

"SICHERHEITS" - GESETZENTWÜRFE APRIL 1989

DOKUMENTATION • KRITIK • MATERIALIEN:

VERFASSUNGSSCHUTZ - G. • MAD - G. • BND - G. •

B. - DATENSCHUTZ - G. • VERWALTUNGSVERFAHRENS - G.

NOVELLE ABHÖR - GESETZE (G - 10 - G.; 100 a StPO)

STRAFVERFAHRENSÄNDERUNGS - G. (SPUDOK etc.)

32

Bürgerrechte & Polizei

Cilip 32

Nr. 1/1989

Preis 9,-DM

Bürgerrechte & Polizei

Cilip Informationsdienst

Herausgeber:

H. Busch, A. Funk,
K. Dieckmann, U. Kauss,
C. Kunze, W.-D. Narr
M. Walter, F. Werkentin

Preis/ Einzelheft: DM 9 p.V.
Jahresabo (3 Hefte)-
Personen: DM 21 p.V.
Institutionen: DM 40 p.V.

Buchhandelsbestellungen
an die Redaktion:

Bürgerrechte & Polizei
c/o FU Berlin
Malteserstr. 74-100
1000 Berlin 46
Tel.: 030/7792-378
-462
-454

Einzelbestellungen/Abos:
Kirschkeim Buchversand
Hohenzollerndamm 199
1000 Berlin 31

ISSN 01721895

Wozu ein Informationsdienst Bürgerrechte & Polizei?

Im Gegensatz zu Fragen des Militärs und der äußeren Sicherheit sind Polizei und Innere Sicherheit nur in geringem Maße Gegenstand kritischer Auseinandersetzung.

Nur angesichts spektakulärer Polizeieinsätze oder zufällig aufgedeckter Skandale gerät die Polizei vorübergehend in den Mittelpunkt öffentlicher Diskussion. Die gesellschaftliche Funktion der Apparate Innerer Sicherheit, Veränderungen liberaler Demokratie, die durch den Funktionswandel der Polizei und ihre veränderten Instrumente bewirkt werden, bleiben einer kritischen Auseinandersetzung entzogen.

Will man nicht den Apparaten und ihren Vorstellungen von Sicherheit und Ordnung ausgeliefert sein, ist eine kontinuierliche und kritische Beobachtung von Polizei und Nachrichtendiensten vonnöten.

Seit 1978 dokumentiert und analysiert der Informationsdienst **Bürgerrechte & Polizei** (CILIP) die gesetzlichen, organisatorischen und taktischen Veränderungen innerer Sicherheitspolitik in der Bundesrepublik. Über diesen Schwerpunkt hinaus liefert **Bürgerrechte & Polizei** Berichte, Nachrichten, Analysen zur

- Polizeientwicklung in den Ländern Westeuropas
- Polizeihilfe für Länder der Dritten Welt
- Arbeit von Bürgerrechtsgruppen zur Kontrolle und Begrenzung polizeilicher Macht.

Bürgerrechte & Polizei erscheint jährlich mit drei Ausgaben und einem Seitenumfang von ca. 100 Seiten

Inhalt:

Editorial:

"Sicherheits"gesetze 3

I. Geheimdienstgesetze - Stand Mai 1989

- * Zur Gesetzgebungsgeschichte der Geheimdienstgesetze 16
- * Dokumentation: Bundes-Verfassungsschutz-Gesetz-Entw. 20
- * Stellungnahme zum BVerfSchG-Entwurf 31
- * Dokumentation: MAD-Gesetz-Entwurf 61
- * Stellungnahme zum MADG-Entwurf 61
- * Dokumentation: BND-Gesetz-Entwurf 73
- * Stellungnahme zum BNDG-Entwurf 76
- * Dokumentation (Auszüge): Poststruktur-Gesetz -
Zur Novellierung des G-10-Gesetzes und der §§ 100a u. b StPO 80
- * Stellungnahme: Von der Post- zur Kommunikationskontrolle 82

II. Datenschutzrechtliche Querschnittgesetze, Stand: Mai 1989

- * Dokumentation (Auszüge): Bundesdatenschutz-Gesetz-
Entwurf 87
- * Stellungnahme zum BDSG-Entwurf 92
- * Dokumentation (Auszüge): Änderung des Verwaltungs-
verfahrens-Gesetzes, Entwurf 103
- * Stellungnahme zur Änderung des VwVfG, Entwurf 105

III. Die Verpolizeilichung der Strafprozeßordnung

- * Das Strafverfahrensänderungsgesetz 1988 108

IV. Verabschiedet:

- * Das Artikel-Gesetz zum Demonstrationsrecht, zur
Kronzeugenregelung etc. 121

V. Ergänzende Materialien

* § 12a Versammlungsgesetz: n.F.	123
* "Sicherheits"-Gesetzgebung in der 11. Legislaturperiode des Deutschen Bundestages, Stand: Mai 1989	5
* Aus dem 7.Tätigkeitsbericht des Hamburger Datenschutzbeauftragten: - Stellungnahme zur Novellierung des BVerfSchG	58
* Was ist NADIS?	38
* NADIS-Ausdruck des Kabarettisten Kittner 1982	48
* Aus dem 11.Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz: - NADIS-Kontrolle - Informationsweitergabe an ausländische Dienste - MAD-Kontrolle	51 51 73
* Denn Nachricht ist alles... (aus Stefan Zweigs "Fouché")	79
* Entschließungen der Konferenz der Datenschutzbeauftragten: - vom 14.März 1988 - "Polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen - vom 6.Juni 1988 zur Neufassung des BDSG - vom 5./6.April 1989 zur Änderung des G-10-Gesetzes und der StPO im Rahmen der Poststrukturreform - vom 5./6.April 1989 zum Entwurf eines Strafverfahrensänderungs-Gesetzes 1988	114 102 86 118
Chronologie der laufenden Ereignisse	124
Summary	127

Impressum:

Redaktion dieser Ausgabe: Falco Werkentin
 Satz: Marion Schapkow
 Übersetzungen: Sabine Lang
 Umschlaggestaltung: Jürgen Grothus
 Druck: AGIT-DRUCK

(c) Verlag CILIP, Berlin, Mai 1989

Zitlervorschlag: Bürgerrechte & Polizei (CILIP), Heft 32 (1/1989)

Editorial: "Sicherheitsgesetze"

1. Der Stand der Dinge

"Sicherheitsgesetze - und kein Ende" - so heißt der Titel des Editorials unserer letzten Ausgabe vom Dezember 1988, in der wir die Entwürfe zum Ausländerzentralregister-Gesetz und zur Neufassung des BKA-Gesetzes öffentlich machten.

Kaum kam dieses Heft vom Buchbinder, lag ein nächstes Paket sog. "Sicherheits"-Gesetze auf dem Tisch. Unter dem vielversprechenden Titel "Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes" ist dieses Paket am 30.12.1988 dem Bundesrat vorgelegt worden. Unter geringer öffentlicher Resonanz erfolgte die 1. Lesung am 28.4. dieses Jahres im Bundestag (Drs.11/4306).

Dieses Artikel-Gesetz - nicht zu verwechseln mit dem vom Bundestag am 21. April d.J. verabschiedeten Artikel-Gesetz zum Abbau des Demonstrationsrechts, zur Einführung der Kronzeugenregelung etc. (vgl. Kritik in dieser Ausg.) - faßt jene Gesetzesentwürfe zur Regelung staatsschützerischer Informationsverarbeitung zusammen, deren erste Fassungen wir bereits 1985 (CILIP 21) aus den Schreibtischen ihrer Autoren gezogen hatten:

- * Bundesverfassungsschutz-Gesetz
- * MAD-Gesetz,
- * BND-Gesetz,
- * Bundesdatenschutz-Gesetz,
- * Änderung des Verwaltungsverfahren-Gesetzes.

Während die ersten drei Entwürfe unmittelbar die Informationsverarbeitung der Geheimdienste regeln, betreffen die beiden Querschnitts-

Gesetze BDSG und VwVfG insgesamt die Datenverarbeitung, jedoch mit Sonderregelungen für den Staatsschutzverbund.

Unser Gesamturteil vorab:

1) Die Bundesregierung und ihre exekutiven Ghostwriter haben seit der massiven und breiten Kritik an den ersten Entwürfen von 1985 in nichts zurückgesteckt. Sie zeigen in ihrem Gesetzgebungs-Slalom eine außerordentliche Treue gegenüber dem Gehalt der Ursprungsentwürfe. Das Ziel, den seit langem bestehenden unbegrenzten Informationsverbund in Staatsschutzangelegenheiten zwischen allen beteiligten Teilapparaten des "Sicherheitssystems" rechtlich abzusichern, ist geblieben. Allerdings, der Entwurf eines "Zusammenarbeitengesetzes" von 1985/86, wie der unter dem Titel "VfS-Mitteilungsgesetz" folgende Entwurf 1988 ist inzwischen preisgegeben worden. Beide waren Kristallisationspunkte der öffentlichen Kritik. Als weniger verräterische Lösung sind die zuvor in diesen Entwürfen verfolgten Intentionen nun in die Befugnisregeln der einzelnen Geheimdienst-Gesetze untergebracht worden.

2) Weiter verfolgt wird auch das Ziel, alle Stellen der öffentlichen Verwaltung (vom TÜV, soweit er Aufgaben der öffentl. Verwaltung erfüllt, über die AOK bis zur Universität, von der Bundesversicherungsanstalt bis zur Gemeindeverwaltung) auf eine Zuarbeit für den Staatsschutzverbund rechtlich bindend zu verpflichten. Wird für den

Datentransfer zwischen den Staatsschutzapparaten nur festgeschrieben, was immer schon Praxis war, so schaffen jene Normen, die nun "sonstige Stellen" in Übermittlungspflichten gegenüber den Staatsschutzapparaten rechtlich verbindlich einschließen, eine qualitativ neue Situation mit durchgreifenden Konsequenzen für den Alltag staatschützerischer Informationserhebung.

Zwar haben sich die Dienste auch bisher schon Daten von der AOK, dem Arbeitsamt etc. besorgt, zwar gab es auch bisher schon von spontaner Denunziationsfreude getriebene Beschäftigte in den deutschen Universitäten etc., die von sich aus "Erkenntnisse" an die Geheimdienste lieferten. Nur waren hier die Dienste mehr oder weniger angewiesen auf die Bereitschaft der Beschäftigten zur Zusammenarbeit. Diese hatten die Möglichkeit, nicht mitzuspielen, bewegten sich solche Praktiken doch im Graubereich zwischen Recht und Rechtsbruch. Das mit den vorliegenden Entwürfen verfolgte Ziel, den Staatsschutzbehörden auch und gerade für den präventiven Staatsschutz weit im Vorfeld konkreter Handlungen den **rechtlich verbindlichen** Zugriff auf nahezu alle Datenbestände öffentlicher und semiöffentlicher Stellen zu ermöglichen, schafft für diese Stellen und ihre Beschäftigten - damit aber auch für die BürgerInnen und ihren Datenschatten in den Verwaltungen - eine qualitativ neue Situation. Der Zugriff wird systematisiert und soll den VfS-Behörden die Möglichkeit eröffnen, alle Behördendateien für strategische Auswertungen (für Rasterfahndung etc.) heranziehen zu können. In dieser systematischen Zugriffsmöglichkeit liegt die qualitative Neuerung.

3) Die Gesetzesautoren haben inzwischen gelernt, durch Gesetzgebungstechnik und Sprache ihren präventive Datensammlungs-Extremismus zu verstecken. Dies wird deutlich, wenn man auf die Geschichte dieser Gesetzgebung und die Vielzahl von Entwürfen zurückschaut, die chameleonhaft ständig verändert wurden, ohne daß auch nur ein Zipfelchen an Intentionen preisgegeben wurde. Wir halten dies für so symptomatisch und lehrreich, daß wir der sich ständig wandelnden Gesetzgebungstechnik und den nutzbar gemachten Sprach- und Begriffs-Tricks in diesem Editorial einen eigenen Abschnitt gewidmet haben. Zur Gesetzgebungsgeschichte dieser Entwürfe vgl. den dem Editorial folgenden Beitrag.

4) Schließlich ist daran zu erinnern, daß mit den hier dokumentierten Entwürfen keineswegs die geplante Gesamtrevision des "Rechts" der Sicherheitsapparate abgeschlossen ist. Der Kasten auf der folgenden Seite gibt eine Übersicht über weitere, in Arbeit befindliche "Sicherheits"-Gesetze.

5) Im Handstreich - und damit nahezu ohne öffentliche Diskussion und Protest - haben die Bonner Koalitionsparteien zudem im letzten Monat während laufender Gesetzgebungsverfahren zwei für die Informationserhebung und -verarbeitung der "Sicherheitsbehörden" zentrale Gesetzesregelungen nachgeschoben und umgehend verabschiedet:

* Dem Poststruktur-Gesetz, das am 20. April d.J. verabschiedet wurde, war kurz zuvor eine "Ergänzung" untergeschoben worden, die den Zugriff von Polizei, Ge-

"Sicherheits"-Gesetzgebung in der 11. Legislaturperiode des Deutschen Bundestages, Stand: Mai 1989

Bisher wurden verabschiedet:

- * "Entwurf eines Gesetzes zur Änderung des StGB, der StPO und des Versammlungsgesetzes und zur Einführung einer Kronzeugenregelung bei terroristischen Straftaten" (BT-Drs. Nr.: 11/2834) in der Fassung der "Beschlußempfehlung und des Berichts des Rechtsausschusses vom 18.4.89" (BT-Drs. Nr.: 11/4359); verabschiedet am 21.4.88 (vgl. Kommentierung in dieser Ausgabe)
- * "Entwurf eines Gesetzes zur Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost (PostStruktG)" (BT-Drs. Nr.: 11/2854) in der Fassung der "Beschlußempfehlung und des Berichts des Ausschusses für das Post- und Fernmeldewesen" (BT-Drs. Nr.:11/4316); verabschiedet am 20.4.88 (vgl. Kommentierung der mit diesem Gesetz verbundenen Novellierungen des G-10-Gesetzes und des § 100 StPO in dieser Ausgabe)

Als Bundestags-Drs. vorgelegt ist:

- * Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (BT-Drs. Nr.: 11/4306 vom 6.4.89, BDSG, VwVfG, BNDG, MADG, BVerfSchG, vgl. Dok. und Kritik in dieser Ausg.)

Als Vorentwürfe liegen vor:

- * BKA-Gesetz, Stand: 1.8.88 (dok. in CILIP 31)
- * Ausländerzentralregister-Gesetz, Stand: 12.7.88 (dok. in CILIP 31)
- * Strafverfahrensänderungsgesetz 1988, Stand: 22.12.88 (vgl. Kommentierung in dieser Ausgabe; Vorentwürfe dok. in CILIP 29)
- * Justiz-Mitteilungsgesetz, Stand: 8.9.86 (dok. in CILIP 29)
- * Entw. einer gesetzlichen Regelung für ein länderübergreifendes staatsanwaltschaftliches Informationssystem, Stand: 22.12.88

Angekündigt sind :

- * ein Geheimschutz-Gesetz, dessen blueprint in bereits geltender "Sicherheitsüberprüfungsrichtlinien" vorliegt (dok. in CILIP 29, S.125 ff.)
 - * ein Bundesgrenzschutz-Gesetz
- Dieses "Gesamtwerk" entspricht der Bonner Koalitionsvereinbarung zur Rechts- und Innenpolitik vom März 1987 (zur Koalitionsvereinbarung CILIP 26, S.2 f.).

Länder-Gesetzgebung:

Auf Länderebene hat inzwischen fast jedes Bundesland Entwürfe zur Novellierung der Länder-Polizeigesetze vorgelegt, in denen es gleichfalls um die Anpassung des Rechts an die Praxis polizeilicher Datenerhebung und Verarbeitung einschließlich des Einsatzes nachrichtendienstlicher Mittel und Methoden geht (Übersicht in CILIP 31). Zudem gibt es von einigen Ländern Datenschutzgesetz-Entwürfe.

heimdiensten und Staatsanwaltschaften auf alle neuen Formen der Kommunikation eröffnet - auch und gerade dort, wo diese Formen von privaten Unternehmen betrieben werden (siehe unsere Dokumentation und Kommentierung in dieser Ausgabe).

* Das Artikel-Gesetz zur Demonstration des Demonstrationsrechts, zur Einführung des Kronzeugen etc., das am 21. April d.J. verabschiedet wurde, war kurz zuvor um einen neuen § 12a Versammlungs-Gesetz bereichert worden, der nun als Bundesrecht für alle Länder verbindlich regelt, was bisher im Polizeirecht der Länder - seit 1985 mit dem ME PolG der IMK vorbereitet - normiert werden sollte: präventive Ton- und Bildaufnahmen bei und in Vorbereitung auf Demonstrationen (Zu diesem Handstreich siehe unsere Kritik in dieser Ausgabe).

2. Zur Rechtsqualität der "Sicherheitsgesetze"

Art. 20 GG formuliert die prinzipielle Gesetzesbindung exekutiven Handelns; d.h. jedweder Verwaltungsakt bedarf der gesetzlichen Grundlage, bedarf mithin der Vorabentscheidung und Ermächtigung durch das Parlament. Recht, soll es mehr sein als eine in Gesetzesform gegossene Verwaltungsvorschrift zur internen Regulierung und Standardisierung von Verwaltungshandeln, soll aber nicht nur ermächtigen, sondern gleichermaßen mit der Ermächtigung auch begrenzen. Es soll mithin den Bereich des zulässigen von dem des unzulässigen, also rechtswidrigen Handelns anhand möglichst klarer tatbestandlicher Definitionen trennen.

"Wenn das Spiel (die Begrenzungsfunktion des Rechts - Red.) Sinn

machen soll, muß der Bewertungsmaßstab entscheidbar machen, ob eine bestimmte Maßnahme zulässig ist oder nicht. In der Begrifflichkeit des Justizsylogismus formuliert: es ist essentiell für diese Bewertungsoperation, daß auch Voraussetzungen (Sachverhalte) denkbar sind, die nicht zu einer positiven Subsumtion führen, also zu dem Ergebnis: diese Maßnahme wäre unzulässig. Das eben ist die Begrenzungsfunktion einer Norm." (Wagner 1989)

Nur so läßt sich auch ein grundlegendes rechtsstaatliches Versprechen einhalten: das Prinzip der Rechtssicherheit im Sinne tatbestands- und normenklarer allgemeiner Regeln, die Bürger wie Verwaltung in die Lage versetzen, eigenes Handeln in der Orientierung am Recht zu kalkulieren - und zwar eigenes Handeln, nicht die eigene Gesinnung.

Mißt man die seit 1985 vorgelegten Geheimdienstgesetze, aber auch das Polizeirecht der Länder, das sich seit Anfang der siebziger Jahre in einem ständigen Novellierungsprozeß befindet, an diesen Maßstäben, so fällt das Urteil eindeutig aus.

Normenklarheit und Bestimmtheit, die zentralen Voraussetzungen von Rechtssicherheit, sind schubartig preisgegeben worden. Es gibt schlechterdings keine Sachverhalte mehr, die nicht bei gelinder Interpretationskunst unter die Eingriffsvoraussetzungen des teilwirklicherten neuen Polizeirechts und der in diesem Heft dokumentierten Gesetze für die Geheimdienste fallen könnten. Dies hat seine Logik.

Ein Staat, der auf Risikoversorge und Prävention aus ist, verlangt einen juristischen Eingriffsrahmen,

der auf Berechenbarkeit qua Bestimmtheit der Eingriffsnormen verzichten muß. "Dem einzelnen wird allerdings so just die Sicherheit genommen, die ihm die Kodifizierung garantieren soll. Er handelt nicht in Kenntnis bestimmter, jederzeit nachvollziehbarer, ihn ebenso wie jeden anderen bindenden Erwartungen, sondern unter dem Vorbehalt einer in ihren Inhalten und Konsequenzen prinzipiell offenen, richterlichen und administrativen Instanzen vorbehaltenen Korrektur" (Simitis 1988, S.37).

Als Tendenz war diese Durchbrechung der Bestimmtheit und Kalkulierbarkeit dem Recht der Sicherheitsapparate schon immer immanent.

Dies gilt gerade für das Gefahrenabwehrrecht. So sehr das Polizeirecht auch früher mit Gefährlichkeitsvermutungen und damit auch mit systematischen Irrtumswahrscheinlichkeiten und Optionen für Willkür operierte, so beinhaltete es doch in der Bindung des Eingriffs an konkretisierbare Gefahren und dessen Einschränkung auf den Verursacher dieser Gefahren (Störer) rechtlich überprüfbare Kriterien.

Immer schon unbestimmt war demgegenüber der Eingriffsspielraum der Geheimdienste, der durch die vorliegenden Entwürfe neu- bzw. erstverrechtlicht werden soll. Der Vfs sollte und soll ja gerade die Ungewißheit über politische Entwicklungen im Lande und ihre sozialen Träger weit im Vorfeld des Vorfalles konkreter Angriffshandlungen abklären. Daher kam bereits der Gesetzgeber von 1951 beim Vfs-Gesetz über ganz pauschale Aufgabennormen nicht hinaus - geschweige denn, daß klare Befugnisnormen statuiert

worden wären. Die Konsequenz: nicht das Parlament entschied aufgrund gesetzlich detailliert formulierter Eingriffsvoraussetzungen, wer Objekt geheimdienstlicher Operationen und nachrichtendienstlicher Aufklärung werden durfte, sondern die Dienste selbst. Solange Parlament, Geheimdienste und breiteste Teile der Bevölkerung gemeinsam vom starren und militanten Antikommunismus mit seinen relativ klar konturierten Feindbild geprägt waren, fiel die damit geschaffene Eingriffsaunomie der Geheimdienste kaum auf.

Kurz: seit jeher bestimmte nicht das Recht, sondern die Praxis der Dienste und ihr Wandel vor dem Hintergrund einer sich verändernden Gesellschaft Aufgaben und Befugnisse der Vfs-Ämter.

In dieser Hinsicht sind die vorliegenden Entwürfe nicht von "neuer Qualität". Wie zuvor, ob 1950 oder 1972, sind die neuen Gesetze nur die Legitimation für Eingriffe, über deren allgemeine Voraussetzungen nicht der Gesetzgeber, sondern die Administration entscheidet.

Neu ist allerdings der gesetzgeberische Aufwand, mit dem versucht wird, Erfüllung rechtsstaatlicher Gesetzesformalien, Präzision und die Berücksichtigung von Strukturprinzipien des sich seit den siebziger Jahren herausbildenden Datenschutzrechts vorzugaukeln.

3. Zur gesetzgeberischen Technik der politischen Täuschung

Kamen MAD und BND bis dato ohne gesetzliche Grundlagen und das BfV mit Gesetzen aus, die sich 1950 und 1972 mit sechs Paragraphen begnügten, so wird in den seit 1985 vielfältig mutierten

Gesetzentwürfen das Recht der Geheimdienste und des informationellen Staatsschutzverbundes in einem schier endlosen Paragraphenwald versteckt, dessen einziger Zweck es zu sein scheint, vor lauter Bäumen blind zu machen. Gemessen an den Erst-Entwürfen von 1985 ist die Technik des gesetzgeberischen Verwirrspiels ohne Zweifel perfektioniert worden.

* Das, was die Intention dieser Gesetzgebung war und geblieben ist, die Absicherung der informationellen Gesamtvernetzung, war in den ersten Entwürfen - insbesondere im ZAG - noch unmittelbar angesprochen worden. Das "Zusammenarbeits-Gesetz" nannte nicht nur en detail alle Teilapparate sondern beschrieb noch relativ konkret die spezifischen Formen der Zusammenarbeit - etwa die Zuarbeit des BGS für den BND. Das ZAG, und das folgende, in seiner Detailfreunde schon kargere VfS-Mitteilungsgesetz sind als selbstständige Gesetze nun gestrichen, die Zusammenarbeitspflichten und Befugnisse stattdessen inkorporiert in die jeweiligen "Organisations"-Gesetze für den VfS, MAD und BND.

* Nahezu die Hälfte der Gesetzesparagrafen in den jeweiligen Einzelgesetzen sind der neuen Datenschutzhetorik gewidmet. Da gibt es Nachberichtigungs- und Lösungsverpflichtungen; da müssen die Empfänger von personenbezogenen Daten darauf hingewiesen werden, daß sie Daten nur für den Zweck, zu dem sie ihnen übermittelt wurden, nutzen dürfen; da werden die Ämter verpflichtet, Daten nur insoweit zu speichern und zu nutzen, wie dies für ihre jeweiligen Aufgaben notwendig ist; da gibt es die Verpflichtung zu Errichtungsanordnungen für Da-

teilen usw. Ganze Paragraphen wiederholen geltende Rechtssätze wie das Verhältnismäßigkeitsprinzip oder den Grundsatz, daß spezialgesetzliche Regelungen denen dieser Gesetze vorausgehen etc. Es sind Selbstverständlichkeiten, die auch gelten würden, wenn sie nicht zur Füllung dieser Gesetze dienen müßten und die nur ein Ziel haben - hinter einem Wortschwall zu verstecken, daß das Gesamtpaket durch einen schlichten Satz ersetzt werden könnte:

Im Interesse des Staatsschutzes sind die Dienste zu jeder nur denkbaren Form der Informationserhebung und -weitergabe befugt!

* Ein weiteres Instrument politischer Täuschung sind die redaktionellen Überschriften zu einzelnen Paragraphen, deren Inhalt die Überschrift jeweils "dementiert". So findet sich in allen Entw. eine Überschrift, die da heißt: "Geltung des BDSG und des VwVfG". Anschließend werden jene Paragraphen dieser Querschnittsgesetze benannt, die gerade nicht für den staatsschützerischen Informationsverbund gelten sollen.

* Ähnlich strukturiert ist der "Minderjährigenschutz" in den Entwürfen der Geheimdienstgesetze. Der Titel suggeriert, daß Informationen über das Verhalten von Minderjährigen nicht erhoben werden dürfen. Der Inhalt besagt, daß Informationen über Minderjährige (bis zum 16. Lebensjahr) nicht in **automatisierten** Dateien gespeichert und nur restriktiv weitergegeben werden dürfen, wobei die Restriktionen immer schwachbrüstiger werden, je mehr die Minderjährigen das Alter erreichen, in dem Jugendliche überhaupt anfangen, politische Interessen zu entwickeln.

* Kennzeichnend für den Entw. ist auch ein Spiel mit Begriffen, die normativ gleich verwendet werden, faktisch aber unterschiedliche Bedeutung besitzen. Dies gilt vor allem für die Begriffe "Information" und "personenbezogene Daten" (letzteres ein Begriff aus der Datenschutzrechts-Dogmatik, der im engeren Sinne automatisiert gespeicherte Daten meint). Zwischen diesen Begriffen changieren diese "Sicherheitsgesetze" deshalb ständig, weil sie datenschutzrechtlich sehr unterschiedliche Formen und Inhalte der Informationsverarbeitung fassen. Die Paragraphen zu den Erhebungs- und Übermittlungsbefugnissen operieren mit dem Informationsbegriff. Die "speziellen Datenschutzvorschriften" einschließlich jener zum "Minderjährigenschutz" operieren mit dem engen Dateienbegriff - ein vorläufiger Begriffwechsel mit dem Ziel der Täuschung. Denn beim Vfs liegt unbeschadet der technischen Aufrüstung mit ADV der Großteil der Informationen über relativ knappe Raster und Fundstellenhinweise hinaus, in konventionellen Akten. Gerade da, wo eine Begrenzung ansetzen müßte, bei der Erhebung von personenbezogenen Informationen unabhängig von der Form ihrer Archivierung, wird operiert mit dem Informationsbegriff - dort, wo Begrenzungen suggeriert werden sollen, mit dem Dateienbegriff. Die Informationsmenge wird keineswegs begrenzt.

* Gleichermaßen aussagekräftig ist das Changieren zwischen den Begriffen "Behörde", "bundesunmittelbare juristische Personen öffentlichen Rechts", "Stellen, die Aufgaben der öffentlichen Verwaltung übernehmen", sonstige "Stellen", "amtliche Register" etc.

Auch dies ist keineswegs nur redaktionelle Schlamperei. Je konturenloser jene "Stellen" rechtlich definiert werden, die informationspflichtig sind bzw. von den Diensten mit "Erkenntnissen" beliefert werden dürfen, desto mehr wird es ins Belieben der Dienste gestellt, wer Daten abzuliefern hat und wen die Dienste mit Verdächtigungen und Feindbestimmungen zu beliefern befugt sind.

* Beispielhaft auch das Schicksal des sog. Trennungsgebots von Polizei und Geheimdiensten. Der Satz, daß letztere keiner polizeilichen Dienststelle angegliedert werden dürfen war in den Ursprungsentwürfen von 1985 enthalten, wurde zwischenzeitlich fallengelassen und taucht nun wieder auf. Um die organisatorische Zusammenlegung von Polizei und Geheimdiensten ging es aber nie. Vielmehr zielt das Gesamtpaket auf die funktionale Zusammenarbeit der Behörden bei organisatorischer Selbstständigkeit. Daß aus dem Trennungsgebot allerdings auch die informationelle Gewaltenteilung und informationelle Trennung der Datenbestände abzuleiten wäre - dieser Gedanke ist den Autoren allemal fern (zum Trennungsgebot ausführlich R. Gössner in CILIP 27, S.38 ff.).

4. Die politische Logik der "Sicherheitsgesetze"

Das Volkszählungsurteil des Bundesverfassungsgerichts von 1983, damals emphatisch als "Bergpredigt des Datenschutzes" titulierte, hat vor allem Gesetzgebungsbedarf erzeugt (Urteil in CILIP 21 u. 23). Nach 6 Jahren läuft auch der vom Gericht zugestandene sog. Übergangsbonus aus, so daß der "Gesetzgeber" derzeit in der Tat un-

ter formalem Gesetzgebungsdruck steht.

Das ist indes nur ein äußerer Anlaß. Im Kern läßt sich der aktuelle "Gesetzgebungsbedarf" auf gesellschaftliche Veränderungen und einen Wandel des staatlichen Politikmodells zurückführen - zwei Prozesse, die sich seit Mitte der sechziger Jahre ankündigten.

a) Die demokratische "Kulturrevolution"

Schon im Ausklang der autoritären Kanzler-Demokratie Adenauers gab es bereits erste Zeichen wachsenden demokratischen Selbstbewußtseins in diesem Lande, sichtbar bei der öffentlichen Reaktion auf die Spiegel-Affäre 1962, verstärkt mit der Anti-Notstandsbevewegung und der Studentenbewegung und schließlich in den 70er und 80er Jahren weiterentwickelt im sozial und politisch buntscheckigen Feld von Bürgerinitiativen, in der Umwelt-, der Friedensbewegung, etc. Das "Volk", im Grundgesetz von 1949 systematisch mediatisiert, meldete in Gestalt außerparlamentarischer Initiativen und Bewegungen politische Teilhabe- und Mitentscheidungsansprüche an. Gewiß, es war und ist nicht das "ganze Volk", sondern es sind artikulationsstarke Minderheiten - weder von ihrer Klassen- und Schichtzugehörigkeit her homogen, noch von ihren Organisations- und Artikulationsformen, Zielen und ideologischen Konzepten. Aber gerade diese schwere Faßlichkeit sozialer Träger und politischer Ziele der neuen demokratischen Unruhe jenseits der hierarchisch gegliederten und geführten Marschkolonnen der traditionellen Fundamentalopposition Arbeiterbewegung schuf neuen Kontrollbedarf.

Die Sozialdemokratie, dank dieses demokratischen Aufschwungs Ende der 60er Jahre bundesweit zur führenden Regierungspartei geworden, reagierte in doppelter Weise. Zum einen versprach sie, "mehr Demokratie zu wagen" und begann, Mitbestimmungsmodelle etwa im Hochschulbereich durchzusetzen. Gleichzeitig begann sie in politischer Koalition mit der CDU/CSU, sich des veränderten politischen Prozesses in der Bundesrepublik herrschaftlich zu vergewissern. Nicht die Bürger oder gar Massenbewegungen, sondern eine mit kraftvoll-neuen Muskeln versehene staatliche Bürokratie sollte, ganz in sozialdemokratischer Tradition, "Subjekt" sozialdemokratischen Krisenmanagements und der Gesellschaftsreform werden. Der demokratisch selbstbewußte Bürger, der mitbestimmen und mitentscheiden wollte, war eher ein Störfaktor. Wie seit Beginn bundesdeutscher Geschichte und Vorgeschichte blieb auch in den sozialliberalen 70er Jahren die "Innere Sicherheit" das verbindende Geschäft der Allparteienkoalition von CDU/CSU, SPD und FDP. Das "Sofortprogramm zur Verbrechensbekämpfung" der Bundesregierung aus dem Jahre 1970, das "Programm für die innere Sicherheit" der IMK von 1972, die Ausweitung der Befugnisse von BGS, BKA und Vfs im Jahre 1972 zusammen mit dem massiven personellen Ausbau dieser Apparate bei parallelen Entwicklungen auf Länderebene, der sog. Radikalenerlaß von 1972 - all dies war das verschreckte Bemühen der Parteien und Bürokratien, jenen neuen sich außerhalb des parlamentarischen Repräsentationssystems der Bundesrepublik entwickelnden politischen Prozeß

repressiv zu überwachen und zu beherrschen.

Diesen Zusammenhang von gesellschaftlicher Demokratisierung und repressiver Reaktion formulierte u.a. die Landesregierung Niedersachsens 1972 programmatisch in ihrem Landesentwicklungsprogramm "Niedersachsen 1985":

"Die wachsende Kompliziertheit des gesellschaftlichen Lebens mit ihren durch die Demokratie nur in langwierigen Prozessen zu lösenden Problemen sowie das steigende politische Bewußtsein der Bevölkerung werden wahrscheinlich dazu führen, daß die Neigung zur öffentlichen Konfrontation ansteigt. Die Polizei geht deshalb davon aus, daß auch im kommenden Jahrzehnt eine erhebliche Anzahl von Einsätzen aus Anlaß von Demonstrationen notwendig werden wird" (S.447).

Das, was sich an demokratischen Fundamentalansprüchen seit Ende der 60er Jahre artikuliert und nicht mehr - wie KPD/DKP und Umfeld - einem im Rahmen der Ostpolitik ebenfalls an Konturen verlierenden äußeren Feind zugeordnet werden konnte, führte zur Entdeckung des Verfassungsfeindes. Dieser neue Begriff ergänzte die Kategorie des "Verfassungswidrigen" und sollte gerade den nicht durch das Verfassungsgericht verbotenen und auch nicht illegalen, wohl aber inopportunen politischen Kampf bezeichnen und ihn mit Sanktion bedrohen.

Die neue Kategorie zu füllen und zu definieren oblag zuvörderst den VfS-Ämtern, deren Personal sich innerhalb von 10 - 15 Jahren verdoppelte und verdreifachte, unterstützt durch die Zuarbeit der Polizisten von Bund und Ländern. Hätte es nur neue Befugnisse, jedoch keine neuen Ressourcen an

Rössern und Reitern, Personal und neuen technischen Instrumenten wie der herausragenden EDV gegeben, so hätten die neuen Befugnisse nur zu mehr Willkür, nicht aber zur Ausweitung des staatschützerischen Überwachungs-wahnes führen können.

Die soziale, organisatorische und politische Diffusität der neuen demokratischen Bewegungen in der Bundesrepublik bedeutete dabei auch ein erhebliches internes Problem für die "Sicherheits"-Bürokratien. Diese "neue Unübersichtlichkeit", deren Akteure durch alle lieb gewonnenen Raster das traditionellen Antikommunismus der 50er und 60er Jahre fielen, für die Apparate übersichtlich werden zu lassen, verlangte ganz neue Raster und einen qualitativ breiteren, überwachenden Zugriff auf die Gesellschaft. Die Infrastruktur und die Methoden für diesen neuen Zugriff wurden in den 70er Jahren aufgebaut und entwickelt.

Soweit dieser Prozeß auch rechtlich zu fassen und zu legitimieren versucht wurde, drückte er sich in neuen, juristisch-dogmatisch nicht fixierten Kategorien aus, deren Konturenlosigkeit mit der Diffusität ihrer Anwendung korrespondierte.

Ordnet man die aktuell zur Debatte stehenden "Sicherheits"-Gesetze der CDU/CSU/FDP-Koalition in die hier holzschnittartig skizzierte Entwicklung ein, so ist zum wiederholten Male festzuhalten, daß diese Gesetze eine zu Zeiten der sozialliberalen Bonner Koalition forcierte Entwicklung bei den "Sicherheits"apparaten nur noch rechtlich festschreiben und mit der Weihe der Gesetzlichkeit ausstatten sollen.

Auch das Problem "Sicherheitsgesetze" ist vor allem ein Problem der lange unbefragten Anerkennung staatlicher Gefahrendefinitionen und darauf bezogener administrativer Sicherheitsversprechungen.

Erst das Akzeptieren dieser Gefahrendefinitionen und der Glaube an die ausschließliche Lösung von politischen und sozialen Problemen durch polizeiliche Maßnahmen läßt die mit den gewachsenen Befugnissen und technischen Möglichkeiten von Polizei und Geheimdiensten verbundenen Einschränkungen unserer Freiheiten als notwendige Folge erscheinen.

Dieser widerspruchslose Glaube beginnt auch in Bezug auf Polizei und Innenpolitik zu bröckeln. Auch hier gibt es Erosionsprozesse. Der Kreis derer, die die innerstaatlichen Feinderklärungen der VfS-Ämter ohne Zweifel akzeptieren, ist kleiner geworden. Mit Fleiß haben sich diese Ämter ideologisch selbst demontiert, so daß inzwischen auch jenseits des linksradikalen Spektrums öffentlich über ihre ersatzlose Abschaffung nachgedacht werden kann. Zugleich haben die öffentlichen Verrufserklärungen dieser Ämter längst nicht mehr die Wirksamkeit, wie noch vor fünf oder zehn Jahren. Von den Ämtern als Verfassungsfeinde deklarierte Personen sitzen heute in Parlamenten und Untersuchungsausschüssen über die Rolle dieser Ämter.

Auch in Bezug auf andere Bereiche - etwa den Drogenhandel und den Terrorismus, die seit Jahren die zentralen Rechtfertigungen für verdeckte polizeiliche Ermittlungen und Rasterfahndungen darstellen - wächst in der Öffentlichkeit die Überzeugung, daß politische und soziale Lösungen den Problemen eher gewachsen sind und ihnen

eher gerecht werden als rein polizeiliche. Diese Überlegungen gilt es zu fördern. Statt den Streit nur um einzelne Gesetze und einzelne polizeiliche Maßnahmen zu führen - so notwendig dies auch ist - gilt es, der Scheineffektivität polizeilicher Festnahmeerfolge und beschlagnahmter Drogenmengen andere, politische Konzepte entgegenzusetzen - von der innenpolitischen Liberalisierung und der Wiedereingliederung von RAF-Mitgliedern in die legale politische Auseinandersetzung bis zu Alternativen in der Drogenpolitik.

In Ansätzen scheint auch die für die bundesdeutsche Geschichte so charakteristische Allparteienkoalition in Sachen "Innerer Sicherheit" löchrig zu werden. Innerhalb der SPD, so in der Arbeitsgemeinschaft sozialdemokratischer Juristen, wird langsam begriffen, daß mit immer mehr Polizisten keineswegs mehr innere Sicherheit zu garantieren ist, Alternativen werden gesucht. Die Vereinheitlichung des Polizeirechts aller Bundesländer scheint gestorben, schaut man auf die Vielzahl im Detail unterschiedlicher Länderentwürfe; vehement ist die Kritik sozialdemokratischer Datenschutzbeauftragter an den Bonner Gesetzesentwürfen. Ein paar Schwalben machen noch keinen Sommer. Und daß es diese "Schwalben" gibt, ist vor allem ein Verdienst außerparlamentarisch arbeitender Gruppen und Bewegungen. Sie haben das traditionell herrschende Parteienkartell in politischen Teilbereichen zu Rücksichtnahmen - und sei es nur aus Opportunismus - gezwungen. Die neue Gesetzgebungswelle in Bonn bietet neue Chancen, die Diskussion darüber offensiv zu führen, wie der Schutz der BürgerInnen vor alltäglichen Gefährdungen

qualitativ neu zu bestimmen wäre, wie mit anderen denn polizeilichen und geheimdienstlichen Methoden mit Bedrohungen umgegangen und ihnen begegnet werden könnte. Es gilt, die Risse im herrschenden Parteienkartell zu erkennen und nach Möglichkeit zu vertiefen, ohne dabei eigene Hoffnungen und Utopien aufzugeben.

Aus dem 7. Tätigkeitsbericht des Hamburger Datenschutzbeauftragten:

Nochmals: Zum Übergangsbonus

Sollte das Paket mit den Datenschutz- und Sicherheitsgesetzen erneut im Bundestag scheitern, wären die Folgen insbesondere für die betroffenen Sicherheitsbehörden dramatisch. Nach — soweit ich sehe — übereinstimmender Auffassung in der Literatur und einer sich verfestigenden Rechtsprechung ist der Übergangsbonus, den der Gesetzgeber für die Schaffung gesetzlicher Grundlagen für die Informationstätigkeit beispielsweise der Polizei und der Nachrichtendienste in Anspruch nehmen kann, spätestens mit dem Ende dieser Wahlperiode des Bundestages verbraucht. Das bedeutet, daß ab 1991 Grundrechtseingriffe der Sicherheitsbehörden, die sich weiterhin nicht auf die erforderlichen bereichsspezifischen gesetzlichen Grundlagen stützen könnten, wegen fehlender verfassungsrechtlicher Legitimation als rechtswidrig angesehen werden müßten mit der Folge etwa, daß gleichwohl gespeicherte Daten gelöscht und dazugehörige Unterlagen vernichtet werden müßten.

Schon heute ist absehbar, daß zahlreiche Gesetze, die als Grundlage für Informations-eingriffe von Sicherheitsbehörden unabdingbar sind, bis zum Ende dieser Legislaturperiode nicht verabschiedet werden. Das gilt z.B. für das Gesetz über das Bundeskriminalamt und das Gesetz über das Ausländerzentralregister, für die bislang erst — kaum als Diskussionsgrundlage geeignete — Arbeitsentwürfe vorliegen, aber auch für die notwendigen Änderungen der Strafprozeßordnung, für die der Bundesjustizminister erst vor einigen Wochen einen Referentenentwurf versandt hat. Die Bundesregierung hat selbst eingeräumt (in Beantwortung einer Großen Anfrage des SPD-Bundestagsfraktion), daß es ihr nicht mehr möglich sein wird, eine Vorlage zur Novellierung der StPO noch rechtzeitig im Bundestag einzubringen. Das heißt, daß derselbe Bürger, dessen Antrag auf Löschung seiner Daten in der Zentralen Namenskartei der Staatsanwaltschaft Frankfurt das OLG Frankfurt durch Beschluß vom 14. Juli 1988 zurückgewiesen hatte, im Jahre 1991 seinen Antrag mit Erfolg wiederholen kann. Eben dies hat ihm das OLG Frankfurt in der Begründung seiner Entscheidung bescheinigt. Hiernach wird auch ein Hamburger Bürger nicht mehr hinnehmen müssen, daß seine Daten über das Jahr 1990 hinaus in der Zentralkartei der hiesigen Staatsanwaltschaft gespeichert bleiben.

I. Geheimdienst-Gesetze, Stand: Mai 1989

Zur Gesetzgebungsgeschichte der Geheimdienstgesetze

Daß das Bundesamt für Vfs und die parallelen Landesämter personenbezogene Informationen nicht nur aus eigener Ermittlungstätigkeit gewinnen, sondern ihre staatsschützerische Neugier auch mit Informationen befriedigen, die die Länderpolizeien, die Grenzkontrollbehörden (Bundesgrenzschutz, Bayer. Grenzschutz, Zoll), Staatsanwaltschaften etc. liefern, prägte die Arbeit dieser Ämter von Beginn an. In verschiedenen untergesetzlichen Regelungen, beginnend mit den sog. Unkeler Richtlinien von 1953, fortgesetzt u.a. mit den "Zusammenarbeitungsrichtlinien" von 1973, sind die beteiligten Staatssicherheitsbehörden auch entsprechend "in die Pflicht" genommen worden.

Daß sonstige staatliche Behörden, aber auch nicht-staatliche Organisationen wie der DGB, dessen Referat "Feinde der Demokratie" bereits 1951 mit dem Bundesamt für Vfs zur Abwehr von Kommunisten Namenslisten austauschte, ohne rechtlichen Zwang sich an diesem Informationsverbund beteiligten, ist gleichfalls bereits aus den 50er Jahren satzsaam bekannt.

In den siebziger Jahren wurde diese Praxis zum einen nachhaltig ausgeweitet, da der sog. Radikalenerlaß von 1972 mit der Regelanfrage beim Vfs für Bewerber um Stellen im öffentlichen Dienst und die Verdoppelung bis Verdreifachung des Personalbestandes der Vfs-Ämter die personellen Kapazitäten und Anlässe für diese Praxis systematisch erweiterten. Zum zweiten reagierte eine aufmerksamer werdende Öffentlichkeit auf diese sich qualitativ ausweitende Praxis mit wachsender Sensibilität und Empörung. Als Folge des "Radikalenerlasses" und der offenen Berufsverbotspraxis wurde über die entsprechenden Anhörungen von Bewerbern für den öffentlichen Dienst zudem etwas transparenter, in welchem Umfang die Vfs-Ämter personenbezogene Daten sammelten und wer alles als Zuträger sich anheischig gemacht hatte, respektive welche Behörden und Verwaltungen als Lieferanten in die Pflicht genommen worden waren - selbstverständlich von der Polizei bis zu universitären Immatrikulationsbüros, selbstverständlich von den Melderegistern bis hin zur AOK; von Denunzianten aus Leidenschaft, wie die "Nofu - Notgemeinschaft Freie Universität", noch abgesehen.

Nachhaltige Spuren im öffentlichen Bewußtsein hinterließ auch die 1978 bekanntgewordene Praxis, daß der BGS anhand von Publikationslisten, die das Bundesamt für Vfs lieferte, Vermerke über Lesegewohnheiten von Reisenden an das Bundeamt weiterleitete. Daß diese Praxis nicht aufgegeben wurde, zeigt die jüngste Antwort der Bundesregierung auf eine kleine Anfrage der Fraktion der GRÜNEN im Bundestag (vgl. Kästchen). Ein großes öffentliches Echo rief auch die 1979 bekanntgewordene Praxis hervor, daß der BGS-Einzeldienst auch für den BND an der Grenze zuarbeitete - dies auf Grundlage einer von Bundesinnenminister Maihofer 1975 erlassenen "Sonderanweisung über die Erfassung bestimmter Erkenntnisse bei grenzpolizeilichen Kontrollen (SOK-GK)". Sie wurde 1981 von Innenminister Baum durch die "Dienstanweisung zur Durchführung des Amtshilfeersuchens für die Vfs-Behörden und den BND" ersetzt.

