeigen die verschiedenen Alternativen dieses Satzes, welch bunte sprachliche Blüten gesetzgeberisches Schaffen hervorbringen kann.

Von Normenklarheit ist man hier weit entfernt und man kommt ihr auch nicht näher, wenn man sich stattdessen mit den Formeln „volksverhetzend“ und „militant“ begnügt. Dies illustriert die Begründung mit Beispielen wie der „international organisierten rechtsextremistischen Vertriebsszene für Hasspropaganda“, mit „militanten Rechtsextremisten“, „rechtsterroristischen Gruppierungen“, dem „Islamismus bzw. islamistischen Terrorismus“ sowie „Hasspredigern“.

Wer die Verfassungsschutzberichte oder andere Publikationen des BfV liest, weiß jedoch, dass das Amt durchaus auch linke Organisationen und Bewegungen als „militant“ einstuft: „Militante Autonome – Einig im Hass“, heißt es etwa in einem Faltblatt, mit dem das BfV der Öffentlichkeit seine Leistungen bei der Bekämpfung des „Linksextre-

mismus“ anpreist.[5] Zu KandidatInnen für die angeblich geringen Grundrechtseingriffe, die mit verfassungsschützerischen Auskunftsanfragen verbunden sind, werden vor diesem Hintergrund beispielsweise auch jene Personen und Organisationen, die die Proteste gegen den G8-Gipfel im Juni 2007 in Heiligendamm organisieren.

Mehr Befugnisse für alle Dienste

„Infolge der Erstreckung der Auskunftsregelungen auch auf die Aufgaben nach § 3 Abs. 1 Nr. 1 BVerfSchG sowie der teilweisen Absenkung der Anordnungsvoraussetzungen ist mit einer Erhöhung der Auskunftsfallzahl zu rechnen“, erklärt die Bundesregierung in der Begründung zum Entwurf. Ob diese Zunahme sich tatsächlich „innerhalb der bisherigen Größenordnung halten wird“, bleibt abzuwarten. Sicher ist dagegen, dass das „Terrorismusbekämpfungsergänzungsgesetz“ noch weiter von seinem Titel entfernt ist, als dies bei seinem Vorläufer von Ende 2001 der Fall war.

Dass es sich hier um ein allgemeines Gesetz zur Ergänzung von Geheimdienstbefugnissen handelt, zeigt sich auch daran, dass die Regelungen des § 8a BVerfSchG schlicht und einfach auf den Bundesnachrichtendienst (BND) und den Militärischen Abschirmdienst (MAD) übertragen werden. Bisher konnte der MAD nur Auskünfte zu TK-Verkehrsdaten einholen. Dem BND war es zusätzlich erlaubt, Daten über Kontenbewegungen nachzufragen.

Gleiches Recht für alle drei Geheimdienste des Bundes lässt das TBEG auch bei zwei anderen Befugnissen gelten: BfV, MAD und BND dürfen nun „zur Erfüllung ihrer durch Gesetz übertragenen Aufgaben“ – also ohne Einschränkung – Fahrzeug- und Halterdaten online aus dem Zentralen Verkehrsinformationssystem des Kraftfahrtbundesamtes abfragen. Ferner erlaubt ihnen das Gesetz, Personen und Fahrzeuge zur Beobachtung im Schengener Informationssystem (SIS) auszuschreiben. Die Möglichkeit, den Bundesgrenzschutz bzw. die heutige Bundespolizei mit einer solchen gezielten, aber verdeckten Kontrolle an den deutschen Grenzen zu beauftragen, war bereits bei der Neufassung des Geheimdienstrechts 1990 gesetzlich verankert worden (§ 17 Abs. 2 BVerfSchG). Zuvor wurde sie auf der Basis von Sonderanweisungen des BMI prakti-

5 BfV: Verfassungsschutz gegen Linksextremismus, Köln o.J., S. 6, auch auf der Homepage des Amtes abrufbar: www.verfassungsschutz.de/de/publikationen/linksextremismus/

ziert. Die Aufhebung der Kontrollen an den Schengener Binnengrenzen habe der Grenzfahndung ihre Bedeutung genommen. Das gelte es jetzt zu kompensieren, lautet die Begründung, nachdem elf Jahre seit dem Inkrafttreten des Schengener Durchführungsübereinkommens und dem Abbau der Schlagbäume vergangen sind.

Kohle zum Nachlegen

Nicht im Gesetz enthalten ist die Befugnis der Geheimdienste zur Auskunft über die bei der Bundesanstalt für die Finanzdienstleistungsaufsicht gespeicherten Kontostammdaten, über deren Einführung sich schon die Parteien der rot-grünen Regierungskoalition einig waren.[6] Diese Daten geben „nur" Aufschluss darüber, wer wo ein Konto hat. Der grüne Innenpolitiker Volker Beck meinte seinerzeit, dieser Eingriff sei verglichen mit der seit 2002 möglichen Abfrage sämtlicher Kontenbewegungen bei den Banken der geringere. Allerdings macht der angeblich so kleine Grundrechtseingriff den größeren erheblich einfacher. Die Anfrage bei der Bundesanstalt erspart die Suche nach der zuständigen Bank, an die die Anfrage über die Kontenbewegungen zu richten wäre. Diese Zeit- und Arbeitsersparnis dürfte die Zahl der Auskunftsanfragen (29 Anfragen in den Jahren 2002-2004) erheblich steigen lassen.

Der neuen Koalition mangelte es nicht am Willen. Sie wartet vielmehr auf ein Urteil des Bundesverfassungsgerichts. Das hat zwar bereits einen Eilantrag gegen das „Gesetz zur Förderung der Steuerehrlichkeit" abgelehnt und damit Finanzämtern, Sozialbehörden und Gerichten ab dem 1. April 2005 vorläufig den Zugriff auf Kontostammdaten erlaubt.[7] Die Entscheidung in der Hauptsache steht jedoch noch aus. Sobald die ergeht, will die Bundesregierung gemäß ihrer Begründung zum TBEG-Entwurf „unverzüglich" entsprechende geheimdienstliche Befugnisse nachschieben und das Terrorismusbekämpfungsgesetz erneut ergänzen.

Keinen Bedarf sieht sie demgegenüber für eine Regelung, mit der die angefragten Banken, Fluggesellschaften oder TK-Unternehmen zu einer Auskunft an die Geheimdienste verpflichtet würden. Bisher haben die brav geantwortet und die Rechte ihrer KundInnen ignoriert. Ob das so bliebe, wenn in Zukunft die Zahl der Anfragen ansteigen würde, ist jedoch fraglich – und zwar nicht wegen der Betroffenen, die von der Wei-

6 Frankfurter Rundschau v. 28.4.2005

7 Beschluss v. 22.3.2005, Az.: 1 BvR 2357/04 und 1 BvQ 2/05

tergabe ihrer Daten nichts erfahren (dürfen), sondern wegen des wachsenden Aufwandes, der mit einer Zunahme der Anfragen verbunden ist. Eine verpflichtende Regelung stößt aber auf Schwierigkeiten: Sie würde voraussetzen, dass die formalen Reste des Gebots der Trennung und Unterscheidung von Polizei und Geheimdiensten hinsichtlich ihrer Aufgaben und Befugnisse beseitigt würden. § 8 Abs. 3 BVerfSchG schreibt immer noch vor: „Polizeiliche Befugnisse und Weisungsbefugnisse stehen dem Bundesamt für Verfassungsschutz nicht zu." Eine entsprechende Formulierung findet sich in allen Landesverfassungsschutzgesetzen sowie im BND- und im MAD-Gesetz. Auch wenn das Trennungsgebot faktisch zur Makulatur geworden ist, Polizei und Geheimdienste längst in institutionalisierten Formen zusammenarbeiten und beide Seiten arbeitsteilig das „Vorfeld" beackern, brauchen die SicherheitspolitikerInnen die organisatorische Trennung und Unterscheidung derzeit noch als ideologischen Schmuck. Vorsorglich hat man im TBEG die Auskunftsbefugnisse so formuliert, als seien die Antworten obligatorisch: In § 8a BVerfschG ist statt von „Ersuchen" und „Angefragten" penetrant die Rede von „Anordnungen" und „Verpflichteten".

Auf zur nächsten Ergänzung

Seit dem „Otto-Katalog" von 2001 ist klar, dass der Terrorismus als universelle Begründung für alles, was man sonst noch möchte, dienen kann. Der Innenausschuss des Bundestages hat das auch realisiert und das Paket kurz vor Toresschluss um ein weiteres Element ergänzt. Die Einführung von Fingerabdrücken auf den Chips der neuen biometrischen Pässe muss getestet werden. Auch für die versuchsweise Erhebung der Fingerabdrücke und die Verarbeitung dieser Daten durch die Passhersteller bedarf es in einem Rechtsstaat einer gesetzlichen Grundlage. Warum sollte man sie also nicht in ein Gesetz stopfen, das ohnehin schon beliebig ist.

In fünf Jahren laufen die neuen Geheimdienstbefugnisse wieder aus. Vorher werden sie evaluiert. Spätestens dann wird es bestimmt eine Reihe neuer Ideen geben, wie man das Terrorismusbekämpfungsergänzungsgesetz weiter ergänzen könnte.

Polizeirecht durch die Bremer Brille

Zum Einsatz beim Hamburger Schanzenfest

von Helmut Pollähne

Die Bremer Polizei hält es für „verhältnismäßig", festgenommene DemonstrantInnen nicht nur zu fesseln, sondern ihnen zur Desorientierung auch abgedunkelte Brillen aufzusetzen.

Samstag, 9. September 2006: Die Hamburger Polizei hat vorsorglich um Unterstützung aus den benachbarten Bundesländern gebeten. Beim Fußball-Pokalschlager St. Pauli gegen Bayern muss sie die Fans betreuen, und nebenan steigt das alljährliche Schanzenfest. Dort macht eine Bremer Festnahmeeinheit von sich reden, die den Festgenommenen nicht nur, wie üblich, die Hände auf dem Rücken in Plastikfesseln legt: Sie setzt ihnen zusätzlich abgedunkelte Brillen auf, um sie bis zum Abtransport zu „desorientieren".

Der Vorgang hat einiges öffentliches Aufsehen erregt und Nachfragen im politischen Raum provoziert. Es laufen nicht nur interne Ermittlungen der Hamburger Polizei, gegen die Verantwortlichen ist auch Strafanzeige erstattet worden. Die Ermittlungen gestalten sich offenbar schwierig, die Rechtslage soll sich aber – jedenfalls durch die Brille der Bremer Polizei betrachtet – einfach gestalten.

Auf Anfrage der Grünen in der Bremer Bürgerschaft beteuerte das Innenressort zur Rechtfertigung des Einsatzes der verharmlosend „Sichtschutzbrille" genannten binokularen Augenbinde: Sie werde von der Beweissicherungs- und Festnahmeeinheit (BFE) der Bereitschaftspolizei Bremen „ausschließlich gegen besonders gewalttätige und häufig bewaffnete Teilnehmer von Versammlungen" eingesetzt und diene „der Durchsetzung von Festnahmen und Zuführungen im Rahmen besonders konfliktreicher und gewaltorientierter Einsatzsituationen". Der Einsatz werde „immer im Einzelfall geprüft und sehr restriktiv" entschieden. Seit dem Jahre 2003 habe man dieses Mittel bei sechs von 80 BFE-Einsätzen gegen insgesamt 34 Personen gebraucht – „stets nur für einen

Zeitraum von wenigen Minuten“. Die Maßnahme sei nicht nur „einsatztaktisch notwendig und effektiv, um das rasche und möglichst konfliktfreie Verbringen von besonders gewalttätigen Personen aus einer Personenansammlung heraus zum Einsatzfahrzeug zu realisieren“, sie vermeide zudem die „ansonsten häufig notwendige Anwendung zusätzlicher körperlicher Gewalt“ und wirke in der Regel „eher deeskalierend“.

Der einsatztaktische Wert der Dunkelbrille wird wie folgt auf den Punkt gebracht: „Durch seine kurzzeitige Desorientierung wird der Betroffene sowohl an weiterem Widerstand und einem Fluchtversuch als auch an einer Kontaktaufnahme zu anderen Störern gehindert. Somit wird einerseits ein Solidarisierungseffekt unterbunden, andererseits dem Gebot der Eigensicherung der eingesetzten Polizeikräfte Rechnung getragen.“ Nach allem handele es sich nicht nur um ein geeignetes, sondern auch „den Betroffenen kaum beeinträchtigendes Mittel zur erfolgreichen Gefahrenabwehr und Eigensicherung“.[1]

Hamburger Ermittlungen

Ob die vom Bremer Innenressort beschworenen „Grundsätze der Verhältnismäßigkeit“ in Hamburg verletzt wurden, müssten die weiteren Ermittlungen ergeben, heißt es abschließend. Das dürfte spannend werden, denn einiges deutet darauf hin, dass gleich mehrere der vorgeblich „immer“, „ausschließlich“ und „stets“ geltenden Grundsätze missachtet wurden. Überraschend ist, dass über derartige Polizeipraktiken bisher nichts an die Öffentlichkeit gedrungen ist, und zwar weder in Bremen noch andernorts.[2] Auch die Bundesregierung erklärt, „eine solche Praxis und Ausstattung“ sei ihr unbekannt und „bei den zahlreichen bisherigen Einsatzbeobachtungen“ nicht aufgefallen.[3]

Die Ermittlungen in Hamburg waren bei Redaktionsschluss noch nicht abgeschlossen, denn selbst die Dienststelle Interne Ermittlungen

---

1 Antwort des Innenressorts in der Fragestunde der Bremischen Bürgerschaft am 11.10.2006 in Anlehnung an eine Stellungnahme des Leiters der Fachdirektion Recht und Personal der Bremer Polizei vom 12.9.2006 an die Hamburger Innenrevision

2 Ausnahme sind allerdings mittlerweile Vorführungen Tatverdächtiger per Hubschrauber bei der Bundesanwaltschaft, die mit Augenbinde und Ohrenstöpsel erfolgen; exemplarisch nach der Festnahme zweier Verdächtiger am 20.4.2006 wegen des vermeintlich rechtsradikalen Überfalls auf einen Schwarzafrikaner in Potsdam.