Ergebnis dieser Skandale und der Fortentwicklung der datenschutzrechtlichen Diskussion, in der sich die Position festigte, daß auch die Erhebung von personenbezogenen Informationen rechtlich als Eingriff zu qualifizieren sei, entsprechend also gesetzlicher Grundlagen bedürfe, war die Forderung nach einem "Amtshilfe-Gesetz", das die Informationsströme zwischen den diversen "Sicherheitsbehörden" regeln sollte. Das Volkszählungsurteil von 1983 statuierte schließlich die Pflicht des Gesetzgebers zur gesetzlichen Regelung von Datenerhebung, Speicherung und Weitergabe.

Das Anfang der 80er Jahre diskutierte Amtshilfe-Gesetz wandelte sich im Laufe der Jahre zum "Zusammenarbeitsgesetz der Sicherheitsbehörden des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes" - kurz ZAG -, dessen 1. Entwurf diese Zeitschrift im Nov. 1985 öffentlich machte (Nr.21, S.95).

Als Querschnittsgesetz formulierte das ZAG Zusammenarbeitspflichten zwischen dem Bundesamt für VfS, dem MAD, dem BKA, dem BGS, den Landesämtern für VfS und den Länderpolizeien. Die zweite, 1986 dem Bundestag vorgelegte ZAG-Fassung (dok. in CILIP Nr.23) bezog auch die Staatsanwaltschaften und den BND in diese Zusammenarbeitspflichten mit ein und unterschob dem neuen Entwurf zudem einen Paragraphen 15, der als BND-Aufgaben- und Befugnisnorm ausgegeben wurde. Simitis, Hessens Datenschützer, formulierte in seiner Stellungnahme vom 22.1.86, daß mit Verabschiedung dieses Gesetzes "zum ersten Mal in der Geschichte der Bundesrepublik das Tor für die Geheimpolizei offen stünde".

Nun - soweit diese These am Informationsverbund zwischen den Staatsschutz-Apparaten festgemacht wird - war diese weniger eine Prognose als die Qualifizierung des Ist-Zustandes.

Der Versuch, diesen Entwurf zusammen mit weiteren Gesetzesentwürfen (VfS-Gesetz, MAD-Gesetz, Bundesdatenschutz-Gesetz, Verwaltungsverfahren-Gesetz) möglichst schnell durch den Bundestag zu jagen, schlug fehl. Die Detailfreude des ZAGs, in dem für die je konkreten Praktiken der informationellen Zusammen- und -arbeit aller Sicherheitsbehörden Einzelregelungen formuliert waren, erwies sich als allzu verräterisch und damit skandalisierbar.

Im Januar 1988 lege Bundesinnenminister Zimmermann ein überarbeitetes Paket sog. "Sicherheitsgesetze" mit denselben Regelungsbereichen wie im Paket von 1985/86 vor.

Zu den Retuschen, mit denen der bisherigen Kritik begegnet werden sollte, zählte eine Umbenennung des alten ZAG. Es hieß nun "VfS-Mitteilungsgesetz" (dok. in CILIP Nr.29, S.36 ff.). Aus dem Geltungsbereich des ZAG-Entwurfs wurden die Staatsanwaltschaften wieder herausgenommen. Ihre Mitteilungspflichten sollte ein Justizmitteilungsgesetz gesondert regeln (Vorentwurf dokumentiert in CILIP 29, S.61 ff.). Gesetzgebungstechnisch wurde der Entw. des VfS-Mitteilungs-Gesetzes - bei unverändert gleichbleibenden Intentionen - drastisch verändert, indem auf Einzelregelungen für den Datenfluß zwischen den einzelnen Sicherheitsapparaten verzichtet und die Zulässigkeit respektive die Verpflichtungen zur wechselseitigen Zuarbeit abstrakter formuliert wurden. Wie beim ZAG enthielt auch dieser Entwurf in § 10 Sätze, die in der Kommentierung als Aufgaben- und Befugnisnorm für den BND ausgege-

Aus:

Antwort der Bundesregierung

auf die Kleine Anfrage der Fraktion DIE GRÜNEN

- Drucksache 11/4198 -

Kontrolle von Zeitungs-Redaktionen und Überwachung von Bezieherinnen /innen "extremistischer" Literatur durch Bundeskriminalamt und Bundesamt für Verfassungsschutz

Deutscher Bundestag – 11. Wahlperiode

Drucksache 11/4294

4. a) Existiert – vergleichbar der Ende der 70er Jahre bei Grenzschutzbehörden kursierenden Liste – eine Aufzählung bestimmter verdächtiger Publikationen, deren erkannte Besitzer auf Anweisung von Bundesbehörden (oder nach Kenntnis der Bundesregierung: welcher Landesbehörden) zu registrieren bzw. zu melden sind?
- b) Welche Publikationen sind darauf enthalten?
- c) Welche Bundesbehörden insbesondere der Polizei und des Grenzschutzes sind mit dieser Liste ausgestattet?
- d) Seit wann sind diese Behörden angewiesen, erkannte Besitzer/innen von Publikationen dieser Liste in welcher Weise zu registrieren?

Seit Januar 1988 wird durch das Bundeskriminalamt eine Loseblattsammlung über terroristische Publikationen herausgegeben. Diese Sammlung enthält Schriftwerke, die Gegenstand von Ermittlungsverfahren des Generalbundesanwalts sind. Es handelt sich dabei um sogenannte illegale Untergrundzeitschriften. Die Sammlung dient dazu, alle beteiligten Dienststellen über das Erscheinen neuer illegaler Untergrundpublikationen zu unterrichten, bei Durchsuchungsmaßnahmen gezielt diese Schriften als Beweismittel sicherzustellen sowie die für das Herstellungs- und Vertriebssystem verantwortlichen Personen zu erkennen. Die Sammlung wird regelmäßig bereinigt. Das Auffinden solcher illegaler Druckwerke kann bei Mehrfachbesitz zur Einleitung von Ermittlungsverfahren führen, wenn eine Weiterverbreitung, d. h. eine Unterstützungshandlung nach § 129a StGB, vorliegt. Da die Sammlung – wie ausgeführt – Schriftwerke enthält, die Gegenstand von strafprozessualen Ermittlungsverfahren sind, ist eine Darstellung der einzelnen Schriften nicht möglich. Die Sammlung wird an folgende Bundesbehörden übermittelt: Bundesminister des Innern, Bundesamt für Verfassungsschutz, Grenzschutzdirektion, Zollkriminalinstitut.

ben wurden. Verzichtet wurde schließlich auf Blendwerk, mit dem noch das ZAG geschmückt war (so dem Hinweis auf das Trennungsgebot von Polizei und Geheimdiensten, so die ausdrückliche Einschränkung der Übermittlung von Daten Minderjähriger und die Unterscheidung der Mitteilungspflichten auf und ohne Ersuchen).

Parallel zu den Bemühungen des BMI arbeitete das Bundesministerium für Justiz daran, die StPO den Datenerhebungs- und Verarbeitungsbeugnissen der Polizei anzupassen. Die Innenministerkonferenz meldete polizeiliche Bedürfnisse in diversen "Musterentwürfen für ein einheitl. Polizeigesetz des Bundes und der Länder" an (Dokumentation/Kritik in CILIP 29).

Daran zu erinnern ist insoweit notwendig, als zum einen der Polizei der Einsatz nachrichtendienstlicher Mittel (vgl. insb. den § 8c ME, "besondere Formen der Datenerhebung", CILIP 24, S.76) zugebilligt werden soll, also geheimdienstliche Mittel. Diese Angleichung der Methoden und Mittel von Polizei und Geheimdiensten macht andererseits die in § 6 Abs.1 des BVerfSchG-Entw. formulierte Einschränkung praktisch obsolet, daß die Dienste der Polizei nur jene personenbezogenen Informationen abverlangen dürfen, die sie auch aus eigener Zuständigkeit erheben dürften; in dem Maße, wie sich die Polizei "aus eigenem Recht" geheimdienstlicher Methoden und Mittel bedient, werden die damit gewonnenen personenbezogenen Informationen auch den Diensten zugänglich.

Aus dem nun vom Bundestag am 28.4. d.J. in 1. Lesung verabschiedeten Gesetzes-Paket sind - wie gesagt - ZAG und Mitteilungsgesetz als eigenständige Querschnittsgesetze in Gänze verschwunden.

Als neue Lösung wurde der Weg gewählt, entsprechende Zusammenarbeitspflichten in den Gesetzen zu verstecken, die die Aufgaben und Befugnisse der einzelnen beteiligten Geheimdienstbehörden regeln (BVerfSchG, dem MAD- und dem BND-Gesetz). Da ein Querschnittsgesetz entfallen ist, in dem bisher jeweils eine BND-Aufgaben- und -Befugnisnorm hineingeschoben worden war, ergab sich die Notwendigkeit, nun auch ein eigenständiges BND-Gesetz zu formulieren.

Der Regelungsbereich des ZAGs und des folgenden VfS-Mitteilungsgesetzes ist gesetzgebungstechnisch nicht verschwunden, sondern auf eine Fülle von Einzelparagraphen in einer Reihe von Einzelgesetzen verteilt. Im Kern lassen sich ZAG und Folgeentwurf nun finden in den §§ 12-18 des vorliegenden BVerfSchG, jetzt durchmischt - und damit noch unübersichtlicher - mit Befugnissen des Bundesamtes für VfS zur Datenabforderung gegenüber Stellen außerhalb des staatschützerischen Sicherheitsverbundes. Im MAD- und BND-Gesetz wird nur noch auf die parallelen Regelungen im BVerfSchG verwiesen.

Dieser Systematik folgend, liegt das Schwergewicht unserer Detailkritik beim BVerfSchG. Soweit das MAD- und BND-Gesetz jenseits der Aufgabennormen auf das BVerfSchG verweist, bitten wir, dieser Logik folgend, unsere dortige Kommentierung anzuschauen.

Dokumentation:

Artikel 3

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz - BVerfSchG -)

ERSTER ABSCHNITT

Zusammenarbeit, Aufgaben der Verfassungsschutzbehörden

§ 1

Zusammenarbeitspflicht

(1) Der Verfassungsschutz dient dem Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes und der Länder.

(2) Der Bund und die Länder sind verpflichtet, in Angelegenheiten des Verfassungsschutzes zusammenzuarbeiten.

(3) Die Zusammenarbeit besteht auch in gegenseitiger Unterstützung und Hilfeleistung.

§ 2

Verfassungsschutzbehörden

(1) Für die Zusammenarbeit des Bundes mit den Ländern unterhält der Bund ein Bundesamt für Verfassungsschutz als Bundesoberbehörde. Es untersteht dem Bundesminister des Innern. Das Bundesamt für Verfassungsschutz darf einer polizeilichen Dienststelle nicht angegliedert werden.

(2) Für die Zusammenarbeit der Länder mit dem Bund und der Länder untereinander unterhält jedes Land eine Behörde zur Bearbeitung von Angelegenheiten des Verfassungsschutzes.

§ 3

Aufgaben der Verfassungsschutzbehörden

(1) Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern der Verfassungsorgane des Bundes oder eines Landes zum Ziele haben,
2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,

3. Bestrebungen im Geltungsbereich dieses Gesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden.

(2) Die Verfassungsschutzbehörden des Bundes und der Länder wirken mit

1. bei der Überprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können,
2. bei der Überprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen,
3. bei technischen Sicherheitsmaßnahmen zum Schutz von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnisnahme durch Unbefugte.

Das Bundesamt für Verfassungsschutz darf, soweit gesetzlich nichts anderes bestimmt ist, eine Überprüfung nach Satz 1 nur mit Kenntnis des Betroffenen durchführen; wird der Ehegatte, Verlobte oder die Person, mit der der Betroffene in ehelicher Gemeinschaft lebt, in die Überprüfung miteinbezogen, so ist auch deren Kenntnis erforderlich.

§ 4

Gegenseitige Unterrichtung der Verfassungsschutzbehörden

(1) Die Verfassungsschutzbehörden unterrichten einander über alle Angelegenheiten, deren Kenntnis zur Erfüllung ihrer Aufgaben erforderlich ist.

(2) Die Verfassungsschutzbehörden sind verpflichtet, beim Bundesamt für Verfassungsschutz zur Erfüllung der Unterrichtungspflichten nach Absatz 1 gemeinsame Dateien zu führen, die sie im automatisierten Verfahren nutzen. Diese Dateien enthalten nur die Daten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Die Speicherung personenbezogener Daten ist nur unter den Voraussetzungen des § 8 zulässig. Der Abruf im automatisierten Verfahren durch andere Stellen ist nicht zulässig. Die Verantwortung einer speichernden Stelle im Sinne der allgemeinen Vorschriften des Datenschutzrechts trägt jede Verfassungsschutzbehörde nur für die von ihr eingegebenen Daten; nur sie darf diese Dateien verändern, sperren oder löschen. Die eingebende Stelle muß feststellbar sein. Das Bundesamt für Verfassungsschutz trifft für die gemeinsamen Dateien die technischen und organisatorischen Maßnahmen nach § 8 des Bundesdatenschutzgesetzes. Textdateien oder Dateien, die weitere als die in Satz 2 genannten Daten enthalten, dürfen unter den Voraussetzungen dieses Absatzes geführt werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, daß jemand eine der in § 2 Abs. 1 Nr. 1 bis 7 des Gesetzes zu Artikel 10 Grundgesetz genannten Straftaten plant, begeht oder begangen hat.

§ 5

Weisungsrechte des Bundes

Die Bundesregierung kann, wenn ein Angriff auf die verfassungsmäßige Ordnung des Bundes erfolgt, den obersten Landesbehörden die für die Zusammenarbeit der Länder mit dem Bund auf dem Gebiete des Verfassungsschutzes erforderlichen Weisungen erteilen.

ZWEITER ABSCHNITT

Bundesamt für Verfassungsschutz

§ 6

Befugnisse des Bundesamtes für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen erheben, verarbeiten und nutzen, soweit nicht die §§ 7 bis 15 die Erhebung und Übermittlung personenbezogener Informationen sowie die Verarbeitung und Nutzung personenbezogener Daten in Dateien besonders regeln. Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung (nachrichtendienstliche Mittel) anwenden; diese sind in einer Dienstvorschrift zu benennen. Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesamt für Verfassungsschutz nicht zu; es darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen es selbst nicht befugt ist.

(2) Von mehreren geeigneten Maßnahmen hat das Bundesamt für Verfassungsschutz diejenige zu wählen, die den Betroffenen voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

§ 7

Erhebung personenbezogener Informationen mit nachrichtendienstlichen Mitteln

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Informationen mit nachrichtendienstlichen Mitteln erheben, wenn tatsächliche Anhaltspunkte dafür vorhanden sind, daß

1. auf diese Weise Erkenntnisse über Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 oder die zur Erforschung solcher Erkenntnisse erforderlichen Nachrichtenzugänge gewonnen werden können oder
2. dies zur Abschirmung der Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge des Bundesamtes für Verfassungsschutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist.

Die Erhebung nach Satz 1 ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, den Betroffenen weniger beeinträchtigende Weise möglich ist; eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen oder durch eine Auskunft nach § 12 Abs. 2 oder § 13 Abs. 2 gewonnen werden kann. Die Anwendung des nachrichtendienstlichen Mittels darf nicht erkennbar außer Verhältnis zur Bedeutung des

aufzuklärenden Sachverhaltes stehen. Die Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich Anhaltspunkte dafür ergeben, daß er nicht oder nicht auf diese Weise erreicht werden kann.

(2) Die Kommission nach § 9 Abs. 2 des Gesetzes zu Artikel 10 Grundgesetz ist in regelmäßigen Abständen über Erhebungen nach Absatz 1, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, zu unterrichten.

§ 8

Speicherung, Veränderung und Nutzung personenbezogener Daten in Dateien

(1) Das Bundesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben personenbezogene Daten in Dateien speichern, verändern und nutzen, wenn

1. tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 vorliegen,
2. dies für die Erforschung und Bewertung von Bestrebungen und Tätigkeiten nach § 3 Abs. 1 erforderlich ist oder
3. das Bundesamt für Verfassungsschutz nach § 3 Abs. 2 tätig wird.

(2) Daten über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres dürfen nicht in Dateien gespeichert werden. Daten über das Verhalten Minderjähriger nach Vollendung des 16. Lebensjahres sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, daß nach Eintritt der Volljährigkeit weitere Erkenntnisse nach § 3 Abs. 1 angefallen sind.

(3) Das Bundesamt für Verfassungsschutz hat die Speicherdauer auf das für seine Aufgabenerfüllung erforderliche Maß zu beschränken.

§ 9

Berichtigung, Löschung und Sperrung von personenbezogenen Daten in Dateien

(1) Das Bundesamt für Verfassungsschutz hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, wenn sie unrichtig sind.

(2) Das Bundesamt für Verfassungsschutz hat die in Dateien gespeicherten personenbezogenen Daten zu löschen, wenn ihre Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, daß durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden. In diesem Falle sind die Daten zu sperren. Sie dürfen nur noch mit Einwilligung des Betroffenen übermittelt werden.

(3) Das Bundesamt für Verfassungsschutz prüft bei der Einzelfallbearbeitung und nach festgesetzten Fristen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind.

§ 10

Dateianordnungen

(1) Für jede automatisierte Datei beim Bundesamt für Verfassungsschutz nach § 4 Abs. 2 oder § 8 sind in einer Dateianordnung, die der Zustimmung des Bundesministers des Innern bedarf, festzulegen:

1. Bezeichnung der Datei,
2. Zweck der Datei,
3. Voraussetzungen der Speicherung, Übermittlung und Nutzung (betroffener Personenkreis, Arten der Daten),
4. Anlieferung oder Eingabe,
5. Zugangsberechtigung,
6. Überprüfungsfristen, Speicherdauer,
7. Protokollierung.

Der Bundesbeauftragte für den Datenschutz ist vor Erlaß einer Dateianordnung anzuhören.

(2) Die Speicherung personenbezogener Daten ist auf das erforderliche Maß zu beschränken. In angemessenen Abständen ist die Notwendigkeit der Weiterführung oder Änderung der Dateien zu überprüfen.

§ 11

Berichtspflicht des Bundesamtes für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz unterrichtet den Bundesminister des Innern laufend und auf Anforderung über seine Tätigkeit und die Mitglieder der Bundesregierung unmittelbar über Bestrebungen und Tätigkeiten nach § 3 Abs. 1, die für ihren Zuständigkeitsbereich von Bedeutung sind. Hierbei ist auch die Übermittlung personenbezogener Informationen zulässig.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch den Bundesminister des Innern über Bestrebungen und Tätigkeiten nach § 3 Abs. 1. Dabei dürfen auch personenbezogene Informationen bekanntgegeben werden, wenn schutzwürdige Interessen des Betroffenen nicht vorliegen oder die Interessen der Allgemeinheit überwiegen.

DRITTER ABSCHNITT

Übermittlungsvorschriften

§ 12

Übermittlung von Informationen an das Bundesamt für Verfassungsschutz

(1) Die Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts dürfen von sich aus dem Bundesamt für Verfassungsschutz die ihnen bekanntgewordenen Informationen

übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz nach § 3 Abs. 1 erforderlich ist.

(2) Das Bundesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben die Übermittlung der erforderlichen Informationen von jeder Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, verlangen, wenn die Informationen nicht aus allgemein zugänglichen Quellen oder nur mit übermäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden können. Würde durch die Übermittlung nach Satz 1 der Zweck der Maßnahme gefährdet oder der Betroffene unverhältnismäßig beeinträchtigt, darf das Bundesamt für Verfassungsschutz amtliche Register einsehen. Das Bundesamt für Verfassungsschutz braucht Ersuchen nicht zu begründen, soweit dies dem Schutz des Betroffenen dient oder eine Begründung den Zweck der Maßnahme gefährden würde. Es hat die Ersuchen aktenkundig zu machen. Über die Einsichtnahme nach Satz 2 hat das Bundesamt für Verfassungsschutz einen Nachweis zu führen, aus dem der Zweck, die ersuchte Behörde und die Aktenfundstelle hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten.

§ 13

Übermittlung von Informationen durch Strafverfolgungs- und Sicherheitsbehörden an das Bundesamt für Verfassungsschutz

(1) Die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie der Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, und der Bundesnachrichtendienst übermitteln dem Bundesamt für Verfassungsschutz von sich aus die ihnen bekanntgewordenen Informationen, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz nach § 3 Abs. 1 erforderlich ist.

(2) Das Bundesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben von den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien sowie vom Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, und vom Bundesnachrichtendienst die Übermittlung der erforderlichen Informationen verlangen. Das Bundesamt für Verfassungsschutz braucht Ersuchen nicht zu begründen, soweit dies dem Schutz des Betroffenen dient oder eine Begründung den Zweck der Maßnahme gefährden würde. Es hat die Ersuchen aktenkundig zu machen.

(3) Die Übermittlung personenbezogener Informationen, die aufgrund einer Maßnahme nach § 100 a der Strafprozeßordnung bekanntgeworden sind, ist nach den Vorschriften der Absätze 1 und 2 nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, daß jemand eine der in § 2 des Gesetzes zu Artikel 10

Grundgesetz genannten Straftaten plant, begeht oder begangen hat. Auf die dem Bundesamt für Verfassungsschutz nach Satz 1 übermittelten Unterlagen findet § 7 Abs. 3 und 4 des Gesetzes zu Artikel 10 Grundgesetz entsprechende Anwendung.

§ 14

Übermittlung personenbezogener Informationen durch das Bundesamt für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Informationen an Behörden übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder der Empfänger die Informationen zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. Der Empfänger darf die übermittelten Informationen, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

(2) Das Bundesamt für Verfassungsschutz darf personenbezogene Informationen an Dienststellen der Stationierungsstreitkräfte im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Streitkräfte vom 3. August 1959 (BGBl. 1961 II S. 1183) übermitteln. Der Empfänger ist darauf hinzuweisen, daß die übermittelten Informationen nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden.

(3) Das Bundesamt für Verfassungsschutz darf personenbezogene Informationen an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist. Die Übermittlung unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Die Übermittlung ist aktenkundig zu machen. Der Empfänger ist darauf hinzuweisen, daß die übermittelten Informationen nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden.

(4) Personenbezogene Informationen dürfen an andere Stellen nicht übermittelt werden, es sei denn, daß zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes erforderlich ist und der Bundesminister des Innern seine Zustimmung erteilt hat. Das Bundesamt für Verfassungsschutz führt über die Auskunft nach Satz 1 einen Nachweis, aus dem der Zweck der Übermittlung, die Aktenfundstelle und der Empfänger hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten. Der Empfänger darf die übermittelten Informationen nur für den Zweck verwenden, zu dem sie ihm übermittelt wurden.

§ 15

Übermittlung von Informationen durch das Bundesamt für Verfassungsschutz an Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes

(1) Das Bundesamt für Verfassungsschutz übermittelt den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien von sich aus die ihm bekanntgewordenen Informationen, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung zur Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist. Delikte nach Satz 1 sind die in §§ 74 a und 120 des Gerichtsverfassungsgesetzes genannten Straftaten sowie sonstige Straftaten, bei denen aufgrund ihrer Zielsetzung, des Motivs des Täters oder des Beschuldigten oder deren Verbindung zu einer Organisation tatsächliche Anhaltspunkte dafür vorliegen, daß sie gegen die in Artikel 73 Nr. 10 Buchstabe b oder c des Grundgesetzes genannten Schutzgüter gerichtet sind. Das Bundesamt für Verfassungsschutz übermitteln dem Bundesnachrichtendienst von sich aus die ihm bekanntgewordenen Informationen, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der gesetzlichen Aufgaben des Empfängers erforderlich ist.

(2) Die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien dürfen zur Verhinderung oder Verfolgung von Staatsschutzdelikten nach Absatz 1 Satz 2 vom Bundesamt für Verfassungsschutz die Übermittlung der erforderlichen Informationen verlangen. Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben vom Bundesamt für Verfassungsschutz die Übermittlung der erforderlichen Informationen verlangen. Die Ersuchen nach Satz 1 und 2 sind aktenkundig zu machen. Sie brauchen nicht begründet zu werden, soweit dies dem Schutz des Betroffenen dient oder eine Begründung den Zweck der Maßnahme gefährden würde; bei Ersuchen zu Zwecken der Strafverfolgung genügt die Angabe des Ermittlungsverfahrens.

§ 16

Übermittlung von Informationen an die Verfassungsschutzbehörden der Länder

(1) Die Verfassungsschutzbehörden der Länder dürfen zur Erfüllung der ihnen durch Gesetz übertragenen Aufgaben von den Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts die Übermittlung von Informationen unter den Voraussetzungen des § 12 Abs. 2 verlangen.

(2) Der Bundesnachrichtendienst, der Militärische Abschirmdienst, die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie der Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, übermitteln den Verfassungsschutzbehörden der Länder Informationen unter den Voraussetzungen des § 13. Auf die Übermittlung von Informationen zwi-

schen Behörden desselben Bundeslandes findet Satz 1 keine Anwendung.

§ 17

Übermittlung von Informationen durch die Verfassungsschutzbehörden der Länder an Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes

(1) Die Verfassungsschutzbehörden der Länder übermitteln den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien Informationen unter den Voraussetzungen des § 15 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1, 3 und 4. Auf die Übermittlung von Informationen zwischen Behörden desselben Bundeslandes findet Satz 1 keine Anwendung.

(2) Die Verfassungsschutzbehörden der Länder übermitteln dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst Informationen unter den Voraussetzungen des § 15 Abs. 1 Satz 3 sowie Abs. 2 Satz 2 bis 4.

§ 18

Übermittlung von Informationen durch die Staatsanwaltschaften und Polizeien an den Militärischen Abschirmdienst

Für die Übermittlung von Informationen durch die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie den Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, an den Militärischen Abschirmdienst findet § 13 entsprechende Anwendung.

§ 19

Übermittlungsverbote

Die Übermittlung nach den Vorschriften dieses Abschnitts unterbleibt, wenn

1. für die übermittelnde Stelle erkennbar ist, daß unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen,
2. überwiegende Sicherheitsinteressen dies erfordern oder
3. besondere gesetzliche Übermittlungsregelungen entgegenstehen.

§ 20

Minderjährigenschutz

(1) Die Übermittlung von Informationen über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres durch die Strafverfolgungs- und Sicherheitsbehörden nach den Vorschriften dieses Abschnitts ist nur zulässig

1. durch die Verfassungsschutzbehörden, wenn die Übermittlung zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich ist,
2. durch die Staatsanwaltschaften und Polizeien sowie zwischen den Verfassungsschutzbehörden, dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst, wenn jemand eine der in § 2 des Gesetzes zu Artikel 10 Grundgesetz genannten Straftat plant, begeht oder begangen hat.

(2) Informationen über das Verhalten Minderjähriger nach Vollendung des 16. Lebensjahres dürfen durch die Verfassungsschutzbehörden nach den Vorschriften dieses Abschnitts übermittelt werden, solange die Voraussetzungen der Speicherung nach § 8 Abs. 2 Satz 2 erfüllt sind. Liegen diese Voraussetzungen nicht mehr vor, bleibt eine Übermittlung nur zulässig, wenn sie zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich ist.

(3) Die Absätze 1 und 2 gelten nicht, wenn der Betroffene nach § 3 Abs. 2 Nr. 1 oder 2 überprüfbar wird; sie gelten auch nicht für minderjährige Staatsangehörige aus Staaten, deren Staatsangehörige vor der Einreise in den Geltungsbereich des Ausländergesetzes einer Aufenthaltserlaubnis bedürfen oder minderjährige Staatenlose aus diesen Staaten.

§ 21

Pflichten des Empfängers

Der Empfänger prüft, ob die nach den Vorschriften dieses Gesetzes übermittelten personenbezogenen Informationen für die Erfüllung seiner Aufgaben erforderlich sind. Ergibt die Prüfung, daß sie nicht erforderlich sind, hat er die Unterlagen zu vernichten. Die Vernichtung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unververtretbarem Aufwand möglich ist; in diesem Fall sind die Informationen zu sperren.

§ 22

Nachberichterstattung

Erweisen sich personenbezogene Informationen nach ihrer Übermittlung nach den Vorschriften dieses Gesetzes als unvollständig oder unrichtig, so sind sie unverzüglich gegenüber dem Empfänger zu berichtigen, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

§ 23

Automatisierte Abrufverfahren

Die Einrichtung eines automatisierten Verfahrens für Übermittlungen von personenbezogenen Daten nach §§ 13, 15, 16 Abs. 2, §§ 17 und 18 ist nach Maßgabe des § 9 des Bundesdatenschutzgesetzes in der Fassung des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes nur zulässig, wenn eine erhebliche Beeinträchtigung der freiheitlichen demokratischen Grundordnung droht oder eine konkrete Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes besteht und der für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesminister oder deren Vertreter der Einrichtung des Verfahrens zugestimmt haben. Die Einrichtung des Verfahrens ist zu befristen und der Abruf bei der speichernden Stelle aufzuzeichnen.

VIERTER ABSCHNITT

Schlußvorschriften

§ 24

Geltung des Verwaltungsverfahrensgesetzes und des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 3 durch das Bundesamt für Verfassungsschutz finden die §§ 3 a und 3 c des Verwaltungsverfahrensgesetzes und die §§ 12 bis 16 und § 18 des Bundesdatenschutzgesetzes in der Fassung des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes keine Anwendung.

§ 25

Berlin-Klausel

Dieses Gesetz gilt nach Maßgabe des § 13 Abs. 1 des Dritten Überleitungsgesetzes auch im Land Berlin.

Zu Artikel 3 (Bundesverfassungsschutzgesetz)**A. Allgemeines****1. Ziel der Novelle**

Der Gesetzentwurf verfolgt das Ziel, das Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes vom 27. September 1950 (BGBl. S. 682), geändert durch Verfassungsschutzänderungsgesetz vom 7. August 1972 (BGBl. I S. 1382), fortzuentwickeln. Hierbei ist die Rechtsfortbildung in der Bundesrepublik Deutschland im wesentlichen in zwei Bereichen bestimmend: Zum einen handelt es sich um die Tendenz, neben einer Aufgabenbeschreibung auch das Instrumentarium für hoheitliches Handeln in Form von „Befugnisnormen“ durch den Gesetzgeber selbst festzulegen; zum anderen legt das durch Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (E 65, 1 ff.) unter dem Gesichtspunkt moderner Datenverarbeitung eingehend interpretierte allgemeine Persönlichkeitsrecht mit Blick auf die Tätigkeiten der Verfassungsschutzbehörden eine ausdrückliche Regelung seiner Einschränkungen durch den Bundesgesetzgeber nahe.

Das Bundesverfassungsgericht hat sich in seinem Urteil zum Volkzählungsgesetz vom 15. Dezember 1983 (BVerfGE 65, 1 ff.) mit der zwangsweisen Erhebung personenbezogener Daten zu statistischen Zwecken und mit der Zulässigkeit ihrer Nutzung für Zwecke des Verwaltungsvollzugs befaßt. Nach allgemeiner Meinung enthält die Entscheidung darüber hinaus grundsätzliche rechts- und verfassungspolitisch bedeutsame Aussagen zum allgemeinen Persönlichkeitsrecht. Es ist mithin für alle Bereiche der Verwaltung, in denen personenbezogene Daten erhoben und verarbeitet werden, zu beachten.

Der Gesetzentwurf soll Rechtsgrundlagen und Tätigkeiten des Bundesamtes für Verfassungsschutz klarer beschreiben und insbesondere näher bestimmen, unter welchen Voraussetzungen es personenbezogene Informationen erheben, verarbeiten und nutzen darf. Die Frage, ob und inwieweit die gesetzlichen Änderungen im einzelnen verfassungsrechtlich geboten oder lediglich rechtspolitisch erwünscht sind, kann letztlich unbeantwortet bleiben. Im Hinblick auf die Vielzahl der Änderungen ist eine gesetzliche Neufassung erfolgt.

2. Gesetzgebungskompetenz des Bundes

Der Bund besitzt für die Regelung der Zusammenarbeit zwischen Bund und Ländern zum Zwecke des Verfassungsschutzes einschließlich des Schutzes auswärtiger Belange der Bundesrepublik Deutschland die ausschließliche Gesetzgebungskompetenz nach Artikel 73 Nr. 10 Buchstaben b und c GG.

Zweck des Verfassungsschutzes und der darauf gerichteten Zusammenarbeit ist der Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes und der Länder und

der Schutz gegen Bestrebungen im Bundesgebiet, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden. Die Befugnis des Bundes zur Regelung der Zusammenarbeit bezieht sich ihrem Inhalt nach darauf, die Zusammenarbeit sowohl des Bundes mit den Ländern als auch der Länder untereinander zu regeln.

Die Gesetzgebungskompetenz des Bundes umfaßt mehr als die bloße Befugnis, die Einrichtung von Behörden vorzuschreiben, die im Bund und bei den Ländern zur Bearbeitung von Angelegenheiten des Verfassungsschutzes zuständig sein sollen. Der Bundesgesetzgeber kann insbesondere den in Artikel 73 Nr. 10 GG und Artikel 87 Abs. 1 Satz 2 GG verwendeten Begriff des Verfassungsschutzes sowie des Schutzes auswärtiger Belange näher umschreiben und inhaltlich konkretisieren, wie dies für den Aufgabenbereich des nachrichtendienstlichen Verfassungsschutzes bereits durch das Verfassungsschutzgesetz von 1950 vorgenommen wurde. Die Regelung der Zusammenarbeit schließt auch das Abstimmen und Koordinieren der Tätigkeit von Bundes- und Landesbehörden ein. Eine derartige Abstimmung und Koordination ist nur möglich, wenn ein Mindestmaß gemeinsamer Aufgabenbereiche von Bundes- und Landesbehörden konkretisiert und festgelegt wird.

B. Im einzelnen

Zur Gesetzesüberschrift

Die Überschrift des Gesetzes wird um eine Kurzform und um eine amtliche Abkürzung ergänzt. Hierdurch werden das Zitieren des Gesetzes und die Unterscheidung von den Verfassungsschutzgesetzen der Bundesländer erleichtert.

Zu §§ 1ff.

Alle Vorschriften erhalten eine Überschrift. Dies entspricht der heutigen Gesetzgebungspraxis.

Zu § 1

Die Vorschrift übernimmt in Absatz 2 und 3 wortgleich den § 1 des geltenden Rechts.

Zu § 2

Bund und Länder sind zur Unterhaltung von Verfassungsschutzbehörden verpflichtet. Die Vorschrift entspricht weitgehend dem bisherigen § 2. Da die Verfassungsschutzbehörden fast 40 Jahre bestehen, kann im Zuge der Neufassung der Vorschrift auf die Verpflichtung zur Errichtung oder Bestimmung der Verfassungsschutzbehörden verzichtet werden.

Zur Klarstellung der Rechtslage, die schon bisher aus der Auslegung des § 1 Abs. 1 des geltenden Gesetzes

abzuleiten war, wird die Zusammenarbeit der Verfassungsschutzbehörden der Länder untereinander in § 2 Abs. 2 ausdrücklich normiert.

Zu § 3

§ 3 regelt die Aufgaben der Verfassungsschutzbehörden (nachrichtendienstlicher Verfassungsschutz). Sie müssen von allen Verfassungsschutzbehörden des Bundes und der Länder wahrgenommen werden. Daneben bleibt es den Gesetzgebern der Länder freigestellt, im Rahmen ihrer Gesetzgebungskompetenz den jeweiligen Verfassungsschutzbehörden weitergehende Aufgaben zuzuweisen, soweit hierdurch nicht eine Beeinträchtigung der Aufgabenstellung nach diesem Gesetz stattfindet.

§ 3 Abs. 1 führt den Begriff der „Information“ ein, der in weiteren Regelungen mehrfach Verwendung findet. Information ist ein Oberbegriff, der sowohl personenbezogene als auch sachbezogene Vorgänge umfaßt, als auch unabhängig vom Medium ist, auf dem die Information verfestigt ist; zu den „Unterlagen“ sind beispielsweise Flugschriften, Broschüren, Fotografien und ähnliches zu rechnen. Für Informationen mit Dateibezug verwendet der Entwurf den Begriff Daten.

Unter dem Begriff „Bestrebungen“ i. S. von § 3 Abs. 1 Nr. 1 und 3 sind aktive Verhaltensweisen zu verstehen, die auf die Beseitigung oder Beeinträchtigung von Grundwerten der freiheitlichen Demokratie in der Bundesrepublik Deutschland oder eines sonstigen der im Gesetz aufgezählten Schutzgüter gerichtet sind. Die Prinzipien der freiheitlichen demokratischen Grundordnung sind durch die Rechtsprechung (BVerfGE 2, 1ff. und 5, 85ff.) sowie durch den Gesetzgeber in § 92 des Strafgesetzbuches inhaltlich festgelegt worden. Darüber hinaus knüpft § 3 Abs. 1 Nr. 1 und 3 an die Begriffe „Bestand und Sicherheit der Bundesrepublik Deutschland“ an, so wie sie der Gesetzgeber in § 92 StGB ebenfalls definiert hat.

§ 3 Abs. 2 Satz 1 entspricht dem geltenden Recht; er regelt auch die Mitwirkung des Bundesamtes für Verfassungsschutz im Bereich des Geheimschutzes. Er wird im Vorgriff auf ein künftiges Geheimschutzgesetz um einen Satz 2 ergänzt. Danach dürfen Sicherheitsüberprüfungen grundsätzlich nur mit Kenntnis des Betroffenen und der ggf. in die Überprüfung einbezogenen Personen durchgeführt werden. Die Bundesregierung beabsichtigt, alsbald den Entwurf eines Geheimschutzgesetzes vorzulegen, in dem u. a. die Mitwirkung des Bundesamtes für Verfassungsschutz an Sicherheitsüberprüfungen abschließend geregelt wird. Zugleich wird dann § 3 Abs. 2 Satz 2 entbehrlich; die Befugnisnormen des Gesetzes werden entsprechend anzupassen sein.

Soweit in § 3 Abs. 3 des geltenden Gesetzes Befugnisse des Bundesamtes für Verfassungsschutz geregelt sind, finden sich entsprechende Normen bei den Befugnisvorschriften der §§ 6ff. dieses Entwurfs.

Zu § 4

Die Vorschrift regelt die gegenseitige Unterrichtung der Verfassungsschutzbehörden von Bund und Ländern. Sie stellt die schon bisher geltende Rechtslage (§ 4) dahin gehend klar, daß die Zusammenarbeitspflicht auch für die Länder untereinander gilt (vgl. BVerwG NJW 1984, 1636). Übermittlungsmaßstab sind die Angelegenheiten, deren Kenntnis zur Erfüllung der gesetzlich übertragenen Aufgaben erforderlich ist.

Absatz 2 regelt ausschließlich die Voraussetzungen für Einrichtung und Nutzung von automatisierten Verbunddateien durch die Verfassungsschutzbehörden. Eine Speicherung — auch durch die Verfassungsschutzbehörden der Länder — darf nur unter den Voraussetzungen des § 8 erfolgen. Es sind zwei Arten von Verbunddateien zu unterscheiden: Aktenhinweissysteme (Satz 2) sowie Dateien mit Textzusätzen (Satz 8). Solche Textdateien dürfen nur zur Aufklärung von geheimdienstlichen Tätigkeiten oder zur Beobachtung von bestimmten Formen des politischen Extremismus, insbesondere wenn sie darauf gerichtet sind, Gewalt anzuwenden, eingerichtet werden.

Absatz 2 setzt voraus, daß speichernde Stelle hinsichtlich des gesamten Datenbestandes alle beteiligten Verfassungsschutzbehörden, aber auch nur diese, sind. Der Abruf von Daten aus diesen Dateien ist demnach als Nutzung und nicht als Abruf im automatisierten Verfahren im Sinne von § 9 des Bundesdatenschutzgesetzes zu qualifizieren. Die Verantwortung als speichernde Stelle nach allgemeinem Datenschutzrecht trägt allerdings ausschließlich die eingebende Stelle. Sie entscheidet beispielsweise über Auskunfts- und Berichtigungsbegehren. Nach § 6 Abs. 2 des Bundesdatenschutzgesetzes kann sich der Betroffene jedoch an jede speicherungsberechtigte Stelle wenden, um seine Datenschutzrechte geltend zu machen.

Die Voraussetzung für die Errichtung von nur dem Bundesamt für Verfassungsschutz zur Verfügung stehenden Dateien (Amtdateien) sind in § 8 geregelt. Für die Verfassungsschutzbehörden der Länder sieht der Entwurf keine vergleichbare Regelung vor.

§ 4 Abs. 3 des geltenden Rechts, der neben der Information der Verfassungsschutzbehörden auch die der Innenminister der Länder vorsieht, wird in den Entwurf nicht übernommen, da ein entsprechender Informationsaustausch zwischen Landesbehörde für Verfassungsschutz und jeweiligem Landesinnenminister ohnehin nach Landesrecht stattfindet. Insofern besteht für den Bund kein Regelungsbedarf.

Zu § 5

Die Vorschrift gibt den § 5 Abs. 1 des geltenden Rechts wieder. Sie folgt aus der Bundeskompetenz zur Regelung der Angelegenheiten des Verfassungsschutzes gemäß Artikel 73 Nr. 10 Buchstaben b und c GG.

Zu § 6

Die Vorschrift stellt die grundlegende Befugnisnorm für das Bundesamt für Verfassungsschutz dar, nach der es berechtigt ist, zur Erfüllung seiner Aufgaben die erforderlichen Erkenntnisse zu beschaffen, weiterzugeben und zu verwenden. Absatz 1 Satz 1 verwendet hierfür den Begriff „Informationen erheben, verarbeiten und nutzen“. Von einer darüber hinausgehenden Regelung der Sammlung personenbezogener Informationen in Akten wird abgesehen.

§ 6 ist gegenüber den §§ 7 bis 15 keine Auffangvorschrift, es besteht das Verhältnis Generalbefugnis zu Spezialbefugnissen.

In Satz 2 wird der Begriff „nachrichtendienstliche Mittel“ gesetzlich definiert. Erfäßt sind danach auch die Methoden, mit denen getarnt werden soll, daß das Bundesamt für Verfassungsschutz eine Information gewinnen will, wie z. B. die Benutzung von Tarnausweisen.

Absatz 2 betont, daß alle Tätigkeiten des Bundesamtes für Verfassungsschutz unter der Herrschaft des verfassungsrechtlichen Verhältnismäßigkeitsgebots stehen. Dies entspricht einer neueren Rechtssetzungspraxis, wie sie vor allem in die Polizeigesetze Eingang gefunden hat. Auf diese Weise soll dem Anwender das Verhältnismäßigkeitsprinzip besser gegenwärtig gemacht werden.

Zu § 7

§ 7 regelt als gegenüber § 6 Abs. 1 speziellere Vorschrift die Befugnis des Bundesamtes für Verfassungsschutz zur Erhebung personenbezogener Informationen durch den Einsatz nachrichtendienstlicher Mittel.

Die Hervorhebung des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit in § 7 Abs. 1 Sätze 2 bis 4 soll dafür sorgen, daß dem Gesetzesanwender vor jedem Einsatz von nachrichtendienstlichen Mitteln zur Erhebung personenbezogener Informationen die Notwendigkeit vor Augen geführt wird, beabsichtigte Eingriffe in die Privatsphäre von Bürgern auf das unerläßliche Minimum zu beschränken. Das gilt besonders bei Dritten, die selbst keine Tätigkeiten oder Bestrebungen nach § 3 Abs. 1 verfolgen, soweit deren Einbeziehung zur Feststellung solcher Tätigkeiten oder Bestrebungen unumgänglich ist. In diesen Fällen sind an den Nachweis der Verhältnismäßigkeit besonders hohe Anforderungen zu stellen. § 7 Abs. 2 Satz 2 berücksichtigt, daß die Informationsgewinnung mit Hilfe von nachrichtendienstlichen Mitteln für den Betroffenen im Einzelfall das geringer belastende Mittel gegenüber einer offenen Informationsbeschaffung, von der das soziale Umfeld des Betroffenen Kenntnis erhalten würde, sein kann.

Absatz 2 sieht die Unterrichtung der G 10-Kommission beim Einsatz von technischen Observationsmitteln unter der Voraussetzung vor, daß es sich um Grundrechtseingriffe handelt und diese in ihrer Art und Schwere einem G 10-Eingriff gleichkommen.

§ 7 ermöglicht keinen Eingriff in das Wohnungsgrundrecht aus Artikel 13 GG.

Zu § 8

§ 8 regelt als Spezialvorschrift zu § 6 Abs. 1 die Speicherung, Veränderung und Nutzung personenbezogener Daten in Dateien. Dabei wird der Dateibegriff des Bundesdatenschutzgesetzes zugrunde gelegt. Inhaltlich wird die Vorschrift durch die die Speichervoraussetzungen im einzelnen festlegenden sog. Verkartungspläne konkretisiert.

§ 8 enthält aus Praktikabilitätsgründen keine Regelung, ob und ggf. unter welchen Voraussetzungen die elektronische Datenverarbeitung eingesetzt werden darf.

Absatz 2 schafft eine Sonderregelung zugunsten Minderjähriger. Die Vorschrift soll das Mitschleppen von „Jugendstünden“ in Dateien verhindern. Erstmals wird gesetzlich bestimmt, daß Daten über das Verhalten von Personen vor Vollendung des 16. Lebensjahres überhaupt nicht gespeichert werden dürfen.

Absatz 3 ordnet die zeitliche Begrenzung der Speicherung aller in Dateien gespeicherter personenbezogener Daten an. Ein geeignetes Mittel hierfür ist das Institut der Zeitspeicherung.

Bis zum Inkrafttreten eines Geheimschutzgesetzes gilt § 8 auch für Speicherungen im Rahmen von Sicherheitsüberprüfungen.

Zu § 9

§ 9 bringt eine spezielle verfahrensrechtliche Schutzvorschrift für die Speicherung personenbezogener Daten in Dateien. Die Fristen für die nach Absatz 3 vorzunehmenden Prüfungen sind in der Dateianordnung (§ 10 Abs. 1 Satz 1 Nr. 6) differenziert nach Art der Dateien und der Daten festzulegen.

Zu § 10

§ 10 bringt eine weitere spezielle Datenschutzvorschrift, die die Voraussetzungen für die Errichtung und den Betrieb automatisierter Dateien regelt.

Absatz 1 gilt für alle automatisierten Dateien des Bundesamtes für Verfassungsschutz, auch für Verbunddateien, an denen es nach § 4 Abs. 2 beteiligt ist. Die materielle Zulässigkeit solcher Verbunddateien richtet sich nach § 4 Abs. 2; § 10 stellt darüber hinaus eine Reihe zusätzlicher formeller Kriterien auf, die vom Bundesamt für Verfassungsschutz zu beachten sind.

In den Dateianordnungen des Bundesamtes für Verfassungsschutz sind bereits bei Errichtung eine Reihe verfahrenstechnischer und verfahrensrechtlicher Schranken einzubauen, die sicherstellen, daß die gespeicherten personenbezogenen Daten nicht über das für die Aufgabenerfüllung erforderliche Maß verwendet, weitergegeben oder aufbewahrt werden. Um dies zu erreichen, sind — abgestimmt auf den Zweck der

jeweiligen Datei — die im Katalog der Vorschrift aufgezählten Einzelfragen detailliert zu regeln, insbesondere solche Einzelheiten über die Speichervoraussetzungen, die in der jetzigen Praxis in den sogenannten Verkartungsplänen enthalten sind. Hinsichtlich des Schutzes der Daten vor unbefugtem Zugriff kommt den Regelungen über Zugangsberechtigung und Protokollierung des Abrufs besondere Bedeutung zu.

Die Vorschrift stellt Dateianordnungen und damit die Errichtung, einschließlich des in § 14 festgelegten Inhalts, unter den Zustimmungsvorbehalt durch den Bundesminister des Innern, der damit eine besondere Kontrolle im Rahmen der Fachaufsicht ausübt; zugleich gewährt sie dem Bundesbeauftragten für den Datenschutz ein Anhörungsrecht.

Zu § 11

Die Vorschrift stellt klar, daß eine Hauptaufgabe des Bundesamtes für Verfassungsschutz, die Information der Regierung der Bundesrepublik Deutschland, durch ständige Berichterstattung sichergestellt wird. Die Berichtspflicht folgt aus dem Sammlungs- und Auswertungsauftrag des Bundesamtes für Verfassungsschutz. Sie entspricht auch der bisherigen Praxis. Die ständige Unterrichtung des Bundesinnenministers folgt aus dem Prinzip der Ressortverantwortlichkeit.

Die höchstrichterliche Rechtsprechung [vgl. BVerfGE 40, 287 (292f.)] hat ausdrücklich anerkannt, daß die Bundesregierung berechtigt ist, sich öffentlich mit Verfassungsfeinden unter Verwendung von Informationen des Bundesamtes für Verfassungsschutz politisch auseinanderzusetzen. Dies entspricht der heutigen Praxis, wie sie zum Beispiel in den jährlichen Verfassungsschutzberichten des Bundesinnenministeriums ihren Niederschlag gefunden hat. Die öffentliche Bekanntgabe personenbezogener Informationen ist nach Absatz 2 Satz 2 nur zulässig, wenn eine Abwägung ergibt, daß Interessen des Betroffenen nicht berührt sind oder daß das Allgemeininteresse im konkreten Fall überwiegt.

Zum Dritten Abschnitt

Der Entwurf enthält eine Reihe von verschiedenartigen Übermittlungsvorschriften; dies ist Folge der unterschiedlich ausgestalteten Übermittlungstatbestände, die sich streng an der Aufgabenstellung der beteiligten Stellen orientieren. Aus Gründen der Normklarheit beschränken sich die Übermittlungsvorschriften (§§ 12 bis 18) auf die Regelung der Übermittlungstatbestände und der Adressaten, während die §§ 19 bis 22 spezielle Datenschutzvorschriften enthalten, die für alle Übermittlungsvorgänge des Abschnittes gelten.

Die §§ 12 ff. regeln die Weitergabe von Informationen an und durch das Bundesamt für Verfassungsschutz. Die §§ 12 und 13 betreffen Übermittlungen an das Bundesamt für Verfassungsschutz, die §§ 14 und 15 solche durch das Bundesamt für Verfassungsschutz. Der Entwurf unterscheidet zwischen Übermittlungen,

die die Behörden von sich aus oder auf Ersuchen vornehmen; er unterscheidet darüber hinaus zwischen Staatsanwaltschaften und Sicherheitsbehörden sowie anderen Stellen. Nur bei Staatsanwaltschaften und Sicherheitsbehörden ist in Staats- und Verfassungsschutzangelegenheiten eine Übermittlungspflicht vorgesehen (§§ 13, 15); im übrigen beschränkt sich der Entwurf auf die Einräumung von Befugnissen (§§ 12, 14).

Der Entwurf regelt ferner die Übermittlung von Informationen an und durch die Verfassungsschutzbehörden der Länder insoweit, wie die Länder selbst keine Gesetzgebungskompetenz besitzen (§§ 16, 17).

Wegen der beabsichtigten gleichzeitigen Schaffung eines Gesetzes über den Militärischen Abschirmdienst sowie über den Bundesnachrichtendienst ist die Übermittlung von Informationen an und durch den Militärischen Abschirmdienst sowie den Bundesnachrichtendienst grundsätzlich in deren Fachgesetzen geregelt. Aus Kompetenzgründen trifft § 18 eine Übermittlungsregelung für die Staatsanwaltschaften und Polizeien an den Militärischen Abschirmdienst.

Zu § 12

§ 12 regelt die Übermittlung von Informationen an das Bundesamt für Verfassungsschutz. Die Vorschrift unterscheidet zwischen sogenannten Spontanübermittlungen (Absatz 1), für die eine Befugnis der Bundesbehörden ausgesprochen wird, und solchen auf entsprechende Ersuchen durch das Bundesamt für Verfassungsschutz (Absatz 2). Die gesonderte Aufbewahrung personenbezogener Informationen in Verzeichnissen nach Absatz 2 Satz 5 soll eine wirksame Prüfung der Übermittlungspraxis erleichtern.

Zu § 13

§ 13 regelt als Spezialvorschrift in Angelegenheiten des Staats- und Verfassungsschutzes gegenüber § 12 die Übermittlung von Informationen an das Bundesamt für Verfassungsschutz durch die Staatsanwaltschaften, Polizeien sowie den Bundesnachrichtendienst. Für diese Behörden besteht eine Informationspflicht. Absatz 3 verpflichtet das Bundesamt für Verfassungsschutz, Unterlagen, die aus strafprozessualen Telefonüberwachungsmaßnahmen stammen, wie die entsprechenden Unterlagen aus der Telefonkontrolle nach dem G 10 zu behandeln.

§ 13 – und dem folgend §§ 15 bis 17 – nennen u. a. Polizeien und Staatsanwaltschaften als Normadressaten. Die Vorschriften weisen jeweils auf die Sachleitungsbefugnis der Staatsanwaltschaften im Ermittlungsverfahren hin. Damit wird der besonderen Stellung der Staatsanwaltschaften, die diesen gesetzlich, z. B. durch die Strafprozeßordnung, im Ermittlungsverfahren zugewiesen ist, Rechnung getragen. Dies bedeutet, daß die Staatsanwaltschaften sich gegenüber den Polizeien die Übermittlung und den Empfang von Informationen in einem einzelnen Ermittlungsverfahren, aber auch für gleichartige Fälle (z. B. Sammelverfahren) vorbehalten können. Unzulässig

wären allerdings Weisungen, die generell den Staatsanwaltschaften die Übermittlung und den Empfang von Informationen vorbehalten.

Zu § 14

§ 14 ist hinsichtlich der Weitergabe personenbezogener Informationen durch das Bundesamt für Verfassungsschutz Spezialvorschrift zu § 6 Abs. 1. Er regelt die Weitergabe personenbezogener Informationen an Stellen außerhalb der Verfassungsschutzbehörden. Ausgenommen sind als Empfänger auch die Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes (§ 15).

Absatz 1 regelt die Übermittlung personenbezogener Informationen an Behörden. Er läßt die Übermittlung von Informationen für die Zwecke Schutz der freiheitlichen demokratischen Grundordnung sowie öffentlichen Sicherheit zu. Die Vorschrift bedient sich damit zweier in Rechtsprechung und Lehre hinreichend ausgedeuteter Rechtsbegriffe. Öffentliche Sicherheit bedeutet staatlichen Rechtsgüterschutz und umfaßt die Summe der Normen, die zum Schutz des Staates, seiner Einrichtungen und seiner Rechtsordnung aufgestellt worden sind. Absatz 2 läßt eine Übermittlung personenbezogener Informationen an NATO-Stationierungstreitkräfte in der Bundesrepublik Deutschland zu ihrem Schutz zu. Dies ist eine Folge von Artikel 1 a NATO-Truppenstatut in Verbindung mit Artikel 3 des Zusatzabkommens. Eine Übermittlung an Behörden, die nicht Dienststellen der Truppe sind, oder an NATO-Behörden außerhalb der Bundesrepublik Deutschland ist nach dieser Vorschrift ausgeschlossen; für sie gilt Absatz 3. Absatz 3 regelt die Informationsübermittlung durch das Bundesamt für Verfassungsschutz an ausländische öffentliche sowie über- und zwischenstaatliche Stellen. Weitere Einschränkungen ergeben sich aus einer Dienstvorschrift, die der Bundesminister des Innern genehmigt hat und die vor Inkrafttreten dem Bundesbeauftragten für den Datenschutz zugeleitet worden ist. Absatz 4 läßt die Weitergabe personenbezogener Informationen an Private nur in Ausnahmefällen zu, die hier näher umschrieben werden; dies entspricht der geltenden Rechtslage und Praxis.

Zu § 15

§ 15 regelt als Spezialvorschrift zu § 14 Abs. 1 die Übermittlung von Informationen durch das Bundesamt für Verfassungsschutz an die Staatsanwaltschaften, Polizeien und den Bundesnachrichtendienst in Angelegenheiten des Staats- und Verfassungsschutzes. Die Vorschrift verpflichtet das Bundesamt für Verfassungsschutz im Gegensatz zur Befugnisregelung des § 14 zur Informationsweitergabe.

Zu § 16

§ 16 regelt in Absatz 1 die Befugnis der Landesämter für Verfassungsschutz, bei den Bundesbehörden Ersuchen auf Informationsweitergabe zu stellen. Durch

Absatz 2 wird sichergestellt, daß die Landesämter für Verfassungsschutz, ebenso wie das Bundesamt für Verfassungsschutz nach § 13, Informationen von den Strafverfolgungs- und Sicherheitsbehörden erhalten. Die Regelung der Informationsbeziehungen der Landesämter für Verfassungsschutz mit den Strafverfolgungs- und Sicherheitsbehörden innerhalb desselben Bundeslandes bleibt der Regelung durch den jeweiligen Landesgesetzgeber vorbehalten.

Zu § 17

§ 17 regelt, daß die Landesämter für Verfassungsschutz, wie das Bundesamt für Verfassungsschutz nach § 15, Informationen an die Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes weiterzugeben haben.

Zu § 18

§ 18 regelt, daß der Militärische Abschirmdienst die zur Erledigung seiner Aufgabenstellung benötigten Informationen von den Strafverfolgungs- und Sicherheitsbehörden erhält.

Zu § 19

§ 19 ordnet eine Reihe von Übermittlungsverboten an.

Bei der nach Nummer 1 vorzunehmenden Güterabwägung sind vor allem die Sensibilität der betreffenden Informationen (z. B. Sozialmerkmale) sowie die Art ihrer Erhebung und die damit verbundene Intensität des Eingriffs in das Persönlichkeitsrecht des Betroffenen zu berücksichtigen. Ein schwerwiegender Eingriff, der bei der Abwägung besonders ins Gewicht fällt, ist beispielsweise gegeben, wenn Daten durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes erhoben worden sind.

Nummer 3 soll das Verhältnis der in §§ 12 bis 18 enthaltenen Übermittlungsregelungen zu besonderen gesetzlichen Übermittlungsregelungen klarstellen. Unter die besonderen gesetzlichen Übermittlungsregelungen fallen Übermittlungsverbote, zu denen auch Berufs- und besondere Amtsgeheimnisse zählen, sowie spezielle, abschließende Zweckbindungsregelungen. Darunter sind Regelungen zu verstehen, aus denen sich ausdrücklich oder konkludent ergibt, daß eine Verwendung nur für die im Gesetz geregelten Zwecke und unter den im Gesetz geregelten Voraussetzungen zulässig ist.

Zu § 20

§ 20 ordnet an, daß Übermittlungen über Minderjährige, von einigen Ausnahmen abgesehen, durch die Strafverfolgungs- und Sicherheitsbehörden nicht zulässig sind. Der Minderjährigenschutz zielt nicht nur auf einen Schutz vor einer Speicherung (§ 8 Abs. 2),

sondern schränkt zusätzlich strikt die Weitergabe von Informationen über Minderjährige ein.

Zu § 21

§ 21 ordnet die Prüfpflicht des Empfängers von Informationen an, ob das, was ihm übermittelt wurde, für seine Aufgabenerledigung erforderlich ist. Die Vorschrift ist vor allem ein Regulativ für die vom Gesetz zugelassenen Möglichkeiten, Informationen ohne Ersuchen des Empfängers zu übermitteln.

Zu § 22

Die Vorschrift verfestigt – insbesondere im Interesse des Betroffenen – eine Verwaltungspraxis des Bundesamtes für Verfassungsschutz, wonach es unrichtige oder unvollständige Informationen gegenüber dem Empfänger zu berichtigen hat.

Zu § 23

§ 23 beschränkt die Möglichkeit des on line-Zugriffs auf Dateien zwischen den Nachrichtendiensten (ausgenommen den Verfassungsschutzbehörden untereinander) sowie zwischen den Nachrichtendiensten einerseits und den Polizeien und Staatsanwaltschaften andererseits auf extreme Ausnahmesituationen. Im Falle einer Massierung terroristischer Anschläge – wie 1977 bei Entführung und Ermordung des Arbeitgeberpräsidenten Schleyer sowie der Entführung einer Lufthansamaschine – ist von einer solchen Ausnahmesituation auszugehen, da die Sicherheit der Bundesrepublik Deutschland gefährdet wäre.

Zu § 24

Die Vorschrift stellt klar, daß der Entwurf eine Reihe von Spezialvorschriften über den Umgang mit Informationen für das Bundesamt für Verfassungsschutz beinhaltet, die den korrespondierenden Normen des Verwaltungsverfahrensgesetzes und des Bundesdatenschutzgesetzes vorgehen. Dies gilt jedoch nur, soweit das Bundesamt für Verfassungsschutz in Erledigung der Aufgaben nach § 3 tätig wird; bei anderen Tätigkeiten, z. B. im Rahmen der Personalverwaltung des eigenen Personals, gelten alle in Frage kommenden Vorschriften der genannten „Querschnittsgesetze“ des Bundes.

Zu § 25

Die Vorschrift enthält die übliche Berlin-Klausel.

Stellungnahme zum Bundesverfassungsschutzgesetz-Entwurf vom 6.4.1989

1. Generelle Anmerkungen

Der vorliegende Entwurf ist der 4. Anlauf zur Novellierung des BVerfSchG von 1972. Er hat gegenüber seinen Vorgängern wiederum beträchtliche Veränderungen erfahren. Sie rühren davon, daß der neue Entwurf eine zusätzliche Funktion übernommen hat:

* Er soll die Zusammenarbeit des Geheimdienstes mit allen anderen Sicherheitsbehörden umfassend absichern und damit ein gesondertes "Zusammenarbeitsgesetz" erübrigen.

Daneben behält der Entwurf zwei Funktionen, die schon in den Vorentwürfen deutlich wurden:

* Er soll die Arbeitsbereiche und die dabei angewandten Methoden der Nachrichtenbeschaffung rechtlich umfassend absichern. Schließlich soll er

* insbesondere auch die Verarbeitung von Informationen mit Hilfe der EDV und ihre Speicherung in Dateien regeln.

Kennzeichnend für den Entwurf ist, daß er dort, wo es um die Festlegung der zentralen Aufgaben und Befugnisse der VfS-Ämter geht, die geringfügigsten Änderungen gegenüber dem geltenden Recht aufweist. Diese Eigenart bedeutet aber nicht, daß die tatsächliche Aufgabewahrnehmung unverändert geblieben wäre, denn die materiellen Bedingungen der Tätigkeit der Ämter haben sich seit Ende der sechziger Jahre beträchtlich verändert:

* Verändert hat sich zunächst die personelle Stärke des Bundesamtes für VfS (BfV), das in der Hochzeit der Kommunistenverfolgung der fünfziger Jahre gerade 250 Mitarbeiter, 1968 knapp 1.000 Mitarbeiter umfaßte; heute beschäftigt es rund 2.500 Personen.

* Verändert hat sich auch das Aufgabenverständnis;

Ursprünglich dazu auserkoren, mögliche Umstürzbewegungen auszuforschen, die - so das BVerfSchG von 1950 - "eine Aufhebung, Änderung oder Störung der verfassungsmäßigen Ordnung des Bundes ... zum Ziele haben", wurde seit Ende der sechziger Jahre das Vorfeld des Verdachts immer weiter ausgebaut. Die sozialliberale Koalition war es, die durch die Novellierung des GG und des BVerfSchG und den Radikalenerlaß im Jahre 1972 die Richtung gewiesen hat.

* Neu sind außerdem viele Mittel, die den Ämtern heute bei ihrer Arbeit zur Verfügung stehen. Dies gilt nicht nur für die unbegrenzten Möglichkeiten der Verarbeitung von Informationen durch die EDV. Neu sind vor allem auch viele nachrichtendienstliche Mittel (nd-Mittel): Vor zwanzig Jahren kannten die Ämter die Möglichkeiten des Einsatzes von Richtmikrofonen oder "Wanzen", von Videoüberwachung und der beobachtenden Fahndung durch den polizeilichen Staatsschutz höchstens aus der Literatur. Heute jedoch sind sie gängige "nachrichtendienstlichen Mittel".

Die enorm gewachsene Informations- und Definitionsmacht der Ämter erwächst also nur zu einem Teil aus den neuen Möglichkeiten der elektronisch gesteuerten Informationsverarbeitung. Selbst wenn man hypo-

thetisch von sehr starken rechtlichen Begrenzungen der Datenverarbeitung bei den Geheimdiensten ausginge, blieben die zentralen Probleme des nachrichtendienstlichen VfS weiter bestehen. Das zeigt auch ein Blick auf die diversen Skandale um die Ämter für VfS (in Bonn, Hannover, Berlin):

1) Es bliebe bei einer allein vom jeweiligen politischen "Zeitgeist" und von bürokratischer Opportunität bestimmten Festlegung der Verdachtsmomente angeblich verfassungsfeindlicher Tätigkeit.

Die "liberalen Errungenschaften" des neuen Entwurfes - die Wiedererwähnung des institutionellen Trennungsgebots von Polizei und VfS und der "Minderjährigenschutz" - erscheinen demgegenüber als bloße symbolische Begrenzungen der Aufgaben und Befugnisse, die im Kern dem exekutiven Ermessen Tür und Tor öffnen.

2) Es bliebe die unbegrenzte Möglichkeit, alle den VfS-Ämtern erreichbare Informationen über Personen und Institutionen, die den Ämtern überprüfenswert erscheinen, in Karteien zu speichern und Akten zu verwahren.

3) Es bliebe der faktisch unbegrenzte Spielraum zur Sammlung von Informationen mit Hilfe "nachrichtendienstlicher Mittel", der auch durch den durchgängigen Verweis auf das Verhältnismäßigkeitsprinzip nicht kleiner wird: Denn niemand außer den Geheimdienstlern selbst kontrolliert dessen Einhaltung.

Da wir unlängst 2 Schwerpunktheft zur Organisation, Geschichte und zu aktuellen Praktiken der Ämter für VfS vorgelegt haben, die auch einen ausführlichen Literaturbericht enthalten, ersparen wir es uns, hier auf Geschichte und Praxis dieser Ämter einzugehen. Wir verweisen auf die Ausgaben Nr.27 und 28.

2. Detailkritik

Zu § 1:

Zusammenarbeitspflicht

Die Abs.2 und 3 finden sich bereits im BVerfSchG von 1950. Dieses wiederum greift in seinen Formulierungen direkt auf die im Grundgesetz 1949 (Art.73 Nr.10) dem Bund zugestandene Möglichkeit zurück, für die "Zusammenarbeit in Angelegenheiten des Verfassungsschutzes" Gesetze zu erlassen. Was darunter konkret zu verstehen war, blieb bei der erst im letzten Moment ohne Debatte erfolgten Aufnahme dieses Satzes in das GG weitgehend offen. Heute werden darunter alle möglichen Ausformungen des Konzepts der "streitbaren Demokratie" verstanden werden (also auch Parteienverbot, Grundrechtsverwirkung). Im BVerfSchG des Jahres 1950 konkretisierte sich diese Zusammenarbeit in Angelegenheiten des VfS dann durch die Errichtung von geheimdienstlich arbeitenden Behörden.

Der im jetzigen Entw. auftauchende Abs.1 scheint demgegenüber nur eine bloße Umschreibung der Arbeitsbereiche des Staatsschutzes und des VfS im engeren Sinne zu sein, die angesichts der ausführlichen Bestimmungen des § 3 überflüssig wirkt. Motive für diesen Einschub werden in der Begr. nicht genannt; bedeutsam ist dieser Abs.1 jedoch gleichwohl. Er hat die Funktion, eine bislang strittige Regelungskompetenz des Bundes in diesem Bereich umfassend abzusichern. Dies gilt in zweifacher Hinsicht:

zum einen im Hinblick auf den Umfang der, einer Zusammenarbeitspflicht unterliegenden Aufgaben (a),

zum anderen im Hinblick auf die Reichweite der Kompetenz des Bundes, die Zusammenarbeit zu regeln (b).

Zu a):

Schon in dem Moment, als der Bundestag, gestützt auf Art.73 Nr.10 GG, geheimdienstlich arbeitende Behörden zum Zwecke des VfS schuf, wies die Exekutive diesen Ämtern darüber hinaus gehende Funktionen zu - die der Spionageabwehr und der Sicherheitsüberprüfungen. Rechtlich gesehen hatte in diesen Bereichen der Bund keinerlei Kompetenz zur Regelung der Zusammenarbeit. In der Praxis spielte der Kompetenzmangel kaum eine Rolle (immerhin weigerte sich der Amtschef von Niedersachsen anfänglich, auf dem Gebiet der Spionageabwehr tätig zu werden).

Noch weniger reichten die im Grundgesetz zugestandenen Kompetenzen aus, um diese Ämter mit umfassenden Staatsschutzaufgaben zu betrauen (Terrorismus, Ausländer, Staatssicherheit). Deshalb strebte die sozialliberale Koalition 1972 eine Novellierung des GG an. Der hierbei in Art.73 Nr.10 GG eingeführte VfS-Begriff ist - wie der Hausjurist des Bundesamtes vermerkt - "geeignet, ... alle spezielleren instrumentalen Verfassungsschutzdefinitionen zu umfassen" (Roewer 1987, § 1 RN 5). Der neue § 1 Abs.1 des Entw. enthält die Kurzformel dieses alles umfassenden Begriffs und vollzieht für das BVerfSchG nur die richtungsweisende GG-Änderung von 1972 nach.

Zu b):

Der gewachsene Umfang der Zusammenarbeit entspricht dem Zuwachs an Aufgaben, die von den VfS-Ämtern sukzessive übernommen worden waren. Entscheidend für die organisatorische Struktur des VfS ist nun, welche Konsequenzen man aus der in § 1 konstatierten Pflicht zur Zusammenarbeit zieht.

Sowohl Adenauer wie die SPD strebten 1949/50 einen bundesstaatlichen Inlandsgeheimdienst an; Teile der CDU und insbesondere die CSU machten sich demgegenüber für ein strikt föderales System stark, bei dem der Bund allenfalls Zentralstellen für die Zusammenarbeit errichten können sollte. Einer Zusammenarbeit nach dem Prinzip der Gleichberechtigung, wie der bayerische Vertreter bei der Debatte des BVerfSchG forderte (Bundesrat, 30.3.1950, 17.Sitzung, S.287), standen die Bemühungen der Zentralisten entgegen, in § 5 ein generelles Weisungsrecht des Bundes gegenüber den Länderministerien zu verankern. Damit scheiterte Adenauer. Das in § 5 Abs.2 dem Bundesministerium

konzedierte Recht, den Landesämtern Weisungen für die Zusammenarbeit zu erteilen, blieb verfassungsrechtlich strittig. Der Bund blieb in der Praxis darauf verwiesen, im Sinne eines "kooperativen Föderalismus" - der der Sache nach häufig eine große Koalition der Sicherheitsexperten war - nach einvernehmlichen Lösungen zwischen Ländern und Bund zu suchen. Bis auf wenige bekannt gewordene Konflikte scheint dies fast vierzig Jahre lang keine allzu großen Probleme bereitet zu haben.

Doch der Zwang zu kooperativen Lösungen nimmt durch die zunehmende Vernetzung der Arbeit der Landesämter zu; ein Ausscheren nur eines Landes - wie dies bei der Polizei im Bereich Meldedienst Landfriedensbruch der Fall war - wäre aus der Sicht des Bundesamtes zerstörerisch - deshalb der neue Abs.1. Der Rückgriff auf das in § 5 Abs.2 des geltenden Gesetzes enthaltene Weisungsrecht des BMI ist verfassungsrechtlich problematisch. Es ist auf den Fall einer Bedrohung der verfassungsmäßigen Ordnung des Bundes beschränkt und enthält kein Weisungsrecht für den geheimdienstlichen Alltag. Es entfällt im vorliegenden Entwurf völlig. Statt dessen beansprucht nun der Bund - wie aus der allgemeinen Begründung hervorgeht - eine weitreichende allgemeine Gesetzgebungskompetenz für die in § 1 Abs.1 umrissenen Bereiche: Nicht über Weisungen, Erlasse, Richtlinien u.ä. will der Bund die Länder in die Pflicht nehmen, sondern über die im Entw. enthaltene Vorschrift der Zusammenarbeit.

Zu § 2: Errichtung von Verfassungsschutzbehörden

Die Regelungen des Entw. entsprechen den schon 1950 getroffenen, bis auf drei kleine, aber signifikante Änderungen bzw. Klarstellungen:

- a) Nach 40 Jahren nachrichtendienstlichen VfS erscheint es logisch, daß nicht mehr die Errichtung solcher Behörden angeordnet wird, sondern die Pflicht, diese weiter zu unterhalten.
- b) Wieder in den Entw. aufgenommen wurde die bereits im Gesetz von 1950 in § 3 Abs.2 und im Entw. vom 28.1.86 enthaltene Feststellung, daß das Bundesamt einer polizeilichen Dienststelle nicht angegliedert werden darf. Dies ist ein Erfolg der FDP über die Vertreter einer Position, die zumindest theoretisch an einer möglichen Integration von polizeilichem Staatsschutz und Verfassungsschutz festhielt und davon ausging, daß die alliierte Vorgabe eines Trennungsgebots zwischen Polizei und Geheimdienst im Polizeibrief vom 14.4.49 den bundesdeutschen Gesetzgeber nicht binde.

Doch der Wert des Satzes 2 des § 2 Abs.1 ist fraglich. Er besagt nur, daß der VfS nicht einer Dienststelle angegliedert werden darf. Konsequenzen aus den Erfahrungen der Herrschaft des Nationalsozialismus werden damit nur sehr oberflächlich gezogen. Auch das Reichssicherheitshauptamt war nur die quasi ministerielle Postadresse von "Ämtern", die an unterschiedlichen Orten residierten und eigenständige Amtsleiter besaßen (SD, Gestapo, Ordnungspolizei). Entscheidend für die

Qualität der Trennung bzw. der Integration einzelner Sicherheitsbehörden ist ein Doppelpes:

* die Reichweite der funktionellen Zusammenarbeit im Rahmen der in Deutschland seit alther gepflegten Amtshilfe und

* die Formen der informationellen Integration von Behörden.

Kennzeichnend für das Verhältnis von VfS und Polizei seit Anfang der siebziger Jahre ist die zunehmende Verflechtung polizeilicher Informationserhebung und nachrichtendienstlicher Auswertung. An dieser Verflechtung ändert auch das Trennungsgebot in der vorliegenden Form nichts.

In § 6 Abs.1 und im dritten Abschnitt finden sich nur unzureichende Beschränkungen der Zusammenarbeit von Polizei und VfS. Insgesamt bleibt gerade nicht die Trennung, sondern die funktionale Integration kennzeichnend für diesen Entwurf.

c) Neu ist schließlich, daß § 2 Abs.2 - gestützt auf die Gesetzgebungskompetenz im Bereich der Zusammenarbeit - auch die Zusammenarbeit der Länder regeln will. Verfassungsrechtlich ist dies nach Auffassung etwa von Gusy (1982) fragwürdig; sachlich dient diese Regelung dazu, der durch die Datenverarbeitung erzwungenen Vernetzung der Ämter Rechnung zu tragen.

Zu § 3:

Die allgemeine Aufgabennorm

Der Entw. lehnt sich - bis auf einen Punkt - an die Formulierungen an, mit denen 1972 die erweiterten Funktionen des Verfassungsschutzes rechtlich abgesichert wurden (vgl. § 3 VfS-Gesetz von 1972, die Abs.2 und 3 von 1972 werden im hier kommentierten Entw. nun ausführlicher in §§ 6 ff. geregelt).

Neu gegenüber der geltenden Fassung ist in Abs.1 S.1 der Begriff "Informationen", der gegenüber dem in diesem Gesetz benutzten Begriff "personenbezogene Daten in Dateien" allumfassend ist. Die Differenz ist deshalb wichtig, weil bei den folgenden Erhebungs-, Speicherungs- und Übermittlungsregeln zwischen diesen Begriffen mit deutlicher Absicht changiert wird. Schließlich wird eine zum umfassenden Informationsbegriff korrespondierende Befugnis formuliert: "insbesondere sach- und personenbezogene Auskünfte..." sammeln zu dürfen.

Abs.1 Nr.1: FdGO-Schutz:

In Bezug auf die bereits geltende Aufgabenbestimmung des VfS bleibt festzuhalten, daß mit diesen Bestimmungen nicht abgrenzbare, dem Inhalt und dem Umfang nach bestimmbare Handlungsfelder des Amtes umrissen werden - wie von Politikern und manchen Juristen gerne suggeriert wird. Bei der Formel von den "Bestrebungen gegen die freiheitlich-demokratische Grundordnung", mit der der sog. administrative VfS gemeint ist, bleibt schon die Umschreibung der Aktivität selbst - die sogenannten Bestrebungen - weitgehend dunkel. (Der Begriff hat im übrigen seinen Ursprung in den Sozialistengesetzen von 1878). Zur Ausle-

gung des Inhalts der Bestrebungen sei hier auf den hilflosen Versuch von H. J. Schwagerl (1985, S.13) verwiesen, Referent für positiven Verfassungsschutz in Hessen:

"Die Auslegung des Inhalts (der FdGO, d.V.) besonders an den Grenzen, bereitet nach wie vor erhebliche Schwierigkeiten. Es herrscht über die konkreten Grenzen des Inhalts, den es zu schützen gilt, keine allgemeine Übereinstimmung".

Wo die Grenzen dessen liegen, was als demokratische Äußerung innerhalb des Spektrums der von den großen Parteien bestimmten "Grundordnung" betrachtet werden kann, was dagegen als "verfassungsfeindliche" oder "extremistische" Bestrebung gilt, hängt nur sehr bedingt vom Recht ab. VfS und Politiker bestimmen diese Grenzen des "Verfassungsfeindlichen" nach politischen Opportunitätsgesichtspunkten.

"Wie die Staatspolitik sich wandelt", so der ehemalige Hamburger Senator Helmut Schmidt in den sechziger Jahren, "muß auch der Verfassungsschutz mit seinen konkreten Objekten der Zeit folgen und sich ihr anpassen" (BML, 1966, S.15 ff.).

Abs.1 Nr.3: Ausländerüberwachung

Diese Norm stützt sich auf eine aus den Ausländergesetzen bekannte und berüchtigte rechtliche Blankettformulierung, die zu allem dienen kann: nämlich die Gefährdung der "auswärtigen Belange".

Abs.2 Nr.2: Die Sicherheitsüberprüfungen

Seit längerer Zeit wird ein "Geheimsschutz-Gesetz" angekündigt, das umfassend diesen Bereich regeln soll. Bisher liegen bereits die seit dem 1.Mai 1988 geltende "Sicherheitsrichtlinien vor (vgl. Dokumentation und Kritik in CILIP 29, S.125 ff.). Die Regelungen in diesem Entw. sind insoweit ein Vorgriff.

Neu ist der Schlußsatz des Abs.2. Er ist ein Musterbeispiel für die semantischen Betrügereien dieses Entwurfs. Einen "Fortschritt" erbringt dieser Satz, indem er bei formellen Sicherheitsüberprüfung vorschreibt, daß der/die Betroffene bzw. der/die davon mitbetroffene Ehemann/frau etc. davon Kenntnis erhalten muß. Diese Normierung entspricht nicht nur den gängigen Richtlinien in Bund und Ländern; sie läßt sich auch in der Praxis kaum vermeiden. Denn eine solche Überprüfung beginnt in der Regel mit dem Ausfüllen eines ausführlichen Fragebogens durch den Betroffenen.

Das entscheidende Problem bei den Sicherheitsüberprüfungen ist also gar nicht, daß der Betroffene davon Kenntnis erhält. Die Frage ist vielmehr, ob ohne Einwilligung der davon mitbetroffenen Personen (Ehefrauen, Lebensgefährten etc.) eine solche Überprüfung vorgenommen werden darf. In den Ursprungsfassung der Entwürfe wurde die Überprüfung der davon Mitbetroffenen von deren Zustimmung abhängig gemacht. Dies entfällt mit der neuen Fassung.

Anzumerken bleibt schließlich, daß die von Datenschützern und Verwaltungsexperten geforderten materiellen Verbesserungen bei den Sicherheitsüberprüfungen nicht einmal ansatzweise zu finden sind: Weder erhält der Betroffene ein Anhörungsrecht, bei dem er zu den vielfach dubiosen "Erkenntnissen" der Ämter Stellung nehmen könnte, noch trifft

der Entw. Vorkehrungen dagegen, daß die mit "Einwilligung" des Betroffenen erhobenen Informationen für andere Zwecke des VfS verwendet werden.

Abs.3, Nr.2: Spionageabwehr

Wenn die in § 3 Abs.1 Nr. 2 erwähnte "sicherheitsgefährdende oder geheimdienstliche Tätigkeit ... für eine fremde Macht" leichter mit einem konkreten Arbeitsfeld des VfS identifiziert werden kann, so liegt dies weniger an der Gesetzesformulierung, als an der festen Vorstellung über "die fremden Mächte" und der Tätigkeiten, die für diese ausgeübt werden.

Zu § 4:

Gegenseitige Unterrichtung, NADIS

Abs.1 entspricht dem geltenden Recht.

Abs.2 schafft - neu - eine Rechtsgrundlage für NADIS. Sie zielt darauf ab, das bestehende Datensystem ohne Einschränkungen rechtlich abzusichern (vgl. Kästchen auf der folgenden Seite).

1. Der Entw. faßt die Rechtsgrundlage von NADIS unter die gemeinsamen Unterrichtungspflichten und nicht unter die Übermittlung von Daten (§§ 12 ff.). Es handele sich nicht um eine Übermittlung zwischen den VfS-Ämtern, die auf NADIS online Zugriff haben, sondern um eine gemeinsame Nutzung. Für den Dateieninhalt ist jeweils das speichernde Amt verantwortlich, für das Funktionieren des Systems insgesamt das BfV, bei dem die Zentrale des Systems untergebracht ist.

2. Der Entw. gibt ferner die gesetzliche Grundlage ab für die Errichtung der bereits bestehenden Verbunddateien - sowohl der Hinweisdateien wie der PersonenZentralDatei (PZD), als auch der Textdateien. Während das Betreiben der PZD (und auch der Amtsdateien) an keine weiteren Voraussetzungen geknüpft ist, nennt der Entw. für die "gemeinsame Nutzung" von Textdateien eigenständige Bedingungen: Sie dürfen nur eingerichtet werden "zur Aufklärung von geheimdienstlichen Tätigkeiten oder zur Beobachtung von bestimmten Formen des politischen Extremismus, insbesondere wenn sie darauf gerichtet sind, Gewalt anzuwenden" (Begr.). Rechtlich soll das ausgedrückt werden in der Formel des § 2 G-10-Gesetz: Danach reichen für die Eröffnung einer solchen Datei "tatsächliche Anhaltspunkte für den Verdacht" aus, daß "jemand" eine der dort genannten politischen Straftaten plant, begeht oder begangen hat. "Tatsächliche Anhaltspunkte" sind aber nicht identisch mit einem Anfangsverdacht im Sinne des Strafprozeßrechts. Es handelt sich hierbei um einen allgemeinen Verdacht, für den es einzelne Hinweise gibt. Die Formulierung bezieht sich ferner nicht darauf, daß dieser Verdacht sich gegen den dort zu Speichernden selbst richtet. Es geht vielmehr darum, daß eine solche Tat möglicherweise von irgendjemand geplant wird. Die Frage der Speicherung wird ausschließlich in § 8 behandelt. Die Regelung legitimiert damit das Betreiben solcher Dateien auf längere Sicht, denn solche vagen Verdachtsmomente werden sich immer finden lassen.

N A D I S

1. Was ist NADIS?

NADIS, das nachrichtendienstliche Informationssystem, ist ein in erster Linie durch die Vfs-Ämter genutztes Datensystem. Die Zentrale des Systems steht beim BfV, die Landesämter können direkt eingeben und abfragen (online-Verbund).

2. Welche Dateiformen gibt es in NADIS?

Es sind grundsätzlich zwei Dateiformen, die zwischen den Vfs-Ämtern als Verbunddateien betrieben werden:

a) Hinweisdateien

Die wichtigste ist die Personenzentraldatei (PZD), in der jeweils die Personengrunddaten sowie weitere sog. Formatdaten (Bankkonto, Auto-Kennzeichen etc.) erfaßt werden. Darüber hinaus enthält der PZD-Datensatz eine Kennnummer, über die einerseits der Zugang zu den entsprechenden Akteninhalten und Vorgängen möglich ist, die aber zweitens auch bereits ohne Kenntnis des Akteninhalts Aufschluß über den Bereich verfassungsschützerischer Arbeit gibt, in dem die Akten angefallen sind. Die PZD ist die wichtigste Vfs-Datei, da eine Anfrage in ihr den ersten Aufschluß über die jeweils in Frage kommende Person gibt. Neben der PZD existiert eine weitere Hinweisdatei auf "Objekte".

b) Textdateien

In diesen Dateien sind nicht nur formatierte Daten, sondern auch Freitext enthalten. Über die Struktur dieser Dateiformen ist nichts genaueres bekannt. Vermutlich handelt es sich hier um Dateien, die ähnlich wie die polizeilichen SPUDOK - und PIOS-Dateien eine weitergehende Auswertungsmöglichkeit durch Suchworte und Zusammenführung von Informationen aus verschiedenen Datenbereichen eröffnen. Soweit bekannt, existieren diese Dateien im "Extremismus"-, im "Terrorismus"bereich und bei der Spionageabwehr.

Neben den Verbunddateien führen die Ämter jeweils **Amtsdateien**, auf die nur sie direkt Zugriff haben.

3. Wer nutzt sonst noch NADIS und wie?

MAD und BND, die jeweils ihre eigenen Datensysteme betreiben, sind nicht direkt mit dem System des Vfs verbunden. Sie erhalten ihre Informationen aus NADIS im Zuge monatlicher Bandabgleiche. Damit verfügen sie über eine monatlich aktualisierte Personen-Zentral-Datei (PZD) des Vfs. Die sie interessierenden Informationen können dann auf konventionelle Weise (Telefon, Telex) abgefragt werden.

Die bis 1979 existierende feste Standleitung zwischen dem polizeilichen Informationssystem INPOL und NADIS ließ der damalige Innenminister Baum nur teilweise kappen. Gleichwohl speichert die Staatsschutz-Abteilung des BKAs weiterhin ihre Daten in der PZD. Sie benutzt diese Datei gewissermaßen als ihr Hinweissystem - mit dem Effekt, daß der Vfs Mitwisser eines großen Teils der polizeilichen Staatsschutzdaten ist. Nach offiziellen Angaben kann das BKA umgekehrt nur auf die Daten direkt zugreifen, die es selbst in NADIS eingegeben hat, also nicht auf Daten des Vfs.

Diese Regelung sollte nur provisorischen Charakter haben, bis eine eigene Staatsschutzdatei im BKA aufgebaut sei. Diese Datei, eine Zusammenführung der alten PIOS-Dateien Terrorismus und Staatsgefährdung, existiert bereits seit einiger Zeit und trägt den Namen APIS, Arbeitsdatei PIOS Innere Sicherheit. Für APIS wurde das Systemkonzept von PIOS neu bearbeitet, um weitere Auswertungsmöglichkeiten in dieser Textdatei bereitzustellen. NADIS wird jedoch ungeachtet der wiederholten Kritik des Bundesdatenschutzbeauftragten (BfD) von der BKA-Staatsschutzabteilung weitergenutzt.

In seinem Bericht über die "Datenschutzrechtliche Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamts" vom 7.12. letzten Jahres (siehe "Spiegel" vom 13.2.89, S. 72 f.) weist der BfD darauf hin, daß NADIS zu einer "Auffangdatei" für Daten geworden ist, die in APIS aufgrund der restriktiveren Dateianordnung nicht gespeichert werden dürfen. Innerhalb von 10 Monaten hat das BKA 1290 Fälle in APIS gespeichert, während es im gleichen Untersuchungszeitraum 2976 Fälle in NADIS unterbrachte. Insgesamt ist der Strom von Daten vom BKA zum BfV genauso breit wie zwischen den Staatsschutz-Polizeiabteilungen der Länder und dem BKA. Die informationelle Verschmelzung zwischen Polizei und VfS ist also längst vollzogen.

4. Sonstige Informationswege Polizei - VfS

Der VfS hat aber nicht nur Zugriff auf diese in NADIS gespeicherten Polizeidaten. Übermittelt wurden z.B. bei einem Bandabgleich im August 1987 die ge-

samten Datenbestände der "Arbeitsdatei PIOS Landfriedensbruch", früher "Meldedienst Landfriedensbruch", die sich insbesondere auf Demonstrationsdelikte und ähnliches (auch Hausfriedensbruch etwa) bezieht.

Kenntnis von Polizeidaten erhält der VfS darüber hinaus durch Informationshilfersuchen bei einer rund um die Uhr besetzten Verbindungsstelle im BKA.

◆ Max Watts: US-Army-Europa. Von der Desertion zum Widerstand in der Kaserne oder wie die U-Bahn zu RITA fuhr. 108 S., 9,80 DM.

Während des Vietnamkriegs desertierten 432.000 GIs. Nicht wenige von ihnen aus Einheiten der 7. US-Armee in der BRD. Max Watts beschreibt das Entstehen der Untergrundbahn für US-Deserteure in Westeuropa und die Arbeit der Deserteursgruppe „RITA ACT“ im Pariser „Exil“. Mit aktuellen Adressen!

COUNTERINSURGENCY Planning Guide., Handbuch zur Anti-Guerilla-Kriegsführung aus der US-Army Special Warfare School, Ft. Bragg. In deutscher Sprache, 106 S., 8,80 DM.

Roger Fallgot: The Kitson Experiment. (engl.), 242 S., 25 DM. Nordirland als Labor für Aufstandsbekämpfung in Westeuropa.

Nieder mit der Disziplin! Hoch die Rebellion! Anarchistische Soldaten-Agitation im Deutschen Kaiserreich. 92 S., 8,80 DM. Enthält das von dem Anarcho-Syndikalisten Siegfried Nacht verfaßte „Soldatenbrevier“, das 1907 als Propagandaschrift des Kriegsministeriums getarnt verbreitet wurde.

Bezug: **Harald Kater Verlag**,
Görlitzer Straße 39, 1000 Berlin 36
☎ 030/618 26 47

Zu § 5: Weisungsrecht

Das verfassungsrechtlich fragwürdige Weisungsrecht des Bundesinnenministers an die Landesämter entfällt. In der Praxis ist es ohnehin nie zur Anwendung gekommen. Dies ist eine Neuerung - sowohl gegenüber dem geltenden Recht als auch gegenüber den Vorentwürfen. Das Ziel, die Zusammenarbeit vom Bund her verbindlich festzulegen und zu bestimmen, wird durch eine extensive Auslegung der Gesetzgebungskompetenz des Bundes (vgl. Kommentar zu § 1) weiterverfolgt.

Zu § 6: Die allgemeine Befugnisnorm

Begnügt man sich bis heute mit rund fünfzig Worten, um die Befugnisse des BfV zu regeln (§ 3 Abs.3 und 4 des geltenden BVerfSchG), so wird jetzt ein beträchtlicher Paragraphenwald produziert, der eines nicht leistet: die Reichweite der Befugnisse des VfS klar zu definieren oder gar zu begrenzen.

§ 6 regelt als allgemeine Befugnisnorm dieselben umfassend, aber keineswegs abschließend, wobei dieser weitgehend (bis auf die in b) und c) angesprochenen Punkte) dem Entw. vom 19.11.87 folgt.

a) Umfassend regelt der § 6 die Befugnisse zur Sammlung von Informationen, soweit diese nicht in Dateien gespeichert werden (§ 8 ff.) oder aber personenbezogen mit "nachrichtendienstlichen Mitteln" erhoben werden (§ 7). Dies heißt aber, daß für den allergrößten Teil verfassungsschützerischer Arbeit, nämlich die Sammlung aller erreichbarer Informationen in Sach- und Personalakten etc. keinerlei Regelung getroffen wird. Weder wird der Umfang der zu sammelnden Informationen begrenzt noch der Kreis der Personen, für die beim VfS Personalakten angelegt werden dürfen. Dies alles bleibt im Belieben der Ämter, soweit sie dies mit der Aufgabe des VfS in Verbindung bringen können. Der in den §§ 8 ff. unternommene Versuch, die maschinelle Verarbeitung dieser Informationen, insbesondere über die allgemeine Aktenhinweisdateien in NADIS, zu regeln und zu begrenzen, greift deshalb nur äußerst begrenzt. Diese Regelung beschneidet bestenfalls (bei strengen datenschutzrechtlichen Normen) die Kapazität der Ämter, die gesammelten Informationen möglichst effektiv zu nutzen, nicht aber die Sammlung von Informationen und deren Archivierung.

b) § 6 Abs.1 ist zugleich die Norm, die den Ämtern allgemein die Möglichkeit zum Einsatz nachrichtendienstlicher Mittel einräumt (soweit nicht der § 7 als Spezialnorm greift). Auf eine Legaldefinition dessen, was als "nachrichtendienstliches Mittel" zu gelten hat, wird - wie schon in den früheren Entw. - ausdrücklich verzichtet. Auch "die geringfügige Beschädigung einer Gefängnismauer mittels Sprengstoff" -

gemeint ist das Cellar Loch - fällt nach Meinung der exekutiven Sicherheitsrechtsinterpreten unter die legalen nachrichtendienstlichen Hilfsmittel (Borgs/Ebert 1987, S.111).

Der Verzicht auf eine abschließende Normierung bedeutet, daß jenseits der direkten Zwangsmittel den Ämtern alles erlaubt ist, was nicht öffentlich wird ("nd-Mittel").