3 Antwort auf eine Schriftliche Frage von Ulla Jelpke (Linksfraktion), BT-Drs. 16/2812 v. 29.9.2006, S. 6 f.

(DIE) hat sich bisher vergeblich um eine Kopie des Bremer Einsatzvideos bemüht. Für die interne Legitimation des Einsatzes wäre dieses aber von besonderer Bedeutung, soll sich daraus doch ergeben, ob es sich tatsächlich um „besonders gewalttätige und häufig bewaffnete" Demonstranten gehandelt hat und nach Festnahme und Fesselung weiteren Widerstands- und Fluchtversuchen zu begegnen war, um die dadurch bedrohte Eigensicherung der eingesetzten Polizisten zu gewährleisten. All das wird von Seiten der Demonstranten durchaus bestritten – nicht auszuschließen, dass das Videomaterial deshalb unauffindbar ist.[4]

Bestritten wird auch, dass der Brilleneinsatz nur „wenige Minuten" gedauert habe: Selbst nach Angaben der Bremer Polizei waren es mindestens zwanzig Minuten. Zudem steht die Aussage zweier Beamter des Gefangenentransportkommandos im Raum, einer der Beschuldigten habe die Brille auch „während seines Transportes" getragen, der insgesamt rund drei Stunden dauerte.[5] Die „taz nord" wiederum zitierte am 12. September einen Anwalt mit der Aussage, sein Mandant habe „mit dieser Brille eine Dreiviertelstunde lang orientierungslos auf der Straße stehen müssen". Von „wenigen Minuten" kann offenkundig keine Rede sein. Und für die Betroffenen ist ohnehin entscheidend, dass sie ja auch hinsichtlich der Dauer „desorientiert" sind – sie haben nur geduldig darauf zu hoffen, dass sie irgendwer irgendwann aus der Dunkelheit befreit.

Derweil können sich die Festgenommenen nicht von der Stelle bewegen, ohne Kollisionen und Stürze zu riskieren – und damit ist man schließlich zur Frage gelangt, ob es sich tatsächlich um ein „kaum beeinträchtigendes Mittel" gehandelt hat, wobei die mehr oder weniger lang andauernde „Desorientierung" der Betroffenen ja gar nicht bestritten, vielmehr explizit bezweckt wird (s.o.). Dem zitierten Anwalt zufolge habe sein Mandant „unter Übelkeit und Panikanfällen gelitten".

Zur Rechtslage (mit und ohne Bremer Brille gesehen)

Der Zweck des Einsatzes blieb zunächst unklar: Einer ersten Stellungnahme der Bremer Polizei zufolge sollten die Festgenommenen mit den Brillen „separiert" werden, um „Gespräche oder Augenkontakt zu ver-

4 Einem DIE-Schreiben vom 12.9.2006 zufolge waren „den bisher vorliegenden Berichten ... Hinweise auf Widerstandshandlungen ... nicht zu entnehmen".

5 DIE-Bericht v. 10.9.2006

hindern“, damit sie „ihre Aussagen gegenüber der Polizei (nicht) absprechen“.[6] Die Betroffenen wurden festgenommen wegen des Verdachts des Landfriedensbruchs (Flaschenwürfe gegen Wasserwerfer)[7] – offenbar wurden sie aber auch in Gewahrsam genommen zur Unterbindung weiterer Störungen.

Über die Art und Weise der Durchführung einer vorläufigen Festnahme schweigt sich die Strafprozessordnung (in § 127) aus, allgemein wird aber angenommen, dass die Grenzen der Festnahmemittel durch das jeweilige Polizeirecht bestimmt werden, insbesondere durch die Vorschriften über die Anwendung unmittelbaren Zwangs; für die Ingewahrsamnahme gilt dasselbe. Darauf berufen sich auch die Polizei-Justiziare in Bremen und Hamburg: Bei den Brillen handele es sich um sonstige „Hilfsmittel körperlicher Gewalt“, die gesetzlich (z.B. in § 18 Abs. 3 des Hamburger Sicherheits- und Ordnungsgesetzes, HmbSOG) zwar nicht explizit vorgesehen seien, von dem nicht abschließenden Katalog aber erfasst würden; unter Beachtung der Verhältnismäßigkeit bestünden gegen den Einsatz „keine rechtlichen Bedenken“.[8]

Dem ist zu widersprechen, denn Bedenken bestehen (jedenfalls nach dem derzeitigen Stand der Ermittlungen) hinsichtlich des konkreten Hamburg-Einsatzes nicht nur in puncto Verhältnismäßigkeit, sondern auch im Grundsätzlichen: Selbstverständlich sind nicht alle Hilfsmittel erlaubt, nur weil die Polizei sie für „einsatztaktisch notwendig und effektiv“ hält. Dass weder solche Brillen noch vergleichbare Mittel in irgendeiner polizeirechtlichen Vorschrift oder in einem der einschlägigen Kommentare oder Handbücher Erwähnung finden, sollte skeptisch machen.[9] Erniedrigende und unmenschliche Methoden haben jedenfalls auszuscheiden, ebenso „seelische und körperliche Misshandlungen“

6 taz nord v. 12.9.2006; eine andere – nicht weniger bedenkliche – Methode wählte die Hamburger Polizei am Rande der Proteste gegen einen Naziaufmarsch am 14.10.2006: Festgenommenen wurde kurzerhand der Mund zugehalten, junge Welt v. 26.10.2006.

7 Pikantes am Rande: Mindestens eine der Flaschen, die in den Reihen der Polizei landeten, wurde offenbar von einem MEK-Kollegen in Zivil geworfen, der mit weiteren Beamten jenseits der Barrikaden angeblich privat auf Zechtour war, taz nord v. 18.9.2006.

8 so die Rechtsabteilung der hamburgischen Polizei in einer äußerst knapp gehaltenen Stellungnahme an die DIE v. 12.9.2006

9 exempl. Alberts, H.W.; Merten, K.; Rogosch, K.J.: Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung (SOG) Hamburg, Stuttgart 1996, § 18 Rn. 3 f.; Schmidt, R.: Bremisches Polizeigesetz, Grasberg 2006, § 41 Rn. 4; Rachor, F.: Polizeihandeln, in: Lisken, H; Denninger, E. (Hg.): Handbuch des Polizeirechts, 3. Aufl. München 2001, Rn. F 784 ff.

(Art. 104 Abs. 1 S. 2 Grundgesetz), damit aber auch Hilfsmittel, denen das Risiko solcher Methoden und Misshandlungen von vorneherein immanent ist. Gerade deshalb begegnet der Einsatz jener Dunkelbrillen erheblichen Bedenken, denn sie beinhalten unkontrollierbare Risiken für die physische und psychische Integrität der Festgenommenen.

Riskant und unverhältnismäßig

Ungeachtet dessen ist fraglich, ob überhaupt die gesetzlichen Voraussetzungen dieser Form des unmittelbaren Zwangs beachtet wurden: So kann insbesondere von der vorgeschriebenen Androhung unmittelbaren Zwangs[10] nur abgesehen werden, wenn „die sofortige Anwendung des Zwangsmittels (hier also: Einsatz der Dunkelbrille nach Ingewahrsamnahme und Fesselung, d. Verf.) zur Abwendung einer unmittelbar bevorstehenden Gefahr notwendig ist“ (§ 22 Abs. 1 HmbSOG). Die bisherigen Ermittlungen geben das nicht her: Ob die besonderen Voraussetzungen für eine Fesselung vorlagen (gemäß § 23 HmbSOG) mag hier dahinstehen, dass es aber nach der Fesselung ohne weitere Androhung eines sofortigen Dunkelbrilleneinsatzes bedurfte, erscheint doch fraglich.

Jenseits prinzipieller Bedenken und juristischer Detailprobleme liegt schließlich auch eine Verletzung des Verhältnismäßigkeitsprinzips nahe, selbst wenn die Polizei versucht, genau das Gegenteil zu belegen: Die Brille sei gewissermaßen als milderes Mittel eingesetzt worden, denn damit werde die „ansonsten häufig notwendige Anwendung zusätzlicher körperlicher Gewalt“ vermieden.[11] Das klingt zunächst plausibel, entbehrt bei näherer Betrachtung aber nicht einer perfiden Logik, zumal völlig offen bleibt, ob „zusätzliche körperliche Gewalt“ überhaupt notwendig und verhältnismäßig gewesen wäre: Die Dunkelbrillen werden aber offenbar vorsorglich eingesetzt.

Maßnahmen zur Gefahrenabwehr dürfen „keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg

10 vgl. Rachor a.a.O. (Fn. 9), Rn. F 803 ff.

11 Ähnlich die empörte GdP in einer Stellungnahme als Reaktion auf die öffentlichen Debatten: „Meine Kollegen könnten nach dem PolG auch Pfefferspray anwenden oder die Arme der oft um sich schlagenden Tatverdächtigen auf den Rücken drehen. Der kurzzeitige Einsatz einer Dunkelbrille, die Tobende orientierungslos werden lässt, ist das deutlich mildeste Mittel“, zit. nach Weser-Kurier v. 15.9.2006.

steht“ (§ 4 Abs. 1 HmbSOG). Dass es jenseits der Fesselung und in Anbetracht der Übermacht hochgradig geschützter Polizeibeamter überhaupt weiterer Maßnahmen zur Eigensicherung bedarf (bzw. in Hamburg bedurfte), erscheint bereits mehr als zweifelhaft – die damit herbeigeführten oder doch zumindest in Kauf genommenen Nachteile auf Seiten der Festgenommenen sind inakzeptabel.

Etwas von Folter?

In den öffentlichen Debatten nach dem Hamburger Einsatz stand schnell der Folter-Vorwurf im Raum, zumindest handele es sich um „folterähnliche“ Methoden, die an Guantánamo Bay und Abu Ghraib erinnerten.[12] In der Tat fragt man sich, was denn den Einsatz binokularer Augenbinden unterscheidet vom sog. „hooding“ (Sack oder Kapuze über den Kopf), mediale Ästhetik einmal beiseite gelassen (Dunkelbrillen sehen definitiv „cooler“ aus). Es sei daran erinnert, dass jegliche Form der Dunkelhaft gemäß Art. 3 der Europäischen Menschenrechtskonvention (EMRK) streng verboten ist.[13] Sollte sich die Bremer Brille von solchen „unmenschlichen oder erniedrigenden“ Behandlungen nur durch die Dauer des Einsatzes[14] unterscheiden, ist der Polizei von dem Einsatz einer menschenrechtlich derart riskanten Methode dringend abzuraten.

---

12 vgl. taz nord v. 14.9.2006 und junge Welt v. 26.10.2006

13 Eine entsprechende Konkretisierung des Art. 3 EMRK („Niemand darf gefangengehalten werden und einem Übermaß an ... Dunkelheit ... ausgesetzt werden, so dass er darunter psychisch leidet“) wurde nicht übernommen, weil die Bestimmung vom später in Kraft getretenen Text „unmenschliche oder erniedrigende Behandlung“ mit erfasst ist; siehe Frowein, J.; Peukert, W.: EMRK-Kommentar, Kehl, Straßburg, Arlington 1996, Art. 3 Rn. 17 m.w.N.; vgl. auch Europäisches Komitee zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (CPT): Die Standards des CPT, Straßburg 2004 (Europarat: CPT/Inf/E (2002) 1 – Rev. 2004, (www.cpt.coe.int/lang/deu/deu-standards-s.pdf)), S. 26 (Kap. 2 – Gefängnishaft, Auszug aus dem 11. Jahresbericht 2001, Abs. 30); siehe ferner § 115 Abs. 2 S. 4 Jugendgerichtsgesetz (JGG).

14 Im Fall Öcalan billigte der Europäische Gerichtshof für Menschenrechte (EGMR) (Urteil vom 12.3.2003 – Beschw.-Nr. 46221/99) den mehrstündigen Transport mit Handschellen und Augenbinde nur in Anbetracht der besonderen Gefährlichkeit der Beschuldigten; verhaltene Kritik daran bei Kühne, H.H.: Die Entscheidung des EGMR in Sachen Öcalan, in: Juristenzeitung 2003, H. 13, S. 670-674 (671); vgl. zur Folter-Übung mit Bundeswehr-Rekruten im Jahre 2004 den Beschluss des Oberlandesgerichts Hamm vom 25.7.2006 (Az.: 4 Ws 172-188/06, dok. in juris) u.a. zu §§ 30, 31 Wehrstrafgesetz (Misshandlung und entwürdigende Behandlung Untergebener).

Inland aktuell

Große Lauschangriffe 2005

Im Jahr 2005 wurden in Deutschland in sechs Bundesländern sechs Objekte im Rahmen strafrechtlicher Ermittlungen akustisch überwacht. Der entsprechende Bericht der Bundesregierung vom 7. September 2006[1] führt Lauschangriffe in Bayern, Hessen, Hamburg, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein auf. Eine weitere Überwachung in Niedersachsen wurde angeordnet, aber nicht ausgeführt. Insgesamt waren 26 Beschuldigte sowie drei nicht beschuldigte Personen betroffen. Bei drei der abgehörten Objekte handelte es sich um Privatwohnungen. Bis zum Zeitpunkt der Erstellung des Berichts waren drei Betroffene (noch) nicht über die Bespitzelung informiert.

Nach Angaben des Berichts bestand in vier Verfahren ein Bezug zur organisierten Kriminalität. Während für diese Fälle eine Relevanz der durch die Überwachung gewonnenen Erkenntnisse für das Verfahren bejaht wurde, brachten die beiden anderen Lauschangriffe keinerlei brauchbare Informationen. Abgehört wurde 2005 über eine Dauer von bis zu 26 Kalendertagen.

Verwirrend sind wie jedes Jahr die Angaben zu den verursachten Kosten. So werden die Übersetzungskosten bei einem Verfahren mit zwei überwachten Personen in Bayern auf 45,24 Euro beziffert, bei ebenfalls zwei Personen in Nordrhein-Westfalen stiegen die Kosten der Übersetzung hingegen auf 50.000 Euro. Das Verfahren dauerte aber lediglich drei Tage länger.