Die im vorliegenden Entwurf erstmals enthaltene Vorschrift, daß die nd-Mittel in einer internen, geheimen Dienstvorschrift festzuhalten sind, dürfte in der Praxis kaum eine begrenzende Wirkung besitzen.

c) Wieder aufgenommen wurde in der vorliegenden Fassung eine bereits im Entwurf von 1986 enthaltene Formulierung, nach der die Ämter der Polizei nicht um Maßnahmen ersuchen dürfen, zu denen sie selbst nicht befugt sind. D.h., sie dürfen nicht die Polizei anweisen, ein sie interessierendes Objekt zu durchsuchen, um die Mitgliedskartei einer Organisation zu erhalten, Personenkontrollen an bestimmten Orten fordern etc. Dieser Fortschritt im Recht bleibt praktisch weitgehend folgenlos. Denn zum einen wird in der Praxis die Polizei nicht formell um eine solche Maßnahme ersucht, sondern diese wird höchstens bei den Kollegen vom polizeilichen Staatsschutz auf dem kleinen Dienstweg ange-regt. Zum anderen bleibt der breiter Strom an Informationen von der Polizei zum VfS, die für diese Ämter im weitesten Sinne von Interesse sein könnten. Ja, die geheimdienstliche Personenzentraldatei in NADIS dient - wie der letzte Prüfbericht des Bundesdatenschutzbeauftragten enthüllte - dem polizeilichen Staatsschutz als "Auffangdatei" für alle Fälle, die im polizeilichen Bereich nicht gespeichert werden dürfen. Beide Formen der funktionalen Integration von Polizei und VfS läßt der vorliegende Text völlig unberührt. Er sichert diese sogar rechtlich ab.

d) Abs.2 ist ein typisches Beispiel für den symbolischen Gebrauch von Recht, wiederholt er doch nur einen allgemeinen Verwaltungsgrundsatz. Es soll - wie es in der Begr. ohne Ironie heißt - "auf diese Weise dem Anwender das Verhältnismäßigkeitsprinzip besser gegenwärtig gemacht werden". Wenn man schon nicht - wie der frühere Innenminister Höcherl feststellte - den Verfassungsschützern zumuten könne, dauernd mit dem Grundgesetz unter dem Arm herumzulaufen, so soll ihnen wohl zumindest vor Augen gehalten werden, daß man im deutschen Rechtsstaat - "zum Schutze der Verfassung" - nicht mit Kanonen auf Spatzen schießen sollte.

Zu § 7: Nachrichtendienstliche Mittel

Dieser Paragraph ist neu - weniger in der Sache, denn der Form nach -, da er sich auf die "nachrichtendienstlichen Mittel" bei der Erhebung personenbezogener Daten konzentriert und auf eine bereits in § 6 enthaltene allgemeine Befugnis zur Sammlung personenbezogener Informationen verzichtet. Sachlich entspricht der neue § 7 Abs.1 weitgehend den Regelungen in § 6 Abs.2 der Vorentwürfe.

a) Wie schon für diese bleibt festzuhalten, daß die Regelungen keinerlei materiell-rechtliche Begrenzung des Einsatzes der "nd-Mittel" für die Aufgaben des VfS - "Extremismusbekämpfung", Spionageabwehr, Staatsschutz und Ausländerüberwachung - enthalten. Denn in den Fällen, in denen eine Person als "Verfassungsfeind" definiert oder der geheimdienstlichen Tätigkeit verdächtigt wird, sollen die Ämter die Möglichkeit zum Einsatz nd-Mittel haben. Sie sollen auch dann zum Einsatz kommen können, wenn die Abklärung eines solchen Verdachts (auf "Verfassungsfeindlichkeit" etc.) auf andere Weise nicht möglich erscheint - also "zur Ausforschung der für solche Erkenntnisse notwendigen Nachrichtenzugänge".

Auf die dann wortreich folgenden Ausführungen zum Verhältnismäßigkeitsprinzip könnte verzichtet werden; dieses Prinzip gilt unmittelbar für die rechtsstaatliche Tätigkeit jeder Behörde.

b) Neu ist schließlich der Abs.2. Immerhin werden durch diesen die neuen technischen Überwachungsmaßnahmen (Wanzen, Richtmikrofonen) erstmals offiziell zur Kenntnis genommen, wenngleich mit unbefriedigendem Ergebnis. Denn welche Maßnahmen nach Ansicht des Gesetzgebers einer G-10-Maßnahme gleichkommen, wird offengelassen. Ob aber eine nachrichtendienstliche Maßnahme in Art und Schwere einer G-10-Maßnahme entspricht, ergibt sich nicht aus den Instrumenten selbst. Der Einsatz von V-Männern, das gebräuchlichste und als harmlos erachtete nd-Mittel, kann in Art und Schwere eine G-10-Maßnahme weit übersteigen (denkt man etwa an die - bei der "tageszeitung" mutmaßlich versuchte - Einschleusung eines V-Mannes).

Doch es fehlt nicht nur an Kriterien, mit denen Art und Schwere beurteilt werden sollen. Die schwierige Abwägung wird vielmehr dem Amt überlassen. Und in den Fällen, in denen das Amt von der Schwere der Maßnahme überzeugt ist, genügt es, nachträglich der G-10-Kommission Meldung zu erstatten. Deutlicher läßt sich deren Kontrollkompetenz kaum ad absurdum führen - ein Grund, der jeden rechtsstaatlich denkenden Parlamentarier zum Austritt aus dieser Kommission bewegen müßte.

Eine weitere Folge dieser G-10-Regelung liegt darin, daß der Datenschutzbeauftragte von der Kontrolle ausgeschlossen wird.

Zu den §§ 8-10: Allgemeine Datenschutzfloskeln

Die genannten §§ sind in dieser oder ähnlicher Form in allen sog. "Sicherheits"Gesetzen einschließlich der Entwürfe zur Novellierung der StPO und des Polizeirechts nach dem Volkszählungsurteil zu finden. Das Urteil des BVerfG von 1983 bestätigte zum einen die Existenz eines aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Rechts auf informationelle Selbstbestimmung und machte damit zum anderen klar, daß es sich bei allen Formen der Informationsverarbeitung um Eingriffe handelt. Für Eingriffe in Grundrechte bedarf es allerdings einer ge-

setzlichen Grundlage, was nichts anderes heißt, als daß die Regierung gezwungen wurde, in einem angemessenen Zeitraum gesetzliche Grundlagen zu schaffen.

Ergebnis dessen sind Paragraphen wie die folgenden, die im Grunde nur das Zitiergebot erfüllen, d.h. formal dem Anspruch des Urteils genügen, inhaltlich aber dessen Erwägungen auf den Müll werfen, indem sie all das legalisieren, was auch bisher schon Praxis war.

Zu § 8: Speicherungsvoraussetzungen

So ist in § 8 Abs.1 die Speicherung, Veränderung und Nutzung von Daten nur an die Erwägung des VfS gebunden, daß solche Daten für ihn erforderlich seien. Die Nummern 1-3 decken die verfassungsschützerische Arbeit lückenlos ab:

- Nach Nr.1 darf gespeichert werden, wenn die entsprechende Person bereits als Beobachtungsobjekt der Ämter ausgemacht ist, d.h. wenn diese "tatsächliche Anhaltspunkte" für "extremistische Bestrebungen" bzw. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erkannt haben.

- Nach Nr.2 sind Datenverarbeitungsmaßnahmen möglich, um zu eruieren, ob die betreffende Person zum Beobachtungsobjekt gemacht werden soll, juristisch ausgedrückt: "zur Erforschung und Bewertung von Bestrebungen oder Tätigkeiten" der o.g. Art.

- Nr.3 regelt, daß Datenverarbeitungsmaßnahmen auch eingesetzt werden dürfen, wenn das BfV im Rahmen von Sicherheitsüberprüfungs- oder Geheimschutzmaßnahmen tätig wird.

Der Dateibegriff, der hier angewandt wird, entspricht dem des Datenschutzgesetzentwurfs, d.h. er erfaßt nur die automatisierten Dateien, nicht die Erfassung in Akten, die nach wie vor ins Belieben der Ämter gestellt wird.

Abs.2: Minderjährigen"schutz"

Dies zählt zu den "Essentials" der FDP, die für die Annahme der Gesetzentwürfe im Kabinett zur Bedingung gestellt hat, daß ein Minderjährigenschutz eingeführt werde. Während hier der "Schutz" Minderjähriger bei der Speicherung in Dateien geregelt ist, formuliert § 20 eine entsprechende Regelung für die Datenübermittlung.

In der Tat hat der VfS insbesondere in den 70er Jahren massiv auch an Schulen gespitzelt, so daß ein Schutz von Kindern gegen den verfassungsschützerischen Zugriff durchaus seine Berechtigung hätte. Indes, das Kernproblem hat die FDP gerade nicht angetastet:

Die Erhebung von Informationen über Minderjährige. Hierzu gibt es keinerlei Sonderregelung. Es soll also weiter zulässig sein, daß der VfS sich z.B. an Schulen umtut, d.h. z.B. V-Leute einschleußt, Veranstaltungen überwacht etc. Desgleichen ist weiter zulässig, daß der VfS die Informationen, die er durch diese Überwachung gewonnen hat, in Akten archiviert. Speicherungs- und Übermittlungsverbote (bis zum 16.Lebensjahr) respektive -beschränkungen (ab dem 17. bis zum 18.Lebens-

jahr) auszusprechen, macht überhaupt nur Sinn, wenn personenbezogene Informationen über Kinder, Jugendliche und Heranwachsende zuvor erhoben worden sind.

Aber dieser Entw. enthält Einschränkungen nur für die Folgen der Erhebung: der Speicherung in Dateien und der Übermittlung von Daten (in § 20).

Aber selbst dieser Anspruch wird über die Altersregelung faktisch preisgegeben. Daten von Personen über 16 Jahren dürfen sehr wohl gespeichert werden, wenn auch zunächst nur für zwei Jahre. Daten von Schülern der Sekundarstufe II werden sich deshalb weiter in Dateien des VfS auffinden lassen. Die Speicherung wird ab einem Alter zulässig, in dem Jugendliche überhaupt erst beginnen, sich politisch zu interessieren.

Die Entscheidung über die Weiterspeicherung von Daten 16-18jähriger liegt beim VfS. Es ist ihre Ermessensentscheidung, ob sie einen Schüler weiter beobachten und damit weiter Daten produzieren, oder ob sie den einzelnen oder die beobachtete Gruppe in Ruhe lassen und damit nach 5 Jahren die Speicherungshöchstdauer erreicht ist.

Nur ein Erhebungsverbot hätte effektiven Minderjährigen-Schutz bedeutet.

Abs.3: Speicherungsfristen

Die Festlegung, daß die Zeit der Speicherung auf das erforderliche Maß beschränkt werden muß, kann datenschutzrechtlich nicht greifen, sondern schützt bestenfalls die Ämter vor allzuviel Datenmüll. Der Entwurf legt nur für die 16-18jährigen eine Regelfrist für die Überprüfung weiterer Erforderlichkeit fest, und diese kann leicht unterlaufen werden. Alles weitere bleibt offen und wird im Rahmen einer Dateianordnung von den Ämtern selbst festgelegt - zur Zeit 15 Jahre. Durchsetzbare Rechtsansprüche ergeben sich daraus nicht.

Zu § 9:

Berichtigung, Löschung, Sperrung

Der Anspruch auf die Berichtigung gespeicherter falscher Daten zählt inzwischen zu den datenschutzrechtlichen Selbstverständlichkeiten. Die Entwurfsregelung suggeriert einen Anspruch des Bürgers - ein "Subjekt-recht" - auf Berichtigung, Löschung und Sperrung falscher Daten, um den es hier gerade nicht geht. Sollte der betroffenen Bürger geschützt werden, so hätte zwingend ein Auskunftsanspruch des Bürgers aufgenommen werden müssen, der ihn befähigt, die Qualität der über ihn gespeicherten Daten zu beurteilen.

Ein Auskunftsanspruch über die zur eigenen Person gespeicherten Daten wird jedoch im derzeit geltenden wie im Entwurf BDSG für die Geheimdienste prinzipiell ausgeschlossen, für die Polizei letztlich in deren Ermessen gestellt (vgl. unsere Kommentierung zum BDSG). Eine Regelung über Berichtigung, Löschung und Sperrung ist unter diesen Bedin-

gungen bestenfalls ein Hinweis für das Personal der Ämter, auf die Qualität "ihrer" Daten zu achten - Unsinn zu löschen oder zu berichtigen.

Zu § 10: Dateianordnung

Sie wird vom BfV selbst erstellt, der BMI muß seine Zustimmung erteilen. Der Datenschutzbeauftragte hat nur das Recht, angehört zu werden, über ein Einspruchsrecht verfügt er nicht. Zudem unterliegt er der Geheimhaltungspflicht, so daß er sich auch nicht an die Öffentlichkeit wenden kann. Diese "Vorkontrolle" bleibt ohne Biß.

Zudem, weder wird eine Höchstspeicherungsdauer, noch eine feste Überprüfungsfrist für die Speicherung in oder für die Fortführung von Dateien vorgeschrieben. Dadurch wird es in der Folge trotz gesetzlicher Grundlage weiterhin dabei bleiben, daß die Dateimodalitäten von den Betreibern bzw. allenfalls vom Dienstherrn festgelegt werden können.

Zu § 11: Berichtspflicht

Die Regelung entspricht der Fassung des Entw. von 1986. Es geht um die Möglichkeit der Regierungsmitglieder, das beim VfS gespeicherte Geheimwissen über jeden Bundesbürger abzufragen. Zum anderen wird mit dem Abs.2 darüber hinaus dem BMI die Möglichkeit eröffnet, Informationen über einzelne Bürger gezielt in die Öffentlichkeit zu lancieren - also mit Material der Ämter öffentliche Verrufs- oder Feindereklärungen zu betreiben. Daß dabei an mehr als nur an die Nennung einzelner Namen in den VfS-Berichten gedacht ist, legt die Praxis des derzeitigen Staatssekretärs im BMI, Spranger, nahe. So leitete er nicht nur Berichte über "linksextreme Einflüsse bei den Grünen" mit langen Namenslisten an den Abgeordneten Todenhöfer weiter, sondern ließ zugleich auch für den Abg. Dregger die "Erkenntnisse" über den Abg. Schily abfragen.

Zu den §§ 12 - 18: Die Übermittlungsregelungen

Zur Systematik und Begrifflichkeit

Mit dem ersten Paket sog. Sicherheitsgesetze von 1985 ist gesetzgebungstechnisch eine neue Systematik eingeführt worden:

- Bei der Übermittlung personenbezogener Daten wird unterschieden zwischen Übermittlungen **ohne** (die Spontan-Übermittlung oder Denunziation) und **auf Ersuchen**.

- Während die Übermittlungen auf Ersuchen bei dem entsprechenden Datenlieferanten die Pflicht zur Herausgabe der Daten auslöst, wird

bei der "Spontan"-Übermittlung differenziert.

- Stellen außerhalb der Sicherheitsbehörden **dürfen** von sich aus Informationen übermitteln, ohne daß sie hierzu verpflichtet sind. Diese Regelung soll die Beschäftigten der "Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentl. Rechts" (Bundesgesundheitsamt, Bundesversicherungsanstalt für Angestellte etc.) davor schützen, wegen eines Verstoßes gegen das datenschutzrechtliche Zweckbindungsprinzip belangt werden zu können (vgl. § 12 Abs.1).

- Stellen innerhalb des Verbundes der Staatsschutzapparate **müssen** "von sich aus" überliefern. Hier entfällt der einschränkende Begriff "dürfen" bei der Formulierung der Übermittlungsbefugnisse (vgl. § 13 Abs.1).

- Weiteres generelles Merkmal ist, daß bei der Pflicht zur Datenlieferung auf Ersuchen der Datenbesitzer nicht über die Rechtmäßigkeit der Nachfrage und Preisgabe der Daten zu entscheiden hat - dementsprechend muß das BfV seine Aufforderung nicht begründen -, sondern ausschließlich die die Daten abfordernde Stelle. Gebrochen wird hier mit dem datenschutzrechtliche Besitzerprinzip, d.h. der Verantwortlichkeit der die Daten erhebenden Stelle für den rechtmäßigen Umgang mit den Daten.

- Schließlich changiert seit den ersten Entwürfen die Begrifflichkeit, soweit es die Definitionen der zur Datenlieferung auf Ersuchen betroffenen Institutionen der öffentl. Verwaltung betrifft.

Einerseits werden die einzelnen Apparate des Staatsschutzverbundes genannt (Staatsanwaltschaft, Polizei, BND etc.), andererseits wird von "Behörden des Bundes und den bundesunmittelbaren juristischen Personen des öffentl. Rechts", dann aber auch von "jeder Stelle, die Aufgaben der öffentl. Verwaltung wahrnimmt" gesprochen, schließlich werden alle Verwaltungen, die "amtliche Register" führen, in die Pflicht zur Datenlieferung bzw. Einsichtpreisgabe aufgeführt.

- Hierzu parallel changiert die Begrifflichkeit bei der Definition von Empfängern personenbezogener Informationen, die das BfV beliefert (vgl. § 14).

Zunächst werden "Behörden" genannt, dann "Dienststellen der Stationierungsstreitkräfte", darüber hinaus "ausländische öffentliche Stellen sowie über- und zwischenstaatliche Stellen" und als Auffangdefinition (§ 14 Abs.4) nur noch "andere Stellen".

Abgedeckt wird mit dieser changierenden Begrifflichkeit die Befugnis für das VfS-Amt, jeder nur denkbaren "Stelle" nach eigenem Ermessen Daten liefern zu können.

Die Einzelregelungen:

Zu § 12: Übermittlungen an das BfV

Abs.1 erlaubt die sog. Spontan-Übermittlung seitens der Beschäftigten aller Bundesbehörden und aller "bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentl. Rechts" ("bundesunmittelbare ju-

rist. Personen"). Es ist eine Pauschalermächtigung zur Zweckumwidmung, die dem so agierenden Beschäftigten davor schützt, wegen des Verstoßes gegen das im BDSG festgelegte Prinzip der Zweckbindung von Daten belangt zu werden. Die im Erstentwurf dieser Regelung im Jahre 1985 noch formulierte **Pflicht** dieses Lieferantenkreises, Erkenntnisse von sich aus zu liefern, ist fallengelassen worden (vgl. CILIP 21, S.69, § 8 BVerfSchG). Diese "Einschränkung" verrät den Verwaltungspraktiker unter den Entwurfsautoren. Eine ohnehin nicht überwachbare und durchsetzbare Unterrichtungspflicht gegenüber Beschäftigten des Bundes wird fallengelassen.

Diese Einzelregelungen, die Datenübermittlungsrechte und -pflichten von Stellen außerhalb der Staatsschutz-Apparate gegenüber diesen Apparaten normieren, dürften die nachhaltigste Wirkung des gesamten Gesetzespaketes zeitigen.

Zwar gab es die Praxis von Spontanndenunziationen und die Datenlieferung auf Verlangen von sonstigen Behörden und Stellen der öffentl. Verwaltung an die VfS-Ämter auch schon zuvor. Sie war jedoch nicht rechtlich formalisiert und damit skandalisierbar; sie war rechtlich nicht durchsetzbar und soweit abhängig vom "good will" der sich hierzu hergebenden Beschäftigten. Die Neuregelung, gerade dort, wo sie Übermittlungspflichten statuiert, also sanktionsbewehrt ist, wandelt private Denunziationslust zur Verwaltungspflicht.

Abs.2 statuiert diese Übermittlungspflichten und erweitert zugleich den Kreis jener, die zur Übermittlung auf Anforderung verpflichtet wird, indem der Behördenbegriff aus Abs.1 ersetzt wird durch den Begriff "jede Stelle, die Aufgaben der öffentl. Verwaltung" wahrnimmt, und zudem ergänzend der Zugriff auf alle "amtlichen Register" in die Regelung aufgenommen wird.

Wird in Abs.1 das Recht zur Spontan-Übermittlung begrenzt auf Mitarbeiter von Bundesbehörden, so bezieht sich die Übermittlungspflicht auf Ersuchen des Bundesamtes für VfS auf den gesamten Bereich öffentlicher Aufgaben - vom Bund bis zur Gemeinde - und greift zudem über die Beschäftigten der öffentl. Verwaltung noch insoweit hinaus, als auskunftspflichtig auch jene Bürger sind, die nur punktuell "Aufgaben der öffentl. Verwaltung wahrnehmen" - z.B. der Schornsteinfeger, der nach dem Bundes-Emissionsgesetz in der Wohnküche die Gastherme auf ihr Abgaswerte mißt oder der TÜV-Beschäftigte, der die jährliche ASU-Kontrolle ausführt.

Die in Abs.2 formulierte Pflicht des BfV, Ersuchen aktenkundig zu machen und einen Nachweis über die Einsicht in amtl. Register zu führen, ist Bestandteil jener generellen datenschutzrechtlichen Rhetorik, mit der die Gesetzesentwürfe gespickt sind - Rhetorik deshalb, weil weder betroffene Bürger einen Rechtsanspruch auf Auskunft der über sie erhobenen und gespeicherten Daten haben noch ansonsten eine von außen kommende Kontrollinstanz wirkungsvolle Befugnisse hat, für die das aktenkundig machen unter dem Kontrollaspekt sinnvoll wäre.

Zu § 13: Übermittlung innerhalb des Staatsschutzverbundes

Dies ist gegenüber § 12 eine Spezialvorschrift in Angelegenheiten des Staats- und Verfassungsschutzes. Sie übernimmt in Gestalt einer Generalklausel die mit dem alten ZAG und dem folgenden VfS-Mitteilungsgesetz intendierte informationelle Gesamtvernetzung aller Staatsschutzapparate, soweit es das Verhältnis zum Bundesamt betrifft.

Staatsanwaltschaften, Polizei, Zoll, BGS und BND sind zur Spontanübermittlung an das Bundesamt verpflichtet gemäß der scheunentorbreiten Aufgabennorm des Amtes (vgl. Kommentierung zu § 3). Eine von Datenschutzrechtlern zumindest geforderte Ausdifferenzierung und unterschiedliche Gewichtung der Übermittlungspflichten - bei der Spontanübermittlung wie bei der auf Ersuchen - entlang der Einzelaufgaben des Bundesamtes (Extremismus-Erfassung, Spionageabwehr, Sicherheitsüberprüfungen) unterbleibt.

Abs. 2 statuiert Übermittlungspflichten dieser Sicherheitsbehörden auf Verlangen des Bundesamtes, wobei tunlichst jede Festlegung darüber vermieden wird, ob die liefernden Behörden bereits über diese Daten verfügen - oder ob das Ersuchen des Bundesamtes überhaupt erst zum Anlaß der Erhebung wird. Zu erinnern ist etwa an die Zeitschriften-Listen, die das Bundesamt dem Bundesgrenzschutz-Einzeldienst in den siebziger Jahren in die Hand gab, um Lesegewohnheiten von Reisenden zu erfassen.

Im Ergebnis jedenfalls erhält das Bundesamt Zugang zu Daten, die mit polizeirechtlichen respektive strafprozessualen Zwangsbefugnissen erhoben worden sind. Das sog. Trennungsgebot wird somit nicht nur unter dem Gesichtspunkt der informationellen Gewaltenteilung unterlaufen, sondern zudem unter dem Gesichtspunkt jedweden Ausschlusses exekutiver Befugnisse für die VfS-Ämter - ein Element des Trennungsgebots, das bisher auch von den Apologeten des VfS nicht in Frage gestellt worden ist.

In früheren Fassungen (vgl. § 7 ZAG vom 31.1.88, CILIP Nr.23, S.43) wurde dieses Problem noch insoweit angesprochen, als durch Hausdurchsuchungen gewonnene Daten nur bei "überwiegendem Allgemeininteresse" weitergegeben werden durften.

Zur Frage, ob die um Datenlieferung ersuchten Sicherheitsbehörden vom Bundesamt mit dem Ersuchen auch angehalten werden können, die abverlangten Daten aus Anlaß des Ersuchens überhaupt erst zu erheben, gibt es zwar in § 6 Abs.1 eine eindeutig scheinende Klarstellung. Das Amt darf nicht um Maßnahmen ersuchen, zu denen es nicht selbst befugt ist. Allerdings machte die aml. Begründung zu § 7 des ZAGs in der Fassung von 1988 deutlich, wie dieses Problem zu umgehen sei: "Anfragen und Anregungen sind dagegen nicht ausgeschlossen".

In der Begründung zu der hier diskutierten Fassung ist eine so offenkundige Anregung zur Umgehung des Problems vermieden worden.

Abs.3 thematisiert die Übermittlung von Daten, die nach § 100a StPO (Strafprozessuale Telefonüberwachung) gewonnen worden sind. Er bindet die Befugnis an den Straftatenkatalog des § 2 des G-10-Gesetzes. Die

Breite dieses Katalogs zeigt sich daran, daß u.a. der § 129a StGB darin enthalten ist.

Anders formuliert, "wenn tatsächliche Anhaltspunkte dafür bestehen, daß jemand" "plant", für eine terroristische Vereinigung "zu werben", greifen bereits die Übermittlungsbefugnisse nach Abs.3. Dies bedeutet die Umwidmung von Daten, die zur repressiven Verfolgung konkreter Straftaten erhoben worden sind, für beliebige nachrichtendienstliche Zwecke.

Es entspricht der immanenten Normierungs-Logik der "Sicherheitsgesetze", daß Geheimdiensten jene Daten überliefert werden dürfen, die sie auch aus "eigenem Recht" erheben können - also Telefonüberwachung nach dem G-10-Gesetz. § 7 Abs.3 G-10-Gesetz formuliert ein - eingeschränktes - Verwendungsverbot der so gewonnenen Daten für andere Zwecke als dem Ursprungsanlaß, § 10 Abs.3 G-10-Gesetz statuiert eine Vernichtungspflicht für diese Daten, sofern sie nicht mehr benötigt werden.

Zu § 14: Übermittlungen durch das Bundesamt

Als Spezialvorschrift zu § 6 (Informationsaustausch zwischen den VfS-Behörden) wird hier die Datenlieferung des Bundesamtes an Stellen außerhalb des Verbundes der VfS-Ämter geregelt; für den Verbund mit den sonstigen bundesdeutschen "Sicherheits"-Behörden gibt es die Spezialvorschrift des § 15.

Abs.1 erweitert gegenüber der Ursprungsfassung von 1985/86, in der als Empfängerkreis nur Bundesbehörden benannt wurden, den Empfängerkreis um alle Behörden (Bund, Länder, Gemeinden). Die genannten Voraussetzungen (Erfüllung der Aufgaben des Bundesamtes, Schutz der FdGO durch den Empfänger, sonstige Zwecke der öffentl. Sicherheit) gelten nicht kumulativ sondern alternativ. Damit wird die Übermittlungsbefugnis grenzenlos. Über die inhaltsleere FdGO-Formel hinaus ist für die Ausweitung der Übermittlungsbefugnis besonders signifikant die Formel von dem "Zwecke der öffentl. Sicherheit". Dieser, der polizeilichen Generalklausel entnommene Begriff "öffentl. Sicherheit" deckt nach allgemeiner Rechtsauffassung die Schutzgüter der gesamten Rechtsordnung einschließlich der Rechte privater Personen ab. Daß die Übermittlungsbefugnis nicht an den traditionellen polizeirechtlichen Begriff der "Abwehr von Gefahren für die öffentliche Sicherheit", sondern an den rechtlich nicht definierten Begriff des "Zweckes" gebunden wird, ist ein ergänzender semantischer Trick, diese Übermittlungsbefugnis konturenlos offen zu halten - anything goes.

Abs.2 schließt sämtliche NATO-Partner in den Kreis der Empfänger ein, behandelt sie wie deutsche Stellen, ohne daß sie den Kautelen deutschen Rechts im Umgang mit diesen Daten unterlägen. Der sanktionslose Hinweis, daß die Empfänger sich an die Zweckbindung zu halten hätten, bleibt datenschutzrechtliche Rhetorik. Dieser Abs. sichert die geheimdienstliche Vernetzung sämtliche NATO-Geheimdienste ab.

Abs.3 gibt dem Bundesamt die Befugnis, entweder zur Erfüllung der ei-

Aus dem 11. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zum 1. Januar 1989

16.3.2 NADIS

Einen weiteren Schwerpunkt der Kontrolle bildete die Speicherung von Daten durch das Bundeskriminalamt in NADIS. Diese Praxis hatte ich bereits wiederholt beanstandet (vgl. zuletzt 10. TB S. 771 f.). Der Bundesminister des Innern hat meine Beanstandungen bislang stets zurückgewiesen, und das Bundeskriminalamt fährt fort, Daten in NADIS zu speichern. Der BMI begründet dies im wesentlichen damit, daß alle vom BKA in NADIS gespeicherten Fälle für die Verfassungsschutzbehörden relevant seien. Das BKA sei auf die Speicherung in NADIS nicht angewiesen, denn es verfüge über eigene Dateisysteme, in denen es die Speicherung vornehmen könnte. Die Speicherung in NADIS erfolge im Interesse der Informationsübermittlung an den Verfassungsschutz.

In früheren Stellungnahmen hatte der BMI die Relevanz der durch das BKA in NADIS gespeicherten Fälle für den Verfassungsschutz daraus abgeleitet, daß nur solche Fälle in NADIS gespeichert würden, die auch die Erfassungskriterien für APIS erfüllten; aus diesen ergebe sich die Verfassungsschutzrelevanz. Ich habe demgegenüber festgestellt, daß das BKA doppelt so viele Fälle in NADIS wie in APIS speichert. NADIS ist sozusagen die „Auffangdatei“ für die Fälle, die die — ohnehin zu weiten — Voraussetzungen für die Erfassung in APIS nicht erfüllen (vgl. oben 16.3.1). Dies betraf beispielsweise zwei Personen, die die Rede eines Staatssekretärs der Bayerischen Staatsregierung in einem Festzelt mit dem Zwischenruf „Heil-Gauleiter“ gestört hatten. Eine andere Person hatte ein Verwarnungsgeld wegen Falschparkens bezahlt und auf dem begleitenden Anschreiben „mit deutschem Gruß“ unterschrieben. Eine weitere Person rief in betrunkenem Zustand im Schützenzelt auf dem Münchener Oktoberfest „Sieg heil“. Diese und weitere von mir aufgeführte Fälle wurden vom BKA nicht in APIS, wohl aber in NADIS gespeichert und damit an die Verfassungsschutzbehörden übermittelt.

Der BMI räumt nunmehr ein, daß in NADIS auch Fälle erfaßt werden, die nicht in APIS gespeichert sind. Im übrigen ist seine Auffassung in dieser Frage unverändert. Meine Feststellung, daß mehr als die Hälfte der von der Abteilung Staatsschutz des BKA erteilten konventionellen Auskünfte in dem von mir untersuchten Zeitraum an Verfassungsschutzbehörden gingen, hält der BMI für einen Beleg für die Notwendigkeit des engen Informationsaustauschs zwischen Polizei und Verfassungsschutz.

Die Speicherung von Daten durch die Abteilung Staatsschutz des BKA in der NADIS-Personenzentraldatei (NADIS-PZD) bedeutet, daß routinemäßig personenbezogene Daten übermittelt und gespeichert werden, ohne daß die jeweils verantwortliche Behörde die Zulässigkeit der konkreten Einzelmaßnahmen prüft. Eine solche Verfahrensweise ist mit dem geltenden Recht nicht vereinbar. Aber auch die Entwürfe für das Verfassungsschutzgesetz sowie für das BKA-Gesetz sehen keine einschlägige Rechtsgrundlage vor. Der Entwurf eines Verfassungsschutzgesetzes schließt im Gegenteil die Beteiligung anderer als Verfassungsschutzbehörden an NADIS-PZD ausdrücklich aus.

10.4 Konsequenzen aus früheren Kontrollen

Ferner hatte ich früher bemängelt, daß in zusammenfassenden Lageberichten personenbezogene Daten enthalten waren, ohne daß dies in jedem Fall erforderlich war. Bei derartigen Lageberichten steht zum Zeitpunkt ihrer Abfassung nicht immer fest, an welche Empfänger sie übersandt werden. Ich habe in einzelnen Fällen auch festgestellt, daß solche Berichte ausländischen Nachrichtendiensten zugänglich gemacht worden sind. Durch eine Änderung der entsprechenden Dienstvorschrift des BfV ist nunmehr ausdrücklich klargestellt worden, daß personenbezogene Daten in Berichte des BfV für inländische und ausländische Behörden nur aufgenommen werden, wenn dies erforderlich ist und schutzwürdige Belange betroffener Personen dabei berücksichtigt sind. Ich gehe davon aus, daß es bei derartigen Berichten in der Regel genügt, wenn Personen ohne Namensnennung mit ihrer politischen Funktion beschrieben werden, so daß die Notwendigkeit der Aufnahme personenbezogener Daten in derartige Berichte die Ausnahme ist.

Ich konnte auch erreichen, daß Daten, die im Rahmen einer Sicherheitsüberprüfung erhoben worden sind, nur noch in geringerem Umfang an ausländische Nachrichtendienste übermittelt werden. Die Dienstvorschrift über die Beziehungen des BfV zu ausländischen Nachrichtendiensten wurde dahin ergänzt, daß Daten, die den Bereich der persönlichen Lebensführung betreffen, an diese nur noch für Zwecke der Sicherheitsüberprüfung und der Spionageabwehr übermittelt werden dürfen.

Das BfV wird von ausländischen Nachrichtendiensten nicht selten um Übermittlung von Informationen ersucht, die für eine dort durchzuführende Sicherheitsüberprüfung benötigt werden. Bei einer Sicherheitsüberprüfung nach deutschem Recht ist dem Betroffenen rechtliches Gehör zu gewähren, falls seine Ermächtigung zum Umgang mit Verschlusssachen abgelehnt werden soll. Dies ist nicht in allen Ländern so, an deren Nachrichtendienste das BfV Daten zum Zwecke der Sicherheitsüberprüfung übermittelt.

Nach meiner Auffassung wäre es notwendig, daß das BfV entweder auf der Gewährung von rechtlichem Gehör durch die dortigen Behörden besteht oder aber selbst dem Betroffenen rechtliches Gehör gewährt, wenn es belastende Daten über ihn an einen ausländischen Nachrichtendienst übermittelt. Immerhin konnte ich nunmehr erreichen, daß das BfV alle ausländischen Nachrichtendienste angeschrieben und sie gebeten hat, entsprechend den Regelungen in der Bundesrepublik Deutschland den Betroffenen rechtliches Gehör zu geben, wenn ihre Ermächtigung zum Umgang mit Verschlusssachen aufgrund von Informationen abgelehnt werden soll, die vom BfV übermittelt worden sind. Es bleibt abzuwarten, ob dies eine ausreichende Maßnahme ist, um die schutzwürdigen Belange der Betroffenen zu gewährleisten.

genen Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen ausländischer Stellen und über-zwischenstaatlicher Stellen diese mit personenbezogenen Informationen zu beliefern.

Die "Einschränkung", daß die Lieferung unterbleibt, wenn "auswärt. Belange der Bundesrepublik" dem entgegenstehen, besagt nur, daß die Lieferung nicht einem rechtlichen, sondern einem außenpolitisches Kalkül unterworfen ist. Die zweite Abwägung "schutzwürdige Belange des Betroffenen" bleibt konturenlos, da sie nicht angibt, mit welchen "Interessen" die Belange des Betroffenen "abgewogen" werden müssen.

Abs.4 genehmigt schließlich die Datenlieferung an private Dritte. In der Ursprungsfassung von 1985/86 wurde noch klarstellend von "anderen als öffentlichen Stellen" gesprochen. Jetzt wird nicht einmal eine Differenz Ausland/Inland getroffen, mithin die Lieferung auch an ausländische private Dritte gesichert.

Zu § 15:

Übermittlung an Staatsschutzbehörden und dem BND

Abs.1 begründet die prinzipielle Pflicht des BfV, den Strafverfolgungsbehörden von sich aus sowohl für präventive wie repressive Zwecke "die ihm bekanntgewordenen Informationen" in Angelegenheiten des strafrechtlichen Staatsschutzes zu liefern. Der Begriff der Staatsschutzdelikte ist schier unbegrenzt. Er umfaßt nicht nur die im Gerichtsverfassungsgesetz festgehaltenen Delikte, für die der Generalbundesanwalt und die Staatsschutzkammern der OLGs erstinstanzlich zuständig sind, sondern auch alle anderen, sofern die vermuteten "Motive, Zielsetzungen" eine Beeinträchtigung der FdGO bzw. der "Sicherheit des Bundes oder eines Landes" erkennen lassen.

In § 19 Nr.2 (vgl. Kommentierung) wird diese Übermittlungspflicht wieder eingeschränkt, wenn "überwiegende Sicherheitsinteressen" dies erfordern. D.h., wenn das operative Kalkül es verlangt, darf das BfV entsprechende Straftaten auch begehen lassen, ohne sie der Strafverfolgung zu überantworten oder das Wissen über die Begehung von Straftaten zurückhalten ("Lex Berger", "Lex Loudil").

Die BND-Regelung bedeutet eine pauschale Zweckumwidmung der dem VfS erschlossenen Informationen. Da die Aufgaben des BND auch nicht im Ansatz formuliert sind (vgl. Kommentar zum BND-Gesetz), ergibt sich auch von dieser Seite her keine Eingrenzung.

Abs.2 formuliert spiegelbildlich zu Abs.1 die Ansprüche von Polizei, Staatsanwaltschaften und BND, ihrerseits vom Bundesamt erforderliche Informationen abfordern zu dürfen, mit der korrespondierenden Pflicht des Bundesamtes, die Daten zu liefern - eingeschränkt durch § 19.

Zu § 16:

Informationspflichten der Bundesbehörden gegenüber den Landesämtern für VfS

Aus der föderalen Struktur der Bundesrepublik folgt, daß die Landesge-

setzgeber gegenüber Bundesbehörden keine Auskunftspflichten statuieren können. Entsprechend der Befugnisse des Bundesamtes gegenüber den Bundesbehörden (vgl. § 12 Abs.2) erhalten die Landesämter identische Rechte. Die Bundesbehörden sind im Gegenzug den Landesämtern gegenüber in derselben "Pflicht" wie gegenüber dem Bundesamt.

Abs.2 folgt der Normierungslogik dieses Gesetzes: allgemeine Norm für Bundesbehörden, Spezialnormen für Sicherheitsapparate. Er verpflichtet BND, MAD, die Polizeien des Bundes und der Länder (soweit es nicht die Landespolizei des anfragenden Landesamtes für VfS betrifft), unter den gleichen Kautelen auch die Staatsanwaltschaften, von sich aus den Landesämtern Informationen unter den Voraussetzungen des § 13 zu liefern - dito auf Ersuchen der Landesämter.

Der letzte Satz nennt nur die verfassungsrechtliche Lage. Der Bundesgesetzgeber darf landesinterne Beziehungen nicht regeln.

Zu § 17:

Übermittlungspflichten der Landesämter gegenüber Polizei und Staatsanwaltschaften sowie BND und MAD

Abs.1 ist die korrespondierende Regelung zum § 15 für die Landesämter für VfS. Es gilt die Kommentierung zu § 15. Abs.2 statuiert, daß 1. die Landesämter von sich aus BND und MAD beliefern müssen und 2. BND und MAD verbindliche Ersuchen mit korrespondierenden Lieferpflichten an die Landesämter stellen können. Es gilt jedoch auch hier die Ausnahmeklausel des § 19 (überwiegende Sicherheitsinteressen, die die Übermittlungspflicht ausschließen).

Diese vom Bundesgesetzgeber geregelte Informationspflicht der Landesämter für VfS gegenüber dem MAD mag mit der Begründung gerechtfertigt werden, daß der MAD eine Verfassungsschutzbehörde mit sachlicher Beschränkung auf die Bundeswehr ist. Beim BND kann diese Begründung nicht greifen. Er ist keine Verfassungsschutzbehörde. Der Bundesgesetzgeber greift hier ohne verfassungsrechtliche Deckung in Länderbefugnisse ein.

Zu § 18:

Informationsfluß auf und ohne Ersuchen seitens Staatsanwaltschaft, Polizei und Zoll an MAD

Es wird klargestellt, daß im Rahmen der MAD-Aufgaben die Staatsanwaltschaft, Polizeien und der Zoll (soweit er Grenzschutzaufgaben erfüllt) diesem gegenüber in identischer Pflicht stehen wie gegenüber dem BfV. Es gelten dieselben Regelungen - und damit die identische Kritik - wie im § 13.

**Zu den §§ 19 - 22:
Spezielle "Datenschutzvorschriften" für alle Übermittlungsvorgänge zwischen den Staatsschutzapparaten**

Die hier zusammengefaßten §§, in der Begr. als "spezielle Datenschutzvorschriften" ausgegeben, sind eine Mischung aus verfassungsrechtlichen Selbstverständlichkeiten und innerorganisatorischen Effizienzkalkülen, die bestenfalls helfen könnten, die Qualität der zwischen den Staatsschutzbehörden wandernden Informationen zu heben.

**Zu § 19:
Übermittlungsverbote**

Abs.1 erinnert an das mit Verfassungsrang ausgestattete Verhältnismäßigkeitsprinzip in Form der Güterabwegung. Abs.2 sichert in letzter Instanz die Herrschaft des jeweiligen Datenbesitzers (VfS, BND, MAD, Polizei) über seine Daten - ungeachtet der zuvor statuierten Übermittlungspflichten, sofern das organisationsspezifische Sicherheitsinteresse dem entgegensteht. Dieses datenschutzrechtliche "Besitzerprinzip", das ansonsten mit dem hier vorliegenden Artikel-Gesetz generell durchbrochen wird, dient allerdings nicht der Erfüllung datenschutzrechtlicher Prinzipien, sondern ausschließlich operativen Kalkülen der nicht nur kooperierenden, sondern gleichzeitig auch konkurrierenden verschiedenen Sparten des "Sicherheitsverbundes". Recht und Interessen der betroffenen Personen bleiben außerhalb dieses Kalküls. Diese Regelung war bereits in den Vorentwürfen zu finden. Abs.3 benennt die Selbstverständlichkeit, daß besondere Übermittlungsausschlußregelungen, sofern es sie gibt - etwa die des Sozialgesetzbuches X - Vorrang haben. Im Regelfall wird jedoch in anderen Spezialgesetzen (vgl. Ausländerzentralregister-G., Melde-G., ZEVIS-G., Bundeszentralregister-G.) die Übermittlung an Polizei und Geheimdienste ausdrücklich zugelassen.

In der Summe: § 19 enthält keinerlei datenschutzrechtliche Übermittlungsverbote über das hinaus, was generell rechtlich gilt.

**Zu § 20:
Minderjährigenschutz**

Da die Erhebung und Archivierung von Informationen über Minderjährige jenseits der Dateien nicht einmal thematisiert wird (vgl. Kommentierung zu § 8 Abs.2 (Minderjährigen"schutz" bei der automatisierten Speicherung), dient diese Regelung wie zuvor jene in § 8 der Täuschung.

Die eingegrenzte Übermittlungsbefugnis für Daten von Kindern (bis zum 16. Lebensjahr) durch VfS-Behörden macht überhaupt nur unter der Voraussetzung Sinn, daß solche personenbezogenen Informationen erhoben und jenseits der Dateien archiviert sind, da ihre Speicherung in Dateien verboten ist.

Die Übermittlungsbefugnis für Daten über Jugendliche ab dem 16. Lebensjahr folgt operativer Logik. Diese generelle Befugnis setzt zu einem Lebensabschnitt an, in dem Jugendliche überhaupt erst beginnen, politische Interessen zu entwickeln und politisch zu handeln.

Abs.1 Nr.1 gibt den VfS-Behörden die Befugnis, Kinder-Daten zur Strafverfolgung bei Straftaten von erheblicher Bedeutung und zur Abwehr erheblicher Gefahren weiterzuleiten. Dieser Erheblichkeitsbegriff spielt auch im Bereich des neueren Polizeirechts eine "erhebliche" Bedeutung. Welche rechtsdogmatischen Kriterien ihn definieren, ist völlig unklar. Allerdings gibt es Indizien für die Uferlosigkeit des Begriffs "erheblich". In einigen Polizeigesetzesentwürfen ersetzt der Begriff "erhebliche Straftaten" einen Katalog von nahezu 100 Einzelatbeständen, die z.T. bis in den Bereich des schweren Diebstahls herabreichen, also in äußerst gewöhnliche Kriminalitätsbereiche. Wagner (1988) spricht daher in seinem Kommentar zum NRW-Polizeigesetz von einer "Scheinvertatbestandlichung".

Abs.1 Nr.2 läßt Datenaustausch über Kinder unter 16 Jahren zwischen allen Staatsschutz- und Geheimdienstbehörden zur Strafverfolgung zu, soweit es um Katalog-Straftatbestände nach § 2 des G-10-Gesetzes geht (vgl. Kommentierung zu § 13 Abs.3). Man muß sich zudem klar machen, daß nicht der/die Jugendliche verdächtig sein muß, eine der entsprechenden Straftaten begangen zu haben, sondern "jemand" - und es in diesem Ermittlungskontext den Staatsschutzbehörden sinnvoll erscheint, die Kinder-Daten zu übermitteln.

Abs.2 eröffnet (unter Verweis auf den § 8 Abs.2) den generellen Datentransfer über Jugendliche ab dem 16. Lebensjahr unter Berücksichtigung der in § 8 Abs.2 genannten Lösungsfristen. Anders formuliert: sind die Daten nicht gelöscht worden, dürfen sie auch transferiert werden - ins Ausland, an private Dritte etc.

Abs.3 hebt für Sicherheitsüberprüfungen, in die Kinder und selbstverständlich Jugendliche eingeschlossen werden können, die zuvor genannten Übermittlungs"-begrenzungen" generell auf; für Kinder ausländischer Eltern gibt es keinerlei Begrenzungen. Damit dürfen deren Daten u.a. wiederum auch an ausländische Stellen geliefert werden (vgl. § 14 Abs.3).

Zu § 21: Pflichten des Empfängers

Eine allgemein geltende datenschutzrechtliche Floskel. Der Empfänger, soweit er dem Geltungsbereich dieses Gesetzes unterworfen ist - die Regelung kann für ausländische und übernationale Stellen nicht greifen - hat zu prüfen, ob er die Daten benötigt. Ist dies nicht der Fall, so muß er die Daten löschen oder sperren. Dies ist insoweit als Regelung notwendig, da bei Datenlieferanten außerhalb des Sicherheitsbereichs an die Sicherheitsbehörden die Lieferanten einem Ersuchen zu folgen haben, ohne prüfen zu dürfen oder gar zu müssen, ob es rechtens sei. Die Entscheidung wird vom Empfänger getroffen. Eine informationelle

Gewaltenteilung durch gegenseitige Kontrolle wird gerade ausgeschlossen.

Es ist eine unter bürokratischen Effizienzgesichtspunkten sinnvolle Erinnerung, sich vor Daten zu schützen, die für die Aufgabenerfüllung nutzlos sind.