Im Vergleich zu den Vorjahren war die Zahl der akustischen Wohnraumüberwachungen rückläufig. 2004 waren noch in elf Verfahren Wanzen installiert worden. Gründe für den Rückgang sieht die Bundesjustizministerin im Urteil des Bundesverfassungsgerichts vom März 2004 und der ihm folgenden Novellierung der Strafprozessordnung, die Anfang Juli 2005 in Kraft trat.[2]

1 www.bmj.de/files/-/1319/Bericht%20Wohnraumüberwachung_270906.pdf
2 www.bmj.de/enid/58.html?presseartikel_id=2575

Telekommunikationsüberwachungsstatistik 2005

Auf Nachfrage veröffentlichte die Bundesregierung im Oktober die Statistik der Landesjustizverwaltungen und des Generalbundesanwalts zur Telekommunikationsüberwachung (TKÜ) im Jahr 2005:[3] Bundesweit kam es demnach zu TKÜs in insgesamt 4.925 Verfahren; das entsprach einer Steigerung von 4,5 % gegenüber dem Vorjahr. Auffallend an der Statistik sind die geografischen und deliktischen Ungleichheiten. So führt Bayern mit 885 TKÜ-Verfahren die Rangliste an; Nordrhein-Westfalen kam trotz größerer Bevölkerung und mehr registrierten Straftaten mit fast der Hälfte an Überwachungen aus. In einigen Bundesländern stieg die Zahl der TKÜs weiter: mit 116 Verfahren verdoppelte sie sich im Saarland fast; Thüringen (+36 %), Hamburg (+31 %), Rheinland-Pfalz (+28 %), Mecklenburg-Vorpommern (+27 %) und Schleswig-Holstein (+24 %) wiesen ebenfalls erhebliche Steigerungsraten auf.

Das Gros der Überwachungen betraf auch in diesem Jahr Verstöße gegen das Betäubungsmittelgesetz (3.331 Verfahren); auch hier liegt Bayern vorn (599 Verfahren) – während etwa Berlin nur 42 TKÜ-Verfahren im Rauschgiftbereich meldete. Auffällig ist die ungewöhnlich hohe Zahl von 24 bayerischen Verfahren wegen Straftaten gegen die Landesverteidigung, denen nur ein einziges Verfahren in Nordrhein-Westfahlen gegenüber stand. In 47 vom Generalbundesanwalt geführten Verfahren kam es zu TKÜs. Bei 34 dieser Verfahren wurde wegen „Straftaten gegen die öffentliche Ordnung“ ermittelt, also u.a. wegen des Verdachts der Mitgliedschaft etc. in kriminellen oder terroristischen Vereinigungen.

Bereits im April hatte die Bundesnetzagentur ihre Statistik der TKÜs vorgelegt.[4] Im Unterschied zu den Justizverwaltungen zählt die Netzagentur nicht die Ermittlungsverfahren, sondern die Anordnungen auf Überwachung und die davon betroffenen Anschlüsse: 2005 wurden in der Bundesrepublik insgesamt 42.508 Überwachungen der Telekommunikation angeordnet. Diese betrafen 49.243 „Kennungen“ (= Anschlüsse bzw. Telefonnummern). Mit einer Steigerungsrate von mehr als 20 % im Vergleich zum Vorjahr (2004 waren 40.973 Anschlüsse überwacht worden) wurden 2005 so viele Telefon, Fax- und Internetanschlüsse staat-

3 Antwort auf die Schriftliche Frage des Abg. Hans-Christian Ströbele (Bündnis 90/Die Grünen), BT-Drs. 16/3054 v. 20.10.2006, S. 5 ff.

4 abgedruckt ebd., S. 8

lich abgehört wie nie zuvor. Wie in den vergangenen Jahren entfiel der Großteil der Überwachungen auf Mobiltelefone (42.011 Anschlüsse). Nach wie vor niedrig ist die Zahl der Überwachungen im Bereich der digitalen Medien. Obgleich die 193 überwachten Internetzugänge eine Verdopplung und die 365 E-Mail-Zugänge mehr als eine Vervierfachung der Fälle gegenüber dem Vorjahr darstellen.
(beide: Jan Wörlein)

Durchsetzung des Schulzwangs in Bayern

Im Rahmen ihres Schulschwänzerprogramms griff die bayerische Polizei im vergangenen Schuljahr insgesamt 1.779 SchülerInnen auf.[5] Das sind geringfügig weniger als im Schuljahr 2004/2005. Einstmals ein Pilotprojekt der Nürnberger Polizei,[6] gilt die Schulschwänzerinitiative heute in ganz Bayern als wichtiges Standbein der Bekämpfung von Kinder- und Jugendkriminalität: „Mancher Jugendlicher muss eben notfalls von einer Polizeistreife wieder auf Kurs gebracht werden," weiß Dr. Günther Beckstein, bayerischer Staatsminister des Innern.[7]

Die Polizei vollzieht einerseits auf Antrag der zuständigen Schulbehörde „Vorführungen". Das bedeutet, dass nach in der Regel zehn unentschuldigten Fehltagen SchülerInnen von einem/einer (Jugend-)BeamtIn – auf Anforderung der Schule in Uniform – der Schule „überstellt" werden. Mit 1.465 Fällen ist die Zahl im Vergleich zum Vorschuljahr (1.562) leicht gesunken. Andererseits wird die Polizei eigeninitiativ tätig und führt Kontrollen insbesondere an bekannten Treffpunkten Jugendlicher durch. Die BeamtInnen in Zivilkleidung sprechen „Verdächtige" an und überprüfen telefonisch ihre Angaben. Mit 314 Fundfällen ist die Zahl im Vergleich zum Vorjahr (289) leicht gestiegen.

Vorgesehen ist, dass die SchülerInnen in das Sekretariat der Schule gebracht werden, sie dürfen jedoch auch vor der Klassenzimmertür dem zuständigen Lehrpersonal übergeben werden – der untersagten Übergabe im Klassenzimmer dürfte dies in der Praxis sehr nahe kommen.

Die Rechtsgrundlage für den Polizeieinsatz findet sich im bayerischen Erziehungs- und Unterrichtsgesetz. Gemäß diesem begehen

5 www.stmi.bayern.de/presse/archiv/2006/311.php
6 www.sicherheitspakt.nuernberg.de/download/schulschwaenzer_kurz.pdf
7 www.stmi.bayern.de/presse/archiv/2006/311.php

Schulpflichtige, die am Unterricht oder an verbindlichen Schulveranstaltungen vorsätzlich nicht teilnehmen, eine Ordnungswidrigkeit.

Die Datei der „tickenden Zeitbomben“

Seit Oktober 2006 gibt es im süddeutschen Freistaat eine neue Datei, betitelt HEADS, die die bayerische, aber auch die bundesdeutsche Bevölkerung zukünftig besser vor Sexualstraftaten schützen soll. HEADS steht für „Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter“.[8] Erfasst werden Personen, die wegen Straftaten gegen die sexuelle Selbstbestimmung oder wegen Tötungsdelikten mit sexuellen Tatmotiven oder unklarem Motiv verurteilt und zudem von der Staatsanwaltschaft als RisikoprobandInnen eingestuft worden sind. Zu einer solchen Einstufung kann es kommen, wenn (1) eine Person, die aus der Haft entlassen werden soll, ohne in den Bereich der Sicherungsverwahrung zu fallen, weiterhin als rückfallgefährdet gilt oder (2) eine Person vorzeitig aus der Haft entlassen wurde und erneut auffällig geworden ist.

Während früher die Staatsanwaltschaft die Polizeidirektionen direkt benachrichtigte,[9] wurde mit der „Zentralstelle HEADS“ beim Polizeipräsidium München eine Einrichtung geschaffen, die die relevanten Daten bayernweit systematisch erfassen und die zuständigen Direktionen informieren soll. Ziel ist es, das Bewegungsbild der Registrierten nachvollziehbar zu machen und gegebenenfalls „eine auf den Einzelfall bezogene Überwachung“ sicherzustellen. Neben der Polizei sollen Jugendämter, Führungsaufsicht, Bewährungshilfe und Kreisverwaltungsreferate im Rahmen von „Runden Tischen“ besser in den Informationsaustausch und die Konzipierung von Maßnahmen eingebunden werden.[10]

Um den Schutz der ehemaligen Häftlinge geht es bei HEADS nicht: „Ich darf dabei an dieser Stelle vorwegschicken, dass nicht nur Opferschutz vor Täterschutz geht, sondern dass dann auch Fragen des Datenschutzes zurückgestellt werden müssen, wenn es bei Sexualstraftaten um den Schutz von Opfern geht“, so der Staatsekretär des Innern, Georg Schmidt.[11]

(beide: Hanna Noesselt)

8 Bayerische Staatskanzlei, Pressemitteilung Nr. 357 v. 18.9.2006, S. 5-7
9 Bayerischer Landtag, Drs. 15/5767 v. 18.7.2006
10 Bayerische Staatskanzlei a.a.O. (Fn. 8)
11 Bayerischer Landtag, Plenarprotokoll 15/63 v. 8.3.2006, S. 4770

Chronologie

zusammengestellt von Hanna Noesselt

September 2006

01.09.: **Konfrontationen im Berliner Wahlkampf:** Zwölf Angehörige der linken Szene attackieren einen Wahlstand der Republikaner in Friedrichshain. Sechs der Angreifer werden vorläufig festgenommen. Nachdem es bei Veranstaltungen von SPD und CDU zu wiederholten Konfrontationen kommt, attackieren am 8. September in Marzahn zwei Anhänger der rechten Szene zwei SPD-Mitglieder beim Aufhängen von Plakaten. Die Staatsanwaltschaft ermittelt wegen schwerer Körperverletzung gegen die beiden Neonazis.
Deutsch-niederländischer Polizei- und Justizvertrag in Kraft: Durch den Vertrag wird die Kooperation der Polizeien erweitert. Unter anderem dürfen PolizistInnen nun zur Gefahrenabwehr und TäterInnenverfolgung die gemeinsame Landesgrenze überschreiten.

09.09.: **Einsatz von schwarzen Brillen beim Schanzenfest:** Nach dem Hamburger Straßenfest kommt es zu gewalttätigen Auseinandersetzungen mit der Polizei. Diese setzt Schlagstöcke und Wasserwerfer ein. Amtshelfende Bremer Beamte verwenden sogenannte „Sichtschutzbrillen" zur leichteren Kontrolle der Festgenommenen. (Vgl. S. 74 ff. in diesem Heft.)

10.09.: **Anschlag auf Futtermittelfirma gescheitert:** Im brandenburgischen Eberswalde werden unter vier LKW einer Futtermittelfirma, die gentechnisch veränderten Mais aufkauft, Brandsätze gefunden, die nicht explodiert waren. Gentechnik-GegnerInnen bekennen sich zu dem Anschlagsversuch.

12.09.: **Razzia an rechtsextremistischen Treffpunkten:** Im Landkreis Löbau-Zittau (Sachsen) durchsucht die Polizei mit 82 BeamtInnen insgesamt 20 Örtlichkeiten der „Kameradschaft Oberlausitz" und des

„Jungsturm 41“ wegen Verdachts auf Volksverhetzung. Auch in Dresden, Bayern und Baden-Württemberg gibt es einzelne Durchsuchungen.

14.09.: **Vermeintlicher Terrorist wieder frei:** Auf Grund einer Verwechselung hebt der Bundesgerichtshof (BGH) den Haftbefehl gegen den angeblichen dritten Täter des Kofferbomben-Anschlages in NRW wieder auf.

19.09.: **Rechtsbelehrung ist Pflicht:** Nach einem Urteil des Bundesverfassungsgerichts (BVerfG) müssen in Deutschland festgenommene AusländerInnen unverzüglich über ihr Recht, ihr Heimatkonsulat zu informieren, belehrt werden. Das Gericht hebt mit seiner Entscheidung zwei Beschlüsse des BGH auf. (Az.: 2 BvR 2115/01 u.a.)

25.09.: **Mehr politisch motivierte Kriminalität in NRW:** Laut Verfassungsschutz-Zwischenbericht 2006 stiegen die Delikte um 14,3 % im Vergleich zum Vorjahreszeitraum. Mit 72,3 % hatten rechtsextremistisch motivierte Straftaten den größten Anteil, 16,5 % der Delikte wurden dem Linksextremismus zugerechnet, 2,1 % dem Ausländerextremismus.

26.09.: **Festnahme rechtswidrig**: Das Amtsgericht Berlin-Tiergarten erklärt die Festnahme eines 36-Jährigen im Rahmen einer Razzia für rechtswidrig. Im Vorfeld eines Fußballspiels hatte die Polizei eine Berliner Diskothek in der Nacht zum 21. Mai 2005 gestürmt. Bei dem Einsatz waren 158 Menschen festgenommen worden, von denen zwölf der Polizei als Gewalttäter bekannt waren. 20 Menschen wurden verletzt. (Az.: 381 AR 29/06)
4,9 Tonnen Haschisch sichergestellt: Es wird bekannt, dass gemeinsame Ermittlungen des Bundeskriminalamtes (BKA) und der belgischen Polizei zur Sicherstellung von 2.500 kg Cannabis im Mai und weiteren 2.400 kg im September führten.

27.09.: A**kustische Wohnraumüberwachung 2005:** Das Bundesministerium der Justiz (BMJ) teilt mit, dass im letzten Jahr in sechs Ermittlungsverfahren Wohnungen abgehört wurden. (Vgl. S. 80 in diesem Heft.)
Telekommunikationsüberwachung 2005: Das BMJ teilt mit, dass es im Jahre 2005 4.925 Ermittlungsverfahren mit Überwachungsmaßnahmen gab. Die Zahl der von den Überwachungen Betroffenen wird mit 12.606 angegeben. (Vgl. S. 81 in diesem Heft.)

29.09.: **Geldstrafe für Antifa-Symbole:** Das Landgericht Stuttgart verurteilt einen Versandhändler zu 3.600 Euro Geldstrafe wegen Verwendens und Verbreitens von Kennzeichen verfassungswidriger Organisationen. Staatsanwaltschaft und Verteidigung kündigen Revision vor dem BGH an.

Oktober 2006

01.10.: **Neue Datei über SexualstraftäterInnen:** Bayern führt die Haft-Entlassenen-Auskunfts-Datei-Sexualstraftäter (HEADS) ein. (Vgl. S. 83 in diesem Heft.)

03.10.: **Konfrontationen bei Neonazi-Aufmarsch in Leipzig:** Im Rahmen von Gegendemonstrationen von etwa 2.000 Mitgliedern der linken Szene werden Barrikaden errichtet und Flaschen geworfen. Zehn Menschen werden verletzt, darunter vier Polizisten. Nach Angaben der Polizei werden 59 Personen in Gewahrsam genommen.

05.10.: **Demonstration gegen Studiengebühren:** Nach der Einführung von Studiengebühren in Hessen kommt es in Wiesbaden zu Protesten. Zwei Menschen werden in Gewahrsam genommen. Die Polizei hindert Demonstrierende mit dem Einsatz von Schlagstöcken daran, die Absperrung der Bannmeile zu übersteigen.

06.10.: **Neues Abkommen zu Fluggastdaten:** Die EU und die Vereinigten Staaten einigen sich auf ein Abkommen, das bis Juni 2007 gültig ist. Die 34 Datensets dürfen künftig nicht mehr nur an den US-Zoll, sondern auch an andere Sicherheitsbehörden übermittelt werden.

10.10.: **Mutmaßlicher Al-Qaida-Unterstützer festgenommen:** Auf Veranlassung der Bundesanwaltschaft wird ein 36-jähriger Iraker in der Nähe von Osnabrück festgenommen. Ihm wird vorgeworfen, Videobotschaften von Osama bin Laden, Ayman Al Zawahiri und Abu Musab Al Zarqawi im Internet verbreitet zu haben.
Wohnungsdurchsuchungen erneut verfassungswidrig: Das BVerfG veröffentlicht drei Beschlüsse, in denen Wohnungsdurchsuchungen, die ohne richterlichen Beschluss erfolgten oder unverhältnismäßig waren, für verfassungswidrig erklärt wurden. (Az.: 2 BvR 876/06; 2 BvR 1219/05; 2 BvR 1141/05)
Wiederaufnahme des Verfahrens gefordert: Die Anwälte der Schwester eines im April in Dortmund von einem Polizisten getöteten Kongole-

sen erheben Vorwürfe wegen der Einstellung des Verfahrens. Es sei nicht ausreichend geprüft worden, ob der Polizist sich nicht auch mit Pfefferspray hätte verteidigen oder einen Warnschuss hätte abgeben können. Daraufhin prüft die Staatsanwaltschaft den Fall erneut.
BKA startet Biometrieprojekt: Mit Hilfe von 200 freiwilligen PendlerInnen werden von Oktober 2006 bis Januar 2007 am Mainzer Hauptbahnhof drei biometrische Gesichtserkennungssysteme getestet. Ziel der sogenannten „Fotofahndung" ist es, bereits bekannte Gesichter in einer sich bewegenden Menschenmenge durch einen Computerabgleich herausfiltern zu können.

11.10.: **PKK-Führer verurteilt:** Das Oberlandesgericht (OLG) Celle verurteilt einen Kurden wegen Rädelsführerschaft in einer kriminellen Vereinigung zu drei Jahren Haft. (Az.: 2 StE 3/06)

13.10.: **Überwachung mit IMSI-Catchern nicht verfassungswidrig:** Das BVerfG gibt bekannt, dass es am 22. August den Gebrauch von IMSI-Catchern zu Strafverfolgungszwecken für verfassungsgemäß erklärt hat. Weder das Fernmeldegeheimnis noch das Recht auf informationelle Selbstbestimmung seien unzulässig eingeschränkt. (Az.: 2 BvR 1345/03)
Angriff von Rechtsradikalen erfunden: Wegen Vortäuschung eines fremdenfeindlichen Übergriffs im Mai in Berlin wird ein 30-jähriger Italiener vom Amtsgericht Berlin-Tiergarten zu sechs Monaten Haft auf Bewährung und 1.000 Sozialstunden verurteilt. (Az.: 251 A DS 75/06)

15.10.: **Polizist schießt Mann nach Messerattacke an:** Nach Polizeiangaben habe in Lennestadt (Nordrhein-Westfalen) ein Mann im Hinterhof eines Hauses ein Feuer entzündet und zwei Beamte bei ihrer Ankunft mit dem Messer angegriffen. Die daraufhin abgegebenen Schüsse der Polizisten verletzen den 37-Jährigen schwer.

19.10.: **Untersuchungsausschuss zum Fall Kurnaz:** Um die Misshandlungsvorwürfe gegen KSK-Soldaten zu klären, die der ehemalige Guantánamo-Häftling Murat Kurnaz erhoben hat, wird der Verteidigungsausschuss des Bundestages mit den Rechten eines Untersuchungsausschusses ausgestattet.

20.10.: **Big Brother Awards verliehen:** Geehrt wird unter anderem die Innenministerkonferenz (IMK) für die Einrichtung der Anti-Terror-Datei, die Kultusministerkonferenz für das Vorhaben, Bildungsdaten von SchülerInnen zu erheben, und der Landtag von Mecklenburg-Vorpom-

mern für die gesetzliche Erlaubnis, öffentliche Gebäude und Plätze akustisch zu überwachen.

23.10.: **Geldbuße nach Demonstration:** Nach einem Pressebericht muss ein 22-jähriger Student nach einer Demonstration in Frankfurt/Main im Mai wegen Landfriedensbruchs eine Geldbuße von 500 Euro bezahlen. Wegen mangelnder Beweise wird das Strafverfahren gegen ihn eingestellt.

25.10.: **Geiselnahme durch Schuss beendet:** Ein vermutlich psychisch kranker Mann bedroht eine 69-jährige Frau über Nacht mit einem Messer. Die Polizei überwältigt den 35-Jährigen mit einem Schuss in die Schulter. Die Geisel bleibt unverletzt.

26.10.: **Mann stirbt in Polizeizelle:** Am späten Nachmittag wird die Leiche des 41-Jährigen gefunden, der am Abend zuvor aufgefallen war, da er offenbar betrunken und nur bedingt ansprechbar auf einem Gehweg saß. Die Todesursache bleibt unklar.
Verbindungsdaten müssen gelöscht werden: Nach der Zurückweisung der Beschwerde der Telekom durch den BGH ist ein Urteil des Landgerichts Darmstadt rechtskräftig. Danach muss der Internetprovider Verbindungsdaten bei einer Flatrate nach Beendigung der Verbindung löschen. Ein Internetbenutzer hatte die Deutsche Telekom verklagt, die Verbindungsdaten an die Staatsanwaltschaft weitergegeben hatte. (Az.: III ZR 40/06)

27.10.: **Ausschreitungen bei Fußballspiel:** Im Rahmen des Regionalligaspiels Hertha BSC II gegen Dynamo Dresden prügeln sich Anhänger von Dresden mit der Berliner Polizei. 23 Beamte werden nach Polizeiangaben erheblich verletzt, 22 Personen festgenommen. Wasserwerfer kommen zum Einsatz.
Auslieferungsersuchen der Türkei unzulässig: Wegen Teilnahme an einer Demonstration im Ausland darf ein in Mannheim lebender Türke nicht ausgeliefert werden, selbst wenn die Kundgebung gewaltsam verlief. Nach einem Beschluss des OLG Karlsruhe sind auf Grund des Europäischen Auslieferungsübereinkommens aus dem Jahr 1957 Auslieferungen wegen einer politischen Tat nicht zulässig. (Az.: 1 AK 40/05)

28.10.: **Anti-Nazi-Demo in Göttingen:** Als Reaktion auf einen Aufmarsch von 200 AnhängerInnen der NPD und „Freier Kameradschaften“ demonstrieren in Göttingen 4.000 Menschen. Etwa 6.000 PolizistInnen sind im Einsatz.

31.10.: **Polizei stürmt Kirchenasyl:** Unter Androhung von Gewalt entfernt die Polizei eine fünfköpfige kurdische Familie aus einer Kirche in Koblenz, um sie in die Türkei abzuschieben. Es ist der erste Fall einer Missachtung des Kirchenasyls in Rheinland-Pfalz.

November 2006

04.11.: **Polizeiaktion gegen Rocker:** Im Rahmen einer Aktion gegen den Rockerclub „Bandidos MC" nimmt die Polizei in Cottbus 130 Personen vorläufig fest und stellt 170 Hieb- und Stichwaffen sicher.

09.11.: **Räuber bei Überfall erschossen:** Bei einem Überfall auf einen Geldtransporter in Berlin-Friedrichshain schießen zwei Täter auf zwei Wachleute. Als diese zurückschießen, wird einer der Räuber getroffen und stirbt am Tatort, der andere kann fliehen und wird zwei Tage später festgenommen. Es stellt sich heraus, dass der Getötete mit einer Schreckschusspistole geschossen hatte.

10.11.: **Keine Teleskopschlagstöcke in Berlin:** Nach Auskunft der Polizeipressestelle hat es in Berlin keine Testphase der neuen Stöcke gegeben. Hintergrund der Presseberichte sei eine Privatinitiative eines Beamten des Landeskriminalamtes gewesen; die Tauglichkeit der Waffen sei jedoch verneint worden.

11.11.: **Kein Prozess nach Feuertod:** Das Landgericht Dessau lehnt es ab, wegen des nach wie vor ungeklärten Todes eines Asylsuchenden einen Prozess zu führen. Der 21-jährige Mann aus Sierra Leone war im Januar 2005 im gefesselten Zustand in seiner Zelle verbrannt.

12.11.: **Häftling in Zelle getötet:** In der Justizvollzugsanstalt (JVA) Siegburg wird ein 20-jähriger Mann getötet. Die Staatsanwaltschaft Bonn ermittelt gegen drei Mithäftlinge wegen Mordes, sexueller Nötigung und Vergewaltigung. In den folgenden Wochen kommt es zu 17 weiteren angezeigten Übergriffen unter Gefangenen in NRW.
Castor-Transport: Vor und während des Atom-Müll-Transportes kommt es zu Konfrontationen zwischen Polizei und DemonstrantInnen. Der Zug erreicht am 13. November das Zwischenlager.

15.11.: **Haftbefehle gegen mutmaßliche DHKP-C-Mitglieder:** Wegen Verdachts auf Mitgliedschaft im terroristischen Flügel der türkisch-linksextremistischen Vereinigung nimmt die Bundesanwaltschaft in der Nähe von Uelzen in Niedersachsen einen 50-jährigen Türken fest. We-

gen des selben Vorwurfs werden am 28.11. ein 38-jähriger und ein 48-jähriger Türke festgenommen.
Gewalt zwischen Jugendlichen und der Polizei: Im Berliner Wrangel-Kiez kommt es bei der Festnahme von zwei Zwölfjährigen zu Gewaltanwendungen. Nach Angaben der Polizei seien bis zu hundert Jugendliche über vier Beamte hergefallen, als diese die festgenommenen Kinder in Handschellen an die Wand stellten.
Tod in Zelle: Ein 38-jähriger Obdachloser stirbt in einer Einzelzelle der Rüsselsheimer Polizei. Der Mann war wegen eines Streits mit zwei anderen Obdachlosen festgenommen worden.

16.11.: **El Motassadeq doch wegen Beihilfe zu Mord verurteilt:** In einem Revisionsverfahren erklärt der BGH den Angeklagten wegen Beihilfe zum Mord an den 246 PassagierInnen und Besatzungsmitgliedern der zum Absturz gebrachten Flugzeuge vom 11.9.2001 für schuldig. Zur Festsetzung einer neuen Strafe wird die Sache an das OLG Hamburg zurück verwiesen. (Az.: 3 StR 139/06)
Stufenmodell für geduldete AusländerInnen: Auf Beschluss der IMK erhalten Familien mit minderjährigen Kindern, die mindestens sechs Jahre und Alleinstehende, die mindestens acht Jahre in Deutschland leben und zudem gut integriert sind und ihren Lebensunterhalt selbst verdienen, eine befristete Aufenthaltsgenehmigung.

17.11.: **Tod im Polizeigewahrsam:** In Immenstadt im Allgäu wird ein 42-Jähriger wegen Widerstandes bei seiner Festnahme gefesselt und auf die Straße gelegt. Der offenbar geistig verwirrte Mann stirbt an Herz-Kreislauf-Stillstand. Gegen den Einsatzleiter wird wegen fahrlässiger Tötung ermittelt.

20.11.: **Urteil im Potsdamer Antifa-Prozess:** Zwei wegen eines Angriffs auf einen Neonazi angeklagte Mitglieder der linken Szene werden vom Potsdamer Landgericht zu einer sechsmonatigen Haftstrafe auf Bewährung verurteilt, zwei erhalten eine Verwarnung. Sowohl die Staatsanwaltschaft als auch die Verteidigung gehen in Berufung.
Terrorverdacht: Die Generalbundesanwaltschaft nimmt sechs Personen vorläufig fest. Sie werden verdächtigt, mit Vorbereitungen für einen Sprengstoffanschlag auf ein Verkehrsflugzeug begonnen zu haben. In diesem Zusammenhang waren am 17.11. insgesamt neun Wohnungen in Rheinland-Pfalz und Hessen durchsucht worden. Am 23.11. berichtet die Süddeutsche Zeitung aus „Sicherheitskreisen, dass die Terror-Gefahr

offenbar aufgebauscht wurde. Gegen die sechs arabischstämmigen Männer habe es nie ernsthafte Verdachtsmomente gegeben.
Amoklauf in nordrhein-westfälischer Schule: Ein 18-Jähriger stürmt in seine ehemalige Realschule in Emsdetten und verletzt fünf Menschen durch Schüsse, bevor er sich selbst tötet.