Zu § 22: Nachberichtigungspflicht

Regelt § 9 die Pflicht des BfV zur Berichtigung der eigenen, gespeicherten Daten bzw. zur Löschung oder Sperrung unrichtiger Daten, so wird hier gegenüber dem Empfänger eine Nachberichtigungspflicht statuiert.

Aber auch hier geht es nicht um Rechte der unmittelbar betroffenen BürgerInnen, die solange nicht angemeldet und durchgesetzt werden können, wie diese keinen Auskunftsanspruch haben. Die Abwägung über die "Wahrung schützwürdiger Interessen des Betroffenen" trifft nur die liefernde Behörde - ohne daß der/die Betroffene davon Kenntnis hat.

Es ist eine Norm, die bestenfalls die Mitarbeiter der Staatsschutzbehörden daran erinnert, die Qualität der den Kollegen gelieferten Daten - im eigenen Interesse des Verbundes - nachzubessern. Hier und da wird es auch unmittelbar Betroffenen dienlich sein, denkt man daran, in welchem Maße BürgerInnen mit auf Datenschrott gestützten politischen Vorwürfen zu kämpfen hatten.

Zu § 23: Automatisierte Abrufverfahren zwischen den Dateien der Geheimdienste und Polizei

Diese Regelung ist in Zusammenhang mit dem § 4 Abs.2 zu sehen, in dem die Rechtsgrundlage für NADIS gegeben wird. Darin heißt es, daß die gemeinsam von den VfS-Ämtern gefütterten Dateien in NADIS nur diesen Ämtern direkt zugänglich sein sollen. Der noch immer vorhandene Bestand des BKAs in NADIS, von Datenschutzbeauftragten regelmäßig gerügt (vgl. Kästchen auf der folgenden Seite), müßte nach dieser Regelung von dem der VfS-Ämter technisch getrennt sein. Die Übermittlung zwischen Polizei und VfS wäre demnach nicht auf dem Wege der Direktanfrage, wohl aber in Form des Austauschs von Bändern oder der Abfrage über Telex zulässig. Dem entspricht die bisherige Praxis für alle nicht in NADIS gespeicherten Dateien der polizeilichen Staatsschutzabteilungen (so etwa APIS u.a.).

Mehr als um eine Verzögerung des Übermittlungsvorganges handelt es sich dabei nicht. Aber auch sie soll entfallen dürfen, "wenn eine erhebliche Beeinträchtigung der freiheitlichen demokratischen Grundordnung droht oder eine konkrete Gefahr für die Sicherheit des Bundes oder eines Landes besteht". In diesem Fall soll es möglich werden, die polizeilichen Dateien und die der Geheimdienste direkt zusammenzuschalten. Als Beispiel für diesen Fall nennt die Begründung den "deut-

schen Herbst" 1977. Welche anderen Fälle denkbar sind, ob evtl. eine einfache Fahndung nach RAF-Mitgliedern genügt, bleibt der Phantasie der Minister vorbehalten.

Sie müssen der Einrichtung des Online-Verbundes zustimmen. Ein solcher Verbund darf nur befristet hergestellt werden. Wie lange solch eine Frist dauern kann, sagt der Entw. nicht.

Zu § 24:

"Geltung" des BDSG und des Verwaltungsverfahrensgesetzes

Auch diese Überschrift steht exemplarisch für sprachlichen Betrug. Sie hebt für das BfV gerade alle einschlägigen Datenschutzregelungen des BDSG und des Verwaltungsverfahrensgesetz auf, sofern diese nicht bereits selbst Einschränkungen für den "Sicherheits"-Bereich enthalten. Suspendiert werden:

- * die Regelung für Speicherung, Veränderung und Nutzung in § 12 BDSG. An seine Stelle tritt § 8 VfS-Gesetz,
- * die Übermittlungsvorschriften in den §§ 12 - 15 BDSG, die durch den gesamten Abs.3 des VfS-Gesetzes ersetzt werden,
- * § 16 BDSG, der u.a. die schriftliche Festlegung von Dateianordnungen vorschreibt, für die im § 10 des hier diskutierten Entwurfs eigenständige Wege eingeschlagen werden,
- * § 18 BDSG - Berichtigung, Löschung, Sperrung - der ebenfalls durch eine erheblich magere Lösung im § 9 dieses Entwurfs ersetzt wird, sowie
- * die §§ 3a (Erhebung) und 3c (Zweckbindung) des Verwaltungsverfahrensgesetzes (vgl. §§ 6 und 7 VfS-Gesetz).

Keine Einschränkungen enthält diese Vorschrift für folgende §§ des BDSG:

- * § 17 (Auskunftsansprüche), der die Geheimdienste ausdrücklich von Auskunftsansprüchen ausschließt, sowie
- * die §§ 22 und 24, die die Zugangs- und Kontrollmöglichkeiten des Datenschutzbeauftragten in Bezug auf die Geheimdienste einschränken.

Literatur:

BMI (Hg.), Verfassungsschutz, Köln-Berlin-Bonn-München, 1966

Borgs-Maciejewski, Hermann/ Ebert, Frank, Das Recht der Geheimdienste, Stuttgart - München - Hannover 1986

Gusy, Christoph, Bundes- und Landeskompetenzen für den administrativen VfS, in: BayVBL. 1982, Heft 7

Roewer, Helmut, Nachrichtendienstrecht der Bundesrepublik Deutschland, Köln - Berlin - Bonn - München 1987

Schwagerl, H. Joachim, Verfassungsschutz in der Bundesrepublik, Heidelberg 1985

Wagner, Heinz, Kommentar zum Polizeigesetz von NRW - Reihe: Alternativ-Kommentare, Neuwied - Darmstadt 1987

Aus: 7. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, 1. Januar 1989

Novellierung des Bundesverfassungsschutzes

Auch der neueste Entwurf zur Novellierung des Bundesverfassungsschutzgesetzes verfolgt deutlich das Ziel, die bisherige Praxis der Datenverarbeitung beim Verfassungsschutz und des Datenaustausches mit anderen Behörden festzuschreiben oder gar auszuweiten, soweit es — vorgeblich — Sicherheitsinteressen dienen könnte. Der Entwurf hält überwiegend daran fest, daß bei der Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz die vom Bundesverfassungsgericht geforderte Zweckbindung nicht gelten soll. Der von dem früheren Regierungsentwurf (1986) unternommene Versuch, einige Befugnisse des Verfassungsschutzes auf die Bereiche Spionage und Terrorismus zu beschränken, wird weitgehend wieder aufgegeben. Auch verzichtet der Entwurf auf eingrenzende Regelungen für Datenerhebung und Datenübermittlung des Bundesgrenzschutzes im Zusammenhang mit Amtshilfeersuchen der Nachrichtendienste. Würde der von der Bundesregierung vorgelegte Entwurf Gesetz, würde der Bürger weiterhin nicht wissen können, wer was wann und bei welcher Gelegenheit über ihn in Erfahrung gebracht hat.

Informationsverarbeitung

Da sich der zulässige Umfang der Informationsverarbeitung maßgeblich nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer abschließenden, möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Die im Entwurf verwendeten Begriffe, wie etwa "Bestrebungen gegen die freiheitlich-demokratische Grundordnung" oder "Gefährdung auswärtiger Belange" bleiben indessen hinter den Anforderungen, die an die Normenklarheit einer Vorschrift zu stellen sind, weit zurück. Für den einzelnen ist weiterhin nicht erkennbar, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Insbesondere bleibt unklar

- welchen Grad an organisatorischer Verfestigung Gruppierungen erreicht haben müssen, damit eine "Bestrebung" vorliegt und ob auch solche "Bestrebungen" beobachtet werden, die erkennbar nicht gegen die freiheitlich demokratische Grundordnung gerichtet sind, an denen aber Personen beteiligt sind, die an anderen gegen diese Grundordnung gerichteten Bestrebungen mitwirken;
- ob und ggf. in welchem Umfang Informationen über demokratische Organisationen gesammelt und gespeichert werden dürfen, die Gegenstand extremistischer Beeinflussung(versuche) sind;
- ob die Beobachtung von nicht organisierten Einzelpersonen grundsätzlich ausgeschlossen ist bzw. wann, unter welchen Voraussetzungen und in welchen Grenzen sie zulässig sein soll.

Bei einer derartig vagen Umschreibung der Aufgaben wäre es umso notwendiger, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten je nach dem, welche seiner ganz unterschiedlichen Aufgaben (Extremismusbeobachtung, Spionageabwehr, Mitwirkung an Sicherheitsüberprüfungen etc.) der Verfassungsschutz wahrnimmt, differenziert, präzise und für den Bürger transparent zu regeln. Auch dies ist aber nicht der Fall. Ich vermisse insbesondere Regelungen darüber, ob und ggf. in welchem Umfang, für welche Zwecke und mit welchen Speicherungsfristen Daten über Unverdächtige und unbeteiligte Personen erhoben und gespeichert werden dürfen.

Darüber hinaus wird die Informationsverarbeitung des Verfassungsschutzes nicht wirklich bereichsspezifisch geregelt. Da der Entwurf nicht nach verschiedenen Aufgabenbereichen des Verfassungsschutzes differenziert, wird dem Verfassungsschutz vielmehr eine Art Generalbefugnis erteilt. Es müßte demnach sehr viel klarer geregelt werden, unter welchen Voraussetzungen welche Arten von Dateien eingerichtet werden dürfen und in welchen Zusammenhängen welche Textzusätze gespeichert werden dürfen. Es müßte sichergestellt werden, daß in den Dateien die für die Bewertung und Überprüfung von Textzusätzen maßgeblichen Unterlagen angegeben werden. Schließlich sollte klargestellt werden, daß in Textdateien nur Daten über solche Personen gespeichert werden dürfen, die selbst im Verdacht stehen, eine der im Gesetzentwurf aufgezählten Straftaten zu planen, zu begehen oder begangen zu haben.

Auch der neue Entwurf regelt lediglich die Speicherung personenbezogener Daten in Dateien, obwohl die Fortschritte der Informationsverarbeitung es immer leichter möglich machen, auch komplexe Datensammlungen — bestehend aus Akten, Dateien und anderen Unterlagen — gezielt mit Hilfe automatischer Verfahren zu erschließen.

Die für das BfV vorgesehene Befugnis, automatisiert oder herkömmlich geführte "amtliche Register", d. h. alle derartigen Register, einzusehen, wenn die Informationen nicht aus allgemein zugänglichen Quellen oder nur mit unverhältnismäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden können, ist in diesem Umfang nicht hinnehmbar. Dies würde bedeuten, daß das BfV selbst für Zwecke der Extremismusbeobachtung eine Art "Rasterfahndung" in Form der Durchsicht aller amtlich geführten Register betreiben könnte.

Weiterhin nicht hinreichend beachtet wird der Grundsatz, daß die Verwendung von personenbezogenen Daten grundsätzlich auf den Zweck beschränkt ist, für den sie erhoben werden (Zweckbindungsgebot). So darf jede Behörde oder öffentliche Stelle grundsätzlich dem BfV alle Daten übermitteln, wenn nach ihrer Auffassung tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des BfV erforderlich ist und sie entgegenstehende Übermittlungsverbote nicht zu erkennen vermag. Innerhalb des BfV darf jede Information unabhängig von ihrer Herkunft für jede Aufgabe verwendet werden. Das BfV darf grundsätzlich alle Informationen an andere Behörden, ja selbst an private Stellen übermitteln. Die nunmehr vorgesehenen Übermittlungsverbote reichen vor allem deshalb nicht aus, weil das BfV nicht ausdrücklich verpflichtet wird, entgegenstehende schutzwürdige Belange zu ermitteln.

Weiter fehlen befriedigende Lösungsregelungen. Abgesehen davon, daß die Löschung von Daten in Akten nicht einmal erwähnt wird, ist zu fordern, daß schon im Gesetz Regelfristen für die Überprüfung und Löschung der verarbeiteten Daten festzulegen sind. Dabei muß zwischen den einzelnen Aufgabenbereichen unterschieden werden.

Nachrichtendienstliche Mittel

Der Versuch, bei der Regelung des Einsatzes von nachrichtendienstlichen Mitteln mehr Präzision zu schaffen, ist im Ansatz stecken geblieben. Unklar ist insbesondere, welche rechtlichen Grenzen dem Einsatz nachrichtendienstlicher Mittel gesetzt sind. Vorgänge in der jüngsten Zeit lassen es geboten erscheinen klarzustellen, daß der Einsatz nachrichtendienstlicher Mittel Verstöße gegen Straftatbestände auf keinen Fall rechtfertigt, wenn Rechte Privater tangiert werden.

Auch fehlt bislang die Klarstellung, daß sich der Einsatz nachrichtendienstlicher Mittel grundsätzlich nur gegen diejenigen richten darf, der selbst in Verdacht steht, die vom Verfassungsschutz beobachteten Bestrebungen oder Tätigkeiten auszuüben. Soweit beim Einsatz nachrichtendienstlicher Mittel Informationen über andere Personen anfal-

len, sollte entsprechend dem G-10-Gesetz ein Verwertungsverbot statuiert werden.

Ferner sollten beim Einsatz nachrichtendienstlicher Mittel zum Schutz des Betroffenen — über die jetzt vorgesehene Unterrichtung der Kommission nach § 9 Abs. 2 G-10-Gesetz hinaus — zusätzliche Schutzvorkehrungen eingebaut werden. Um dem Betroffenen die Möglichkeit zu geben, sich gegen eine mögliche Verletzung seiner Rechte zur Wehr zu setzen, ist er — jedenfalls bei schweren Eingriffen — über den Einsatz nachrichtendienstlicher Mittel zu informieren, sobald eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. Auch muß die Kontrolle durch die unabhängigen Datenschutzbeauftragten gewährleistet sein.

Trennungsgebot

Das Vorhaben, den Austausch von Informationen in einem eigenen Gesetz — ursprünglich Zusammenarbeitsgesetz (ZAG), dann Verfassungsschutzmitteilungsgesetz (VerfSchMitG) genannt — zu regeln, hat der Bundesinnenminister nunmehr aufgegeben und die vorgesehenen Regelungen in das BVerfSchG integriert. Inhaltliche Änderungen, die der bisher vorgebrachten Kritik Rechnung tragen, sind leider kaum feststellbar. Auch der jetzt vorgelegte Entwurf zieht nicht die gebotenen Konsequenzen aus dem Trennungsgebot für Polizei und Verfassungsschutz, das als eine der Konsequenzen aus demokratiefeindlicher Machtzusammenballung im NS-Staat in unsere Rechtsordnung eingeführt wurde. Ziel dieses aus dem Rechtsstaatsprinzip zwingend abzuleitenden Trennungsgebotes ist nicht nur die rein organisatorische Schaffung zweier unterschiedlicher Behörden für Aufgaben der Polizei und des Verfassungsschutzes. Seine materiell-inhaltliche Bedeutung besteht im Zeitalter der automatisierten Datenverarbeitung vielmehr auch darin, daß durch die Verteilung polizeilicher Befugnisse auf die eine und nachrichtendienstlicher Befugnisse auf die andere der beiden Behörden auch eine Bündelung der mit diesen unterschiedlichen Befugnissen gewonnenen Informationen vermieden werden soll.

Dieses Ziel wird von den in Aussicht genommenen Übermittlungsvorschriften verfehlt. Der Austausch der jeweils mit spezifischen Befugnisnormen gewonnenen Informationen führt dazu, daß das Trennungsgebot von einem Prinzip der Machthemmung zu einem Instrument möglichst effektiver Arbeitsteilung degeneriert. Der Entwurf verpflichtet nicht einmal den Datenempfänger, die übermittelten Daten nur für den Zweck zu verwenden, zu dem sie ihm übermittelt worden sind, und er läßt auch die Weiterübermittlung von Daten über mehrere Stationen zu, ohne daß es auf den Zweck der jeweiligen Übermittlungen ankäme. Würde der jetzige Entwurf Gesetz, bliebe es dabei, daß sich Nachrichtendienste und Polizeien des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes beim Informationsaustausch wie Abteilungen ein und derselben Behörde verhalten könnten.

Informationen, die im Rahmen von Telefonüberwachungsmaßnahmen gewonnen werden, sollen jetzt nur noch unter Einschränkungen an das BfV übermittelt und von diesem verwertet werden dürfen. Ergänzend müßte sichergestellt werden, daß die verfahrensrechtlichen Sicherungen sowie die Benachrichtigungspflicht nach der StPO nicht unterlaufen werden. Aber auch für Daten, die die Polizei bei Hausdurchsuchungen oder durch den Einsatz von V-Leuten, verdeckten Ermittlern oder technischen Geräten, durch polizeiliche Beobachtung oder längerfristige Observationen gewonnen hat, müssen einschränkende Verwertungsregelungen geschaffen werden. Weiter ist klarzustellen, daß es nicht Aufgabe der Polizei sein kann, "Zufallsfunde" zu sammeln und weiterzugeben, die ihr bei Gelegenheit der Erfüllung ihrer Aufgaben bekannt werden, ohne für ihre eigentliche Aufgabenerfüllung erforderlich zu sein. Die Amtshilfe der Grenzpolizeien für den Verfassungsschutz muß einschränkend geregelt werden.

N A D I S

1. Was ist NADIS?

NADIS, das nachrichtendienstliche Informationssystem, ist ein in erster Linie durch die VfS-Ämter genutztes Datensystem. Die Zentrale des Systems steht beim BfV, die Landesämter können direkt eingeben und abfragen (online-Verbund).

2. Welche Dateiformen gibt es in NADIS?

Es sind grundsätzlich zwei Dateiformen, die zwischen den VfS-Ämtern als Verbunddateien betrieben werden:

a) Hinweisdateien

Die wichtigste ist die Personenzentraldatei (PZD), in der jeweils die Personengrunddaten sowie weitere sog. Formatdaten (Bankkonto, Auto-Kennzeichen etc.) erfaßt werden. Darüber hinaus enthält der PZD-Datensatz eine Kennnummer, über die einerseits der Zugang zu den entsprechenden Akteninhalten und Vorgängen möglich ist, die aber zweitens auch bereits ohne Kenntnis des Akteninhalts Aufschluß über den Bereich verfassungsschützerischer Arbeit gibt, in dem die Akten angefallen sind. Die PZD ist die wichtigste VfS-Datei, da eine Anfrage in ihr den ersten Aufschluß über die jeweils in Frage kommende Person gibt. Neben der PZD existiert eine weitere Hinweisdatei auf "Objekte".

b) Textdateien

In diesen Dateien sind nicht nur formatierte Daten, sondern auch Freitext enthalten. Über die Struktur dieser Dateiformen ist nichts genaueres bekannt. Vermutlich handelt es sich hier um Dateien, die ähnlich wie die polizeilichen SPUDOK - und PIOS-Dateien eine weitergehende Auswertungsmöglichkeit durch Suchworte und Zusammenführung von Informationen aus verschiedenen Datenbereichen eröffnen. Soweit bekannt, existieren diese Dateien im "Extremismus"-, im "Terrorismus"bereich und bei der Spionageabwehr.

Neben den Verbunddateien führen die Ämter jeweils **Amtsdateien**, auf die nur sie direkt Zugriff haben.

3. Wer nutzt sonst noch NADIS und wie?

MAD und BND, die jeweils ihre eigenen Datensysteme betreiben, sind nicht direkt mit dem System des VfS verbunden. Sie erhalten ihre Informationen aus NADIS im Zuge monatlicher Bandabgleiche. Damit verfügen sie über eine monatlich aktualisierte Personen-Zentral-Datei (PZD) des VfS. Die sie interessierenden Informationen können dann auf konventionelle Weise (Telefon, Telex) abgefragt werden.

Die bis 1979 existierende feste Standleitung zwischen dem polizeilichen Informationssystem INPOL und NADIS ließ der damalige Innenminister Baum nur teilweise kappen. Gleichwohl speichert die Staatsschutz-Abteilung des BKAs weiterhin ihre Daten in der PZD. Sie benutzt diese Datei gewissermaßen als ihr Hinweissystem - mit dem Effekt, daß der VfS Mitwisser eines großen Teils der polizeilichen Staatsschutzdaten ist. Nach offiziellen Angaben kann das BKA umgekehrt nur auf die Daten direkt zugreifen, die es selbst in NADIS eingegeben hat, also nicht auf Daten des VfS.

Diese Regelung sollte nur provisorischen Charakter haben, bis eine eigene Staatsschutzdatei im BKA aufgebaut sei. Diese Datei, eine Zusammenführung der alten PIOS-Dateien Terrorismus und Staatsgefährdung, existiert bereits seit einiger Zeit und trägt den Namen APIS, Arbeitsdatei PIOS Innere Sicherheit. Für APIS wurde das Systemkonzept von PIOS neu bearbeitet, um weitere Auswertungsmöglichkeiten in dieser Textdatei bereitzustellen. NADIS wird jedoch ungeachtet der wiederholten Kritik des Bundesdatenschutzbeauftragten (BfD) von der BKA-Staatsschutzabteilung weitergenutzt.

In seinem Bericht über die "Datenschutzrechtliche Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamts" vom 7.12. letzten Jahres (siehe "Spiegel" vom 13.2.89, S. 72 f.) weist der BfD darauf hin, daß NADIS zu einer "Auffangdatei" für Daten geworden ist, die in APIS aufgrund der restriktiveren Dateianordnung nicht gespeichert werden dürfen. Innerhalb von 10 Monaten hat das BKA 1290 Fälle in APIS gespeichert, während es im gleichen Untersuchungszeitraum 2976 Fälle in NADIS unterbrachte. Insgesamt ist der Strom von Daten vom BKA zum BfV genauso breit wie zwischen den Staatsschutz-Polizeiabteilungen der Länder und dem BKA. Die informationelle Verschmelzung zwischen Polizei und VfS ist also längst vollzogen.

4. Sonstige Informationswege Polizei - VfS

Der VfS hat aber nicht nur Zugriff auf diese in NADIS gespeicherten Polizeidaten. Übermittelt wurden z.B. bei einem Bandabgleich im August 1987 die ge-

samten Datenbestände der "Arbeitsdatei PIOS Landfriedensbruch", früher "Meldedienst Landfriedensbruch", die sich insbesondere auf Demonstrationsdelikte und ähnliches (auch Hausfriedensbruch etwa) bezieht.

Kenntnis von Polizeidaten erhält der VfS darüber hinaus durch Informationshilfersuchen bei einer rund um die Uhr besetzten Verbindungsstelle im BKA.

◆ Max Watts: US-Army-Europa. Von der Desertion zum Widerstand in der Kaserne oder wie die U-Bahn zu RITA fuhr. 108 S., 9,80 DM.

Während des Vietnamkriegs desertierten 432.000 GIs. Nicht wenige von ihnen aus Einheiten der 7. US-Armee in der BRD. Max Watts beschreibt das Entstehen der Untergrundbahn für US-Deserteure in Westeuropa und die Arbeit der Deserteursgruppe „RITA ACT“ im Pariser „Exil“. Mit aktuellen Adressen!

COUNTERINSURGENCY Planning Guide., Handbuch zur Anti-Guerilla-Kriegsführung aus der US-Army Special Warfare School, Ft. Bragg. In deutscher Sprache, 106 S., 8,80 DM.

Roger Fallgot: The Kitson Experiment. (engl.), 242 S., 25 DM. Nordirland als Labor für Aufstandsbekämpfung in Westeuropa. **Nieder mit der Disziplin! Hoch die Rebellen! Anarchistische Soldaten-Agitation im Deutschen Kaiserreich.** 92 S., 8,80 DM. Enthält das von dem Anarcho-Syndikalisten Siegfried Nacht verfaßte „Soldatenbrevier“, das 1907 als Propagandaschrift des Kriegsministeriums gelammt-verbreitet wurde.

Bezug: **Harald Kater Verlag,**
Görlitzer Straße 39, 1000 Berlin 36
☎ 030/618 26 47

ANFRAGE 465650-00/U NG ST 63 -- VS-NFD --- ZEIT 13.07.57 Datum 23/09/82
PN- 14572473 EK 15.03.82 WV

NA	o	KITTNER							
VN	6	DIETRICH							
GD	30.05.35		GO	OELS	GL	P80	ST	D	
BS	FKM		WO	HANNOVER	WL	NI			
BR	KUNSTLERISCHER BERUF				PG				
FP	BW	0966	085-000000-000/70	P	FP	BR	1168	081-070042-002/72	P
FP	NI	0181	081-087396-000/81	P	FP	3A3	0182	085-200305-000/82	P
FP	ST	0175	041-113594-000/00	P	FP	NW	0070	085-031705-000/70	
FP	HH	0771	085-100023-000/75	S					
AD	BW	HANNOVER		HAN	BOEDECKERSTR				28
					085-000000-000/70			1	
AD	NW	HANNOVER		NI	BOEDECKERSTR				28
					085-000000-000/70			1	
AD	3A1	HANNOVER		NI	ALLEE STR				1
		00.03.70-00.09.74			085-200305-000/77			1	
AD	3A1	HANNOVER		NI	BISCHOFSHOLER DAMM				88
		00.10.74			085-200305-000/77	P		1	
AD	ST	HANNOVER		NI	BISCHOFSHOLER DAMM				88
		00.01.75			041-113594-000/00	P		1	
TF	3A1	HANNOVER		NI	KITTNER DIETRICH				710491
		00.08.71			085-200305-000/77			1	

ANFRAGE	465650-00/U	NG	ST 63	--	VS-NFD	---	ZEIT 13.07.57	DATUM 23/09/82	
	3A3	HANNOVER			NI		KITTNER DIETRICH		851545
		00.01.78					085-200305-000/78		1
KF	3A1	HANNOVER			NI		OPEL ADMIRAL 2800		H-LC-755
		00.08.70			NI		085-200305-000/77		1
KT	3A1	HANNOVER			NI		SPARKASSE		11729260
		00.09.73					085-200305-000/77		1

Aus dem 11. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zum 1. Januar 1989

16.3.2 NADIS

Einen weiteren Schwerpunkt der Kontrolle bildete die Speicherung von Daten durch das Bundeskriminalamt in NADIS. Diese Praxis hatte ich bereits wiederholt beanstandet (vgl. zuletzt 10. TB S. 77 f.). Der Bundesminister des Innern hat meine Beanstandungen bislang stets zurückgewiesen, und das Bundeskriminalamt fährt fort, Daten in NADIS zu speichern. Der BMI begründet dies im wesentlichen damit, daß alle vom BKA in NADIS gespeicherten Fälle für die Verfassungsschutzbehörden relevant seien. Das BKA sei auf die Speicherung in NADIS nicht angewiesen, denn es verfüge über eigene Dateisysteme, in denen es die Speicherung vornehmen könnte. Die Speicherung in NADIS erfolge im Interesse der Informationsübermittlung an den Verfassungsschutz.

In früheren Stellungnahmen hatte der BMI die Relevanz der durch das BKA in NADIS gespeicherten Fälle für den Verfassungsschutz daraus abgeleitet, daß nur solche Fälle in NADIS gespeichert würden, die auch die Erfassungskriterien für APIS erfüllten; aus diesen ergebe sich die Verfassungsschutzrelevanz. Ich habe demgegenüber festgestellt, daß das BKA doppelt so viele Fälle in NADIS wie in APIS speichert. NADIS ist sozusagen die „Auffangdatei“ für die Fälle, die die – ohnehin zu weiten – Voraussetzungen für die Erfassung in APIS nicht erfüllen (vgl. oben 16.3.1).

Dies betraf beispielsweise zwei Personen, die die Rede eines Staatssekretärs der Bayerischen Staatsregierung in einem Festzelt mit dem Zwischenruf „Heil-Gauleiter“ gestört hatten. Eine andere Person hatte ein Verwarnungsgeld wegen Falschparkens bezahlt und auf dem begleitenden Anschreiben „mit deutschem Gruß“ unterschrieben. Eine weitere Person fiel in betrunkenem Zustand im Schützenzelt auf dem Münchener Oktoberfest „Sieg heil“. Diese und weitere von mir aufgeführte Fälle wurden vom BKA nicht in APIS, wohl aber in NADIS gespeichert und damit an die Verfassungsschutzbehörden übermittelt.

Der BMI räumt nunmehr ein, daß in NADIS auch Fälle erfaßt werden, die nicht in APIS gespeichert sind. Im übrigen ist seine Auffassung in dieser Frage unverändert. Meine Feststellung, daß mehr als die Hälfte der von der Abteilung Staatsschutz des BKA erteilten konventionellen Auskünfte in dem von mir untersuchten Zeitraum an Verfassungsschutzbehörden gingen, hält der BMI für einen Beleg für die Notwendigkeit des engen Informationsaustauschs zwischen Polizei und Verfassungsschutz.

Die Speicherung von Daten durch die Abteilung Staatsschutz des BKA in der NADIS-Personenzentraldatei (NADIS-PZD) bedeutet, daß routinemäßig personenbezogene Daten übermittelt und gespeichert werden, ohne daß die jeweils verantwortliche Behörde die Zulässigkeit der konkreten Einzelmaßnahmen prüft. Eine solche Verfahrensweise ist mit dem geltenden Recht nicht vereinbar. Aber auch die Entwürfe für das Verfassungsschutzgesetz sowie für das BKA-Gesetz sehen keine einschlägige Rechtsgrundlage vor. Der Entwurf eines Verfassungsschutzgesetzes schließt im Gegenteil die Beteiligung anderer als Verfassungsschutzbehörden an NADIS-PZD ausdrücklich aus.

19.4 Konsequenzen aus früheren Kontrollen

Ferner hatte ich früher bemängelt, daß in zusammenfassenden Lageberichten personenbezogene Daten enthalten waren, ohne daß dies in jedem Fall erforderlich war. Bei derartigen Lageberichten steht zum Zeitpunkt ihrer Abfassung nicht immer fest, an welche Empfänger sie übersandt werden. Ich habe in einzelnen Fällen auch festgestellt, daß solche Berichte ausländischen Nachrichtendiensten zugänglich gemacht worden sind. Durch eine Änderung der entsprechenden Dienstvorschrift des BfV ist nunmehr ausdrücklich klargestellt worden, daß personenbezogene Daten in Berichte des BfV für inländische und ausländische Behörden nur aufgenommen werden, wenn dies erforderlich ist und schutzwürdige Belange betroffener Personen dabei berücksichtigt sind. Ich gehe davon aus, daß es bei derartigen Berichten in der Regel genügt, wenn Personen ohne Namensnennung nur ihrer politischen Funktion beschrieben werden, so daß die Notwendigkeit der Aufnahme personenbezogener Daten in derartige Berichte die Ausnahme ist.

Ich konnte auch erreichen, daß Daten, die im Rahmen einer Sicherheitsüberprüfung erhoben worden sind, nur noch in geringerem Umfang an ausländische Nachrichtendienste übermittelt werden. Die Dienstvorschrift über die Beziehungen des BfV zu ausländischen Nachrichtendiensten wurde dahin ergänzt, daß Daten, die den Bereich der persönlichen Lebensführung betreffen, an diese nur noch für Zwecke der Sicherheitsüberprüfung und der Spionageabwehr übermittelt werden dürfen.

Das BfV wird von ausländischen Nachrichtendiensten nicht selten um Übermittlung von Informationen ersucht, die für eine dort durchzuführende Sicherheitsüberprüfung benötigt werden. Bei einer Sicherheitsüberprüfung nach deutschem Recht ist dem Betroffenen rechtliches Gehör zu gewähren, falls seine Ermächtigung zum Umgang mit Verschlusssachen abgelehnt werden soll. Dies ist nicht in allen Ländern so, an deren Nachrichtendienste das BfV Daten zum Zwecke der Sicherheitsüberprüfung übermittelt.

Nach meiner Auffassung wäre es notwendig, daß das BfV entweder auf der Gewährung von rechtlichem Gehör durch die dortigen Behörden besteht oder aber selbst dem Betroffenen rechtliches Gehör gewährt, wenn es belastende Daten über ihn an einen ausländischen Nachrichtendienst übermittelt. Immerhin konnte ich nunmehr erreichen, daß das BfV alle ausländischen Nachrichtendienste angeschrieben und sie gebeten hat, entsprechend den Regelungen in der Bundesrepublik Deutschland den Betroffenen rechtliches Gehör zu geben, wenn ihre Ermächtigung zum Umgang mit Verschlusssachen aufgrund von Informationen abgelehnt werden soll, die vom BfV übermittelt worden sind. Es bleibt abzuwarten, ob dies eine ausreichende Maßnahme ist, um die schutzwürdigen Belange der Betroffenen zu gewährleisten.

des BND und der Strafverfolgungsbehörden nutzen. Er darf in diesem Bereich aber nicht selbst erheben oder gar nachrichtendienstliche Mittel einsetzen. Mit dieser Abgrenzung wird also das Maß der dem MAD zugänglichen Informationen keineswegs beschränkt. Gespeichert, genutzt, verarbeitet und übermittelt werden dürfen Daten auch hier - es geht nur um eine funktionale Abgrenzung zum VfS und BND.

**Zu § 7:
"Geltung" des BDSG und Verwaltungsverfahrensgesetzes**

Auch hier wir zum BVerfSchG (vgl. § 24) "paralleliert", d.h. die datenschutzrechtlichen Regelungen dieser Gesetze werden für den MAD suspendiert.

Literatur zum MAD:

Gusy, Christoph, Der Militärische Abschilderndienst, in: Die öffentliche Verwaltung, Heft 2/1983, S. 60 ff.
Kloss, Herbert, MAD - der militärische Abschilderndienst der Bundeswehr, in: Beiträge zur Konfliktforschung 1/1987, S. 99 ff.
Diskussion und Feststellungen des Dt. Bundestages in Sachen Kießling. Zur Sache - Themen parlamentarischer Beratung, 2/1984

**Aus dem 11. Tätigkeitsbericht
des Bundesbeauftragten für den
Datenschutz zum 1.1.1989**

21.1.2 Datenschutzrechtliche Kontrolle beim MAD

Ich habe 1988 die im Abwehrbereich „Verfassungsfeindliche Kräfte“ (VfK) in einem bestimmten Zeitraum angelegten Ermittlungsvorgänge überprüft und statistisch ausgewertet. Dabei stellte sich heraus, daß am Beginn der Ermittlungen in ca. vier Fünfteln der Fälle keine konkret unmittelbar gegen die Bundeswehr gerichteten extremistischen Handlungen vorlagen. Ausgangspunkt der Bearbeitung waren vielmehr in fast jedem zweiten Fall Informationen, die im Rahmen einer Sicherheitsüberprüfung angefallen, im übrigen in der Regel Informationen, die dem MAD von anderen Sicherheitsbehörden übermittelt worden waren. Zumeist handelt es sich dabei um Hinweise auf eine extremistische Betätigung von Bundeswehrangehörigen.

Die Ermittlungen des MAD haben in fast jedem zweiten aller Fälle ergeben, daß der Verdacht extremistischer Bestrebungen widerlegt bzw. ausgeräumt werden konnte. In etwa einem Viertel der Fälle ist es letztlich offengeblieben, ob der Verdacht zutraf oder nicht. Lediglich im verbleibenden Viertel ergaben die Recherchen, daß sich die Person in einer extremistischen Organisation betätigte. Diese Betätigung hatte aber nur in seltenen Fällen etwas mit der Bundeswehr zu tun. Zum großen Teil handelte es sich um die Mitgliedschaft in einer Organisation, deren Tätigkeit gegen die freiheitlich demokratische Grundordnung gerichtet und die von den Verfassungsschutzbehörden als Beobachtungsobjekt eingestuft ist. Im Ergebnis fehlte es bei der weit überwiegenden Zahl der von mir insgesamt ausgewerteten Fälle objektiv an der Voraussetzung einer „unmittelbar gegen die Bundeswehr gerichteten Bestrebung“. Gleichwohl war stets, wenn im Ermittlungszusammenhang auch gegen eine der Wehrüberwachung unterliegende Person ermittelt wurde, eine Speicherung in der Personenzentraldatei des MAD veranlaßt worden. Bei Bestätigung des Verdachts einer extremistischen Betätigung, auch wenn diese sich nicht unmittelbar gegen die Bundeswehr richtete, wurde eine fünfjährige Speicherung verfügt, bei Ausräumung des Verdachts sogar zehn Jahre, was besonders unverhältnismäßig erscheint.

Ich habe den Bundesminister der Verteidigung aufgefordert, diese Regelungen zu überprüfen. Auch wenn man akzeptiert, daß der MAD als Nachrichtendienst bereits beim Verdacht, daß eine unmittelbar gegen die Bundeswehr gerichtete extremistische Bestrebung vorliegen könnte, tätig wird, so dürfen seine Ermittlungen jedenfalls dann, wenn sie die Unzuständigkeit des MAD ergeben haben, nicht zu einer mehrjährigen Speicherung in den Dateien des MAD führen. Ich habe vorgeschlagen, statt dessen die (ursprünglich) meldende Stelle davon zu unterrichten, daß der Verdacht entkräftet wurde. Im übrigen halte ich eine Speicherung derartiger Fälle höchstens nur bis zum Ende der aktiven Bundeswehrzeit des Betroffenen für zulässig. Der Bundesminister der Verteidigung hat angekündigt, daß er die entsprechenden innerdienstlichen Vorschriften ändern und mich dabei beteiligen will.

Aus: 7. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, 1. Januar 1989

Novellierung des Bundesverfassungsschutzes

Auch der neueste Entwurf zur Novellierung des Bundesverfassungsschutzgesetzes verfolgt deutlich das Ziel, die bisherige Praxis der Datenverarbeitung beim Verfassungsschutz und des Datenaustausches mit anderen Behörden festzuschreiben oder gar auszuweiten, soweit es — vorgeblichen — Sicherheitsinteressen dienen könnte. Der Entwurf hält überwiegend daran fest, daß bei der Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz die vom Bundesverfassungsgericht geforderte Zweckbindung nicht gelten soll. Der von dem früheren Regierungsentwurf (1986) unternommene Versuch, einige Befugnisse des Verfassungsschutzes auf die Bereiche Spionage und Terrorismus zu beschränken, wird weitgehend wieder aufgegeben. Auch verzichtet der Entwurf auf eingrenzende Regelungen für Datenerhebung und Datenübermittlung des Bundesgrenzschutzes im Zusammenhang mit Amtshilfeersuchen der Nachrichtendienste. Würde der von der Bundesregierung vorgelegte Entwurf Gesetz, würde der Bürger weiterhin nicht wissen können, wer was wann und bei welcher Gelegenheit über ihn in Erfahrung gebracht hat.

Informationsverarbeitung

Da sich der zulässige Umfang der Informationsverarbeitung maßgeblich nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer abschließenden, möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Die im Entwurf verwendeten Begriffe, wie etwa "Bestrebungen gegen die freiheitlich-demokratische Grundordnung" oder "Gefährdung auswärtiger Belange" bleiben indessen hinter den Anforderungen, die an die Normenklarheit einer Vorschrift zu stellen sind, weit zurück. Für den einzelnen ist weiterhin nicht erkennbar, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Insbesondere bleibt unklar

- welchen Grad an organisatorischer Verfestigung Gruppierungen erreicht haben müssen, damit eine "Bestrebung" vorliegt und ob auch solche "Bestrebungen" beobachtet werden, die erkennbar nicht gegen die freiheitlich demokratische Grundordnung gerichtet sind, an denen aber Personen beteiligt sind, die an anderen gegen diese Grundordnung gerichteten Bestrebungen mitwirken;
- ob und ggf. in welchem Umfang Informationen über demokratische Organisationen gesammelt und gespeichert werden dürfen, die Gegenstand extremistischer Beeinflussung(sversuche) sind;
- ob die Beobachtung von nicht organisierten Einzelpersonen grundsätzlich ausgeschlossen ist bzw. wann, unter welchen Voraussetzungen und in welchen Grenzen sie zulässig sein soll.

Bei einer derartig vagen Umschreibung der Aufgaben wäre es umso notwendiger, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten je nach dem, welche seiner ganz unterschiedlichen Aufgaben (Extremismusbeobachtung, Spionageabwehr, Mitwirkung an Sicherheitsüberprüfungen etc.) der Verfassungsschutz wahrnimmt, differenziert, präzise und für den Bürger transparent zu regeln. Auch dies ist aber nicht der Fall. Ich vermisse insbesondere Regelungen darüber, ob und ggf. in welchem Umfang, für welche Zwecke und mit welchen Speicherungsfristen Daten über Unverdächtige und unbeteiligte Personen erhoben und gespeichert werden dürfen.

Darüber hinaus wird die Informationsverarbeitung des Verfassungsschutzes nicht wirklich bereichsspezifisch geregelt. Da der Entwurf nicht nach verschiedenen Aufgabengebieten des Verfassungsschutzes differenziert, wird dem Verfassungsschutz vielmehr eine Art Generalbefugnis erteilt. Es müßte demnach sehr viel klarer geregelt werden, unter welchen Voraussetzungen welche Arten von Dateien eingerichtet werden dürfen und in welchen Zusammenhängen welche Textzusätze gespeichert werden dürfen. Es müßte sichergestellt werden, daß in den Dateien die für die Bewertung und Überprüfung von Textzusätzen maßgeblichen Unterlagen angegeben werden. Schließlich sollte klargestellt werden, daß in Textdateien nur Daten über solche Personen gespeichert werden dürfen, die selbst im Verdacht stehen, eine der im Gesetzentwurf aufgezählten Straftaten zu planen, zu begehen oder begangen zu haben.

Auch der neue Entwurf regelt lediglich die Speicherung personenbezogener Daten in Dateien, obwohl die Fortschritte der Informationsverarbeitung es immer leichter möglich machen, auch komplexe Datensammlungen — bestehend aus Akten, Dateien und anderen Unterlagen — gezielt mit Hilfe automatischer Verfahren zu erschließen.

Die für das BfV vorgesehene Befugnis, automatisiert oder herkömmlich geführte "amtliche Register", d. h. alle derartigen Register, einzusehen, wenn die Informationen nicht aus allgemein zugänglichen Quellen oder nur mit unverhältnismäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden können, ist in diesem Umfang nicht hinnehmbar. Dies würde bedeuten, daß das BfV selbst für Zwecke der Extremismusbeobachtung eine Art "Rasterfahndung" in Form der Durchsicht aller amtlich geführten Register betreiben könnte.

Weiterhin nicht hinreichend beachtet wird der Grundsatz, daß die Verwendung von personenbezogenen Daten grundsätzlich auf den Zweck beschränkt ist, für den sie erhoben werden (Zweckbindungsgebot). So darf jede Behörde oder öffentliche Stelle grundsätzlich dem BfV alle Daten übermitteln, wenn nach ihrer Auffassung tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des BfV erforderlich ist und sie entgegenstehende Übermittlungsverbote nicht zu erkennen vermag. Innerhalb des BfV darf jede Information unabhängig von ihrer Herkunft für jede Aufgabe verwendet werden. Das BfV darf grundsätzlich alle Informationen an andere Behörden, ja selbst an private Stellen übermitteln. Die nunmehr vorgesehenen Übermittlungsverbote reichen vor allem deshalb nicht aus, weil das BfV nicht ausdrücklich verpflichtet wird, entgegenstehende schutzwürdige Belange zu ermitteln.

Weiter fehlen befriedigende Lösungsregelungen. Abgesehen davon, daß die Löschung von Daten in Akten nicht einmal erwähnt wird, ist zu fordern, daß schon im Gesetz Regelfristen für die Überprüfung und Löschung der verarbeiteten Daten festzulegen sind. Dabei muß zwischen den einzelnen Aufgabenbereichen unterschieden werden.

Nachrichtendienstliche Mittel

Der Versuch, bei der Regelung des Einsatzes von nachrichtendienstlichen Mitteln mehr Präzision zu schaffen, ist im Ansatz stecken geblieben. Unklar ist insbesondere, welche rechtlichen Grenzen dem Einsatz nachrichtendienstlicher Mittel gesetzt sind. Vorgänge in der jüngsten Zeit lassen es geboten erscheinen klarzustellen, daß der Einsatz nachrichtendienstlicher Mittel Verstöße gegen Straftatbestände auf keinen Fall rechtfertigt, wenn Rechte Privater tangiert werden.

Auch fehlt bislang die Klarstellung, daß sich der Einsatz nachrichtendienstlicher Mittel grundsätzlich nur gegen diejenigen richten darf, der selbst in Verdacht steht, die vom Verfassungsschutz beobachteten Bestrebungen oder Tätigkeiten auszuüben. Soweit beim Einsatz nachrichtendienstlicher Mittel Informationen über andere Personen anfal-

len, sollte entsprechend dem G-10-Gesetz ein Verwertungsverbot statuiert werden.

Ferner sollten beim Einsatz nachrichtendienstlicher Mittel zum Schutz des Betroffenen — über die jetzt vorgesehene Unterrichtung der Kommission nach § 9 Abs. 2 G-10-Gesetz hinaus — zusätzliche Schutzvorkehrungen eingebaut werden. Um dem Betroffenen die Möglichkeit zu geben, sich gegen eine mögliche Verletzung seiner Rechte zur Wehr zu setzen, ist er — jedenfalls bei schweren Eingriffen — über den Einsatz nachrichtendienstlicher Mittel zu informieren, sobald eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. Auch muß die Kontrolle durch die unabhängigen Datenschutzbeauftragten gewährleistet sein.

Trennungsgebot

Das Vorhaben, den Austausch von Informationen in einem eigenen Gesetz — ursprünglich Zusammenarbeitsgesetz (ZAG), dann Verfassungsschutzmitteilungsgesetz (VerfSchMitG) genannt — zu regeln, hat der Bundesinnenminister nunmehr aufgegeben und die vorgesehenen Regelungen in das BVerfSchG integriert. Inhaltliche Änderungen, die der bisher vorgebrachten Kritik Rechnung tragen, sind leider kaum feststellbar. Auch der jetzt vorgelegte Entwurf zieht nicht die gebotenen Konsequenzen aus dem Trennungsgebot für Polizei und Verfassungsschutz, das als eine der Konsequenzen aus demokratiefeindlicher Machtzusammenballung im NS-Staat in unsere Rechtsordnung eingeführt wurde. Ziel dieses aus dem Rechtsstaatsprinzip zwingend abzuleitenden Trennungsgebotes ist nicht nur die rein organisatorische Schaffung zweier unterschiedlicher Behörden für Aufgaben der Polizei und des Verfassungsschutzes. Seine materiell-inhaltliche Bedeutung besteht im Zeitalter der automatisierten Datenverarbeitung vielmehr auch darin, daß durch die Verteilung polizeilicher Befugnisse auf die eine und nachrichtendienstlicher Befugnisse auf die andere der beiden Behörden auch eine Bündelung der mit diesen unterschiedlichen Befugnissen gewonnenen Informationen vermieden werden soll.