21.11.: **Freispruch eines Polizisten aufgehoben:** Dem Angeklagten wird vorgeworfen, eine zur Ausnüchterung in eine Haftzelle der Nürnberger Polizei verbrachte Frau sexuell missbraucht zu haben. Wegen Fehlern in der Beweisführung und der Nicht-Erwähnung eines früheren Missbrauchsfalls im Urteil wird die Sache durch den BGH an das Landgericht Nürnberg-Fürth zurückverwiesen. (Az.: 1 StR 392/06)

24.11.: **Milli Görüs siegt vor Gericht:** Nach einem Urteil des Verwaltungsgerichtshofes Baden-Württemberg müssen bestimmte Passagen über die als extremistisch eingestufte islamische Gemeinschaft im Verfassungsschutzbericht 2001 unkenntlich gemacht werden. (Az.: 1 S 2321/05)

28.11.: **Ferndurchsuchung von PC nicht erlaubt:** Nach dem Beschluss eines BGH-Ermittungsrichters stellen weder die Vorschriften zur Wohnungsdurchsuchung noch die zum großen Lauschangriff eine hinreichende gesetzliche Grundlage dar, auf die auf einer Festplatte gespeicherte Daten online zuzugreifen. (Az.: 1 BGs 184/2006; 1 BGs 186/2006)
Waffenarsenal bei rechtsextremistischer Organisation sichergestellt: Das LKA Bayern macht bei einer Großrazzia im Raum Rosenheim ein umfangreiches Waffenarsenal ausfindig und nimmt dreizehn Personen vorläufig fest. Bei dem Einsatz, an dem 370 PolizistInnen teilnehmen, werden 100 Kurz- und Langwaffen gefunden.
Bundesweite Razzia gegen mutmaßliche türkische Extremisten: 350 PolizeibeamtInnen aus Baden-Württemberg, Nordrhein-Westfalen und Bayern durchsuchen 59 Objekte wegen Verdachts auf Verstoß gegen das Vereinsgesetz. Einige Verdächtige werden vorübergehend festgenommen.

29.11.: **Grenzen für Untersuchungshaft gesetzt:** Das Bundesverfassungsgericht bekräftigt den Anspruch eines Mannes, nach vierjähriger Auflagenerfüllung die Rechtskraft des Urteils in Freiheit zu erwarten und setzt die Untersuchungshaft aus. (Az.: 2 BvR 2342/06)

30.11.: **Bundestag schränkt Stasi-Überprüfungen ein:** Die Novelle, die am 15. Dezember den Bundesrat passiert, schafft die Regelüberprü-

fung im öffentlichen Dienst ab. Das Stasi-Unterlagengesetz aus dem Jahr 1991 wäre Ende 2006 ausgelaufen.
Bundestag beschließt Justizmodernisierungsgesetz: Das neue Gesetz soll unter anderem Opfern von Straftaten mehr Rechte einräumen und den Opferschutz bei Prozessen gegen jugendliche Straftäter verbessern. Bei besonders schweren Straftaten können nun auch im Jugendstrafrecht Nebenkläger auftreten. Der Bundesrat stimmt dem Gesetz am 15. Dezember zu.
Bundesweite Razzia gegen Kinderpornographie: Unter der Leitung des bayerischen LKA werden bei zwölf Personen in elf Bundesländern Durchsuchungen durchgeführt, nachdem auf dem Handy eines 36-jährigen Ingolstädters 120 Bilder mit kinderpornographischem Inhalt gefunden worden waren.

Dezember 2006

01.12.: **Bundestag beschließt Anti-Terror-Datei:** Die von Polizei und Geheimdiensten gemeinschaftlich genutzte Datei soll bis März 2007 realisiert werden. Der Bundesrat stimmt dem Gesetz am 15.12. zu. (Vgl. S. 52 ff. in diesem Heft.)
Polizei erschießt Mann: Ein 36-jähriger Libanese randaliert im Kloster Oberzell nahe Würzburg und greift mehrere Personen an. Nach dem Einsatz von Pfefferspray gibt ein Beamter zunächst einen Warn- und dann einen zweiten Schuss ab. Der Mann erliegt seinen Verletzungen.

05.12.: **Wohnungsverweis rechtmäßig:** Das Verwaltungsgericht Koblenz teilt mit, dass die Polizei bei einer Demonstration potenzielle StörerInnen auch der eigenen Wohnung verweisen darf, wenn dies zum Schutz von Leib und Leben der Demonstrierenden notwendig ist. (Az.: 5 K 991/06 KO)

06.12.: **Amok-Drohung in Baden-Württemberg:** Ein per Internet angedrohter Amoklauf löst eine Großfahndung im Raum Offenburg aus. Die Polizei durchsucht unter anderem mehrere Schulen.

09.12.: **BND bezahlt 20 Auslandskorrespondenten:** Nach Angaben des Nachrichtenmagazins Focus wurden während der Kanzlerschaft von Gerhard Schröder etwa 20 JournalistInnen deutscher Medien als geheime InformantInnen eingesetzt und bezahlt. Dies sind 13 Personen mehr, als in dem im Mai veröffentlichten Sonderbericht angegeben wurden.

12.12.: **Großfahndung in Stuttgart:** Mit mehr als 1.000 FahnderInnen durchsucht die Polizei 34 Unternehmen, neun Baustellen und 36 Privatwohnungen. In Deutschland und Italien werden elf Personen festgenommen, die unter anderem verdächtigt werden, im Rahmen einer kriminellen Vereinigung im Baugewerbe Gelder veruntreut zu haben.
Haftbefehl nach Angriff auf Rechte: Wegen versuchten Totschlages wird ein 21-jähriger Berliner Antifaschist festgenommen, nachdem er von zwei Neonazis beschuldigt wurde, sie Ende November tätlich angegriffen zu haben.

15.12.: **Razzia gegen Skinheads:** In Baden-Württemberg werden 44 Objekte durchsucht sowie 277 Personen und 159 Fahrzeuge kontrolliert. Nach eigenen Angaben wollte die Polizei mit der Aktion der rechtsextremen Szene ihre Grenzen aufzeigen und die Verfestigung von Strukturen verhindern.

18.12.: **Idomeneo in Berlin störungsfrei aufgeführt:** Nach einer zwischenzeitlichen Absetzung der Mozartoper wegen befürchteter islamistisch motivierter Anschläge – der abgeschlagene Kopf des Propheten Mohammed wird in der Schlussszene gezeigt –, werden bei der Aufführung intensive Personen- und Taschenkontrollen durchgeführt. Etwa 150 PolizistInnen kommen zum Einsatz.

22.12.: **Verfahren gegen Kameradschaft eingestellt:** Wie die Staatsanwaltschaft Frankfurt mitteilt, reichen die bei Wohnungsdurchsuchungen im Oktober gefundenen Unterlagen nicht aus, um die rechtsextremen „Freien Nationalisten Rhein-Main“ als kriminelle Vereinigung einzustufen.
Suizide nicht mehr melden: Die Berliner Justizsenatorin Gisela von der Aue (SPD) kündigt an, Selbsttötungen in Berliner Haftanstalten zukünftig nicht mehr zu melden, um die Persönlichkeitsrechte der Gefangenen und ihrer Familien zu wahren. Mit zehn Suiziden von Häftlingen liegt die Zahl für das Jahr 2006 so hoch wie noch nie seit der Wiedervereinigung. Am 27.12. kommt es zu einem Anschlag auf den Amtsitz der Senatorin, der laut Bekennerschreiben im Zusammenhang mit ihrer Ankündigung steht.

28.12.: **Ermittlungen gegen Linksextremisten:** Nach zwei Anschlägen in Dessau und Wolfen in Sachsen-Anhalt ermittelt die Bundesanwaltschaft gegen zwei noch unbekannte Tatverdächtige wegen Mitgliedschaft in einer terroristischen Vereinigung.

Meldungen aus Europa

SIS II parlamentarisch abgesegnet

Einmal mehr hat sich das Europäische Parlament (EP) auf einen faulen Deal mit dem Rat eingelassen. Am 25. Oktober 2006 verabschiedete es in erster und einziger Lesung die Rechtsgrundlagen für das Schengener Informationssystem der zweiten Generation (SIS II). Vorausgegangen war ein „Trialog" hinter verschlossenen Türen zwischen VertreterInnen der Kommission, des Rates und des EP, darunter der Berichterstatter des Innen- und Bürgerrechtsausschusses, Carlos Coelho. Am 27. September erzielte man einen „Kompromiss", den das Parlamentsplenum einen Monat später ohne viel Federlesen absegnete.[1]

Anders als das bisherige SIS wird das SIS II nicht mehr durch die Mitgliedstaaten, sondern aus dem EU-Haushalt finanziert. Für den Betrieb der zentralen Einheit (C.SIS) ist vorerst die Kommission zuständig. Zu einem späteren Zeitpunkt soll eine „Agentur" sowohl die Verwaltung des C.SIS als auch des im Aufbau befindlichen Visa-Informationssystems und von Eurodac (Fingerabdrücke von Asylsuchenden) übernehmen. Mit dem jetzt vom EP angenommenen SIS II-Paket wird das System rechtlich sowohl in der ersten Säule der EU (Asyl, Einwanderung, Grenzen) als auch in der dritten (Polizei und Strafrecht) verankert. Die Verordnung „über die Einrichtung, den Betrieb und die Nutzung" des SIS II unterscheidet sich daher von dem gleichnamigen Ratsbeschluss nur in den Datenkategorien: Die Verordnung regelt die Ausschreibung von Nicht-EU-BürgerInnen zur Verweigerung von Einreise und Aufenthalt (bisher Art. 96 Schengener Durchführungsübereinkommen, SDÜ), der Beschluss bezieht sich auf die eigentlich polizeilichen Daten (Ausschreibungen zur Festnahme, Aufenthaltsermittlung, Beobachtung, Sachfahndung – bisher Art. 95, 97-100 SDÜ). Hinzu kommt eine weitere Verordnung (nach Titel V EG-Vertrag – Transport und Verkehr), die den Zugriff der Kfz-Zulassungsstellen auf Daten über gestohlene Fahrzeuge

1 EP: Berichte A6-0353/2006, A6-0354/2006, A6-0355/2006 v. 25.10.2006

ermöglicht. Für den Beschluss musste der Rat das Parlament nur konsultieren, für die beiden Verordnungen galt hingegen das Mitentscheidungsverfahren. Das EP war damit grundsätzlich in einer komfortablen Verhandlungsposition, die es allerdings nicht genutzt hat.

Erreicht hat es u.a. eine allerdings sehr verwässerte Informationspflicht der Behörden gegenüber Personen, die zur Einreise- bzw. Aufenthaltsverweigerung ausgeschrieben werden. Diese Pflicht gilt jedoch nicht, wenn die Daten hinter dem Rücken der Betroffenen erhoben wurden (d.h. in erster Linie, wenn Sicherheits- und nicht nur ausländerrechtliche Gründe für die Einreiseverweigerung ausschlaggebend sind) oder wenn die Information mit einem zu großen Aufwand verbunden wäre. Ferner wird die Kommission zu einer Aufklärungskampagne u.a. über die Rechte zur Auskunft über die gespeicherten Daten verpflichtet. Faktisch ist das Auskunftsrecht aber gerade bei den eigentlich polizeilich-strafrechtlichen Daten (Ausschreibungen zur Festnahme oder zur Beobachtung) nicht gegeben.

Akzeptiert hat das EP dagegen die Verlängerung der Ausschreibungsfristen, was automatisch zu einer Zunahme der im SIS gespeicherten Daten führen wird, die Verknüpfung von Datensätzen und den Einstieg in die biometrische Grenzkontrolle. Dass in den Personendatensätzen des SIS II auch biometrische Daten enthalten sein würden, war von Anfang an klar. Nach dem einschlägigen Artikel der Verordnung und des Beschlusses[2] soll die Speicherung von Fotos und Fingerabdrücken nur nach einer „speziellen Qualitätsprüfung" erlaubt sein. Das Verfahren muss allerdings noch festgelegt werden. Darauf wird das EP keinen Einfluss haben.

Umstritten war lange Zeit, wie diese Daten genutzt werden dürften. Der Kompromiss zwischen Rat und Parlament ist an diesem Punkt von kaum zu überbietender Komik. Unter Buchstabe b des Artikels heißt es hier zunächst: „Lichtbilder und Fingerabdrücke dürfen nur herangezogen werden, um die Identität einer Person zu bestätigen, die durch eine alphanumerische Abfrage im SIS II gefunden wurde." Anders ausgedrückt: Die kontrollierenden BeamtInnen fragen das SIS II nach wie vor nach dem Namen einer Person ab und können nur im Trefferfalle zusätzlich die Fingerabdrücke oder das Foto heranziehen. Das war die Forde-

2 Art. 14ac der Verordnung bzw. 14c des Berichts – jeweils nach der vorläufigen Nummerierung des EP

rung der Datenschutzbeauftragten. Unter Buchstabe c heißt es dann aber sogleich: „Sobald technisch möglich können Fingerabdrücke auch herangezogen werden, um Personen auf der Grundlage ihres biometrischen Identifikators zu identifizieren." Wer in Zukunft an einer polizeilichen Kontrollstelle an der Grenze oder im Inland angehalten wird, muss sich nicht wundern, dass man nicht seine oder ihre Papiere, sondern ihre Finger sehen will. Das Parlament hat erreicht, dass diese Funktionalität erst genutzt wird, wenn sie technisch möglich ist. Was für ein Erfolg!

Auf den in Art. 17 der Verordnung und Art. 37 des Beschlusses ursprünglich vorgesehenen Zugang der Geheimdienste zu den Daten des SIS II hat der Rat vorerst verzichtet. Die finnische Präsidentschaft hat aber bereits klargestellt, dass die Frage weiter zu prüfen und ein zusätzlicher Ratsbeschluss ins Auge zu fassen sei.[3] Zu diesem Beschluss wird das EP dann allerdings nur mehr konsultiert.

„SIS one4all"

Dank der Kompromissbereitschaft des Parlaments sind zwar die Rechtsgrundlagen für das SIS II pünktlich zustande gekommen. Die Pläne für seine Einführung und damit zusammenhängend für die Aufhebung der Kontrollen an den Grenzen zu und zwischen den im Jahre 2004 der EU beigetretenen Staaten können jedoch trotzdem nicht gehalten werden. Auf seiner Tagung am 4. und 5. Dezember 2006 beschloss der Rat der Innen- und Justizminister nun eine Zwischenlösung: Um die Aufhebung der Grenzkontrollen nicht übermäßig hinauszuschieben, sollen die neuen Mitgliedstaaten vorerst an das bestehende SIS angeschlossen werden.[4]

Nach der ursprünglichen Planung hätte das SIS II im März 2007 betriebsbereit sein und nach einer Evaluationsphase Ende Oktober 2007 – zeitgleich mit der Aufhebung der Binnengrenzkontrollen – ans Netz gehen sollen. Schon seit Monaten waren Verzögerungen offensichtlich. Rechtsstreitigkeiten über die Auftragsvergabe für das neue System führten dazu, dass die Kommission die Arbeiten zeitweilig einstellen musste.