Dieses Ziel wird von den in Aussicht genommenen Übermittlungsvorschriften verfehlt. Der Austausch der jeweils mit spezifischen Befugnisnormen gewonnenen Informationen führt dazu, daß das Trennungsgebot von einem Prinzip der Machthemmung zu einem Instrument möglichst effektiver Arbeitsteilung degeneriert. Der Entwurf verpflichtet nicht einmal den Datenempfänger, die übermittelten Daten nur für den Zweck zu verwenden, zu dem sie ihm übermittelt worden sind, und er läßt auch die Weiterübermittlung von Daten über mehrere Stationen zu, ohne daß es auf den Zweck der jeweiligen Übermittlungen ankäme. Würde der jetzige Entwurf Gesetz, bliebe es dabei, daß sich Nachrichtendienste und Polizeien des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes beim Informationsaustausch wie Abteilungen ein und derselben Behörde verhalten könnten.

Informationen, die im Rahmen von Telefonüberwachungsmaßnahmen gewonnen werden, sollen jetzt nur noch unter Einschränkungen an das BfV übermittelt und von diesem verwertet werden dürfen. Ergänzend müßte sichergestellt werden, daß die verfahrensrechtlichen Sicherungen sowie die Benachrichtigungspflicht nach der StPO nicht unterlaufen werden. Aber auch für Daten, die die Polizei bei Hausdurchsuchungen oder durch den Einsatz von V-Leuten, verdeckten Ermittlern oder technischen Geräten, durch polizeiliche Beobachtung oder längerfristige Observations gewonnen hat, müssen einschränkende Verwertungsregelungen geschaffen werden. Weiter ist klarzustellen, daß es nicht Aufgabe der Polizei sein kann, "Zufallsfunde" zu sammeln und weiterzugeben, die ihr bei Gelegenheit der Erfüllung ihrer Aufgaben bekannt werden, ohne für ihre eigentliche Aufgabenerfüllung erforderlich zu sein. Die Amtshilfe der Grenzpolizeien für den Verfassungsschutz muß einschränkend geregelt werden.

Dokumentation:

Drucksache 11/4306

Deutscher Bundestag — 11. Wahlperiode

Artikel 4

Gesetz über den Militärischen Abschirmdienst
(MAD-Gesetz — MADG —)

§ 1

Aufgaben

(1) Der Militärische Abschirmdienst des Bundesministers der Verteidigung nimmt zur Sicherung der Einsatzbereitschaft der Streitkräfte nach Maßgabe dieses Gesetzes Aufgaben wahr, die denen einer Verfassungsschutzbehörde entsprechen.

(2) Aufgabe des Militärischen Abschirmdienstes ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes,
2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht,

wenn sich diese Bestrebungen oder Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministers der Verteidigung richten und von Personen ausgehen oder ausgehen sollen, die diesem Geschäftsbereich angehören oder in ihm tätig sind.

(3) Darüber hinaus obliegt dem Militärischen Abschirmdienst zur Beurteilung der Sicherheitslage

1. von Dienststellen und Einrichtungen im Geschäftsbereich des Bundesministers der Verteidigung und
2. von Dienststellen und Einrichtungen der verbündeten Streitkräfte und der internationalen militärischen Hauptquartiere, wenn die Bundesrepublik Deutschland in internationalen Vereinbarungen Verpflichtungen zur Sicherheit dieser Dienststellen und Einrichtungen übernommen hat und die Beurteilung der Sicherheitslage im Einvernehmen zwischen dem Bundesminister der Verteidigung und den zuständigen obersten Landesbehörden dem Militärischen Abschirmdienst übertragen worden ist,

die Auswertung von Informationen über die in Absatz 2 Nummer 1 und 2 genannten Bestrebungen und Tätigkeiten gegen diese Dienststellen und Einrichtungen, auch soweit sie von Personen ausgehen oder ausgehen sollen, die nicht dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind.

(4) Der Militärische Abschirmdienst wirkt mit

1. bei der Überprüfung von Personen, die dem Geschäftsbereich des Bundesministers der Verteidigung angehören, in ihm tätig sind oder werden sollen und
 - a) denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können, oder

b) die an sicherheitsempfindlichen Stellen des Geschäftsbereichs des Bundesministers der Verteidigung eingesetzt sind oder werden sollen,

2. bei technischen Sicherheitsmaßnahmen im Geschäftsbereich des Bundesministers der Verteidigung zum Schutz von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnisnahme durch Unbefugte.

In die Überprüfung nach Nummer 1 können der Ehegatte, der Verlobte oder die Person, die mit dem zu Überprüfenden in eheähnlicher Gemeinschaft lebt, einbezogen werden, auch wenn bei ihnen die in Nummer 1 genannten Voraussetzungen nicht vorliegen. Der Militärische Abschirmdienst darf, soweit gesetzlich nichts anderes bestimmt ist, eine Überprüfung nach Nummer 1 nur mit Kenntnis des Betroffenen durchführen; wird der Ehegatte, Verlobte oder die Person, mit der der Betroffene in eheähnlicher Gemeinschaft lebt, in die Überprüfung miteinbezogen, ist auch deren Kenntnis erforderlich.

§ 2

Zuständigkeit in besonderen Fällen

(1) Zur Fortführung von Aufgaben nach § 1 Abs. 2 kann der Militärische Abschirmdienst, soweit es im Einzelfall zwingend erforderlich ist, Maßnahmen auf Personen erstrecken, die dem Geschäftsbereich des Bundesministers der Verteidigung nicht angehören oder nicht in ihm tätig sind. Dies ist nur zulässig

1. gegenüber dem Ehegatten oder Verlohten einer in § 1 Abs. 2 genannten Person oder dem mit ihr in eheähnlicher Gemeinschaft Lebenden, wenn angenommen werden muß, daß Bestrebungen oder Tätigkeiten nach § 1 Abs. 2 auch von ihm ausgehen,
2. im Benehmen mit der zuständigen Verfassungsschutzbehörde gegenüber Personen, bei denen tatsächliche Anhaltspunkte dafür bestehen, daß sie mit einer in § 1 Abs. 2 genannten Person bei Bestrebungen oder Tätigkeiten nach § 1 Abs. 2 zusammenarbeiten, und wenn anderenfalls die weitere Erforschung des Sachverhalts gefährdet oder nur mit übermäßigem Aufwand möglich wäre.

(2) Zur Abschirmung seiner Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten kann der Militärische Abschirmdienst in Wahrnehmung seiner Aufgaben nach § 1 Abs. 2, soweit es im Einzelfall zwingend erforderlich ist, im Benehmen mit der zuständigen Verfassungsschutzbehörde Maßnahmen auf Personen erstrecken, die dem Geschäftsbereich des Bundesministers der Verteidigung nicht angehören oder nicht in ihm tätig sind.

§ 3

**Zusammenarbeit
mit den Verfassungsschutzbehörden**

(1) Der Militärische Abschirmdienst und die Verfassungsschutzbehörden arbeiten bei der Erfüllung ihrer Aufgaben zusammen. Die Zusammenarbeit besteht auch in gegenseitiger Unterstützung und Hilfeleistung.

(2) Zur Fortführung von Aufgaben nach § 3 Abs. 1 des Bundesverfassungsschutzgesetzes kann eine Verfassungsschutzbehörde, soweit es im Einzelfall zwingend erforderlich ist, im Benehmen mit dem Militärischen Abschirmdienst Maßnahmen auf Personen erstrecken, die dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind und der Zuständigkeit des Militärischen Abschirmdienstes unterliegen. Dies ist nur zulässig gegenüber Personen, bei denen tatsächliche Anhaltspunkte dafür bestehen, daß sie mit einer Person aus dem Zuständigkeitsbereich der Verfassungsschutzbehörden bei Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 des Bundesverfassungsschutzgesetzes zusammenarbeiten, und wenn anderenfalls die weitere Erforschung des Sachverhalts gefährdet oder nur mit übermäßigem Aufwand möglich wäre.

(3) Der Militärische Abschirmdienst und das Bundesamt für Verfassungsschutz unterrichten einander über alle Angelegenheiten, deren Kenntnis für die Erfüllung ihrer Aufgaben erforderlich ist.

§ 4

Befugnisse des Militärischen Abschirmdienstes

(1) Der Militärische Abschirmdienst hat die dem Bundesamt für Verfassungsschutz zustehenden Befugnisse,

1. Informationen zu erheben, zu verarbeiten und zu nutzen nach § 6 des Bundesverfassungsschutzgesetzes, soweit es zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 und 4 sowie § 2 in Verbindung mit § 1 Abs. 2 erforderlich ist und soweit nicht die Nummern 2 und 3, die Absätze 2 bis 4 und § 5 die Erhebung und Übermittlung personenbezogener Informationen sowie die Verarbeitung und Nutzung personenbezogener Daten in Dateien besonders regeln,
2. personenbezogene Informationen mit nachrichtendienstlichen Mitteln zu erheben nach § 7 Abs. 1 des Bundesverfassungsschutzgesetzes, soweit es
 - a) zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 und § 2 Abs. 1 in Verbindung mit § 1 Abs. 2 sowie zur Erforschung der dazu erforderlichen Nachrichtenzugänge oder
 - b) zur Abschirmung der Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge des Militärischen Abschirmdienstes gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten, auch nach § 2 Abs. 2,

erforderlich ist; § 7 Abs. 2 des Bundesverfassungsschutzgesetzes findet Anwendung,

3. personenbezogene Daten nach § 8 des Bundesverfassungsschutzgesetzes in Dateien zu speichern, zu verändern und zu nutzen, soweit es zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 und 4 sowie § 2 in Verbindung mit § 1 Abs. 2 erforderlich ist,

4. personenbezogene Informationen zu verwenden sowie nach § 8 des Bundesverfassungsschutzgesetzes in Dateien zu speichern, zu verändern und zu nutzen, soweit dies zur Erfüllung seiner Aufgaben nach § 1 Abs. 3 erforderlich ist. Informationen über Personen, die nicht dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind, dürfen für andere Zwecke nicht verwendet werden, es sei denn, die Verwendung wäre auch für die Erfüllung der Aufgaben nach § 1 Abs. 2 zulässig.

(2) Der Militärische Abschirmdienst hat in Dateien gespeicherte personenbezogene Daten nach § 9 des Bundesverfassungsschutzgesetzes zu berichtigen, zu löschen oder zu sperren.

(3) Der Militärische Abschirmdienst hat für jede automatisierte Datei eine Dateianordnung nach § 10 des Bundesverfassungsschutzgesetzes zu treffen; die nach Absatz 1 dieser Vorschrift erforderliche Zustimmung erteilt der Bundesminister der Verteidigung. § 10 Abs. 2 des Bundesverfassungsschutzgesetzes ist anzuwenden.

(4) Der Militärische Abschirmdienst unterrichtet den Bundesminister der Verteidigung laufend und auf Anforderung über seine Tätigkeit. Hierbei ist auch die Übermittlung personenbezogener Informationen zulässig.

(5) Bei Anwendung der Vorschriften des Bundesverfassungsschutzgesetzes entsprechen den Aufgaben des Bundesamtes für Verfassungsschutz

1. nach § 3 Abs. 1 des Bundesverfassungsschutzgesetzes die Aufgabe des Militärischen Abschirmdienstes nach § 1 Abs. 2 und 3 dieses Gesetzes,
2. nach § 3 Abs. 2 des Bundesverfassungsschutzgesetzes die Aufgabe des Militärischen Abschirmdienstes nach § 1 Abs. 4 dieses Gesetzes.

§ 5

Übermittlung von Informationen

(1) Die Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts dürfen von sich aus dem Militärischen Abschirmdienst die ihnen bekanntgewordenen Informationen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 und 3 erforderlich ist.

(2) Der Militärische Abschirmdienst darf von jeder Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, die Übermittlung personenbezogener Informationen verlangen und amtlich geführte Register einsehen nach § 12 Abs. 2 des Bundesverfassungsschutzgesetzes, soweit es zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 bis 4 sowie § 2 in Verbindung mit § 1 Abs. 2 erforderlich ist.

Drucksache 11/4308

Deutscher Bundestag

(3) Der Militärische Abschirmdienst darf personenbezogene Informationen an Behörden und andere Stellen übermitteln nach § 14 Abs. 1 bis 3 des Bundesverfassungsschutzgesetzes, soweit es zur Erfüllung seiner Aufgaben oder für die in den Absätzen 1 und 3 dieser Vorschrift genannten Zwecke der Empfänger erforderlich ist. Die in Absatz 1 dieser Vorschrift genannten Behörden dürfen die übermittelten Informationen, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihnen übermittelt wurden.

(4) Der Militärische Abschirmdienst übermittelt den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien Informationen nach § 15 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1, 3 und 4 des Bundesverfassungsschutzgesetzes.

(5) Der Militärische Abschirmdienst übermittelt dem Bundesnachrichtendienst von sich aus Informationen nach § 15 Abs. 1 Satz 3 des Bundesverfassungsschutzgesetzes. Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben vom Militärischen Abschirmdienst die Übermittlung von Informationen nach § 15 Abs. 2 Satz 2 bis 4 des Bundesverfassungsschutzgesetzes verlangen.

§ 6

Verfahrensregeln für die Übermittlung von Informationen

Für die Übermittlung von Informationen nach § 5 dieses Gesetzes finden die §§ 19 bis 23 des Bundesverfassungsschutzgesetzes entsprechende Anwendung.

§ 7

Geltung des Verwaltungsverfahrensgesetzes und des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 1 Abs. 2 bis 4 sowie § 2 in Verbindung mit § 1 Abs. 2 durch den Militärischen Abschirmdienst finden die §§ 3 a und 3 c des Verwaltungsverfahrensgesetzes und die §§ 12 bis 16 und § 18 des Bundesdatenschutzgesetzes in der Fassung des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes keine Anwendung.

graswurzel revolution



antixistisch, gewaltfrei,
anarchistisch

GWR 125/Juni 88: Staatlichkeit und Anarchie heute/ Anti-Pornographie/ Fritz Oetter(1920): Gewalt oder Gewaltlosigkeit?/ Indische Frauen gegen Weltbankprojekte/Soziale Verteidigung als sozialrevolutionärer Ansatz/ Tieflflug/Gewaltfrei Bewegung im Islam

GWR 126/September 88: Kalberskandal und Vegetarismus/ Aikido/ Intitada/ Dreijahreskonferenz der War Resisters International in Finnland/ Gewaltfreie Revolution Teil I/Clara Wichmann(1922) über Verbrechen und Strafe/Gegen IWF und Weltbank

GWR 127/Oktober 88: Birma - die unbekannte Rebellion/ Herbstmanöverstörungen/ Gewaltfreie Revolution Teil II/Betreuung von Geschlechterrollen/ Platzbesetzung in Lahr/ Aktionen gegen Atomtests in USA/Landbesetzungen in Brasilien/ Anti-AKW-Bewegung in Indien/Willi Eichler (1926) über Rechte der Tiere

GWR 128/November 88: Antimilitaristische Kritik des "Sozialismus" in Jugoslawien/ Psychiatrie - Irrsinn und Autorität/Gustav Landauer und die deutsche Revolution 1918/Geschichte der WRI Teil I/Schwerpunkt Nahost/ Dokumentation der Arbeit des palästinensischen Zentrums für Gewaltfreiheit/Interview mit Mubarak Awad/ Gewaltfreie Bewegung im Libanon/FOGA-Aktionen in Linnich

GWR 129/Dezember 88: Polizei und Bürokratie/ Frauen gegen Gen- und Reproduktionstechnologie/ Kunstausstellung über Deserteure in Gelsenkirchen/ Streiks in Polen und Mythos Walesa/Demo gegen NATO in Hamburg/Gespräch mit israelischen Anarchisten über einen palästinensischen Staat/WRI-Geschichte Teil II

GWR, Schillerstr. 28, 69
Heidelberg (Abo:20DM)

Zu Artikel 4 (MAD-Gesetz)**1. Allgemeines**

- 1.1 Die Sicherung der Einsatzbereitschaft der Streitkräfte, der das Bundesverfassungsgericht in seiner Rechtsprechung Verfassungsrang zuerkennt, ist zur Verteidigung der Bundesrepublik Deutschland von entscheidender Bedeutung. Als Beitrag zur Sicherung dieser Einsatzbereitschaft hat der Bundesminister der Verteidigung aufgrund der ihm nach Artikel 65 a des Grundgesetzes (GG) zustehenden Organisationsgewalt 1956 den Militärischen Abschirmdienst (MAD) als Teil der Streitkräfte errichtet. Der MAD gliedert sich in das dem Bundesministerium der Verteidigung unmittelbar unterstellte Amt für den Militärischen Abschirmdienst (MAD-Amt) sowie die diesem nachgeordneten MAD-Gruppen auf der Ebene der Wehrbereiche und die MAD-Stellen auf der Ebene der Verteidigungsbezirke.

Die Tätigkeit des MAD unterliegt einer strengen parlamentarischen Kontrolle. Sie wird durch die parlamentarische Kontrollkommission nach dem Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes vom 11. April 1978 ausgeübt, ferner durch den Haushaltsausschuß des Deutschen Bundestages, durch das Gremium zur Genehmigung der Wirtschaftspläne der Nachrichtendienste nach § 10 a der Bundeshaushaltsordnung, durch das Gremium und die Kommission nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 GG) vom 13. August 1968 und durch den Verteidigungsausschuß des Deutschen Bundestages. Der MAD unterliegt auch der Kontrolle des Bundesrechnungshofes und des Bundesbeauftragten für den Datenschutz.

- 1.2 Auftrag und Befugnisse des MAD sind bisher gesetzlich nicht geregelt. Die Legitimation seiner Tätigkeit wurde vor dem Hintergrund des Verfassungsauftrages der Streitkräfte durch einen Katalog gesetzlicher Einzelregelungen als abgesichert angesehen, die sich auf ihn als Nachrichtendienst beziehen und ihn mit Rechten und Befugnissen ausstatten. Dabei handelt es sich im einzelnen um folgende Regelungen:

- der MAD ist berechtigt, dem Brief- und Postgeheimnis unterliegende Sendungen zu öffnen und einzusehen sowie den Fernschreibverkehr mitzulesen, den Fernmeldeverkehr abzuhören und auf Tonträger aufzunehmen (§ 1 Gesetz zu Artikel 10 GG);
- der MAD braucht Angaben über die von ihm gespeicherten personenbezogenen Daten nicht zu veröffentlichen (§ 12 Abs. 2 Nr. 1 Bundesdatenschutzgesetz — BDSG);
- der MAD erhält unbeschränkte Auskunft aus dem Zentralregister (§ 41 Abs. 1 Nr. 3 Bundeszentralregistergesetz);

- der MAD erhält zur Erfüllung seiner Aufgaben Daten aus dem Melderegister (§ 18 Abs. 3 Melderechtsrahmengesetz); ihm werden zu diesem Zweck auch personenbezogene Sozialdaten offenbart (§ 72 Sozialgesetzbuch Teil X).

Diese gesetzlichen Einzelregelungen reichen für eine rechtsstaatlich zweifelsfreie Aufgabenerfüllung des MAD nicht mehr aus. Die rechtspolitische Entwicklung im Bereich des allgemeinen Persönlichkeitsrechts, insbesondere unter dem Eindruck des Urteils des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz (E 65, 1 ff.), verlangt eine gesetzliche Grundlage für Eingriffe in das Persönlichkeitsrecht durch die Sammlung, Verarbeitung und Weitergabe personenbezogener Informationen sowie durch Anwendung nachrichtendienstlicher Mittel, wobei der dem einzelnen zustehende Persönlichkeitschutz gegenüber dem Allgemeininteresse abzuwägen ist. Der Entwurf eines Gesetzes über den Militärischen Abschirmdienst, mit dem dieser Forderung in der 10. Legislaturperiode des Deutschen Bundestages entsprochen werden sollte (BT-Drucksache 10/5342), ist nicht mehr verabschiedet worden.

- 1.3 Der vorliegende Gesetzentwurf greift die rechtspolitische Zielsetzung, eine gesetzliche Grundlage für Aufgaben und Befugnisse des MAD zu schaffen, wieder auf. Er enthält eine abschließende Aufgabenbeschreibung und gibt dem MAD zur Wahrnehmung seiner Aufgaben Befugnisse, die denen des Bundesamtes für Verfassungsschutz nach dem Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz — BVerfSchG) entsprechen. Dies geschieht gesetzestechnisch in der Weise, daß der Entwurf hinsichtlich der dem MAD zustehenden Befugnisse im wesentlichen auf das BVerfSchG verweist. Diese Verweisung ist Ausdruck der rechtlich einheitlichen Grundlagen des Verfassungsschutzes in der Bundesrepublik Deutschland. Da der MAD im Geschäftsbereich des Bundesministers der Verteidigung Aufgaben des Verfassungsschutzes anstelle des Bundesamtes für Verfassungsschutz wahrnimmt und damit Funktionsträger des Verfassungsschutzes ist, muß er auch über die gleichen Befugnisse verfügen, wie sie das Bundesamt für Verfassungsschutz besitzt. Dies soll die Verweisung verdeutlichen und sicherstellen. Nur bei gleichen Befugnissen ist auch die für einen wirksamen und erfolgreichen Verfassungsschutz unerlässliche Zusammenarbeit zwischen den Verfassungsschutzbehörden und dem MAD gewährleistet. Zugleich verdeutlicht die Verweisung auf die Befugnisse des BVerfSchG, daß der MAD ein von den Vollzugspolizeien abgegrenzter Organisationsbereich ist, dem für die Wahrnehmung der Verfassungsschutzaufgabe nicht die den Streitkräften durch das UZwGwB zugestandenen Sonderrechte, sondern lediglich die allen Verfassungsschutzbehörden eingeräumten

nachrichtendienstlichen Befugnisse zur Verfügung stehen. Schließlich vermeidet ein Verweisungsgesetz, daß sich die Befugnisse des MAD und der Verfassungsschutzbehörden auseinanderentwickeln, weil der MAD über die Verweisungen automatisch an den Novellierungen des BVerfSchG teilnimmt. Andererseits bringt das Verweisungssystem naturgemäß Schwierigkeiten für das Verständnis der Regelungen, insbesondere die Auslegung und die Anwendbarkeit des Gesetzes mit sich. Diese müssen jedoch nach Abwägung mit den vorgenannten Kriterien, die für das Verweisungssystem sprechen, als vertretbar angesehen und in Kauf genommen werden.

- 1.4 Die Gesetzgebungszuständigkeit des Bundes ergibt sich aus Artikel 73 Nr. 1 und 10 Buchstabe b GG.

Das Gesetz trifft Regelungen für den Verteidigungsbereich. Es gilt nicht im Land Berlin.

2. Im einzelnen

Zu § 1

Der MAD ist Teil der Streitkräfte. Sein Auftrag ist es, in Wahrnehmung von Aufgaben, die denen des Bundesamtes für Verfassungsschutz entsprechen, zur Sicherung der Einsatzbereitschaft der Streitkräfte beizutragen (Absatz 1). Nur ein militärischer Nachrichtendienst ist in der Lage, diesen Auftrag zu erfüllen. Obwohl bei der Aufstellung der Bundeswehr schon Nachrichtendienste des Bundes und der Länder bestanden, ergab sich aus der Eigenart des militärischen Dienstes und aus der Erkenntnis, daß die Bundeswehr ein Hauptangriffsziel gegenseitiger Nachrichtendienste werden würde, die Notwendigkeit, einen militärischen Abschirmdienst zu errichten. Insbesondere die eigenständigen organisatorischen Gliederungsformen der Bundeswehr, ihre Zugehörigkeit zum Nordatlantischen Bündnis und die damit verbundenen organisatorischen und personellen Verflechtungen einschließlich der besonderen Sicherheitenanforderungen integrierter Bereiche schaffen für die Erfüllung des nachrichtendienstlichen Auftrages Bedingungen, die von denen eines zivilen Nachrichtendienstes erheblich abweichen. So ist es unerlässlich, den MAD entsprechend der Dislozierung der Bundeswehr zu gliedern und damit bundesweit einzusetzen; er verfügt über das vor- und ausgebildete Personal, das mit den militärischen Verhältnissen der Bundeswehr und des Bündnisses vertraut ist. Zivile Verfassungsschutzbehörden wären nur bedingt in der Lage, Aufgaben eines militärischen Nachrichtendienstes zu erfüllen. Andererseits ist die Zuständigkeit des MAD auf den Bereich zu beschränken, in dem seine besondere Sachkunde wirksam wird; das ist der Geschäftsbereich des Bundesministers der Verteidigung, bestehend aus dem Bundesministerium der Verteidigung, den Streitkräften nach Artikel 87 a GG, der Bundeswehrverwaltung nach Artikel 87 b GG, den Truppendienstgerichten, dem Wehrdisziplinaranwalt und den Wehrdisziplinar-

anwälten im Rahmen des Artikels 96 Abs. 4 GG und den Dienststellen der Militärseelsorge. Zur Sicherung der Einsatzbereitschaft der Streitkräfte obliegen dem MAD für den Geschäftsbereich des Bundesministers der Verteidigung die Aufgaben, die andernfalls von den zivilen Verfassungsschutzbehörden wahrgenommen werden müßten.

Absatz 2 beschreibt in Anlehnung an den Wortlaut des § 3 Abs. 1 BVerfSchG Aufgaben, die der MAD entsprechend einer Verfassungsschutzbehörde im Geschäftsbereich des Bundesministers der Verteidigung zu erfüllen hat. Sie dienen der Sicherung der Einsatzbereitschaft der Streitkräfte (Absatz 1). Voraussetzung für ein Tätigwerden des MAD nach Absatz 2 ist,

- daß die verfassungsfeindlichen oder nachrichtendienstlichen Bestrebungen oder Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministers der Verteidigung gerichtet sind und
- daß diese Bestrebungen oder Tätigkeiten von Personen ausgehen oder ausgehen sollen, die diesem Geschäftsbereich angehören oder in ihm tätig sind.

Mit dieser Regelung wird vor allem von der (vermuteten) Täterseite her eine Abgrenzung der Zuständigkeit des MAD gegenüber den Verfassungsschutzbehörden vorgenommen. Der MAD darf nur dann eine Sachaufklärung betreiben, wenn der Geschäftsbereich des Bundesministers der Verteidigung sowohl vom personellen oder sachlichen Ziel als auch vom vermuteten Täterkreis her berührt ist.

Bei den zur Klärung eines Verdachtsfalles nach Absatz 2 unerlässlichen Maßnahmen fallen zwangsläufig personenbezogene Informationen auch über Personen an, die dem persönlichen Umfeld der Verdachtsperson zuzurechnen sind (Ehegatten, Verlobte, Lebensgefährten). Ohne Erhebung, Verarbeitung und sonstige Nutzung auch solcher Informationen ist die Erhaltung oder Entkräftung des Verdachts praktisch nicht möglich. Die Erhebung, Verarbeitung und sonstige Nutzung dieser Informationen ist daher untrennbarer Bestandteil der vom MAD nach Absatz 2 übertragenen Aufgaben.

Ergeben sich bei der Klärung eines Verdachtsfalles nach Absatz 2 Verdachtsmomente gegen eine Person im persönlichen Umfeld des Bundeswehrangehörigen, endet die Zuständigkeit des MAD zur Sachaufklärung, sofern diese Person nicht zu dem in Absatz 2 genannten Personenkreis gehört. In diesem Fall übernimmt die zuständige Verfassungsschutzbehörde die Sachaufklärung, es sei denn, § 2 findet Anwendung. Scheidet eine Person aus dem in Absatz 2 genannten Personenkreis aus, obliegt die weitere Aufklärung den dann jeweils zuständig werdenden Verfassungsschutzbehörden des Bundes und der Länder. Der MAD hat für die ordnungsgemäße Überleitung des Falles an die zuständige Verfassungsschutz-

behörde zu sorgen. Dies gilt im umgekehrten Fall auch für die Verfassungsschutzbehörden des Bundes und der Länder gegenüber dem MAD.

Personen gehören dem Geschäftsbereich des Bundesministers der Verteidigung an, wenn sie in einem öffentlich-rechtlichen oder privatrechtlichen Dienst- oder Arbeitsverhältnis zu der Bundesrepublik Deutschland stehen und aus den im Einzelplan 14 des Bundeshaushalts ausgebrachten Haushaltsmitteln bezahlt werden. Personen gehören dem Geschäftsbereich des Bundesministers der Verteidigung auch für die Dauer ihrer Beurlaubung, Entsendung, Kommandierung oder Abordnung an, sofern nicht im Einzelfall aufgrund einer gesonderten Regelung andere Sicherheitsstellen während dieser Zeit zuständig sind. Personen sind im Geschäftsbereich des Bundesministers der Verteidigung tätig, wenn sie dort, ohne ihm anzugehören, ständig oder überwiegend aufgrund anderer Rechtsverhältnisse Dienst- oder Werkleistungen erbringen. Hierunter fallen nicht Personen, die Leistungen aufgrund von Wartungs- oder Lieferungsverträgen erbringen.

Zu den Dienststellen zählen auch die Verbände und Einheiten, zu den Einrichtungen auch alle Liegenschaften des Geschäftsbereichs des Bundesministers der Verteidigung.

Absatz 3 überträgt in Nummer 1 dem MAD die Auswertung von Informationen zur Beurteilung der Sicherheitslage (Abschirmlage) von Dienststellen und Einrichtungen im Geschäftsbereich des Bundesministers der Verteidigung. Wegen der Begrenzung der Aufgaben des MAD auf Personen, die dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind, wird dem MAD diese Aufgabe eigens übertragen. Zur Erfüllung dieser Aufgabe muß er nämlich Informationen über Bestrebungen und Tätigkeiten nach Absatz 2 Nr. 1 und 2 auch anderer als der in Absatz 2 und 4 genannten Personen auswerten dürfen. Mit Absatz 3 Nr. 1 wird auch der Überlegung Rechnung getragen, daß sicherheitsgefährdende Aktionen gegen eine Dienststelle oder Einrichtung im Geschäftsbereich des Bundesministers der Verteidigung in ihren Auswirkungen nicht ohne genaue Kenntnis der jeweiligen Situation in dieser Dienststelle oder Einrichtung beurteilt werden können. Absatz 3 Nr. 2 sieht darüber hinaus die Möglichkeit vor, unter den dort genannten Voraussetzungen dem MAD mit der Auswertung von Informationen zur Beurteilung der Sicherheitslage von Dienststellen und Einrichtungen verbündeter Streitkräfte und internationaler Hauptquartiere im Geltungsbereich dieses Gesetzes im Rahmen der gemeinsamen Verteidigung zu beauftragen.

Die Befugnisse zur Erfüllung der Aufgaben nach Absatz 3 ergeben sich aus § 4 Abs. 1 Nr. 4 sowie § 5 Abs. 2 und 3.

Absatz 4 Satz 1 entspricht § 3 Abs. 2 BVerfSchG. Die Mitwirkung des MAD nach Nummer 1 bei der Sicherheitsüberprüfung betrifft Personen,

die dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind, Bewerber für Dienst- und Arbeitsverhältnisse, für die Mobilmachung beorderte Reservisten und Personen, mit denen Vereinbarungen über Dienst- oder Werkleistungen getroffen werden sollen. Die Mitwirkung des MAD nach Nummer 2 berücksichtigt, daß insbesondere die Tätigkeit des MAD nach § 1 Abs. 2 und 3 wertvolle Erkenntnisse für technische Absicherungsmaßnahmen bringt.

Nach Absatz 4 Satz 2 können die Überprüfungsmaßnahmen auf den Ehegatten, Verlobten oder den Lebensgefährten ausgedehnt werden; die grundsätzliche Einbeziehung dieses Personenkreises in die Überprüfung der in Satz 1 Nr. 1 genannten Personen ist für eine effektive Sicherheitsüberprüfung nach aller Lebenserfahrung unerlässlich. Ehegatte, Verlobter oder in eheähnlicher Gemeinschaft Lebender können daher auch dann in die Überprüfung einbezogen werden, wenn die in Satz 1 Nr. 1 genannten Voraussetzungen bei ihnen nicht vorliegen. Satz 3 ist entsprechend der Regelung des § 3 Abs. 2 Satz 2 BVerfSchG ein Vorgriff auf ein künftiges Geheimsetzungsgesetz. Auch der MAD darf grundsätzlich Sicherheitsüberprüfungen nur mit Kenntnis des Betroffenen – einschließlich der in die Überprüfung einbezogenen Person – durchführen.

Zu § 2

Die Begrenzung der Aufgaben des MAD durch § 1 kann im Einzelfall dazu führen, daß er bei Abklärung des persönlichen Umfeldes eines Angehörigen des Geschäftsbereichs des Bundesministers der Verteidigung, der im Verdacht geheimesdienstlicher Tätigkeit für eine fremde Macht steht, auf einen weiteren Verdächtigen stößt, für den er nach § 1 Abs. 2 nicht zuständig ist (z. B. ein möglicher Mittelsmann des gegnerischen Nachrichtendienstes mit Wohnsitz in der Bundesrepublik Deutschland). Absatz 1 verleiht dem MAD unter den dort genannten strengen Voraussetzungen die Befugnis, notwendige Maßnahmen auf den dort genannten Personenkreis zu erstrecken. Die Zuständigkeit der Verfassungsschutzbehörden des Bundes und der Länder bleibt für diese Personen im übrigen unberührt. Die Maßnahmen des MAD gegenüber den in Nummer 2 genannten Personen sind im Benehmen mit der jeweils zuständigen Verfassungsschutzbehörde vorzunehmen; dies entfällt bei dem Ehegatten, Verlobten oder Lebensgefährten der dem Geschäftsbereich des Bundesministers der Verteidigung angehörenden oder in ihm tätigen Verdachtspersonen (Nummer 1), da in diesen Fällen regelmäßig von einer „Täterinheit“ auszugehen ist.

Absatz 2 erweitert die Zuständigkeit des MAD für die Abschirmung seiner Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge auch auf die Personen, die nicht dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind. Die entspre-

Drucksache 11/4306

Deutscher Bundestag — 11. Wahlperiode

chende Befugnisnorm ist § 4 Abs. 1 Nr. 2 (Buchstabe b).

Zu § 3

Absatz 1 verpflichtet den MAD und die Verfassungsschutzbehörden zur Zusammenarbeit und stellt besonders die Notwendigkeit gegenseitiger Unterstützung und Hilfeleistung heraus.

Absatz 2 gewährleistet den Verfassungsschutzbehörden die Gegenseitigkeit bei erweiterter personeller Zuständigkeit, wie sie dem MAD durch die Regelung des § 2 eingeräumt ist.

Absatz 3 ist Grundlage der informationellen Zusammenarbeit zwischen dem MAD und dem Bundesamt für Verfassungsschutz. Er entspricht § 4 Abs. 1 BVerfSchG; damit sind für die informationelle Zusammenarbeit zwischen dem MAD und dem Bundesamt für Verfassungsschutz die gleichen Grundsätze maßgebend, wie sie für das Verhältnis zwischen dem Bundesamt für Verfassungsschutz und den Verfassungsschutzbehörden der Länder gelten. Gleich den anderen Verfassungsschutzbehörden hat daher auch der MAD beim Informationsaustausch insbesondere den Grundsatz der Verhältnismäßigkeit zu beachten. So hat er z. B. die Erforderlichkeit der jeweiligen Übermittlung zu prüfen und ihm von den Verfassungsschutzbehörden übermittelte Informationen, die er nicht benötigt, zu vernichten oder zu löschen.

Die in Absatz 3 vorgesehene Regelung ist sachnotwendig. Das Bundesamt für Verfassungsschutz könnte seine Zentralstellenfunktion nach Artikel 87 Abs. 1 Satz 2 GG nur unvollkommen wahrnehmen, wenn der besonders sicherheitsempfindliche Geschäftsbereich des Bundesministers der Verteidigung nicht in die zentrale Auswertung eingebunden wäre. Durch die zentrale Auswertung wird sichergestellt, daß die von Verfassungsschutzbehörden und dem MAD gewonnenen Erkenntnisse beiden Bereichen grundsätzlich für die Bearbeitung von Einzelfällen zur Verfügung stehen.

Dabei ist zu bedenken, daß für die Abwehr sicherheitsgefährdender Angriffe auf den Geschäftsbereich des Bundesministers der Verteidigung in Zweifelsfällen zunächst sowohl der MAD als auch die Verfassungsschutzbehörden zuständig sind und erst nach Klärung der Ressortzugehörigkeit der Verdachtsperson die Zuständigkeit des Bundesamtes für Verfassungsschutz oder des MAD feststeht.

Zu § 4

Die Bestimmung legt die Befugnisse des MAD zur Erfüllung seiner Aufgaben sowie damit verbundene Verpflichtungen unter anderem durch Verweisung auf jene Befugnisse und Verpflichtungen fest, die das BVerfSchG dem Bundesamt für Verfassungsschutz gibt und auferlegt. Sinn dieser Regelung ist es, dem MAD jeweils für die vergleichbare Aufgabe auch die gleichen Befugnisse zur Erfüllung seines Auftrages zu geben, wie sie das Bundesamt für Verfassungsschutz

nach den jeweiligen Vorschriften des BVerfSchG hat.

Absatz 1 Nr. 1 ist für den MAD nach § 6 BVerfSchG für die Aufgaben nach § 1 Abs. 2 und 4 sowie § 2 in Verbindung mit § 1 Abs. 2 die Rechtsgrundlage, um unter Beachtung des Grundsatzes der Verhältnismäßigkeit Informationen erheben, verarbeiten und nutzen sowie nachrichtendienstliche Mittel anwenden zu können, soweit sich aus den Nummern 2 und 3, den Absätzen 2 bis 4 sowie aus § 5 nichts anderes ergibt. Polizeiliche Befugnisse oder Weisungsbefugnisse stehen auch dem MAD nicht zu.

Nach Absatz 1 Nr. 2 darf der MAD unter den in § 7 Abs. 1 BVerfSchG genannten Voraussetzungen personenbezogene Informationen mit nachrichtendienstlichen Mitteln erheben. Er hat dieses Befugnis zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 und § 2 in Verbindung mit § 1 Abs. 1 (Buchstabe a) sowie entsprechend § 7 Abs. 1 Nr. 2 BVerfSchG zur Eigensicherung gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten (Buchstabe b).

Der Verweis auf § 7 Abs. 2 BVerfSchG stellt sicher, daß auch der MAD die G 10-Kommission unter den dort genannten Voraussetzungen unterrichtet.

Absatz 1 Nr. 3 enthält die Befugnis des MAD, personenbezogene Informationen unter den in § 8 Abs. 1 BVerfSchG genannten Voraussetzungen in Dateien zu speichern, zu verändern und zu nutzen. Absatz 1 Nr. 4 Satz 1 enthält die für die Erfüllung der Aufgabe nach § 1 Abs. 3 notwendige Befugnisnorm. Hier handelt es sich in der Regel um eine Zeitspeicherung mit kurzen Lösungsfristen. Diese Aufgabe des MAD macht es im übrigen erforderlich, ihm — über die Regelung des § 8 Abs. 1 BVerfSchG hinaus — auch die Verwendung solcher Informationen zu ermöglichen, die nicht in Dateien gespeichert sind. Satz 2 trägt dem Zweckbindungsgrundsatz für die Verwendung personenbezogener Informationen Rechnung.

Auch der MAD darf Daten über ein Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres nicht in Dateien speichern. Personenbezogene Daten Minderjähriger, die das 16. Lebensjahr vollendet haben, sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, daß nach Eintritt der Volljährigkeit weitere Erkenntnisse im Sinne von § 1 Abs. 2 angefallen sind.

Die Speicherdauer ist in jedem der hier genannten Fälle auf das für die Aufgabenerfüllung des MAD erforderliche Maß zu beschränken.

Absatz 2, der auf § 9 BVerfSchG verweist, verpflichtet den MAD, die besonderen Schutzvorschriften für die Speicherung personenbezogener Daten in Dateien einzuhalten.

Absatz 3 legt dem MAD durch die Verweisung auf § 10 BVerfSchG die Verpflichtung auf, für

jede automatisierte Datei in einer Dateianordnung folgendes festzulegen:

Bezeichnung der Datei, Zweck der Datei, Voraussetzungen der Speicherung, Übermittlung und Nutzung (betroffener Personenkreis, Art der Daten), Anlieferung oder Eingabe, Zugangsbechtigung, Überprüfungsfristen, Speicherdauer sowie Protokollierung des Abrufs. Die Dateianordnung bedarf der Zustimmung des Bundesministers der Verteidigung. Der Bundesbeauftragte für den Datenschutz ist vor Erlaß einer Dateianordnung anzuhören.

Absatz 4 Satz 1 begründet für den MAD eine gesetzliche Berichtspflicht gegenüber dem Bundesminister der Verteidigung über seine Tätigkeit. Sie läßt die ohnehin bestehende Meldepflicht aufgrund der truppendienstlichen Unterstellung unberührt. Gegenüber der Unterrichtungspflicht des Bundesamtes für Verfassungsschutz nach § 11 BVerfSchG ist wegen der Beschränkung des MAD auf den Geschäftsbereich des Bundesministers der Verteidigung eine unmittelbare Berichtspflicht gegenüber anderen Mitgliedern der Bundesregierung nicht vorgesehen und auch nicht erforderlich, da eine entsprechende Unterrichtung durch den Bundesminister der Verteidigung sichergestellt ist.

Absatz 4 Satz 2 gewährleistet, daß der Bundesminister der Verteidigung über den gleichen Informationsstand wie der MAD verfügt; dazu gehört, daß der Bundesminister der Verteidigung auch Kenntnis über personenbezogene Informationen erhält.

Bei der Verweiskonzeption des Gesetzes dient Absatz 5 zusätzlich dem Erfordernis der Normenklarheit. Er erleichtert die Anwendung der Vorschriften des BVerfSchG, indem er die gesetzlichen Aufgabenbeschreibungen beider Nachrichtendienste einander gegenüberstellt. Die Vorschrift hat zusätzlich Bedeutung, wenn Strafverfolgungs- und Sicherheitsbehörden Informationen an den MAD nach § 18 in Verbindung mit § 13 Abs. 1 und 2 BVerfSchG übermitteln. Insoweit stellt Absatz 5 Nr. 1 sicher, daß der MAD Informationen auch für die Beurteilung der Sicherheitslage (§ 1 Abs. 3) erhält.

Zu § 5

Die Vorschrift enthält Regelungen zur Übermittlung von Informationen an den MAD und durch den MAD. Die Weitergabe von Informationen durch den MAD an die Verfassungsschutzbehörden der Länder regelt § 16 Abs. 2 in Verbindung mit § 13 Abs. 1 und 2 BVerfSchG. Die Verfassungsschutzbehörden der Länder übermitteln dem MAD Informationen nach Maßgabe des § 17 Abs. 2 BVerfSchG. Absatz 1 entspricht § 12 Abs. 1 BVerfSchG.

Absatz 2 entspricht § 12 Abs. 2 BVerfSchG. Auch der MAD hat insbesondere das Recht, amtliche Register einzusehen. Von dieser Befugnis wird er Gebrauch machen, wenn die benötigte Information nicht durch einen Registerauszug übermit-

telt werden kann, z. B. bei Bild- oder Schriftvergleichen im Rahmen von Identitätsprüfungen. Eine Registereinsicht ist darüber hinaus im Interesse der betroffenen Personen angezeigt, wenn verhindert werden soll, daß sie als Verdachtsperson bekannt wird oder wenn die benötigte Information andernfalls nur durch einen stärkeren Grundrechtseingriff – beispielsweise durch Anwendung nachrichtendienstlicher Mittel – gewonnen werden könnte.

Absatz 3 entspricht § 14 Abs. 1 bis 3 BVerfSchG. Die Übermittlungsbefugnis nach § 14 Abs. 4 BVerfSchG hat für den MAD keine Bedeutung. Die Vorschrift unterscheidet zwischen Behörden im Sinne des § 14 Abs. 1 BVerfSchG und anderen Stellen im Sinne des § 14 Abs. 2 und 3 BVerfSchG. Nur den Behörden kann gesetzlich zur Auflage gemacht werden, die übermittelten Informationen nur zu dem Zweck zu verwenden, zu dem sie ihnen übermittelt wurden.

Absatz 4 entspricht § 15 Abs. 1 und 2 BVerfSchG. Er regelt die Weitergabe von Informationen durch den MAD an die Strafverfolgungsbehörden und die Polizeien. Den umgekehrten Fall – Übermittlung von Informationen durch die Strafverfolgungsbehörden und die Polizeien an den MAD – regelt § 18 BVerfSchG in Verbindung mit § 13 BVerfSchG.

Absatz 5 stellt den Informationsfluß zwischen dem MAD und dem Bundesnachrichtendienst sicher. Der Bundesnachrichtendienst übermittelt dem MAD Informationen auf der Grundlage des § 5 Abs. 3 Satz 2 BNDG in Verbindung mit § 15 BVerfSchG.

Zu § 6

Bei der Übermittlung von Informationen nach § 5 hat der MAD infolge der Verweisung auf die einschlägigen Bestimmungen des BVerfSchG die Übermittlungsverbote des § 19 BVerfSchG, den Minderjährigenschutz des § 20 BVerfSchG, die Nachberichtsspflicht des § 22 BVerfSchG sowie die Möglichkeit des on-line-Zugriffs auf Dateien zwischen den Nachrichtendiensten einerseits sowie den Polizeien und Staatsanwaltschaften andererseits unter den Voraussetzungen des § 23 BVerfSchG zu beachten.

Zu § 7

Die Vorschrift stellt entsprechend § 24 BVerfSchG klar, daß der Entwurf eine Reihe von Spezialvorschriften über den Umgang mit Informationen für den Militärischen Abschirmdienst enthält, die den korrespondierenden Normen des Verwaltungsverfahrensgesetzes und des Bundesdatenschutzgesetzes vorgehen. Dies gilt jedoch nur, soweit der Militärische Abschirmdienst in Erledigung der Aufgaben nach den §§ 1 und 2 tätig wird; bei anderen Tätigkeiten, z. B. im Rahmen der Personalverwaltung des eigenen Personals, gelten alle in Frage kommenden Vorschriften der genannten „Querschnittsgesetze“ des Bundes.

Stellungnahme zum MAD-Gesetz-Entwurf vom 6.4.1989**1. Generelle Anmerkungen**

Der MAD entstand 1956 nach Gründung der Bundeswehr durch einen Organisationsakt des Bundesverteidigungsministers, dem dieser Geheimdienst unterstellt ist. Im Zuge dieses Organisationsaktes wurden das "Amt für die Sicherheit der Bundeswehr" (ASBw) und sechs regionale Untergliederungen des MAD in den Wehrbereichen geschaffen. Das ASBw wurde 1984 nach dem Wörner-/Kießling-Skandal in MAD-Amt umbenannt. Der militärische Geheimdienst der Bundesrepublik verfügt über ein Personal von ungefähr 2.000 Bediensteten.

Legitimiert wird die Tätigkeit des MAD mit der Notwendigkeit, die "Funktionsfähigkeit der Streitkräfte" zu sichern. Ein Auftrag, dem das Bundesverfassungsgericht in mehreren Urteilen Verfassungsrang verliehen hat (BVerfGE, 28, 243 ff.; 48, 127 ff.).