3 Ratsdok. 14490/06 v. 30.10.2006

4 Schlussfolgerungen des Rates über die Erweiterung des Schengen-Raumes, Ratsdok. 15801/06 v. 4./5.12.2006, S. 13-16

Hinzu kamen technische Probleme mit der Kommunikationsinfrastruktur für das SIS II.

Im Oktober präsentierte das portugiesische Innenministerium eine Durchführbarkeitsstudie für eine erneute Ausdehnung des bestehenden Systems unter dem Titel „SIS one4all“.[5] Danach soll das SIS I wie schon beim Anschluss der nordischen Staaten im Jahre 1998 erneut aufgerüstet werden. Diese technischen Voraussetzungen will der Rat bis Juni 2007 geschaffen haben. Ab Januar 2008 sollen dann die Kontrollen an den Land- und Seegrenzen fallen. Ab Ende März soll dasselbe für die EU-Binnenflüge gelten. Voraussetzung bleibt jedoch, dass die nicht mehr ganz so neuen EU-Staaten in der Evaluationsphase in der zweiten Jahreshälfte 2007 beweisen, dass sie den Schengener Besitzstand voll und ganz umsetzen und d.h. vor allem die Außengrenzen der EU nach dem bekannten rigiden Muster kontrollieren können.

Die Ausdehnung des SIS I sei eine einfache und günstige Variante, behauptet das portugiesische Innenministerium. Die Aufrüstung der zentralen Infrastruktur (C.SIS) wird rund sechs Millionen Euro kosten. Das bestehende SIS wird jedoch nicht aus dem EU-Haushalt, sondern noch von den Mitgliedstaaten finanziert. Die neuen Schengen-Staaten müssen sich beteiligen. Sie haben nicht nur ihre Anteile am C.SIS, sondern darüber hinaus auch ihre nationalen SIS-Komponenten zu zahlen. Der Preis für die im Schengener Rahmen ohnehin nur begrenzte Aufhebung der Kontrollen wird für sie daher erheblich höher sein, als für die alten Mitgliedstaaten.

Die Einführung des SIS II wird sich durch die Zwischenlösung weiter verzögern. Inoffiziell ist nun von einem Termin im Jahre 2009 die Rede.[6]
(beide: Heiner Busch)

5 Ratsdok. 13540/06 v. 12.10.2006
6 www.networld.at/articles/0649/15/15498.shtml/print

Literatur

Zum Schwerpunkt

Sicherheitsbehörden können ohne den Umgang mit Informationen nicht arbeiten. Das gilt für die geheimen Nachrichtendienste, die nach herrschender Lesart exklusive Informationen beschaffen, auswerten und vornehmlich die Regierungen mit derartig gewonnenen Erkenntnissen versorgen sollen. Das gilt aber auch für die Polizeien, die ohne Informationen weder abzuwehrende Gefahren zur Kenntnis nehmen noch Straftaten aufklären könnten. Im Informationszeitalter hat sich nicht nur die Bedeutung von Informationen für die Sicherheitsbehörden erhöht, zugleich hat das Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 bewirkt, dass der Schutz personenbezogener Daten Anlass und Gegenstand umfangreicher gesetzgeberischer Reaktionen wurde. Als Folge der verfassungsrechtlichen Vorgaben ist der Umfang der Polizeigesetze seit den 1980er Jahren erheblich gewachsen; und jede neue Technik, jede neue polizeiliche Maßnahme wird im Hinblick auf ihre Folgen für den Datenschutz diskutiert und ggf. auf eine gesetzliche Basis gestellt. Das Sicherheitsrecht ist derart über weite Strecken zu einem Informationsrecht unter der Fahne des Datenschutzes geworden.

Eine aktuelle monografische Darstellung des Datenschutzes im Sicherheitsbereich sucht man vergebens; kein Weg führt deshalb an den einschlägigen Kommentaren des Polizei- und Strafprozessrechts vorbei. (Ein Kommentar zum Recht der Geheimdienste steht seit Ende der 80er Jahre aus!) Die fachliche und wissenschaftliche Öffentlichkeit ist mit der Erörterung der jüngeren Rechtsprechung des Bundesverfassungsgerichts – namentlich zum Großen Lauschangriff und zum Niedersächsischen Sicherheits- und Ordnungsgesetz – sowie den Folgen moderner, meist technikgestützter polizeilicher Instrumente befasst. Neben den Dauerbrennern der Telefonüberwachung – einschließlich „stiller SMS“ und Standortortung – oder der Speicherung von DNA-Daten stehen gegenwärtig die Vorratsdatenspeicherung, die Weitergabe von Fluggastdaten an die USA, die Nutzung der Kfz-Kennzeichen-Erfassung für polizeiliche Zwecke an der Spitze der Debatte.

Der Bundesbeauftragte für den Datenschutz: *Tätigkeitsbericht 2003-2004 – 20. Tätigkeitsbericht –, Bonn 2005 (BT-Drs. 15/5252 v. 19.4.2005; www bfdi.bund.de)*

Die Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten sind eine Fundgrube für alle, die sich über die Entwicklung des Datenschutzrechts und über die Praxis des Datenschutzes in Deutschland informieren wollen. Soweit ersichtlich fehlt es sowohl an einer systematischen Aufbereitung der Berichte (allein in Hessen sind bislang 34 Berichte erschienen) als auch an einer Untersuchung der Wirksamkeit datenschützerischer Interventionen. Stellvertretend für die Arbeit des institutionalisierten Datenschutzes soll an dieser Stelle ein Blick auf den jüngsten Bericht des Bundesbeauftragten geworfen werden.

Der Bericht umfasst 247 Seiten; die Seiten 52 bis 76 gelten dem Thema „Innere Sicherheit". Nach einer „Neue Sicherheitsarchitektur" überschriebenen Einleitung werden aktuelle Datenschutzfragen der einzelnen Sicherheitsbehörden des Bundes dargestellt: Bundeskriminalamt (BKA), Bundespolizei (damals noch „Bundesgrenzschutz"), Zoll sowie Bundesamt für Verfassungsschutz, Militärischer Abschirmdienst und Bundesnachrichtendienst. Die Tätigkeiten des Beauftragten bestehen in Stellungnahmen zu und Beteiligungen an einzelnen Gesetzgebungsvorhaben sowie in Überprüfungen behördlicher Praktiken.

Die Stellungnahmen zum Gesetzgebungsverfahren beziehen sich zum einen auf anstehende Novellierungsvorschläge (Folgen verfassungsgerichtlicher Urteile, Kfz-Kennzeichen-Scan), zum anderen auf Regelungen, die im Berichtszeitraum bereits verabschiedet wurden. Hierzu zählen die Novellierungen des Bundesgrenzschutz- und des Außenwirtschaftsgesetzes und das Luftsicherheitsgesetz. Inhaltlich erschöpft sich die Rolle des Bundesdatenschutzbeauftragten – und seiner KollegInnen aus den Ländern, auf die Entschließungen der Konferenz der Datenschutzbeauftragten wird mehrfach verwiesen – darin, die Belange des Datenschutzes anzumahnen. Dies bedeutet etwa im Hinblick auf die jetzt realisierten Pläne, gemeinsame Dateien von Polizei und Nachrichtendiensten zu schaffen, dass Datenerhebung und -weitergabe an die Aufgaben der Behörden geknüpft werden sollen, dass die Zweckbindung der Daten „strikt" zu wahren sei, dass Protokollierungen für alle Zugriffe auf die Daten vorzuschreiben und dass Auskunftsrechte der Betroffenen „uneingeschränkt zu gewährleisten" seien. Ähnlich ist die Stellungnahme zur Kfz-Kennzeichenerfassung. In der im Bericht zitierten Entschließung der Datenschutzbeauftragten wird der „Sorge" Ausdruck

verliehen, dass „sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln könnte“. Dies führt jedoch nicht zur Ablehnung des automatisierten Kennzeichen-Scans; auch wenn unkommentiert bemerkt wird, „dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen“. Vielmehr wird darauf hingewiesen, dass der Abgleich einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Sofern gesetzliche Regelungen geschaffen würden, müsse „auf jeden Fall ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird“. Im Rahmen von Gesetzgebungsverfahren warnen und mahnen die institutionalisierten Sachwalter des Datenschutzes; in konkreten Fragen bleibt Umfang und Reichweite ihrer Kritik auf die strikte Beachtung datenschutzrechtlicher Standards beschränkt.

Aus dem Bericht ergeben sich auch Hinweise auf die Bedeutung des Amtes des Datenschutzbeauftragten. Im Berichtszeitraum wurde das Bundesgrenzschutz-Gesetz verlängert, weil die 1998 geschaffene erweiterte Befugnis zu verdachts- und ereignisunabhängigen Kontrollen Ende 2003 ausgelaufen wäre. Im Hebst 2003 ersuchte der Bundesbeauftragte das Innenministerium mehrfach um Beteiligung an einer eventuell geplanten Novelle. Diese Anfragen blieben zunächst unbeantwortet. Erst einen Tag vor der abschließenden Beratung der Novelle im Bundestag wurde dem Bundesbeauftragten der Bericht über die Erfahrungen mit den BGS-Kontrollen zugeleitet. Die Befugnis wurde ohne seine Beteiligung bis Mitte 2007 verlängert; erneut wurde eine Evaluierung der Maßnahme vorgeschrieben. Der Bundesbeauftragte hofft, „an der Evaluation diesmal rechtzeitig beteiligt“ zu werden. Bei anderen Vorhaben wurde er „von Beginn an beteiligt“. Etwa bei der Novellierung des Außenwirtschaftsgesetzes (AWG), die durch den Beschluss des Bundesverfassungsgerichts vom März 2004 notwendig geworden war. Inhaltlich bemängelt der Bericht, dass die Neuregelung den Kernbereich privater Lebensgestaltung nicht ausreichend schütze. Wegen dieses Mangels war das Gesetz bis Ende 2005 befristet worden – was der Datenschutzbeauftragte „ausdrücklich“ begrüßt. (Im nächsten Bericht wird er dazu Stellung nehmen müssen, dass das AWG Ende 2005 unverändert verlängert wurde!)

Interessanter als die Rolle des Datenschutzbeauftragten im Gesetzgebungsverfahren sind die Hinweise, die der Bericht auf den Stand polizeilicher Datenverarbeitung enthält. Leider fehlt ein systematischer

Überblick über die bei den Polizeien gebräuchlichen Datenverarbeitungsprogramme und Dateien. Der Bericht des Bundesbeauftragten gibt aber immerhin einen Einblick in einige Praktiken bzw. Entwicklungen. Im Bereich des BKA etwa wurden die Dateien zur Geldwäschebekämpfung kontrolliert. Das BKA führt zum einen die Verbunddatei „Geldwäsche", in der sämtliche auf Verdachtsanzeigen beruhende Informationen eingestellt werden. Zum anderen führt das BKA die Datei „FIU" (für „Finance Intelligence Unit"), die Analysezwecken und dem Datenaustausch mit dem Ausland dient. Der Bericht kritisiert, dass in der „Geldwäsche"-Datei die Daten Verdächtiger auch dann nicht gelöscht werden, wenn über sie keine (weiteren) Erkenntnisse vorliegen. Es ist ihm lediglich gelungen, die Speicherungsdauer für diese Fälle auf vier Jahre zu begrenzen. Zum Vorhaben des BKA, beide Dateien zusammenzufügen, steht eine abschließende Stellungnahme des Datenschutzbeauftragten aus.

Im Hinblick auf „INPOL-neu" will er die weitere Entwicklung „sorgfältig begleiten und darauf achten, dass der gesetzliche Rahmen ... beachtet wird." Seine Sorge äußert der Bericht über die Schaffung „schlafender Bestände" von DNA-Identifizierungsmustern, die die Innenministerkonferenz im November 2004 befürwortet hat. Beim „schlafenden Bestand" handelt es sich um DNA-Informationen, die nach Ablauf der allgemeinen Aussonderungspflichten gelöscht werden müssten, aber stattdessen in einen „gesonderten Recherchepool" überführt werden. Die Innenminister ließen sich von der Argumentation des Datenschutzbeauftragten, dass ein „schlafender Bestand" nicht erforderlich sei, nicht überzeugen.

Einen kleinen Erfolg meldet der Bericht bei den „Auswertedateien" des BKA. Nach der Kritik im vorherigen Tätigkeitsbericht und einem „Beratungs- und Kontrollbesuch" im BKA wurde die Datei „Global" gelöscht. In der Datei sollten Informationen über gewalttätige Aktionen und andere Straftaten militanter Globalisierungsgegner gespeichert werden. Die Kontrolle des Datenschutzbeauftragten ergab, dass sich „die Polizeirelevanz einzelner Daten allein daraus (ergab), dass diese von Polizeidienststellen des In- und Auslandes stammten". So waren Daten von TeilnehmerInnen an und AnmelderInnen von Protestveranstaltungen gespeichert worden, ohne dass es zu strafrechtlichen Ermittlungen gekommen war. Obgleich die Datei „Global" gelöscht wurde, besteht das generelle Problem der „Auswertedateien zur Erkenntnisgewinnung" fort,

das der Bundesbeauftragte im Fehlen einer „normenklare(n) Rechtsgrundlage“ sieht.

Der Bericht gibt auch Hinweise auf den Stand der Datenverarbeitung bei den anderen Sicherheitsbehörden des Bundes: Der Bundesgrenzschutz entwickelte das Projekt PAVOS (Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem), das die bundesweite Online-Recherche im gesamten Bestand ermöglicht, der sich aus den „Elektronischen Tagebüchern“ der BGS-Dienststellen speist. Der Zoll unterhält eine eigene Geldwäschedatei mit mindestens sechsjähriger Speicherungsdauer. Das nachrichtendienstliche Informationssystem „NADIS“ soll auch für Informationen der Verfassungsschutzämter über „Organisierte Kriminalität“ genutzt werden. Beim Bundesamt für Verfassungsschutz wird die Einführung der „Elektronischen Akte“ vorbereitet. Der Militärische Abschirmdienst hat weiterhin Zugriff auf das Personalführungs- und Informationssystem der Bundeswehr (was der Bericht für unzulässig hält). Und der Forderung, einen behördlichen Datenschutzbeauftragten für den MAD zu bestellen, wurde bislang nicht entsprochen – wie gesagt, eine Fundgrube für alle Interessierten.

Rena Tangens; padeluun (Hg.): *Schwarzbuch Datenschutz. Ausgezeichnete Datenkraken der Big Brother Awards, Hamburg (Edition Nautilus) 2006, 192 S., EUR 13,90*

Seit dem Jahr 2000 werden auch in der Bundesrepublik die „Big Brother Awards“ verliehen, mit denen Vorreiter von Überwachungstechniken und Überwachungsstaat ausgezeichnet werden. Der vorliegende Band versammelt eine Auswahl der Preisreden aus den ersten sechs Jahren; er gibt damit zugleich einen Einblick in die sich entwickelnde Überwachungskultur in Deutschland. In den vielen der mittlerweile sieben Preiskategorien tauchen immer wieder Akteure und Institutionen der Inneren Sicherheit auf: vom Berliner Innensenator Eckart Werthebach, dem der Preis in der Kategorie „Politik“ im Jahr 2000 exemplarisch für die Investitionen zur Telefonüberwachung zugesprochen wurde, über das BKA, das wegen seiner Präventiv-Dateien 2002 mit dem Preis für „Behörden und Verwaltung“ geehrt wurde, bis zum rot-grünen Innenminister Otto Schily, der den Preis 2005 für sein „Lebenswerk“ erhielt. Die vielen anderen Preisträger zeigen aber zugleich, dass keineswegs nur staatliche ÜberwacherInnen am Werke sind.

(sämtlich: Norbert Pütter)

Sonstige Neuerscheinungen

Oschmann, Frank: *Die Finanzierung der Inneren Sicherheit am Beispiel von Polizei und Sicherheitsgewerbe, Köln, Berlin, München (Carl Heymanns Verlag) 2005, 381 S., EUR 108,–*

„Ohne Fleiß kein Preis", weiß der Volksmund, und der hier vorgelegte Band verbindet das Credo dieses unreinen Binnenreims aufs Vortrefflichste, handelt es sich doch bei dieser juristischen und rechtspolitischen Abhandlung zu Finanzierungsmöglichkeiten polizeilicher und sicherheitsgewerblicher Tätigkeiten um eine mehrere hundert Seiten umfassende Fleißarbeit, und es sind die 108 Euro für diesen Band, die seinen Kauf zu einer echten Preisfrage machen. Um es vorweg zu nehmen, eine lohnende Investition ist die als Dissertation vom Fachbereich Rechtswissenschaft der Universität Hamburg angenommene Schrift nicht.

In vier Teilen legt die Arbeit zunächst knapp die Finanzierung von Polizei und Sicherheitsgewerbe als Rechtsproblem dar (Teil 1), beschreibt sodann die bisherige und zukünftige Finanzierung der Polizei in der Bundesrepublik (2) und befasst sich mit der Finanzierung des privaten Sicherheitsgewerbes, die sowohl in Hinblick auf private Auftraggeber wie auf die Einbeziehung durch die öffentliche Hand untersucht wird (3). Im vierten Teil wird schließlich das Ergebnis der Arbeit mit „50 Thesen zur Finanzierung der inneren Sicherheit" zusammengefasst.

Nachdem sich Oschmann, der vor wenigen Monaten bereits im Alter von 30 Jahren an einer schweren Krankheit gestorben ist, mit den Hauptfinanzierungsformen der Polizeiarbeit – Steuerfinanzierung und Polizeikostenrecht – sowie im letzteren Fall mit deren Anwendungsfällen auseinandergesetzt hat (Großveranstaltungen, Demonstrationen, Hausbesetzungen, Abschleppen/Umsetzen von Kraftfahrzeugen, Luftsicherheitsgebühr), geht er auf weitere (nicht) mögliche Polizeifinanzierungsformen ein. Detailliert setzt er sich mit der Finanzierung des Bahnschutzes durch die Bundespolizei auseinander (S. 157 ff.). Er entwickelt sodann Grundzüge einer künftigen Polizeifinanzierung (S. 183 ff.), zu der er in Sonderheit die finanzielle Beteiligung von kommerziellen Veranstaltern an den Polizeikosten rechnet (Love Parade), während er „aus rechtspolitischen Gründen" eine Polizeikostenerhebung bei nichtkommerziellen Veranstaltungen – wiewohl möglich – für nicht opportun hält. Beim Schutz von Atommüll-Transporten sieht er die Möglichkeit einer stärkeren Kostenbeteiligung der Kraftwerksbetreiber, nicht jedoch mit Blick auf die damit in Zusammenhang stehenden Kosten wegen der

Demonstrationen gegen diese Transporte, denn diese seien „eine politisch zu behandelnde Aufgabe“ (S. 211). Erträge aus der verstärkten Bestreifung von Wohngebieten schließt Oschmann aus, „in Einkaufspassagen bzw. Energieanlagen“ (S. 230) seien sie jedoch rechtlich möglich, bisher fehle es an der Nachfrage. Zudem schlägt er die Schaffung einer Veranstaltungskostenverordnung vor, die über eine Umlagefinanzierung „Zeit- und Kilometergebühren … sowie eine Rahmengebühr“ (S. 247) umfassen solle. Schließlich favorisiert er das Polizeisponsoring als weitere Einnahmequelle (S. 248 ff.), bevor er sich – nach Würdigung EU-rechtlicher Aspekte – der finanziellen Inanspruchnahme kommerzieller Sicherheitsdienste zuwendet.

Eine informelle Indienstnahme des Sicherheitsgewerbes durch die Polizei hält Oschmann für rechtlich möglich, doch sei dies „rechtspolitisch derzeit abzulehnen“ (S. 301), weil eine entsprechende Normierung kontraproduktiv auf die Motivation wirken und – bei etwaigen Prämienzahlungen – eine „Kopfgeldjäger-Mentalität“ fördern könnte; insoweit sei der „Ausbau der freiwilligen Kooperationsmodelle“ zu bevorzugen (S. 300); schließlich sieht der Autor rechtlich die Möglichkeiten für die Aufgaben- und Abgabenbeleihung der kommerziellen Sicherheitsdienste etwa bei Großveranstaltungen und Verkehrskontrollen gegeben und begrüßt sie als „rechtspolitisch sinnvoll“ (S. 319), zumal, wie er bereits zu Beginn des Buches schreibt, „der Tätigkeit privater Sicherheitsdienste eine staatsmonetäre Bedeutung“ im Präventionsstaat zukommt (S. 7). Mit dieser Orientierung auf die weitere Integration des kommerziellen Sicherheitsgewerbes in die Gewährung innerer Sicherheit liegt der Autor auf der Linie der vom kommerziellen Sicherheitsgewerbe geschaffenen Forschungsstelle Sicherheitsgewerbe an der Universität Hamburg – seinem bisherigen Wirkungsort.

Insgesamt plädiert Oschmann für eine stärkere Einbeziehung des kommerziellen Sicherheitsgewerbes und eine intensivierte Nutzerfinanzierung, zu der er im Besonderen die Aufnahme von Bagatellschäden im Straßenverkehr und die Nutzung von Autobahnen rechnet. Die Steuerfinanzierung der Polizei „könnte und sollte“ durch eine Umlagefinanzierung ergänzend in Angriff genommen werden und dabei vor allem „besonders gewinnträchtige Veranstaltungen“ in den Blick nehmen (S. 326). Zur Durchsetzbarkeit seiner Vorschläge sagt Oschmann relativ wenig, auch empirische Daten, die etwa fiskalische Effekte zumindest skizzieren, fehlen vollständig. Eine kritische Würdigung der Handlungslogik von kommerziellen Dienstleistern – namentlich deren Profitorien-

tierung – im Unterschied zu der der Polizei unterbleibt zugunsten der einfachen Feststellung, diese seien von „stetig steigender Bedeutung" (S. VII). Eine detaillierte rechtliche Würdigung, aber kein rechtspolitisch-kritischer Beitrag zur Diskussion.

Jones, Trevor; Newburn, Tim (eds.): *Plural Policing. A comparative perspective, Oxford (Routledge) 2006, 242 S., £ 24,50*

In den vergangenen rund 30 Jahren haben weltweit die Polizeien neue Kollegen hinzugewonnen, die entweder als lokale Polizei- oder Ordnungsamtskräfte, vor allem aber als kommerzielle Sicherheitsdienste in Erscheinung treten und bei der Produktion von Sicherheit und Ordnung eine zunehmend wichtige Rolle spielen. Sozialwissenschaftliche Aufmerksamkeit hat diese Entwicklung vor allem in den angelsächsischen Ländern unter dem Oberbegriff „Pluralization" gefunden – mithin in jenen Staaten (USA, Kanada und Großbritannien), die als am weitesten entwickelte kapitalistische Länder gelten. Pluralization meint dabei zunächst das exorbitante Wachstum des privaten Sicherheitsgewerbes neben der staatlichen Polizei; der Begriff verweist aber auch auf die Kommodifizierung der Sicherheitsproduktion insgesamt, die auf den Bedeutungsgewinn von Management-Logiken in Polizeiapparaten hinweist, auf einen Konsum-Begriff bei der Gewährung von Sicherheit verweist („Der Bürger als Kunde, der Beamte als Dienstleister") und eine werbende Komponente enthält (Marketing, „Das Produkt Sicherheit").

Dass diese Prozesse – ergänzt um Trends zu stärkerer Bürgerbeteiligung, die Verpolizeilichung weiterer staatlicher Verwaltungstätigkeiten und auch den Rückzug von besser situierten Teilen der Bevölkerung in gated communities (und quasi unter CCTV-Kameras) – sich weltweit finden, zeigen die Herausgeber in diesem Sammelband und verdeutlichen, dass es sich um „broad structural forces" (S. 9) handelt, die hier am Werke sind, die aber zugleich in „local political cultures" (S. 9) eingebunden bleiben und von ihnen überformt werden. Erstmals liegt hier ein Band vor, der sich der Pluralisierung von Sicherheits- und Ordnungsproduktion über das kommerzielle Sicherheitsgewerbe hinaus in komparativer Perspektive widmet.

Die Herausgeber konzentrieren sich auf Großbritannien, das mit seinen Neighbourhood Wardens und Police Security Officers sowie einer Vielzahl von privaten Sicherheitsdiensten eines der ausdifferenziertesten Systeme pluraler Polizeipraktiken aufweist. Beiträge über die Niederlande (van Stedten/Huberts), Frankreich (Ocqueteau) und Griechenland

(Papanicolaou) beschließen den europäischen Block, der mit den USA (Manning), Kanada (Rigakos/Leung), Brasilien (Wood/Cardia), Australien (Prenzler/Sarre), Südafrika (Shearing/Berg) und Japan (Yoshida/Leishman) dokumentieren die globale Dimension des Pluralisierungsprozesses. Plausibilisiert wird diese Länderauswahl freilich nicht, und das Fehlen von wenn schon nicht Deutschland, so doch der skandinavischen Länder und Osteuropas irritiert, selbst wenn man, wie die Herausgeber, in Rechnung stellt, dass ein „general lack of foreign language skills" (S. 2) ein Problem darstellt.

Die Herausgeber verzichten ebenso auf ein Nachwort wie auf eine Einordnung der dargelegten Entwicklungen in Prozesse der Globalisierung oder Neoliberalisierung. Vielmehr werfen sie vorsichtig Fragen nach der Zukunft des staatlichen Gewaltmonopols auf, das in einigen Ländern (Brasilien, Südafrika) wohl ohnehin als eher schwach ausgeprägt gelten muss; sie stellen Beziehungen zwischen dem subjektiven (Un)Sicherheitsgefühl in der Bevölkerung und dem Bestreben staatlicher Akteure her, die ihre Verwaltungen von der Produktion von Sicherheit – vor allem der öffentliche Raum ist hier von Bedeutung – durch die Beteiligung kommerzieller Sicherheitsdienste mal mehr (USA, Großbritannien) und mal weniger (Japan, Griechenland) „entlasten" wollen. Das Beispiel Japan (S. 222-238) zeigt, dass die Beteiligung der Dienste ein Mehr an Arbeit für die staatlichen Polizeistellen gebracht hat. Deutlich wird an den Fallstudien auch, dass das kommerzielle Sicherheitsgewerbe bei der Markteroberung in einigen Ländern „erfolgreicher" agiert (Kanada, USA), als dies in anderen (Frankreich) bisher der Fall ist.

Was die empirische Würdigung des Pluralisierungsprozesses mit Blick auf Bürgerbeteiligungsmodelle, die Integration von Beschäftigungsprojekten für Erwerbslose und lokale Sicherheits- und Ordnungskonzepte angeht, bietet der Band sehr gute (Niederlande, Großbritannien), aber auch schwache Überblicksbeiträge (Frankreich); nicht alle Autoren haben das Ziel des Sammelbandes, „[to] summarize the latest empirical material to illustrate and inform current debates about trends in policing" (S. 3) wirklich einlösen können. Was die angekündigte komparative Perspektive anbetrifft, betonen die Autoren neben der Fremdsprachenproblematik die nur wenig vergleichbaren Datengrundlagen (S. 3). Sie haben aber andererseits keinen Versuch unternommen, das hier ausgebreitete Material mit diesen Einschränkungen – und bei aller Vorsicht – in einem abschließenden Kapitel vergleichend so zu würdigen, dass die von ihnen angesprochenen „commonalities" zwi-

schen den Ländern ebenso herausgearbeitet würden wie die „countervailing trends“ (S. 10). Diese Aufgabe, so scheint es, haben sie, wie die Suche nach „sites of political and social resistance“ (S. 10) bewusst und zunächst den lesenden Kollegen übertragen. Der Band ist dafür allemal ein guter Anfang – und eine lesenswerte Grundlage.
(beide: Volker Eick)

Bosold, Christiane: *Polizeiliche Übergriffe. Aspekte der Identität als Erklärungsfaktoren polizeilicher Übergriffsintentionen, Baden-Baden (Nomos Verlagsgesellschaft) 2006, 211 S., EUR 32,–*
Endlich auch für Deutschland einmal eine wissenschaftliche Studie zu polizeilichen Übergriffen. Das klingt gut für die Arbeit von Menschen- und Bürgerrechtsgruppen, vielleicht sogar für die Polizei selbst – zumindest für etliche der inzwischen neu herangewachsenen progressiveren PolizeiführerInnen. Doch was die Nachwuchswissenschaftlerin Christiane Bosold mit ihrer Dissertationsschrift vorgelegt hat, ist für deren Alltagsarbeit schlichter Murks. Im Rahmen eines Forschungsprojektes des „Kriminologischen Forschungsinstituts Niedersachsen“ mit Unterstützung des niedersächsischen Innenministeriums wurden dabei insgesamt 2.800 PolizistInnen zur Mitarbeit ausgewählt; von den 1.706 zurückgesandten Fragebögen waren immerhin 1.674 auswertungsfähig (S. 113 ff.). Ein Rücklauf von rund 61 % ist eine äußerst gute Quote, dies weiß jeder, der jemals Ähnliches versucht hat. (Ob’s am Ministerium lag?) Jedenfalls hätte daraus etwas werden können – selbst wenn die Mehrheit der Befragten die Frage nach der Beteiligung oder Beobachtung von Übergriffen nicht beantwortet hat. Auch das sagt ja viel. Doch was macht die Autorin daraus! In ellenlangen, schwerverständlichen Kapiteln erläutert sie ihr Vorgehen sowie ihr „experimentelles Forschungsdesign“ (S. 99 ff.) und diskutiert mögliche Erklärungsmuster (S. 57-98).