Gestützt auf diesen Auftrag entfaltete der MAD im Laufe der Jahre eine exzessive geheimdienstliche Tätigkeit. Unter Sicherheit der Bundeswehr wurde vom MAD mehr verstanden als nur die Überprüfung der Loyalität der Soldaten. Die Beobachtung "extremistischer Bestrebungen", der Aufgabe des VfS, die dem MAD im Bereich der Bundeswehr obliegt, führte diesen Geheimdienst schnell aus dem Bereich der Bundeswehr heraus. Beobachtet wurden nicht nur die wenigen Versuche insbesondere der K-Gruppen, Soldaten politisch zu organisieren. Der MAD richtete sein Augenmerk auch regelmäßig auf Aufrufe und Aktionen, die sich von außerhalb des Militärs an Soldaten wendeten - so im Falle der Friedensbewegung. Deshalb war es kein Zufall, daß sich in der inzwischen aufgelösten, etwa 50.000 Personen umfassenden "Zersetzerdatei" des MAD so prominente Friedensbewegte wie Walter Jens, Luise Rinser oder Helga Schuchardt fanden.

In dem Bestreben, der "Zersetzung der Wehr- und Verteidigungsbereitschaft" entgegenzuwirken, trat der MAD dabei auch in Konkurrenz zum VfS. Das bekannteste Beispiel ist die Demonstration gegen das Bremer Bundeswehrgelöbnis am 6. Mai 1980, bei deren Vorbereitung V-Leute von MAD, VfS und polizeilichem Staatsschutz miteinander "Bündnisverhandlungen" als Juso-, KBW- etc. Vertreter führten (vgl. CILIP 17, S.70 ff.).

Der Bremer Fall mag durchaus in seinen Folgen außergewöhnlich sein, Konkurrenzen dieser Art sind aber angesichts der Tatsache, daß in der BRD drei Geheimdienste und ein wichtiger Zweig der Polizei, nämlich der Staatsschutz, auf ähnlichem Gebiet arbeiten, fast unausweichlich. Dies gilt umso mehr für das Verhältnis von MAD und VfS, die - wenn auch auf unterschiedlichem Gebiet, hier im Zivilbereich, dort im militärischen - dieselbe Aufgabenstellung haben: die "Beobachtung extremistischer Bestrebungen und sicherheitsgefährdender und geheimdienstlicher Tätigkeiten".

Zu den Aufgaben des MAD zählt auch die Mitwirkung bei der Sicherheitsüberprüfung der Bundeswehrbediensteten - samt ehelichem oder auch nicht-ehelichem Anhang. Jährlich werden vom MAD etwa 200.000

Sicherheitsüberprüfungen durchgeführt. Auch in dieser Frage unterscheiden sich in erster Linie die Bereiche, in denen die Geheimdienste arbeiten, nicht die grundsätzlichen Aufgabenstellungen.

Im Unterschied zum VfS gibt es für den MAD bisher keine gesetzliche Grundlage, sondern nur Dienstanweisungen. Zu einer gesetzlichen Festlegung kam es auch nach dem Kießling/Wörner-Untersuchungsausschuß des Bundestages 1984 nicht. Der Entwurf für ein MAD-Gesetz 1985/86 blieb wie die anderen Geheimdienstgesetze zunächst liegen. Im Kern dient der Entw. nur dazu, die Arbeitsbereiche und Zuständigkeiten von VfS und MAD besser abzugrenzen, damit Kollisionen wie in Bremen 1980 sich möglichst nicht wiederholen.

2. Detailkommentierung

Zu § 1:

Aufgaben als Verfassungsschutzbehörde

Die Aufgaben des MAD werden mit denen des VfS parallelisiert. In Abs.1 heißt es deswegen: "Der militärische Abschirmdienst ... nimmt ... Aufgaben wahr, die denen einer Verfassungsschutzbehörde entsprechen." In den einzelnen Absätzen dieser Norm erhält er demgemäß dieselben Aufgaben, die auch in § 3 BVerfSchG genannt sind:

- Extremismus-Beobachtung (Abs.2 Nr.1),
- Spionageabwehr (Abs.2 Nr.2),
- Mitwirkung bei Sicherheitsüberprüfungen (Abs.4 Nr.1),
- Mitwirkung beim technischen Geheimschutz (Abs.4 Nr.2).

Diese Aufgaben soll er jeweils innerhalb des militärischen Bereichs ausführen. Seine Arbeit richtet sich einerseits gegen Personen aus diesem Bereich und andererseits gegen Personen, die "extremistische Bestrebungen" oder "sicherheitsgefährdende Tätigkeiten" gegen die Bundeswehr oder militärische Einrichtungen der Stationierungsstreitkräfte und der NATO auf bundesdeutschem Boden unternehmen.

Während die genannten Regelungen sich also noch weitgehend auf den militärischen Bereich beziehen, gibt der Abs.3 ihm eine weit darüber hinaus reichende Vollmacht: die "Beurteilung der Sicherheitslage" der genannten militärischen Institutionen. Zur Erfüllung dieser Aufgabe müßte der MAD auf alle möglichen Informationen und Personen zurückgreifen. Diese Aufgabenstellung ist damit völlig uferlos (vgl. § 4 Abs.1 Nr.4).

Zu § 2:

"Verfassungsschützerischer" Zugriff des MAD auf Personen außerhalb des militärischen Bereichs

Im Rahmen der "Extremismusbeobachtung" und der Spionageabwehr im militärischen Bereich darf der MAD seine Recherchen auch auf Personen außerhalb dieses Bereichs erstrecken:

- auf die Ehegatten oder Lebensgefährten der Beobachteten (Abs.1 Nr.1),
 - auf andere Personen, die möglicherweise mit denen zusammenarbeiten, von denen "extremistische Bestrebungen" und "sicherheitsgefährdende Tätigkeiten" gegen den militärischen Bereich ausgehen (Abs.1 Nr.2) sowie
 - auf weitere Personen zum Schutz seiner "Nachrichtenzugänge", Mitarbeiter etc. (Abs.2).
- Außer im erstgenannten Fall muß er sich mit dem VfS ins Benehmen setzen.

Zu § 3: Zusammenarbeit mit dem VfS

Abs.1 und 3 verpflichten MAD und VfS zur Zusammenarbeit und gegenseitigen Unterrichtung. Die Abs. gebrauchen nahezu die gleichen Formulierungen, die das BVerfSchG für die Zusammenarbeitspflicht und die gegenseitige Unterrichtung der Länderämter- und des BfV (§§ 1 und 4 Abs.1) benutzt.

Abs.2 gibt den VfS-Ämtern die gleichen Befugnisse, ihre Aufgaben auf den militärischen Bereich auszustrecken wie dies dem MAD in § 2 Abs.2 gewährt wird.

Zu den §§ 4, 5 und 6: Befugnisse

Auch die Befugnisse des MAD sind weitestgehend mit denen des BfV identisch. Die entsprechenden Regelungen verweisen deshalb auf die §§ des BVerfSchG. Es sind dies in § 4:

- **Abs.1:** Erhebung von Daten auch durch nachrichtendienstliche Mittel, Speicherung, Verarbeitung und Nutzung von Daten,
- **Abs.2:** die Pflicht zur Berichtigung falscher Daten bzw. zu ihrer Löschung und Sperrung,
- **Abs.3:** die Pflicht, Dateianordnungen aufzustellen,
- **Abs.4:** die Berichtspflicht gegenüber dem Dienstherrn, dem BMVg,
- **in den §§ 5 und 6:** die Pflichten zur Übermittlung von Informationen, wie sie in derselben Form auch der VfS hat.

Zur Erfüllung der Aufgaben einer VfS-Behörde im militärischen Bereich stehen dem MAD alle Befugnisse der Datenverarbeitung zu: von der Erhebung bis zur Übermittlung.

Nur für die Beurteilung der Sicherheitslage des Militärs werden Beschränkungen formuliert: Eine eigenständige Befugnis zur Datenerhebung kommt dem MAD für diese Aufgabenstellung nicht zu. Die Informationen, die er zur Beurteilung der Sicherheitslage braucht, muß er deshalb vom VfS und vom BND beziehen. M.a.W.: der MAD darf zur "Beurteilung der Sicherheitslage" alle möglichen Informationen des VfS sowie

des BND und der Strafverfolgungsbehörden nutzen. Er darf in diesem Bereich aber nicht selbst erheben oder gar nachrichtendienstliche Mittel einsetzen. Mit dieser Abgrenzung wird also das Maß der dem MAD zugänglichen Informationen keineswegs beschränkt. Gespeichert, genutzt, verarbeitet und übermittelt werden dürfen Daten auch hier - es geht nur um eine funktionale Abgrenzung zum VfS und BND.

**Zu § 7:
"Geltung" des BDSG und Verwal-
tungsverfahrensgesetzes**

Auch hier wir zum BVerfSchG (vgl. § 24) "parallelisiert", d.h. die datenschutzrechtlichen Regelungen dieser Gesetze werden für den MAD suspendiert.

Literatur zum MAD:

Gusy, Christoph, Der Militärische Abschirmdienst, in: Die öffentliche Verwaltung, Heft 2/1983, S. 60 ff.
Kloss, Herbert, MAD - der militärische Abschirmdienst der Bundeswehr, in: Beiträge zur Konfliktforschung 1/1987, S. 99 ff.
Diskussion und Feststellungen des **Dt. Bundestages** in Sachen Kießling. Zur Sache - Themen parlamentarischer Beratung, 2/1984

**Aus dem 11. Tätigkeitsbericht
des Bundesbeauftragten für den
Datenschutz zum 1.1.1989**

21.1.2 Datenschutzrechtliche Kontrolle beim MAD

Ich habe 1988 die im Abwehrbereich „Verfassungsfeindliche Kräfte“ (VfK) in einem bestimmten Zeitraum angelegten Ermittlungsvorgänge überprüft und statistisch ausgewertet. Dabei stellte sich heraus, daß am Beginn der Ermittlungen in ca. vier Fünfteln der Fälle keine konkret unmittelbar gegen die Bundeswehr gerichteten extremistischen Handlungen vorlagen. Ausgangspunkt der Bearbeitung waren vielmehr in fast jedem zweiten Fall Informationen, die im Rahmen einer Sicherheitsüberprüfung angefallen, im übrigen in der Regel Informationen, die dem MAD von anderen Sicherheitsbehörden übermittelt worden waren. Zumeist handelt es sich dabei um Hinweise auf eine extremistische Betätigung von Bundeswehrangehörigen.

Die Ermittlungen des MAD haben in fast jedem zweiten aller Fälle ergeben, daß der Verdacht extremistischer Bestrebungen widerlegt bzw. ausgeräumt werden konnte. In etwa einem Viertel der Fälle ist es letztlich offengeblieben, ob der Verdacht zutrifft oder nicht. Lediglich im verbleibenden Viertel ergaben die Recherchen, daß sich die Person in einer extremistischen Organisation betätigte. Diese Betätigung hatte aber nur in seltenen Fällen etwas mit der Bundeswehr zu tun. Zum großen Teil handelte es sich um die Mitgliedschaft in einer Organisation, deren Tätigkeit gegen die freiheitlich demokratische Grundordnung gerichtet und die von den Verfassungsschutzbehörden als Beobachtungsobjekt eingestuft ist. Im Ergebnis fehlte es bei der weit überwiegenden Zahl der von mir insgesamt ausgewerteten Fälle objektiv an der Voraussetzung einer „unmittelbar gegen die Bundeswehr gerichteten Bestrebung“. Gleichwohl war stets, wenn im Ermittlungszusammenhang auch gegen eine der Wehrüberwachung unterliegende Person ermittelt wurde, eine Speicherung in der Personenzentraldatei des MAD veranlaßt worden. Bei Bestätigung des Verdachts einer extremistischen Betätigung, auch wenn diese sich nicht unmittelbar gegen die Bundeswehr richtete, wurde eine fünfjährige Speicherung verfügt, bei Ausräumung des Verdachts sogar zehn Jahre, was besonders unverhältnismäßig erscheint.

Ich habe den Bundesminister der Verteidigung aufgefordert, diese Regelungen zu überprüfen. Auch wenn man akzeptiert, daß der MAD als Nachrichtendienst bereits beim Verdacht, daß eine unmittelbar gegen die Bundeswehr gerichtete extremistische Bestrebung vorliegen könnte, tätig wird, so dürfen seine Ermittlungen jedenfalls dann, wenn sie die Unzuständigkeit des MAD ergeben haben, nicht zu einer mehrjährigen Speicherung in den Dateien des MAD führen. Ich habe vorgeschlagen, statt dessen die (ursprünglich) meldende Stelle davon zu unterrichten, daß der Verdacht entkräftet wurde. Im übrigen halte ich eine Speicherung derartiger Fälle höchstens nur bis zum Ende der aktiven Bundeswehrzeit des Betroffenen für zulässig. Der Bundesminister der Verteidigung hat angekündigt, daß er die entsprechenden innerdienstlichen Vorschriften ändern und mich dabei beteiligen will.

Dokumentation:

Deutscher Bundestag — 11. Wahlperiode

Drucksache 11/4306

Artikel 5

**Gesetz über den Bundesnachrichtendienst
(BND-Gesetz — BNDG —)**

§ 1

Aufgaben und Befugnisse**(1) Der Bundesnachrichtendienst darf**

1. für die Sammlung und Auswertung von Informationen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, zur Unterrichtung der Bundesregierung,
2. zur Abschirmung seiner Mitarbeiter, Einrichtungen, Gegenstände und Nachrichtenzugänge gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten und
3. für die Sicherheitsüberprüfung von Personen, die für ihn tätig sind oder tätig werden sollen,

die erforderlichen Informationen erheben, verarbeiten und nutzen sowie nachrichtendienstliche Mittel anwenden, soweit nicht die §§ 2 bis 5 und § 8 die Erhebung und Übermittlung personenbezogener Informationen sowie die Verarbeitung und Nutzung personenbezogener Daten in Dateien besonders regeln. Die nachrichtendienstlichen Mittel sind in einer Dienstvorschrift zu benennen. Bei der Sicherheitsüberprüfung nach Satz 1 Nr. 3 ist § 3 Abs. 2 Satz 2 des Bundesverfassungsschutzgesetzes entsprechend anzuwenden.

(2) Auf innenpolitischem Gebiet wird der Bundesnachrichtendienst nicht tätig.

(3) Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesnachrichtendienst nicht zu. Er darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen er selbst nicht befugt ist.

(4) Von mehreren geeigneten Maßnahmen hat der Bundesnachrichtendienst diejenige zu wählen, die den Betroffenen voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

§ 2

**Erhebung personenbezogener Informationen
mit nachrichtendienstlichen Mitteln**

Der Bundesnachrichtendienst darf personenbezogene Informationen mit nachrichtendienstlichen Mitteln erheben, wenn tatsächliche Anhaltspunkte dafür vorhanden sind, daß auf diese Weise Erkenntnisse nach § 1 Abs. 1 Satz 1 Nr. 1 oder die zu ihrer Erforschung erforderlichen Nachrichtenzugänge gewonnen werden können, oder wenn dies zur Erfüllung der Aufgaben nach § 1 Abs. 1 Satz 1 Nr. 2 und 3 erforderlich ist. § 7 Abs. 1 Satz 2 bis 4 und Abs. 2 des Bundesverfassungsschutzgesetzes ist entsprechend anzuwenden.

§ 3

**Speicherung, Veränderung und Nutzung
personenbezogener Daten in Dateien**

Der Bundesnachrichtendienst darf personenbezogene Daten speichern, verändern und nutzen, soweit dies zur Erfüllung seiner Aufgaben nach § 1 Abs. 1 erforderlich ist. § 8 Abs. 2 und 3 sowie die §§ 9 und 10 des Bundesverfassungsschutzgesetzes sind entsprechend anzuwenden.

§ 4

**Übermittlung von Informationen
an den Bundesnachrichtendienst**

(1) Die Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts dürfen von sich aus dem Bundesnachrichtendienst die ihnen bekanntgewordenen Informationen übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des Bundesnachrichtendienstes nach § 1 Abs. 1 Satz 1 Nr. 1 und 2 erforderlich ist.

(2) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben nach Maßgabe des § 12 Abs. 2 des Bundesverfassungsschutzgesetzes von jeder Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, die Übermittlung der erforderlichen personenbezogenen Informationen verlangen und amtliche Register einsehen.

(3) Die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie der Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, übermitteln dem Bundesnachrichtendienst von sich aus die ihnen bekanntgewordenen Informationen, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung seiner Aufgaben nach § 1 Abs. 1 Satz 1 Nr. 1 und 2 erforderlich ist. § 13 Abs. 3 des Bundesverfassungsschutzgesetzes ist entsprechend anzuwenden.

(4) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben von den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien sowie vom Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, die Übermittlung der erforderlichen personenbezogenen Informationen verlangen. § 13 Abs. 2 Satz 2 und 3 sowie Abs. 3 des Bundesverfassungsschutzgesetzes ist entsprechend anzuwenden.

§ 5

**Übermittlung von Informationen
durch den Bundesnachrichtendienst**

(1) Der Bundesnachrichtendienst darf personenbezogene Informationen an Behörden übermitteln, wenn dies zur Erfüllung seiner Aufgaben oder zur Wahrung außen- und sicherheitspolitischer Belange der Bundesrepublik Deutschland erforderlich ist oder

wenn der Empfänger die Informationen für Zwecke der öffentlichen Sicherheit benötigt. Der Empfänger darf die übermittelten Informationen, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

(2) Für die Übermittlung an andere Stellen ist § 14 Abs. 2 bis 4 des Bundesverfassungsschutzgesetzes entsprechend anzuwenden; dabei ist die Übermittlung nach Absatz 4 dieser Vorschrift nur zulässig, wenn sie zur Wahrung außen- und sicherheitspolitischer Belange der Bundesrepublik Deutschland erforderlich ist und der Staatssekretär beim Bundeskanzler seine Zustimmung erteilt hat.

(3) Der Bundesnachrichtendienst übermittelt den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien Informationen nach Maßgabe des § 15 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1, 3 und 4 des Bundesverfassungsschutzgesetzes.

(4) Der Bundesnachrichtendienst übermittelt dem Militärischen Abschirmdienst von sich aus Informationen unter den Voraussetzungen des § 15 Abs. 1 Satz 3 des Bundesverfassungsschutzgesetzes. Der Militärische Abschirmdienst darf zur Erfüllung seiner Aufgaben vom Bundesnachrichtendienst die Übermittlung der erforderlichen Informationen verlangen; § 15 Abs. 2 Satz 3 und 4 des Bundesverfassungsschutzgesetzes ist entsprechend anzuwenden.

§ 6

Verfahrensregeln für die Übermittlung von Informationen

Für die Übermittlung von Informationen nach §§ 4 und 5 finden die §§ 19 bis 23 des Bundesverfassungsschutzgesetzes entsprechende Anwendung.

§ 7

Geltung des Verwaltungsverfahrgesetzes und des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 1 Abs. 1 Satz 1 durch den Bundesnachrichtendienst finden die §§ 3a und 3c des Verwaltungsverfahrgesetzes und die §§ 12 bis 16 und § 18 des Bundesdatenschutzgesetzes in der Fassung des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes keine Anwendung.

§ 8

Berichtspflicht

Der Bundesnachrichtendienst unterrichtet die Bundesminister im Rahmen ihrer jeweiligen Zuständigkeitsbereiche unmittelbar über die Erkenntnisse aus seiner Tätigkeit nach § 1 Abs. 1 Satz 1 Nr. 1. Hierbei ist auch die Übermittlung personenbezogener Informationen zulässig.

§ 9

Berlin-Klausel

Zu Artikel 5 (BND-Gesetz)

A. Allgemeines

1. Zweck des Gesetzes

Das Gesetz verfolgt den Zweck, für informationserhebende und -verarbeitende Tätigkeiten des Bundesnachrichtendienstes, soweit sie zur rechtmäßigen Erfüllung seiner Aufgaben im Geltungsbereich des Gesetzes stattfinden müssen, die gesetzliche Grundlage zu schaffen, die nach der Entwicklung des Rechts auf informationelle Selbstbestimmung in Rechtslehre, Rechtsprechung und Gesetzgebung zur Fortsetzung dieser Tätigkeiten notwendig geworden ist.

2. Gesetzgebungskompetenz des Bundes

Für die Sammlung und Auswertung von Informationen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, hat der Bund die ausschließliche Gesetzgebungskompetenz nach Artikel 73 Nr. 1 GG; diese Kompetenz ermächtigt insoweit auch zu Regelungen über die eigene Sicherheit des Bundesnachrichtendienstes.

B. Im einzelnen

Zu § 1

Die Regelung in § 1 Abs. 1 Satz 1 Nr. 1 dient in Verbindung mit § 1 Abs. 2 der Klarstellung, daß Sachverhalte, Personen und Vorgänge des innerstaatlichen politischen Geschehens in der Bundesrepublik Deutschland und in Berlin (West) — auch soweit es im Zusammenhang mit Vorgängen von außen- und sicherheitspolitischer Bedeutung steht — nicht Gegenstand der nachrichtendienstlichen Aufklärung durch den Bundesnachrichtendienst sind. Die Regelung dient ferner der Klarstellung, daß Informationen, die weder für sich allein noch im Zusammenhang mit anderen Informationen von außen- und sicherheitspolitischer Bedeutung sind, kein Gegenstand der nachrichtendienstlichen Aufklärungstätigkeit des Bundesnachrichtendienstes sind. Auch für die in § 2 genannten erforderlichen Nachrichtenzugänge gilt, daß es sich nur um Zugänge zu Informationen handeln darf, die Bedeutung für die Erfüllung der in Absatz 1 genannten Aufgaben haben.

Die zur Anwendung kommenden nachrichtendienstlichen Mittel sind — wie auch in § 6 Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes, der eine Legaldefinition dieser Mittel enthält — in einer Dienstvorschrift zu benennen.

Die Verweisung in Absatz 1 Satz 3 auf § 3 Abs. 2 Satz 2 des Bundesverfassungsschutzgesetzes erfolgt im Vorgriff auf ein künftiges Geheimhaltungsgesetz.

Drucksache 11/4306

Zu §§ 2 bis 7

§ 2 stellt die Zulässigkeit der Erhebung personenbezogener Informationen mit nachrichtendienstlichen Mitteln unter noch engere Voraussetzungen als § 1; er enthält ebenso wie die §§ 3 bis 7 Regelungen, die, bezogen auf die in § 1 Abs. 1 genannten Aufgaben des Bundesnachrichtendienstes, denen der §§ 7 bis 10 und 12 bis 23 des Bundesverfassungsschutzgesetzes entsprechen. Die Gleichartigkeit der Regelungen für den Bundesnachrichtendienst mit den Regelungen für das Bundesamt für Verfassungsschutz gewährleistet, daß die dem Bundesnachrichtendienst im Rahmen des Gesetzeszwecks verliehenen Befugnisse zur Erhebung, Verarbeitung und Nutzung personenbezogener Informationen gleichermaßen vom Grundsatz der Verhältnismäßigkeit begrenzt werden.

Bei der Erfüllung der Aufgabe nach § 1 Abs. 1 Satz 1 Nr. 2 kann die Erhebung personenbezogener Informationen vor allem zur Aufklärung der dort genannten, gegen den Bundesnachrichtendienst gerichteten Tätigkeiten erforderlich sein.

Die Verweisung in § 2 Satz 2 auf § 7 Abs. 1 Satz 2 des Bundesverfassungsschutzgesetzes, der wiederum auf die Regelungen in § 12 Abs. 2 und § 13 Abs. 2 des Bundesverfassungsschutzgesetzes Bezug nimmt, bedeutet, daß Erhebungen nach § 2 Satz 1 nicht zulässig sind, wenn der Bundesnachrichtendienst die benötigten Informationen durch Auskünfte von anderen Behörden einschließlich der Strafverfolgungsbehörden und der anderen Sicherheitsbehörden (Verfassungsschutzbehörden, Militärischer Abschirmdienst) sowie sonstigen Stellen erhalten kann.

In § 3 bedeutet die entsprechende Anwendung des § 10 des Bundesverfassungsschutzgesetzes, daß für die Zustimmung zu Dateianordnungen im Bundesnachrichtendienst der Staatssekretär beim Bundeskanzler zuständig ist.

Die §§ 4 und 5 regeln die Übermittlung von Informationen an und durch den Bundesnachrichtendienst, soweit sie nicht an anderer Stelle gesetzlich geregelt ist. Die Übermittlung von Informationen zwischen dem Bundesnachrichtendienst und den Verfassungsschutzbehörden ist in den §§ 13, 15, 16 Abs. 2 und § 17 Abs. 2 des Bundesverfassungsschutzgesetzes geregelt; für die Übermittlung von Informationen vom Militärischen Abschirmdienst an den Bundesnachrichtendienst gilt § 5 Abs. 4 MAD-Gesetz. Im übrigen ergibt sich der Vorbehalt besonderer gesetzlicher Übermittlungsregelungen aus § 6 in Verbindung mit § 19 Nr. 3 des Bundesverfassungsschutzgesetzes.

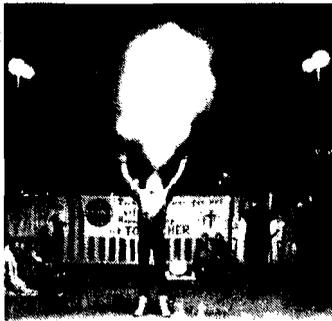
Zu § 8

§ 8 konkretisiert die in § 1 Abs. 1 Satz 1 Nr. 1 genannte Aufgabe der Unterrichtung der Bundesregierung. Dabei dürfen auch personenbezogene Informationen, wenn sie von Bedeutung im Sinne dieser Aufgabe sind, übermittelt werden. Die gegenüber der zuständigen Aufsichtsbehörde (s. Organisationserlaß des Bundeskanzlers vom 17. Dezember 1984, BGBl. I S. 1689) bestehende umfassende Berichtspflicht im Rahmen der Dienst- und Fachaufsicht bleibt unberührt.

atom Nr. 25

Atom Express & Atommiljöbeilage

atom



Aus dem Inhalt

- ★ **AKW Biblis:**
Knapp am GAU vorbei
- ★ **Schacht Konrad:**
Vor der Entscheidung
- ★ **WAA Wackersdorf:**
Großdemonstration 3.6.
- ★ **Hochtemperaturreaktor:**
Groschengrab in Uentrop
- ★ **Brokdorf u.a.:**
SPD windet sich
- ★ **West meets East:**
Atomseminar mit KPdSU
- ★ **Kriminalisierung:**
Knast für Fritz Störim
Hungerstreik
Startbahn-Prozesse

atom erscheint jeden zweiten Monat. Preis: DM 4,—
Abo (5 Ausgaben): 25 DM

Neue Bestelladresse:
atom, Postfach 1109
2120 Lüneburg

Stellungnahme zum BND-Gesetz-Entwurf vom 6.4.1989

1. Generelle Anmerkungen

Mit ca. 6.000 Mitarbeitern ist der BND der größte der drei Geheimdienste des Bundes. Seine Geschichte führt unmittelbar in den deutschen Faschismus zurück. Als Abt. "Fremde Heere Ost" operierte unter General Gehlen eine wehrmachtseigene Geheimdienstabteilung in der Sowjetunion. Bei der Flucht aus der Sowjetunion achtete Gehlen weit-sichtlich darauf, daß die Materialien dieser Abteilung über die Sowjetunion verfilmt und mitgeführt wurden in der Absicht, seine Organi-sation und ihre Kenntnisse den Amerikanern anzubieten - mit Erfolg. Ab 1945 wurde die nun "Organisation Gehlen" genannte Truppe von den Amerikanern finanziert. Im Jahre 1956 wurde Gehlens Geheimdienst von der Bundesregierung als Auslandsspionage-Dienst übernommen. So wurde die Generalstaabsabteilung "Fremde Heere Ost" dialektisch aufgehoben, d.h. nominell beseitigt, real bewahrt.

Bisher gibt es keine, Aufgaben und Befugnisse regelnde gesetzliche Grundlage für den BND. Der internen Steuerung des BND dienen Organi-sationserlasse und Dienstanweisungen (derzeit gilt der Organisations-erlaß des Bundeskanzlers vom 17. Dez. 1984, BGBl. I, S.1689). Gesetz-liche Erwähnung fand der BND zuvor im G-10-Gesetz von 1968 (§ 3). Weitere legitimatorische Weihe erhielt er mit dem Abhör-Urteil des Bundesverfassungsgerichts aus dem Jahre 1984, in dem dem BND die sog. "strategische Postkontrolle" für die postalischen Verkehr mit Län-dern des sozialistischen Lagers generell zugestanden wurde (Urteil in NJW, Nr.47/1984). Jahre zuvor war bekanntgeworden, daß der BND täglich in den Postleitstellen säckeweise Postsendungen aus und nach Ländern des sozialistischen Lagers abholte, um sie zu öffnen (vgl. CILIP 3, S.21 ff.). Das Bundesverfassungsgericht hatte zum Urteilszeit-punkt noch nicht das "informationelle Selbstbestimmungsrecht" ent-deckt.

Nach einer seit 1985 geltenden "Dienstanweisung zur Durchführung der Amtshilfeersuchen der VfS-Behörden und des BND" ist u.a. der Bundes-grenzschutz verpflichtet, dem BND bei der Anwerbung von Reisenden für die BND-Auslandsspionage zu helfen; bekannt wurde auch, daß der BGS für den BND Reisepässe fotografierte (vgl. CILIP 23, S.33 ff.).

In Vorentwürfen waren Aufgaben und Befugnisse des BNDs im ZAG, später im VfS-Mitteilungsgesetz untergebracht worden. Da diese "Quer-schnittsgesetze" nun entfallen sind, bedurfte es eines eigenen BND-Ge-setzes. Der Entwurf sei vom ehemaligen BND-Präsidenten und derzeitigen Staatssekretär des BMJ Kinkel ausgearbeitet worden, meldete die FAZ (29.11.88).

2. Detailkommentierung

Zu § 1: Aufgaben und Befugnisse

Entgegen der sonstigen Gesetzgebungstechnik, Aufgaben und Befugnisse in getrennten Paragraphen zu regeln, sind sie hier in einem Paragraphen zusammengefaßt - offensichtlich ein Versuch, die inhaltsleere Kargheit der Aufgabendefinition in Abs.1 Nr.1 (Sammlung und Auswertung von Informationen, die von außen- und sicherheitspolitischer Bedeutung sind) zu kaschieren.

Nach Nr.2 ist der BND befugt, zur Abwehr von Gegenspionage, nach Nr.3 zur Sicherheitsüberprüfung von Mitarbeitern und potentiell anzusprechenden Mitarbeitern, alle Informationen zu erheben und dabei nachrichtendienstliche Mittel einzusetzen.

Abs.2 soll klarstellen, so die amtliche Begr., daß "Sachverhalte, Personen und Vorgänge des innerstaatlichen politischen Geschehens in der Bundesrepublik und in Berlin-W ... nicht Gegenstand der nachrichtendienstlichen Aufklärung des BND sind".

Dies suggeriert, daß der BND im Geltungsbereich des GG nur insoweit nachrichtendienstlich tätig werden darf, als es darum geht, sich selbst vor Gegenspionage zu schützen und (potentielle) Mitarbeiter aus Sicherheitsgründen auszuspähen.

Gleichwohl, das ganze BND-Gesetz (wie die BND-Verweise im BDSG, im G-10-Gesetz, im Ausländerzentralregister-Gesetz-Entwurf, im ZEVIS-Gesetz, im Entw. BVerfSch-G, im Entwurf MAD-G etc.) erfüllt nur einen einzigen Zweck: Operationen und Informationsinteressen des BND auf dem Gebiet der Bundesrepublik und Berlin (West) rechtlich abzusichern.

Der Satz (Abs.2), "auf innenpolitischem Gebiet wird der BND nicht tätig", bedeutet also nur eine Ressort-Klarstellung (sachl. Zuständigkeit) gegenüber dem BMI und seinem Geheimdienst, dem BfV. Ansonsten aber gelten alle BND-Befugnisse, auch die folgenden Regelungen in den §§ 2 - 9, ausschließlich und nur im Bundesgebiet. Verhielte es sich anders, dann wäre ein solches BND-Gesetz vollkommen überflüssig. Alle anderen Tätigkeiten des BND, im Kern die Auslandsspionage, wären - wenn überhaupt - in Kategorien des internationalen und des Völkerrechts zu thematisieren.

Was heißt also :

"Auf innenpolitischem Gebiet wird der BND nicht tätig"?

Nur dies: er hat die Kompetenzbereiche von Polizei und Staatsanwaltschaft, von MAD und VfS-Ämtern zu beachten - um so mehr, als diese alle ihm zuarbeiten müssen.

An der Aufgabenbestimmung gemessen: "Sammlung und Auswertung von Informationen, die von außen- und sicherheitspolit. Interesse sind", wirkt die Aufgabennorm des BfV im Neu-Entw. geradezu weitschweifig und präzise.

Nur sind innen- und außenpolitische Belange und Interessen viel zu sehr miteinander verschlungen, als daß sie funktional eindeutig trennbar wären. Der Begriff der "sicherheitspolitischen Bedeutung", der von vorn-

herein auf den außenpolitischen Bezug verzichtet, macht die Grenzenlosigkeit dieser "Aufgabennorm" besonders deutlich.

Was der BND als Aufgabe sieht, läßt sich mithin nur über seine Praxis erschließen. So wurde, jenseits der Spionage im Ausland (und in der DDR selbstverständlich), u.a. bekannt, daß die bundesdeutsche Industrie den BND zur Terroristen-Fahndung alimentierte, daß er den Seweso-Gitffässern nachjagte und die internationale Zusammenarbeit der "Ärzte für den Frieden" zu seinem Beobachtungsobjekt machte.

Zu den §§ 2 - 9:

Wie im MAD-Gesetz entsprechen die Befugnisse des BND zur Erhebung, Speicherung und Übermittlung personenbezogener Informationen denen, die im VfS-G für das BfV festgeschrieben sind. Unsere Kritik entspricht mithin der am Entw. des BVerfSchG:

- * Wie die VfS-Ämter hat er Zugriff auf Informationen "jeder Stelle, die Aufgaben der öffentlichen Verwaltung" wahrnimmt,
- * Wie die VfS-Ämter darf er alle Informationen an jedwede Stelle im In- und Ausland streuen,
- * Entsprechend dürfen Beschäftigte des Bundes und bundesunmittelbarer juristischer Personen des öffentlichen Rechts von sich aus den BND beliefern,
- * Entsprechend müssen Polizei und Staatsanwaltschaft sowie der BGS dem BND zuarbeiten.

Dies alles wird noch unangreifbarer, da es nicht die Spur von Kriterien für eine rechtlich greifbare Aufgabenbestimmung gibt, an der gemessen werden könnte, ob die je konkreten Praktiken des BND, sei es, daß er von "Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen", Informationen abverlangt, sei es, daß er diese ins Ausland transferiert, "rechtmäßig" wären.

Den BND an das Verhältnismäßigkeitsprinzip zu erinnern (§ 1 Abs.4), ist angesichts der Konturen- und Maßstabslosigkeit in der Aufgabenbestimmung unverhüllter Spott.

Literatur zum BND:

Felfe, Heinz, Im Dienst des Gegners - 10 Jahre Moskaus Mann im BND, Hamburg 1986

Gehlen, Reinhard, Der Dienst - Erinnerungen 1942 - 71, Mainz - Wiesbaden 1971

ders., Verschlußsache, Mainz 1980

Damm, Diethelm, Die Praktiken des BND, in: Kritische Justiz, 1/1975

Höhne/Zölling, Pullach intern - Die Geschichte des BND, "Spiegel"-Serie ab Heft 11/1971 (auch als Buch erschienen)

Naumann, Michael, Operation großes Ohr - Bericht über strategische Abhöraktionen des BND, in: Die Zeit v. 28.3.1980

Wessel, Gerhard, BND - der geheime Auslandsnachrichtendienst der BRD, in: Beiträge zur Konfliktforschung, 2/1985

Simpson, Christopher, Der amerikanische Bumerang - NS-Kriegsverbrecher im Sold der USA, Wien 1988

Denn Nachricht ist alles...

Jeder Schwatz wird gemeldet, jeder Brief wird geöffnet. Bei der Armee, bei den Kaufleuten, bei den Deputierten, in der Weinstube und Versammlung horcht der Polizeiminister unsichtbar mit, und alle diese tausend Nachrichten laufen täglich in der Richtung seines Schreibtisches zusammen. Dort werden die teilweise richtigen und wichtigen, teils bloß schwatzhaften Denunziationen geprüft, gesiebt und verglichen, bis sich aus tausend Chiffren klare Nachricht ergibt.

Denn Nachricht ist alles; im Krieg wie im Frieden, in der Politik wie in der Finanz. Nicht mehr der Terror, sondern nur das Wissen ist 1799 die Macht in Frankreich. Das Wissen um jeden dieser traurigen Thermidoristen, wieviel Geld er nimmt, von wem er bestochen wird, für wieviel er käuflich ist, um ihn in Schach zu halten und so den Übergeordneten zum Untertanen zu machen; das Wissen um die Verschwörungen, teils um sie niederzuschlagen, teils um sie zu fördern und so in der Politik immer nach der rechten Seite zu lavieren; roben, sie plaudern in den Salons des Faubourg Saint-Germain und schleichen sich anderseits wieder, patriotisch verkleidet, in die Geheimsitzungen der Jakobiner. In der Liste seiner Söldlinge finden sich Marquis und Herzoginnen mit den klingendsten Namen Frankreichs, ja, er darf sich rühmen (phantastisches Faktum!), die höchste Frau des Reiches, Josephine Bonaparte, die spätere Kaiserin, in seinen Diensten zu haben. Im Bureau seines späteren Herrn und Kaisers ist der Sekretär an ihn verkauft, in Hartwell in England der Koch des Königs Ludwig XVIII. von ihm bestochen.

aus:

Stefan Zweig, Josef Fouché -
Bildnis eines politischen Menschen, 4. Kapitel

Dokumentation:

Deutscher Bundestag
11. Wahlperiode

Drucksache 11/4316

07. 04. 89

Beschlüßempfehlung und Bericht

Sachgebiet 901

des Ausschusses für das Post- und Fernmeldewesen (15. Ausschuß)

zu dem Gesetzentwurf der Bundesregierung
— Drucksache 11/2864 —

Entwurf eines Gesetzes zur Neustrukturierung des
Post- und Fernmeldewesens und der Deutschen Bundespost (Poststruktugesetz
— PostStruktG)

(15) Das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 13. August 1968 (BGBl. I S. 949), geändert durch Gesetz vom 13. September 1978 (BGBl. I S. 1546), wird wie folgt geändert:

5. In Artikel 3 werden folgende Vorschriften eingefügt:

- § 10

(1) Wird der Fernmeldeverkehr nach Artikel 1 dieses Gesetzes oder nach den §§ 100 a, 100 b der Strafprozeßordnung überwacht, so darf diese Tatsache von Personen, die eine für den öffentlichen Verkehr bestimmte, nicht von der Deutschen Bundespost betriebene Fernmeldeanlage betreiben, beaufsichtigen, bedienen oder bei ihrem Betrieb tätig sind, anderen nicht mitgeteilt werden.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen Absatz 1 die Tatsache der Überwachung des Fernmeldeverkehrs einem anderen mitteilt.

§ 11

(1) Ordnungswidrig handelt, wer als Betreiber einer für den öffentlichen Verkehr bestimmten, nicht von der Deutschen Bundespost betriebenen Fernmeldeanlage entgegen

1. Artikel 1 § 1 Abs. 2 Satz 2 eine Auskunft nicht erteilt, Sendungen nicht aushändigt oder das Überwachen des Fernmeldeverkehrs nicht ermöglicht oder

2. Artikel 1 § 1 Abs. 2 Satz 3 das erforderliche überprüfte und zum Zugang zu Verschlusssachen des jeweiligen Geheimhaltungsgrades ermächtigte Personal nicht bereithält.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis 30 000 Deutsche Mark geahndet werden.

6. Artikel 3 §§ 10 bis 13 (alt) werden §§ 12 bis 15 (neu).

7. Artikel 3 § 13 (neu) wird wie folgt gefaßt:

- § 13

Die nach diesem Gesetz berechtigten Stellen haben die Leistungen der Deutschen Bundespost oder anderer Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, abzugelten."

(16) Die Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074), zuletzt geändert durch das Gesetz vom 17. Mai 1988 (BGBl. I S. 606), wird wie folgt geändert:

1. In § 100 a Satz 1 werden die Worte „Aufnahme des Fernmeldeverkehrs auf Tonträger“ durch die Worte „Aufzeichnung des Fernmeldeverkehrs“ ersetzt.

2. § 100 b wird wie folgt geändert:

a) In Absatz 1 Satz 1 werden die Worte „Aufnahme des Fernmeldeverkehrs auf Tonträger“ durch die Worte „Aufzeichnung des Fernmeldeverkehrs“ ersetzt.

b) Absatz 3 wird wie folgt gefaßt:

„(3) Auf Grund der Anordnung haben die Deutsche Bundespost und jeder andere Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Hilfsbeamten (§ 152 des Gerichtsverfassungsgesetzes) die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen. § 95 Abs. 2 gilt entsprechend.“

c) Absatz 4 Satz 2 wird wie folgt geändert:

„Die Beendigung ist dem Richter und der Deutschen Bundespost oder dem anderen Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, mitzuteilen.“

(17) Nach § 17 des Gesetzes über die Entschädigung von Zeugen und Sachverständigen in der Fassung der Bekanntmachung vom 1. Oktober 1969 (BGBl. I S. 1756), zuletzt geändert durch Artikel 4 des Gesetzes vom 9. Dezember 1986 (BGBl. I S. 2326), wird folgender § 17a eingefügt:

- § 17a

Herausgabe von Gegenständen,
Überwachung des Fernmeldeverkehrs,
Auskunftsersuchen

(1) Für Dritte, die aufgrund eines Beweiszwecken dienenden Ersuchens der Strafverfolgungsbehörde Gegenstände herausgeben (§ 85 Abs. 1 der Strafprozeßordnung) oder die Pflicht zur Herausgabe entsprechend einer Anheimgabe der Strafverfolgungsbehörde abwenden, Auskunft erteilen oder die Überwachung und Aufzeichnung des Fernmeldeverkehrs ermöglichen (§ 100b Abs. 3 der Strafprozeßordnung), gelten die Vorschriften dieses Gesetzes sinngemäß. Artikel 3 § 13 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses findet keine Anwendung.

(2) Die Dritten werden wie Zeugen entschädigt.

(3) Bedient sich der Dritte eines Arbeitnehmers oder einer anderen Person, so werden ihm die Aufwendungen dafür (§ 11) im Rahmen des § 2 Abs. 2 und 5 ersetzt.

(4) Für die Benutzung von Festverbindungen bei der Überwachung des Fernmeldeverkehrs sind auch die in den allgemeinen Tarifen dafür vorgesehenen Entgelte zu ersetzen."

(18) Absatz 15 gilt nicht im Land Berlin.

9. Anpassung der Regelungen des Gesetzes zu Artikel 10 des Grundgesetzes und der §§ 100a, 100b der Strafprozeßordnung an die Neustrukturierung des Post- und Fernmeldewesens

Nach Artikel 1 § 1 des Gesetzes zu Artikel 10 GG (G 10) sind die der Staatssicherheit dienenden Behörden und nach den §§ 100a, 100b StPO die Strafverfolgungsbehörden berechtigt, unter näher beschriebenen Voraussetzungen Maßnahmen zur Überwachung des Fernmeldeverkehrs zu ergreifen. Nach dem geltenden Recht ist ausschließlich die Deutsche Bundespost dazu verpflichtet, diese Maßnahmen zu ermöglichen. Durch die Neufassung des Gesetzes über Fernmeldeanlagen ist nunmehr privaten Anbietern von Telekommunikationsdienstleistungen ein rechtlich abgesicherter Betätigungsbereich im Fernmeldewesen eingeräumt worden. Es wird daher ein Bedarf gesehen, auch die privaten Diensteanbieter einer gesetzlichen Verpflichtung zu unterwerfen, notwendige Überwachungsmaßnahmen zu ermöglichen.

Die Mitglieder der Fraktionen der CDU/CSU und FDP halten eine gesetzliche Regelung dieses neuen Tatbestands für erforderlich. Da das Poststrukturgesetz bei den Fernmeldediensten grundsätzlich — mit Ausnahme des Telefondienstes — den Wettbewerb zwischen der DBP und privaten Anbietern zulasse, entsteht ein Fernmeldeverkehrsbereich, der nicht gänzlich Überwachungsmaßnahmen entzogen sein darf. Es sei davon auszugehen, daß der Satellitenfunk auch zur Übermittlung von Nachrichten innerhalb des Bundesgebietes in Zukunft in steigendem Maße genutzt werde. Ferner würde im geplanten europäinheitlichen Mobilfunknetz D neben der Deutschen Bundespost ein weiterer privater Anbieter zugelassen. Das dann europäinheitliche, nicht mehr nationale, grenzlose D-Netz werde nach den bisherigen Schätzungen bis Ende der 90er Jahre europaweit über mindestens 10 Millionen Teilnehmer verfügen. Auch im Funkrudienst wie der Stadtfunkrudienst erziele sich generell zur konspirativen Kommunikation Personen, die Straftaten nach § 2 Abs. 1 des Grundgesetzes begehen oder begangen hätten. Daher sei erforderlich, durch Gesetzesänderung die Lücken zu schließen, die im Anwendungsbereich des G 10 durch die §§ 100a, 100b StPO entstehen, wenn weiterhin gesehen private Anbieter Telekommunikationsdienstleistungen für andere über von der Deutschen Bundespost TELEKOM bereitgestellte Verbindungen zu bringen oder ein privates Mobilfunknetz betreiben. Verfolgter Zweck sei die Sicherstellung der Durchführung und Geheimhaltung von Überwachungsmaßnahmen nach dem G 10 und nach den §§ 100a, 100b StPO auch in diesen Fällen. Von dem bisherigen Vorgehen laut der Vorschriften würden private Anbieter von Telekommunikationsdienstleistungen nicht erfaßt. Aus sicherheitspolitischer und strafverfahrensrechtlicher Sicht bedürfe es einer Änderung, da sonst die große Gefahr bestehe, daß Nischen z. B. für die organisierte Kriminalität und den internationalen Terrorismus entstehen könnten. Nach den Erfahrungen der Sicherheitsbehörden würden potentiell Betroffene die fehlenden Überwachungsmöglichkeiten erkennen und verstärkt nutzen.

Die Fraktion der SPD erkennt zwar einen Regelungsbedarf an, hält es aber für bedenklich, das vorliegende Gesetzgebungsverfahren ohne gründliche parlamentarische Beratung dafür zu nutzen, die gesetzlich zulässigen Überwachungsmaßnahmen auf jegliche Art des Fernmeldeverkehrs zu erstrecken. Sie hält überhaupt eine generelle Überprüfung der §§ 100a, 100b StPO für notwendig. Weiter erscheint es ihr unverhältnismäßig und unpraktikabel, das bei der Durchführung von Überwachungsmaßnahmen eingesetzte Personal der privaten Diensteanbieter einer Sicherheitsprüfung zu unterziehen. Schließlich bestünden Zweifel, ob die Überwachungsmaßnahmen bei der Vielzahl der möglichen privaten Unternehmen und ihren vielfältigen Dienstleistungen überhaupt technisch durchführbar seien.