Insgesamt erfährt man nichts Neues, außer dass sich polizeiliches Gewaltverhalten aus der Gruppenzugehörigkeit und dem individuellen Selbstwertgefühl entsprechend Faktor „r.33“ ergibt. Danke, das hilft wirklich weiter. Unterm Strich liest sich das Werk eher wie die Rechtfertigungsschrift eines vom Anwalt eines angeklagten Polizeibeamten beauftragten Gutachters. Nein!! Noch schlimmer: Es ist ein Übergriff auf alle, die sich ernsthaft mit Polizeigewalt auseinandersetzen (müssen). Allein das Buch zu lesen, bereitet körperlichen Schmerz.
(Otto Diederichs)

Aus dem Netz

www.datenschutz.de

Wer sich über den Datenschutz (in Deutschland) informieren will, sollte den Einstieg über dieses Portal wählen. Es wird von den Datenschutzbeauftragten des Bundes und der Länder sowie einiger in- und ausländischer Partner betrieben. Zugänglich über das Portal sind nicht nur die Beschlüsse der Konferenzen der Datenschutzbeauftragten (seit 1992), sondern auch Features zu aktuellen Themen (gegenwärtig z.B. „Flugdaten-Affäre“ und „RFID“ oder die Data mining Projekte der USA), (eher bescheidene) Literaturhinweise sowie über direkte Links die Homepages der Beteiligten und damit deren Stellungnahmen, Tätigkeitsberichte und sonstige Dokumente. Die Unterlagen sind über die Suchfunktionen des Portals unmittelbar recherchierbar. Wegen der Doppelfunktion als Informationsfreiheitsbeauftragte (im Bund und in einigen Ländern) gibt die Seite auch Auskunft über den Stand der Informationsfreiheit.

www.epic.org.privacy

Das Electronic Privacy Information Center (EPIC) bietet nicht nur umfassende Informationen über Datenschutzprobleme, die in den USA politisch diskutiert werden – vom Umgang mit KonsumentInnendaten über RFID-Tags bis hin zu den Überwachungsprogrammen im Bereich Antiterrorismus. EPIC ist auch eine der besten Quellen für Fragen des transatlantischen Datenverkehrs und deren Regelung durch die EU und die USA (Fluggastdaten etc.).

www.privacyalliance.com

Wer sich darüber informieren will, was die Soft- und Hardwareindustrie über „privacy“ zu sagen hat, der oder die kann sich bei der „online privacy alliance“ informieren, in der sich von Microsoft über Nestlé bis hin zur Filmindustrie alle finden, die ein kommerzielles Datenschutzinteresse haben. Zu Fragen des Datenschutzes im Sicherheitsbereich äußert sich diese Allianz jedoch nur selten.
(Albrecht Funk, Norbert Pütter)

Summaries

Helpless data protection

by Heiner Busch

Since the 1980s, Germany has been experiencing a spiral of legalisation regarding the methods and technical instruments of police and security services. The result is not the definition of clear norms limiting state surveillance, but rather a rhetoric of data protection law. Illusions about the effect of the Rule of Law, individualising concepts and depoliticisation have turned data protection into a legitimising accessory.

Data protection in the security sector

by Thilo Weichert

Considering the constant extension of police and secret service remits, data protection can be unexpectedly effective in the security sector. This is not only due to the decisions of the Federal Constitutional Court, but also because sensible police and security representatives have ceased to question the importance of data protection.

Proposed law on the retention of traffic data

by Mark A. Zöller

The conflict about the retention of so-called "communications traffic data" on citizens' telecommunication behaviour and about the use of these data for criminal prosecution has entered the second round. On 8 November 2006, the federal justice minister published a draft proposal which, amongst other things, is supposed to implement the EU Directive of March 2006.

Draft proposal on use of undercover police methods in criminal proceedings

by Norbert Pütter

In November 2006, the federal justice ministry presented the long-awaited amendment act of the criminal procedures law, which is to re-

form undercover investigation methods and particularly the surveillance of telecommunications. By trying to provide a sound legal basis for secret police work, it will contribute to its extension.

Green party proposes surveillance of telecommunications law

by Norbert Pütter

The draft proposal of the Green Party of December 2006 has surprising similarities with the government's proposal (see above), but it explicitly claims to achieve a reduction in the number of interceptions. Instead of using the current list of crimes that automatically legitimise surveillance, the Greens are proposing to rewrite it. This draft cannot be expected to achieve its proclaimed aim, either.

Extremism by association and the "right to know"

by Udo Kauß

For ten years now, Rolf Gössner, publicist, lawyer and president of the Human Rights League (Liga für Menschenrechte) has been arguing with the Federal Office for the Protection of the Constitution (internal security service) about his right to receive information about the collection of his personal data and if this data collection was legal. The Federal Office concedes that Gössner was not a "left-wing extremist". However, in its 36 years of observation, it has nevertheless collected a lot of data on him and it refuses to disclose the really interesting data to him.

EU framework decision on data protection

by Tony Bunyan

The EU is currently working on a framework decision to regulate data protection in police and judicial cooperation. However, because the discussion is taking place in a climate that is determined by the "war on terror", citizens' rights are again subordinated to the wishes of criminal prosecution. The proposal aims to do away with any obstacles to the mutual access to Member States' police data (principle of availability) or the data exchange between the EU and its befriended authorities in countries such as the US.

Common databases for police and secret services

by Heiner Busch

Seventeen years after the separation of the state security division of the Federal Crime Police Authority (Bundeskriminalamt – BKA) from the intelligence information system of the German internal secret service (Bundesamt für Verfassungsschutz – BfV), the parliament has decided to reunite the police with the secret service at the information technology level. The law, passed on 1 December 2006, establishes an "anti-terror" database, to be accessed by secret services, the BKA and other police stations. Further, police and secret services will work closely together in analysis projects, using so-called working data.

Police and secret service against immigrants

by Mark Holzberger

In the fight against unlawful immigration, or rather, foreign "terrorist suspects", police and security services have been working together closely for some time now. At the regional and national level, working groups are explicitly using the deportation and surveillance powers they were given by the new immigration law. In May 2006, the interior ministry has created yet another tool in the fight against immigrants, the common analysis and strategy centre on illegal migration (Gemeinsames Analyse- und Strategiezentrum illegale Migration – GASIM).

Anti-Terrorism Amendment Act

by Heiner Busch

The security authorities will continue to be able to demand information from banks, airlines and telecommunication providers. On 1 December 2006, the Lower House of German parliament renewed the powers it had given the services five years ago.

Bremen's police methods

by Helmut Pollähne

At a police action during the street party "Schanzenstraßenfest" in Hamburg on 9 September 2006, a police unit from Bremen achieved claim to fame by not only shackling the arrested demonstrators but also "disorientating" them, forcing them to wear shaded glasses until their transportation to detention.

Summaries

Helpless data protection

by Heiner Busch

Since the 1980s, Germany has been experiencing a spiral of legalisation regarding the methods and technical instruments of police and security services. The result is not the definition of clear norms limiting state surveillance, but rather a legal rhetoric of data protection. Illusions about the effects of legal regulation, individualising concepts and depoliticisation have turned data protection into a legitimising accessory.

Data protection in the security sector

by Thilo Weichert

Considering the constant extension of police and secret service remits, data protection can be unexpectedly effective in the security sector. This is not only due to the decisions of the Federal Constitutional Court, but also because sensible police and security representatives have ceased to question the importance of data protection.

Proposed law on the retention of traffic data

by Mark A. Zöller

The conflict about the retention of so-called "traffic data" on citizens' telecommunication behaviour and about the use of these data for criminal prosecution has entered the second round. On 8 November 2006, the federal justice minister published a draft proposal which, amongst other things, is supposed to implement the EU Directive of March 2006.

Draft proposal on use of undercover police methods in criminal proceedings

by Norbert Pütter

In November 2006, the federal justice ministry presented the long-awaited amendment act of the criminal procedures law, which is to reform undercover investigation methods and particularly the surveillance

of telecommunications. By trying to provide a sound legal basis for secret police work, it will contribute to its extension.

Green party proposal on surveillance of telecommunication

by Norbert Pütter

The draft proposal of the Green Party of December 2006 has surprising similarities with the government's proposal (see above), but it explicitly claims to achieve a reduction in the number of interceptions. Instead of using the current list of crimes that automatically legitimise surveillance, the Greens are proposing to rewrite it. This draft cannot be expected to achieve its proclaimed aim, either.

Extremism by association and the "right to know"

by Udo Kauß

For ten years now, Rolf Gössner, publicist, lawyer and president of the International Human Rights League (Internationale Liga für Menschenrechte) has been arguing with the Federal Office for the Protection of the Constitution (internal security service) about his right of access to his personal information. The Federal Office concedes that Gössner was not a "left-wing extremist". However, in its 36 years of observation, it has nevertheless collected a lot of data on him and it refuses to disclose the really interesting data to him.

EU framework decision on data protection

by Tony Bunyan

The EU is currently working on a framework decision to regulate data protection in police and judicial cooperation. However, because the discussion is taking place in a climate that is determined by the "war on terror", citizens' rights are again subordinated to the wishes of criminal prosecution. The proposal aims to do away with any obstacles to the mutual access to Member States' police data (principle of availability) or the data exchange between the EU and its befriended authorities in countries such as the US.

Common databases for police and secret services

by Heiner Busch

Seventeen years after the separation of the state security division of the Federal Crime Police Authority (Bundeskriminalamt – BKA) from the intelligence information system of the German internal secret service (Bundesamt für Verfassungsschutz – BfV), the parliament has decided to reunite the police with the secret service at the information technology level. The law, passed on 1 December 2006, establishes an "anti-terror" database, to be accessed by secret services, the BKA and other police organizations. Further, police and secret services will work closely together in analysis projects, using so-called work files.

Police and secret service against immigrants

by Mark Holzberger

In the fight against "illegal immigrants" and foreign "terrorist suspects", police and security services have been working together closely for some time now. At the regional and national level, working groups are explicitly using the deportation and surveillance powers they were given by the new immigration law. In May 2006, the interior ministry has created yet another tool in the fight against immigrants, the common analysis and strategy centre on illegal migration (Gemeinsames Analyse- und Strategiezentrum illegale Migration – GASIM).

Anti-Terrorism Amendment Act

by Heiner Busch

The intelligence services will continue to be able to demand information from banks, airlines and telecommunication providers. On 1 December 2006, the Lower House of the German parliament renewed and extended the powers it had given the services five years ago.

Bremen's police methods

by Helmut Pollähne

At a police action during the street party "Schanzenstraßenfest" in Hamburg on 9 September 2006, a police unit from Bremen achieved fame by not only shackling the arrested demonstrators but also "disorientating" them, forcing them to wear shaded glasses until their transportation to detention.

MitarbeiterInnen dieser Ausgabe

Heiner Busch, Bern, Redakteur von Bürgerrechte & Polizei/CILIP und Vorstandsmitglied des Komitees für Grundrechte und Demokratie

Tony Bunyan, London, Herausgeber von Statewatch

Otto Diederichs, Berlin, freier Journalist

Volker Eick, Berlin, Politikwissenschaftler an der Freien Universität Berlin, John F. Kennedy Institut, Abteilung Politik

Albrecht Funk, z.Zt. Berlin, Mitherausgeber von Bürgerrechte & Polizei/CILIP

Mark Holzberger, Berlin, Referent für Flüchtlings- und Migrationspolitik in der Bundestagsfraktion von Bündnis 90/Die Grünen und Mitglied der Redaktion von Bürgerrechte & Polizei/CILIP

Udo Kauß, Freiburg i. Br., Rechtsanwalt, Mitherausgeber von Bürgerrechte & Polizei/CILIP und Vorstandsmitglied des Landesverbandes Baden-Württemberg der Humanistischen Union

Martina Kant, Berlin, Redakteurin von Bürgerrechte & Polizei/CILIP und Referentin der Bundestagsfraktion von Bündnis 90/Die Grünen für den Untersuchungsausschuss BND/CIA

Katrin McGauran, Amsterdam, Mitarbeiterin von Statewatch

Hanna Noesselt, Berlin, studentische Hilfskraft im Forschungsprojekt „Sicherheitsstrategien im Wandel" an der FU Berlin

Helmut Pollähne, Bremen, wiss. Assistent am Institut für Kriminalpolitik (BRIK) des Fachbereichs Rechtswissenschaft der Universität Bremen und Vorstandsmitglied des Komitees für Grundrechte und Demokratie

Norbert Pütter, Berlin, Redakteur von Bürgerrechte & Polizei/CILIP

Thilo Weichert, Kiel, Schleswig-Holsteinischer Landesbeauftragter für den Datenschutz und Leiter des Unabhängigen Landeszentrums für Datenschutz

Jan Wörlein, Berlin, studentischer Mitarbeiter, Student der Politikwissenschaft an der FU Berlin

Mark A. Zöller, Mannheim, wiss. Assistent am Lehrstuhl für Strafrecht, Strafprozessrecht und Rechtstheorie der Universität Mannheim sowie Mitglied des Arbeitskreises Strafprozess- und Polizeirecht (ASP)