Nach Aufforderung hat die Bundesregierung hierzu erklärt, sie lege schon das geltende Gesetz zu Artikel 10 GG dahin aus, daß unter den dort beschriebenen Voraussetzungen jegliche Art des Fernmeldeverkehrs einer Überwachungsmaßnahme zugänglich sei.

Stellungnahme

Von der Post- zur Kommunikationskontrolle:

Der Änderungsantrag der CDU/CSU zum "Gesetz zur Neustrukturierung des Post- und Fernmeldewesens und der deutschen Bundespost" (PostStruktG)

Im Handstreich haben Bonner Koalitionsabgeordnete dem lange diskutierten PostStruktG wenige Wochen vor der rechtskräftigen Verabschiedung dieses Gesetzes am 20.4.d.J. eine "Ergänzung" nachgeschoben, die die staatlichen Überwachungsbefugnisse auf alle neuen Kommunikationsformen und -techniken ausdehnt. Zeit für öffentlichen Widerspruch gab es so gut wie nicht.

1. Die Angst vor Nischen

In kaum einem der "Sicherheitsgesetze" tritt die Denkweise und -logik der exekutiven Rechtsproduzenten so klar zu Tage, wie bei diesem unscheinbaren Änderungsantrag zum Poststrukturgesetz: "Aus sicherheits- und strafverfahrensrechtlicher Sicht bedarf es der Änderung" (der bisherigen Regelungen im G-10-Gesetz und der StPO) "da sonst die große Gefahr besteht, daß Nischen entstehen, in die z.B. die organisierte Kriminalität und der internationale Terrorismus ausweichen können." Dieser Satz aus der Begr. ist verräterisch. Die Gesetzesgeber versuchen nicht einmal mehr den Eindruck zu erwecken, als hätten sie darüber nachgedacht, wo zur Abwehr schwerwiegender Gefahren Eingriffe in die immer transparenter werdenden Formen der menschlichen Kommunikation und die Kontrolle des dabei Verarbeiteten "unabweisbar notwendig" sei.

Nein, Terrorismus und organisierte Kriminalität werden als Stichworte, die größte Bedrohung von Staat und Gesellschaft symbolisieren, einfach beispielhaft angeführt. Es sind die Nischen an sich die als Bedrohung benannt werden. Diese durch die neuen Kommunikationstechniken und die Privati-

sierung von Teilbereichen des Kommunikationsgeschäfts entstehenden Räume sind es, die a priori der Kontrolle unterworfen werden sollen. Vom Zugriff der Sicherheitsapparate kontrollfreie Räume darf es nach dieser Logik der Gesetzesmacher nicht geben. Denn: "Nach den Erfahrungen der Sicherheitsbehörden würden potentiell Betroffene die sonst fehlenden Überwachungsmöglichkeiten erkennen und verstärkt nutzen."

Wenn aber die "potentiell Betroffenen"- und das sind potentiell alle Bürger - die Überwachung erkennen, was dann? Sie - und mit höherer Professionalität sicher auch Waffenschieber, Hersteller von Giftgasanlagen, korrupte Politiker und Terroristen werden weiter Nischen suchen und finden zur vertraulichen Kommunikation. Und weil nicht etwa nur der Im Entwurf angeführte mobile Funkrufdienst sich "generell zur konspirativen Kommunikation von Personen" eignet, sondern generell jede vertrauliche Form des Gesprächs, des Austauschs von Zeichen auch der Verschwörung dienen kann, wird der Druck wachsen, auch diese Formen der Kommunikation in den Griff zu bekommen: Videoüberwachung, Richtmikrophone, Wanzen usw. kurz nachrichtendienstliche Mittel und Möglichkei-

ten verdeckter Ermittlungen müssen zum Einsatz kommen, um weitere Nischen auszuleuchten. Die liberalen Rechts- und Staatstheorien des 19. Jahrhunderts gingen von der Vorstellung eines in seiner Kommunikation freien und vor staatlicher Kontrolle geschützten Bürgers aus, als Voraussetzung "eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens"- so ganz in dieser Tradition das BVerfG im Volkszählungsurteil. Der vorliegende Entwurf geht demgegenüber von der Notwendigkeit der Auflösung aller, nur als Nischen wahrgenommenen bürgerlichen Freiräume aus und damit vom Postulat eines umfassenden staatlichen Kontrollanspruchs. Konsequenterweise werden die in dem Entwurf enthaltenen schwerwiegenden Beschränkungen des Post- und Fernmeldegeheimnis nicht einmal mehr erwähnt.

2. Die rechtliche "Lösung" im Entwurf

Dies geschieht im vorliegenden Entwurf nun nicht dadurch, daß neue Eingriffsvoraussetzungen in die Kommunikation von Bürgern formuliert werden. In diesem Punkt bezieht man sich schlicht auf § 100 StPO mit seinen weitreichenden Anwendungsmöglichkeiten (etwa Ermittlungen wegen 129a) und auf das in seinen strategischen Kontrollmöglichkeiten noch weitergehende G-10-Gesetz. Doch dem Grundrecht auf Unverletzlichkeit der Privatsphäre und der informationellen Selbstbestimmung, das mit dem G-10-Gesetz schon im Zuge der Notstandsgesetzgebung weitgehend ausgehöhlt worden war, wie Konrad Hesse zu-

treffend vermerkt 1), wird durch den vorliegenden Entwurf der Boden völlig entzogen. Denn in weit höherem Maße als früher vollzieht sich menschliche Kommunikation heute über technische Medien, wie die digitalisierte Vermittlung von Telefongesprächen durch ISDN, Telefax, BTX, die Datenübermittlung durch Datex-L und Datex-P. Diese Medien werden immer weitere, auch private Formen des Verkehrs der Bürger mit seiner Umwelt umfassen, seinen Kontakt mit Behörden, seine Finanzen, sein Konsum, seine Freizeitgewohnheiten usw. Diese Medien ermöglichen jedoch nicht nur Kommunikation, sondern machen es in ganz anderem Maße als früher möglich, diese auch als Daten festhalten.²⁾ Dies gilt zum einen für die Erfassung der Kommunikationsstruktur: wer also mit wem, wann telephoniert oder sonst Nachrichten ausgetauscht hat ³⁾. Zum anderen aber gestatten die neuen Medien "zunehmend auch die Überwachung der Kommunikationsinhalte"; dort insbesondere, wo digitalisierte Daten und Texte übermittelt werden. "Mittels geeigneter Programme lassen sich Mitteilungen mit interessanten Inhalten herausfiltern und aufzeichnen."⁴⁾

Indem nun Fernschreiben nicht mehr nur mitgelesen und Telefongespräche nicht mehr nur abgehört und auf Tonträger aufgenommen werden dürfen (so die alte Fassung), sondern "überwacht" und aufgezeichnet werden dürfen (gemacht hat man dies nach freimütigem Bekunden der Bundesregierung ohnehin schon), wird die Überwachung der privaten Kommunikation intensiviert und extensiviert: Intensiviert durch die effektiveren Kontrollmöglichkeiten

bei den neuen Medien; extensiviert dadurch, daß über die neuen Medien immer weitere Felder privater und gesellschaftlicher Kommunikation erfaßt werden können. Rechtlich findet dies seinen Ausdruck in

a) dem neu formulierten 1 Abs.1 des G-10-Gesetzes

b) der schlichten Ersetzung der Formulierung "Aufnahme des Fernmeldeverkehrs auf Tonträger" durch "Aufzeichnung" des zunehmend digitalisierten Fernmeldeverkehrs in § 100 a und b StPO (auf Bändern und nicht mehr auf Tonträgern).

Art.10 GG wird so zum bloßen Symbol am Wertehimmel der Verfassungsordnung, während die vielfältigsten gesellschaftlichen Kommunikationsformen ob der in ihr liegenden Konspirationsgefahr der staatlichen Totalkontrolle unterworfen werden: sicher nicht alle, doch potentiell jede (etwa im Zuge der strategischen Kontrolle nach § 3 des G-10-Gesetzes).

Mit den Regelungen nähern wir uns dem vorkonstitutionellen Zustand im Österreich Metternichs oder in Bayern Montgelas.5) Der Sache nach übersteigen die heutigen technischen Möglichkeiten all das, wovon ein Fouc oder der preussische Generalpostmeister Nagler je träumen konnte. Der institutionellen Form nach wird jedoch mit dem neuen Poststrukturgesetz der entgegengesetzte Weg eingeschlagen. Wurde im Absolutismus nicht zuletzt aus Gründen der Staatssicherheit der Postdienst verstaatlicht, so werden jetzt wichtige Teilbereiche privatisiert. Um den Zugriff der Sicherheitsapparate auf die privaten Betreiber von Einrichtungen der Telekommunikation abzusichern, wird mit dem vorliegenden Änderungs-

paket die hoheitliche Kontrolle abgesichert. Dies ist seine zweite Hauptfunktion. Sie kommt in vier Punkten zum Ausdruck:

1. Zunächst einmal wird im G-10-Gesetz (§ 1 Abs.2) und in § 100 b Abs.3 der StPO die Pflicht, den Anordnungen der Sicherheitsbehörden oder eines Richters oder Staatsanwaltes im Falle § 100b StPO Folge zu leisten, auch auf private Betreiber von Fernmeldeeinrichtungen ausgedehnt.

2. Danach wird dem im Privatsektor für die Überwachung und Aufzeichnungen zuständige Personal der Status von Geheimnisträger verliehen, die nach der für den öffentlichen Bereich geltenden Verschlusssachenanordnung einer Sicherheitsüberprüfung unterworfen werden (Art.1 Abs.2 G-10-Gesetz)

3. Durch eine Änderung des Gesetzes über Fernmeldeanlagen werden den so zu quasihöheitlichen Geheimnisträgern ohne Pensionsanspruch erhobenen Anzapf- und Lauschspezialisten Freiheitsstrafen bis zu zwei Jahren angedroht für den Fall, daß sie die Tatsache der Überwachung des Fernmeldeverkehrs einem anderen mitteilen (§ 10). Die Unternehmen wiederum haben mit empfindlichen Geldbußen für den Fall zu rechnen, daß sie sich gegen die Anordnungen der Sicherheitsbehörden zur Wehr setzen (§ 11 Abs.1 Nr.1) oder keine sicherheitsüberprüften Angestellte "bereithalten" (§ 11 Abs.1 Nr.2).

4. Schließlich wird die Geltung des § 354 StGB über die Postbediensteten hinaus auch auf das private Personal im Fernmeldebereich erstreckt. Bei diesem Paragraph, der beim Vorliegen eines bloß privaten Interesses genau das unter Strafe stellt, was im Interesse des Staates zu tun ist - nämlich die Ver-

letzung des Post- und Fernmeldegeheimnisses - haben die Gesetzgeber typischerweise darauf verzichtet, die Tatbestände der Verletzung des Post- und Fernmeldegeheimnisses den Bedingungen der modernen Telekommunikation anzupassen.

Zusammengesehen mit den neuen Befugnissen zur Kommunikationsüberwachung in den Geheimdienstgesetzen, dem Versammlungsgesetz (§ 12a) und dem Entw. eines Strafverfahrensgesetz 1988 ist ein nahezu lückenloses rechtliches Reservoir entstanden zur Überwachung, Kontrolle und Aufzeichnung jedweder vertraulichen Kommunikation in jedweder sozialen Situation.

Anmerkungen:

1) Konrad Hesse, Grundzüge der Verfassung der Bundesrepublik Deutschland, RN.377, Heidelberg 1984, 14. Aufl.

2) Siehe ausführlich zum Problem den 7. Tätigkeitsbericht (1988) des Hamburger Datenschutzbeauftragten, S.15 ff.

3) Daß diese Möglichkeit auch denen noch nicht bewußt ist, die solche Gesetze verabschieden und anwenden, illustrierte der Fall Barschel eindrücklich, indem nicht zuletzt die registrierten Daten über seine Kommunikation sein Lügegebäude zusammenstürzen ließen.

4) 7. Datenschutzbericht (1988), Hamburg, a.a.O., S.18

5) vgl. zur damaligen Postkontrolle Wolfram Siemann, "Deutschlands Ruhe, Sicherheit und Ordnung," Tübingen 1985

Durch die Wüste

mehr als nur eine
RECHTSHILFEBROSCHURE

Schwerpunkte:

- Demos und Aktionen:
Von der Vor- bis zur Nachbereitung
- Überwachung:
Observation und Frazzia
- Zum Umgang mit den eigenen Strukturen
- Der Weg des Ermittlungsverfahrens:
Von der Personenkontrolle über Festnahme bis hin zum Verhalten auf der Wache
- Vorladung zu Polizei und Staatsanwaltschaft:
ZeugInnenproblematik und Aussageverhalten
- Strafbefehle und Bußgelder
- Zur Prozeßführung
- Übersicht über das politische Strafrecht

**Autorinnenkollektiv
aus Anti-Repressionsgruppen**

Einzelpreis: 8,- DM

Bestelladressen:

- für Buchläden:
Prolit Buchvertrieb GmbH
Siemensstr. 17 / Postf. 11 1008
6300 Gießen
- Einzelbestellungen und Initiativen:
Antirepressionsgruppe
c/o Umweltsentrum Münster
Scharnhorststr. 57
4400 Münster
(Einzelbestellungen nur gegen Vorkasse:
8,- DM + Porto)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zu den Änderungen des Gesetzes zu Art.10 GG und der Strafprozeßordnung im Rahmen der Poststrukturreform

Der im Rahmen der Ausschußberatungen zur Poststrukturreform aus den Reihen des Bundestages eingebrachte Entwurf zur Änderung des Gesetzes zu Art.10 GG (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) soll die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst u.a. dazu ermächtigen, den Fernmeldeverkehr zu überwachen und aufzuzeichnen. Bisher war den Diensten nach dem Gesetz zu Art.10 GG nur gestattet, "den Fernschreibverkehr mitzulesen, den Fernmeldeverkehr abzuhören und auf Tonträger aufzunehmen". Auch die Überwachungsvorschriften der Strafprozeßordnung (§§ 100a, 100b) sollen entsprechend geändert werden.

Während in der Vergangenheit neben dem Briefverkehr nur Telefongespräche und Fernschreiben kontrolliert und ausgewertet werden durften, soll dies nach dem Entwurf in Zukunft für den gesamten Fernmeldeverkehr (z.B. Btx, Telex, Telefax, Datel-Dienste, ISDN) zulässig sein. Daraus ließe sich ableiten, daß auch Abrechnungs-, Verbindungs- und Nutzungsdaten sowie im Rahmen elektronischer Dienste gespeicherte Inhaltsdaten (z.B. bei Mailboxen, Btx usw.) kontrolliert werden dürfen. Damit würde jedenfalls für den Bereich der Strafprozeßordnung auch eine rückwirkende Kontrolle legalisiert. Nicht auszuschließen ist außerdem, daß Dienstebetreiber dazu verpflichtet werden, für

Überwachungszwecke in größerem Umfang Daten zu speichern, als für ihre betrieblichen Belange erforderlich und zulässig ist.

Die Datenschutzbeauftragten sind deshalb der Auffassung, daß derart weitgehende Eingriffe in Grundrechte einer gründlichen Prüfung durch alle Beteiligten bedürfen. Deshalb sollten im Rahmen der vom Bundestag als dringlich angesehenen Poststrukturreform das Gesetz zu Art. 10 GG und die Strafprozeßordnung nur insoweit geändert werden, als dies in einem unmittelbaren Zusammenhang zu den geplanten ordnungspolitischen Änderungen der Telekommunikation steht. In Betracht käme insofern lediglich die Einbeziehung der Betreiber privater Telekommunikationsdienste in die Regelungen, die bislang nur für die Post gelten.

quer

Arbeitslosenzzeitung
Unabhängig Überregional
★

Gefördert von Unternehmern, Bankern, Politikern:
Sie sorgen dafür, daß uns die Leser nicht ausgehen!
★

Jahresabo 21,80 DM
Probehefte gegen Briefm.
★

"quer" c/o TFM
Heiligkreuzgasse 9a
6000 Frankfurt 1
(mittwochs 069/28 73 63)

II. Datenschutzrechtliche Querschnittsgesetze, Stand: Mai 1989

Dokumentation Bundesdatenschutzgesetz
(Auszüge):

Drucksache 11/4306

Deutscher Bundestag -- 11. Wahlperiode

ERSTER ABSCHNITT

Allgemeine Bestimmungen

§ 1

Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch die Verarbeitung oder Nutzung seiner personenbezogenen Daten in oder unmittelbar aus Dateien in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten und ihre Nutzung durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
 - a) Bundesrecht ausführen oder
 - b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen.

(3) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen:

1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§ 5 und 8.
2. Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§ 5, 8, 35 und 36. Außerdem gelten für Dateien öffentlicher Stellen die §§ 12 und 16 Abs. 1. Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt.

(4) Dieses Gesetz gilt nicht

1. für natürliche Personen, die personenbezogene Daten ausschließlich für private Zwecke und zum persönlichen Gebrauch verarbeiten oder nutzen,
2. a) für öffentlich-rechtliche Religionsgesellschaften sowie die ihnen zugeordneten caritativen und erzieherischen Einrichtungen des öffentlichen Rechts,
 - b) mit Ausnahme der §§ 7, 26, 27, 30 und 31 für die den öffentlich-rechtlichen Religionsgesellschaften zugeordneten caritativen und erzieherischen Einrichtungen des privaten Rechts.

(5) Soweit andere Rechtsvorschriften des Bundes auf in Dateien gespeicherte personenbezogene Daten

einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 3

Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener) in einer Datei.

(2) Eine Datei ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen geordnet, ungeordnet und ausgewertet werden kann (automatisierte Datei) oder
2. eine gleichartig aufgebaute Sammlung personenbezogener Daten, die nach bestimmten Merkmalen geordnet, ungeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren ungeordnet und ausgewertet werden können.

(3) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten in oder aus einer Datei. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, daß
 - a) die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder
 - b) der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsehend oder abrufen,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(4) Nutzen ist jede Verwendung personenbezogener Daten unmittelbar aus Dateien, soweit es sich nicht um Verarbeiten handelt.

(5) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.

(6) Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt.

(7) Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieses Gesetzes personenbezogene Daten im Auftrag verarbeiten.

§ 9

Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben, Geschäftszwecke oder Ziele der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlaß und Zweck des Abrufverfahrens,
2. Datenempfänger,
3. Art der zu übermittelnden Daten,
4. nach § 8 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 11 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 17 Abs. 2 Nr. 1 und 2 genannten Stellen beteiligt sind, bedarf der Zustimmung der für die speichernde und die abrufende Stelle jeweils zuständigen obersten Bundes- oder Landesbehörde.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlaß besteht. Die speichernde Stelle hat zu gewährleisten, daß die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen.

ZWEITER ABSCHNITT

Datenverarbeitung der öffentlichen Stellen

ERSTER UNTERABSCHNITT

Rechtsgrundlagen der Datenverarbeitung

§ 12

Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und, falls eine Erhebung vorausgegangen ist, es für die Zwecke erfolgt, für die die Daten erhoben worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies erlaubt oder anordnet,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, daß es im Interesse des Betroffenen liegt und er in Kenntnis des anderen Zwecks einwilligen würde,
4. die Daten für den anderen Zweck aufgrund einer durch Rechtsvorschrift festgelegten Auskunftspflicht beim Betroffenen erhoben werden dürfen,
5. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist oder
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die speichernde Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die speichernde Stelle.

§ 13

Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 12 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht. § 9 Abs. 4 bleibt unberührt.

(3) Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 12 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

§ 14

Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 12 zulassen würden, oder
2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährdet oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 15

Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes

(1) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereichs dieses Gesetzes sowie an über- und zwischenstaatliche Stellen gilt § 14 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, sowie § 14 Abs. 3.

(2) Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(4) Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie ihm übermittelt werden.

ZWEITER UNTERABSCHNITT

Rechte des Betroffenen

§ 17

Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, sowie über den Zweck der Speicherung Auskunft zu erteilen. In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Eine Verpflichtung zur Auskunftserteilung besteht nicht

1. für die Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militarischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung,
2. für die Behörden der Staatsanwaltschaft und der Polizei, soweit eine Abwägung ergibt, daß das öffentliche Interesse, die Auskunft nicht zu erteilen, das Interesse des Betroffenen an der Auskunftserteilung überwiegt; dies gilt auch für öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern,
3. hinsichtlich der Daten, die nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließ-

lich Zwecken der Datensicherheit oder der Datenschutzkontrolle dienen.

Bezieht sich die Auskunftserteilung auf die Herkunft personenbezogener Daten von in Nummer 1 genannten Behörden, ist sie nur mit Zustimmung dieser Stellen zulässig. Dies gilt auch für die Auskunft über die Übermittlung an diese Behörden. Für die Versagung der Zustimmung gilt Satz 1 Nr. 1 entsprechend. Für die Ablehnung der Auskunftserteilung gilt Absatz 4 Satz 2 entsprechend.

(3) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die Ablehnung der Auskunftserteilung durch die in Absatz 2 Nr. 1 genannten Behörden braucht nicht begründet zu werden.

(5) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(6) Die Auskunft ist unentgeltlich.

§ 18

Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt oder

2. sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(5) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(6) Von der Berichtigung unrichtiger Daten, der Sperrung bestimmter Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

(7) § 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

DRITTER UNTERABSCHNITT

Bundesbeauftragter für den Datenschutz

§ 22

Kontrolle durch den Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes, unbeschadet der ihnen bei der Erfüllung ihrer Aufgaben obliegenden fachlichen Beurteilung und Verantwortlichkeit, die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese

1. die Verarbeitung oder Nutzung personenbezogener Daten in oder unmittelbar aus Dateien regeln oder

2. die Verwendung personenbezogener Informationen außerhalb von Dateien regeln, wenn der Betroffene dem Bundesbeauftragten hinreichende Anhaltspunkte dafür darlegt, daß er dabei in seinen Rechten verletzt worden ist, oder dem Bundesbeauftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen; die Kontrolle ist auf den Einzelfall beschränkt.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Das Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird eingeschränkt, soweit dies zur Ausübung der Kontrolle bei den speichernden Stellen der Deutschen Bundespost erforderlich ist. Das Kontrollrecht erstreckt sich mit Ausnahme von Nummer 2 nicht auf den Inhalt des Post- und Fernmeldeverkehrs. Der Kontrolle durch den Bundesbeauftragten unterliegen nicht:

1. personenbezogene Daten, die durch besonderes Gesetz ausdrücklich von der Kontrolle durch den Bundesbeauftragten ausgenommen sind,
2. personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 GG unterliegen, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten, und
3. a) personenbezogene Daten, die dem Post- und Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes unterliegen,
 - b) personenbezogene Daten, die dem Steuergeheimnis nach § 30 der Abgabenordnung oder dem Arztgeheimnis unterliegen und
 - c) personenbezogene Daten in Personalakten oder in den Akten über die Sicherheitsüberprüfung,
 wenn der Betroffene der Kontrolle durch den Bundesbeauftragten widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 17 Abs. 2 Nr. 1 und 2 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht,

soweit die oberste Bundesbehörde im Einzelfall feststellt, daß die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 23 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, soweit ihre datenschutzrechtliche Kontrolle die Anwendung oder Ausführung von Bundesrecht zum Gegenstand hat.

§ 24

Weitere Aufgaben des Bundesbeauftragten für den Datenschutz; Datenregister

(1) Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 11 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 23 Abs. 1 Nr. 1 bis 3 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 34 hin.

(5) Der Bundesbeauftragte führt ein Register der Dateien, in denen personenbezogene Daten gespeichert werden. Das gilt nicht für die Dateien der in § 17 Abs. 2 Nr. 1 genannten Behörden sowie für Dateien nach § 16 Abs. 3. Die öffentlichen Stellen, deren Dateien in das Register aufgenommen werden, sind verpflichtet, dem Bundesbeauftragten eine Übersicht gemäß § 16 Abs. 2 Satz 2 Nr. 1 bis 6 zuzuliefern. Das Register kann von jedermann eingesehen werden. Die Angaben nach § 16 Abs. 2 Satz 2 Nr. 3 und 5 über Dateien der in § 17 Abs. 2 Nr. 2 genannten Behörden unterliegen nicht der Einsichtnahme. Der Bundesbeauftragte kann im Einzelfall für andere öffentliche Stellen mit deren Einverständnis festlegen, daß einzelne Angaben nicht der Einsichtnahme unterliegen.

2. die Verwendung personenbezogener Informationen außerhalb von Dateien regeln, wenn der Betroffene dem Bundesbeauftragten hinreichende Anhaltspunkte dafür darlegt, daß er dabei in seinen Rechten verletzt worden ist, oder dem Bundesbeauftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen; die Kontrolle ist auf den Einzelfall beschränkt.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Das Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird eingeschränkt, soweit dies zur Ausübung der Kontrolle bei den speichernden Stellen der Deutschen Bundespost erforderlich ist. Das Kontrollrecht erstreckt sich mit Ausnahme von Nummer 2 nicht auf den Inhalt des Post- und Fernmeldeverkehrs. Der Kontrolle durch den Bundesbeauftragten unterliegen nicht:

1. personenbezogene Daten, die durch besonderes Gesetz ausdrücklich von der Kontrolle durch den Bundesbeauftragten ausgenommen sind,
 2. personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 GG unterliegen, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten, und
 3. a) personenbezogene Daten, die dem Post- und Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes unterliegen,
 - b) personenbezogene Daten, die dem Steuergeheimnis nach § 30 der Abgabenordnung oder dem Arztgeheimnis unterliegen und
 - c) personenbezogene Daten in Personalakten oder in den Akten über die Sicherheitsüberprüfung,
- wenn der Betroffene der Kontrolle durch den Bundesbeauftragten widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 17 Abs. 2 Nr. 1 und 2 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht,

soweit die oberste Bundesbehörde im Einzelfall feststellt, daß die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 23 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, soweit ihre datenschutzrechtliche Kontrolle die Anwendung oder Ausführung von Bundesrecht zum Gegenstand hat.

§ 24

Weitere Aufgaben des Bundesbeauftragten für den Datenschutz; Datenregister

(1) Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 11 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 23 Abs. 1 Nr. 1 bis 3 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 34 hin.

(5) Der Bundesbeauftragte führt ein Register der Dateien, in denen personenbezogene Daten gespeichert werden. Das gilt nicht für die Dateien der in § 17 Abs. 2 Nr. 1 genannten Behörden sowie für Dateien nach § 16 Abs. 3. Die öffentlichen Stellen, deren Dateien in das Register aufgenommen werden, sind verpflichtet, dem Bundesbeauftragten eine Übersicht gemäß § 16 Abs. 2 Satz 2 Nr. 1 bis 6 zuzuleiten. Das Register kann von jedermann eingesehen werden. Die Angaben nach § 16 Abs. 2 Satz 2 Nr. 3 und 5 über Dateien der in § 17 Abs. 2 Nr. 2 genannten Behörden unterliegen nicht der Einsichtnahme. Der Bundesbeauftragte kann im Einzelfall für andere öffentliche Stellen mit deren Einverständnis festlegen, daß einzelne Angaben nicht der Einsichtnahme unterliegen.

Stellungnahme zum Bundesdatenschutzgesetz-Entwurf vom 6.4.1989

1. Vorgeschichte

Seit über sieben Jahren werden Entwürfe zur Novellierung des BDSG vorgelegt.¹ Allgemeine Begründung ist, die seit der Verabschiedung des BDSG im Jahre 1977 gemachten Erfahrungen und den technologischen Fortschritt auf dem Gebiet der ADV mit der Neufassung des BDSG zu berücksichtigen. Der vorliegende Regierungsentwurf weist gegenüber den Vorentwürfen vielfältige redaktionelle Änderungen auf, die zum Teil materielle Verbesserungen suggerieren, bei näherer Analyse jedoch die bisherigen Bedenken in aller Regel fortbestehen lassen. Die datenschutzrechtlichen Streitfragen der letzten Jahre werden - so das Urteil vorweg - voll zu Lasten der BürgerInnen entschieden. Im folgenden werden die Auswirkungen der geplanten Novellierung des BDSG insbesondere für die Arbeit der sog. Sicherheitsbehörden untersucht, soweit sie vom BDSG als Querschnittsgesetz betroffen sind.

2. Detalkritik

Zu § 1 Abs.3 Nr.1 und 2: Einschränkung des Geltungsbereichs

Nr.1: Nach Nr.1 sollen Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, von den Bestimmungen des BDSG freigestellt sein. Die tatsächlichen Auswirkungen dieser unscheinbaren Änderung gegenüber der bisherigen Gesetzeslage dürften insbesondere im Sicherheitsbereich erheblich sein. Diese Bestimmung ist interpretationsoffen, denn "verarbeitungstechnische Gründe" können für darüber hinausgehende Nutzungen Vorwand sein sowie diesem Vorschub leisten. Erinnerung sei an den bisher spektakulärsten Fall einer nach geltender Rechtslage unzulässigen, technisch bedingten Zwischendatei: die zentrale Erfassung aller "Kunden" bei der Herstellung des maschinenlesbaren Personalausweises. Hätte man wirklich jede anderweitige Nutzung gesetzlich ausschließen wollen, dann hätte man dies schlicht in den Gesetzestext hineinschreiben können.

Nr.2: Diese neue Bestimmung löst in bedrohlicher Weise den bisher strengen und unzweideutigen Begriff einer "internen Datei" auf. Nach bisherigem Recht ist eine Datei als "interne" dadurch definiert, daß sie nicht dazu bestimmt ist, aus ihr Daten weiterzugeben. Folglich gelten für interne Dateien nicht die datenschutzrechtlichen Schutzbestimmungen. Dieser Entw. läßt ausdrücklich dazu ein, aus internen Dateien "im Einzelfall" Daten weiterzugeben und zu nutzen. Diese Vorschrift muß man vor dem Hintergrund der aktuellen Praxis von Sicherheitsbehörden sehen, überall dort "interne" Dateien anzulegen, wo sie sich den gesetzlichen Bindungen der Datenschutzgesetze entziehen wollen - ein-

schließlich der Kontrolle durch die DS-Beauftragten. Insbesondere in Baden-Württemberg hat die Polizei gerne zu diesem Mittel gegriffen, um jede datenschutzrechtliche Kontrolle fernzuhalten. Absehbare künftige Praxis: Mit internen Dateien wird wie mit übrigen Dateien gearbeitet, d.h. aus ihnen wird "im Einzelfall" übermittelt und in sie eingespeichert, ohne daß sie datenschutzrechtlichen Kautelen und Kontrollen unterliegen.

Zu § 3 Abs. 2: Dateien-Begriff

Anders als im Vorentwurf vom 14.5.85 (vgl. CILIP Nr.21), hat man nun erneut auf eine Präzisierung des Dateien-Begriffs verzichtet und die bisherige Unklarheit im geltenden BDSG über die Dateien-Qualität gemischter Systeme (manuelle Aktenführung und ADV-Hinweissysteme) beibehalten. Es kann also jederzeit wieder der alte Streit aktiviert werden, ob Akten, die über Aktenerschließungssysteme auf ADV-Basis zu orten sind (wie der Kriminalaktennachweis KAN oder NADIS), unter den Dateibegriff fallen. Von Bedeutung ist dies in zweifacher Hinsicht: Erstens bleibt nach wie vor strittig, ob die DS-Beauftragten zur Kontrolle auf die einer Speicherung zugrundeliegenden Akten zurückgreifen dürfen. Zwar wurde nach anfänglichen Differenzen von Seiten der Exekutive dieses Argument nicht mehr benutzt und die Kontrollkompetenz der DS-Beauftragten auch über die Akten hingenommen - jedoch nicht als feste Rechtsposition akzeptiert.

Zwar soll der DS-Beauftragte (vgl. § 22) im **einzelnen** Beschwerdefall ausdrücklich auch auf das in den Akten gespeicherte Basiswissen zugreifen dürfen. Diese Beschränkung auf den einzelnen Beschwerdefall ist jedoch die rechtlich tückische Form, systematische Kontrollen außerhalb eines konkreten Beschwerdefalles als unzulässig zurückweisen zu können (vgl. die Kommentierung zum § 22).

Zweitens hat die fortbestehende Unklarheit im Dateien-Begriff auch für die Anwendung des BDSG selbst Folgen, denn es gilt nur für in Dateien gespeicherte Daten. Der aktuelle SPD-Entwurf zum BDSG (BT-Drs.11/3730) bezieht Akten in den Geltungsbereich des BDSG mit ein.

Zu § 3 Abs.3 Nr.3 b: Generelle Zulassung von online-Verfahren

Die hier erfolgende Neufassung des Übermittlungsbegriffs versteckt die folgenschwerste Veränderung dieses Entwurfs gegenüber dem Gesetz von 1977.

Nach dem Gesetz von 1977 gilt bei Einrichtung eines online-Verfahrens der **gesamte** Datenbestand als übermittelt. Dies hat zur Folge, daß auch für den gesamten Bestand eine Zugriffsberechtigung nachgewiesen werden muß. Die Rechtmäßigkeit des Zugriffs zu jeder Zeit auf jedes beliebige Datum ist nur innerhalb derselben Behörden und nur bei gemeinsamer Aufgabenstellung der betreffenden Stellen gegeben. Selbst

dann, wenn wie im Falle der Staatsschutzabteilungen der Länderpolizeien und der Landesämter für VfS gemeinsame Aufgaben vorliegen, ist die Einrichtung eines Direktabrufverfahrens nach dem Wortlaut des geltenden BDSG nicht zulässig.

Die Datenschutzbeauftragten erhielten dadurch ein begrenztes legalistisches Argument, um gegen die zunehmende Vernetzung (nicht nur im sogenannten Sicherheitsbereich) zu opponieren. Der Aufbau solcher Verbände und die Vorarbeiten dazu - für die Polizei betrifft dies insbesondere die Dateien der Meldebehörden, des Kraftfahrtbundesamtes und des Ausländerzentralregisters - waren Anlaß zu ständiger Kritik. Die Zunahme der Vernetzung konnte dadurch zumindest gebremst werden. Im Ergebnis lief diese Kritik auf sog. bereichsspezifische Datenschutzregelungen hinaus - z.B. im Melderecht oder im Gesetz über ZEVIS.

Die als "Fiktion" bezeichnete Auffassung des Übermittlungsbegriffs im geltenden BDSG, nach der bei online-Verfahren der gesamte Datenbestand als übermittelt anzusehen ist, wird im vorliegenden Entw. durch eine Formel ersetzt, die auch bei automatischen Abrufverfahren nur den einzelnen Abrufvorgang als Übermittlung bewertet. Gleichzeitig wird in § 9 Abs.1 die Einrichtung von online-Verfahren nur noch daran gebunden, daß diese "für die Aufgaben, Geschäftszwecke oder Ziele der speichernden Stelle oder des Empfängers angemessen" seien. Damit bedarf es also nicht mehr eines eigenständigen Gesetzes, sondern nur noch eines bürokratischen Federstrichs, um solche Verfahren einzurichten bzw. bestehende zu legalisieren.

Die Prüfung der Berechtigung zur Übermittlung des jeweiligen Einzeldatums wird in § 13 der anfragenden Stelle allein, dem Empfänger also, überantwortet.

Zu § 9: Automatisierte Abrufverfahren (online)

Hier werden in Fortführung des Änderungsvorschlages in § 3 Abs.3 Nr.3 die Rahmenbedingungen für die Zulassung und den Betrieb automatisierter Abrufverfahren aufgestellt. Anstelle einer bislang notwendigen spezialgesetzlichen Ermächtigung zur Einrichtung von online-Verfahren (vgl. Kommentierung zuvor) begnügt sich der Entw. mit einer nichtssagenden Angemessenheitsformel, die im Zweifelsfall immer zugunsten der Exekutive ausgehen wird. Zwar werden in Abs.2 die online-Anwender verpflichtet, Anlaß und Zweck des Abrufverfahrens, die Datenempfänger, die Art der zu übermittelnden Daten und die erforderlichen technischen und organisatorischen Maßnahmen schriftlich festzulegen. Die Betroffenen, also potentiell jede/r Bürger/in, erhalten jedoch kein Einsichtsrecht in diese, der generellen Zulässigkeitskontrolle der Systeme geltenden Unterlagen. Online-Verfahren bleiben hinter dem exekutiven Geheimnis-Kordon - nur der DS-Beauftragte ist "zu unterrichten".

Eine Scheinbegrenzung erhält die Bestimmung in Abs.3 Satz 2, nach der bei Installierung von online-Verfahren im Sicherheitsbereich die jeweiligen obersten Landes- und Bundesbehörden zustimmen müssen.

Der SPD-Entwurf unterscheidet sich in dieser Frage nur unwesentlich. Es soll für die Einrichtung von online-Anschlüssen ausreichen, wenn eine "Rechtsvorschrift" dies erlaubt, d.h. eine ministerielle Rechtsverordnung (§ 4 SPD-Entw., BT-Drs. 11/3730).

Zu § 12:

Datenspeicherung, -veränderung und -nutzung, Zweckbindung

Dieser Paragraph hebt in Verbindung mit § 13 systematisch das prinzipielle Verbot der Zweckentfremdung von Daten auf. Seine besondere Bedeutung erhält § 12 Abs.2 und der dort aufgeführte Katalog von Zulässigkeitsvoraussetzungen dadurch, daß er durch Verweis auf § 13 Abs.1 Nr.2 und § 14 Abs.1 Nr.1 zugleich auch die bisherigen Grenzen der Weitergabe innerhalb der öffentlichen Verwaltung und der Weitergabe an private Stellen durchbricht.

Danach sollen die Daten, die innerhalb einer Behörde gem. Abs.3 zu anderen Zwecken als den ursprünglich vorgesehenen genutzt bzw. verändert werden dürfen, unter den gleichen Voraussetzungen an alle übrigen Stellen der öffentlichen Verwaltung und an beliebige private Stellen weitergegeben werden können. Hervorzuheben ist besonders Abs.3 Nr.3. Danach soll es genügen, daß die gewünschte Zweckentfremdung "offensichtlich" im Interesse des Betroffenen liegt und von seiner mutmaßlichen Einwilligung gedeckt sei (worüber ausschließlich die Behörde selbst entscheidet!). Mit Nr.4 wird endgültig Abschied genommen vom Prinzip des Zweckentfremdungsverbotes und des Grundsatzes, daß Daten beim Betroffenen zu erheben sind. Denn die Verarbeitung und in der Konsequenz auch die Weitergabe einmal erhobener Daten soll zu allen zulässigen Zwecken ermöglicht werden, wenn nur eine anderwärts vorhandene Rechtsgrundlage theoretisch die Erhebung dieser Daten zulassen würde. Und diese Voraussetzung dürfte für fast alle bei den öffentlichen Verwaltungen gespeicherten Daten vorliegen, da die öffentliche Verwaltung Daten nur aufgrund gesetzlicher Ermächtigungen erheben darf.

Die in den Nr. 6, 7 und 8 zugelassenen Durchbrechungen bedeuten einen umfassenden Vorbehalt zugunsten der Sicherheitsbehörden (vgl. die Verweisungsvorschriften in §§ 13 und 14 sowie die Parallelermächtigungen in den Entw. zum BVerfSchG, MAD-G und BND-G in dieser Ausgabe). Hierauf wird man sich berufen, wenn es wieder einmal um die Zulässigkeit von Rasterfahndungen oder sonstiger massenhafter Durchdringung oder Weitergaben gehen sollte. Da die entsprechenden, hier in Nr.6, 7 und 8 zugelassenen Befugnisse zugleich auch in den Novellierungsvorschlägen zum Polizeirecht (Musterentwurf) und der StPO vorgesehen sind, muß angenommen werden, daß man sie hier nur für den Fall aufgenommen hat, daß die entsprechenden Novellierungen des Polizeirechts und der StPO sich politisch nicht so schnell durchsetzen lassen.

Eine weitere schwerwiegende Verschlechterung des vorliegenden Entwurfs gegenüber dem von 1986 ist der Wegfall einer besonderen Schutzbestimmung für Daten, die einem Berufs- oder Amtsgeheimnis

(z.B. ärztliche Schweigepflicht, Anwaltsgeheimnis etc.) unterliegen (vgl. CILIP 23, dort § 9 Abs.3). Diese Daten können damit wie alle anderen Daten gespeichert und nach § 13 unter denselben minimalen Voraussetzungen wie diese an andere Behörden übermittelt werden. Wissen andere öffentliche Stellen, daß solche besonders schützenswerte Daten gespeichert sind, so können sie auch ihre Übermittlung fordern und werden dabei auf keine besonderen gesetzlichen Hürden des BDSG treffen - es sei denn, bereichsspezifische Gesetze schlossen die Übermittlung ausdrücklich aus.

Zu § 13: Datenübermittlung innerhalb des öffentlichen Bereiches

Zu den bisher schon geltenden Übermittlungsbefugnissen tritt durch Verweis auf § 12 Abs.2 und dem dort aufgezählten Katalog eine zusätzliche Palette von Übermittlungsbefugnissen hinzu. Dadurch verändert das BDSG seinen Charakter. War es bisher zumindest strittig, ob § 9 des derzeit geltenden BDSG (§ 12 des Entw.) allein schon eine Befugnis zur Übermittlung von Daten darstellte, oder ob § 9 BDSG nur auf die Notwendigkeit einer besonderen Befugnisnorm außerhalb der allgemeinen Datenschutzgesetze verwies, so ist nach der Entwurfsfassung der § 13 zu einer sich selbst genügenden Befugnisnorm umstrukturiert worden. Dies wird mittels der Verweisung auf die Vorschriften in § 12 Abs.2 ermöglicht. Denn dadurch werden die geringen Voraussetzungen, die für die Verarbeitung der Daten innerhalb einer Stelle gelten sollten, auch zur Voraussetzung der Übermittlung gemacht. So soll z.B. die von der Behörde als mutmaßlich angenommene Einwilligung der Betroffenen ausreichen, oder es soll die "Abwehr drohender Gefahren für das Gemeinwohl" eine ausreichende Legitimation zur Weitergabe sein. (Die Formel von der "Gefahr für das Gemeinwohl" lehnt sich nur sprachlich an die relativ festumrissene Formel von der "Gefahr für die öffentliche Sicherheit und Ordnung" des Polizeirechts an. Die Gemeinwohl-Formel ist ohne begrenzende Konturen und meint das allgemeine Wohl, so wie es die auslegende Behörde verstehen darf.)

In § 13 Abs.2 und 3 wird eine Änderung und Einschränkung der bisherigen, ohnehin weiten Grundsätze des Amtshilferechts vorgenommen. Bisher trugen sowohl die übermittelnde als auch die ersuchende Behörde Verantwortung für die Rechtmäßigkeit. Nun wird diese Verantwortungslast im Regelfall auf die anfragende Behörde allein übertragen. Dies entspricht im übrigen auch der Systematik der VerfSchG-, MAD-G- und BND-G-Entwürfe.

Die ersuchte Behörde hat überhaupt nur noch dann ein Recht, die Zulässigkeit der Datenübermittlung zu überprüfen, wenn hierzu ein "besonderer Anlaß" besteht. Die ersuchende und an den Daten Interessierte Behörde hat also ihre eigene Berechtigung zu prüfen - ein Unding.

Zu § 14:**Datenübermittlung an Stellen außerhalb des öffentlichen Bereiches**

Bedeutsam ist auch hier wieder die Umgehung des spezifischen Gesetzesvorbehalts durch den Verweis auf die Voraussetzungen in § 12 Abs.2. Es gilt das zu §§ 12 und 13 Gesagte. Gespeicherte Daten können also unter den gleichen - lächerlich geringen - Voraussetzungen an Private weitergegeben werden wie innerhalb der öffentlichen Verwaltung.

Zu § 15:**Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes**

Es gilt das zu § 12 und § 13 Gesagte. Ausländische Geheimdienste und Polizeidienststellen sind nach dieser Vorschrift mit bundesrepublikanischen Stellen gleichberechtigte Adressaten personenbezogener Daten (vgl. die "bereichsspezifischen" Regelungen in § 14 Entwurf BVErfSchG).

Zu § 17:**Auskunft an den Betroffenen**

Generell soll das Auskunftsrecht des Einzelnen über ihn betreffende Daten dahingehend erweitert und verbessert werden, daß zusätzlich die Herkunft der Daten sowie deren eventuelle Empfänger in die Auskunftspflichtung miteinbezogen sind. Für den Sicherheitsbereich bleibt jedoch alles beim Alten. Abs.2 stellt klar, was durch die Rechtsprechung und durch die Praxis bereits gehandhabt wird: Den Sicherheitsbehörden ist es **nicht untersagt**, Auskunft zu erteilen.

Die "Sicherheitsbehörden" nach Abs.2 Nr.1 (VfS, BND, MAD sowie "andere Behörden des Bundesministers der Verteidigung") können nach ihrem eigenen Gusto Auskunft erteilen oder nicht. Die Sicherheitsbehörden in Nr.2 hingegen (Staatsanwaltschaft und Polizei) sind zur Auskunft verpflichtet, es sei denn, daß oem das "öffentliche Interesse" entgegensteht. Diese Klarstellung entspricht der keineswegs bürgerfreundlichen einschlägigen Rechtsprechung (vgl. Hase in CILIP Nr. 16; Blanke in Nr. 28) .

Hintergrund für dieses Zwei-Klassen-Auskunftsrecht ist die Befürchtung, daß die Geheimdienste unter Legitimationsdruck geraten könnten, in dessen Gefolge sie zwar nicht die verweigerten Daten selbst preisgeben müßten, aber doch von ihnen insbesondere im Gerichtsverfahren erwartet würde, ihre Weigerung und die Gründe dafür zumindest erahnbar werden zu lassen. Während diese Konsequenz für den Bereich der Polizei für noch hinnehmbar gehalten wird, sollen die Geheimdienste erst gar nicht in diese Lage geraten.

Reduzierte sich das gerichtliche Prüfungsrecht bisher allein auf die Frage, ob die Behörde die Auskunft pauschal - und damit in unzulässig-

ger Weise - abgelehnt hatte oder ob sie erkennen ließ, daß sie sich zumindest Gedanken darüber gemacht hatte (Betätigung des Ermessens), so wird für den Bereich der Geheimdienste nun auch de jure jede gerichtliche Überprüfung ausgeschlossen. Für sie gilt das Justizgewährleistungsrecht (Art.19 Abs.4 GG) nicht. Konsequenz heißt es deshalb auch in Abs.4 Satz 2, daß Auskunftsverweigerungen der Geheimdienste generell keiner Begründung bedürfen. Als Trostpflaster kann der Bundesdatenschutzbeauftragte eingeschaltet werden (Abs.5).
Im übrigen: Die Auskunftsanfrage soll kostenlos werden.

Zu § 18 Abs. 6:

Pflicht zur nachträglichen Berichtigung bereits übermittelter Daten

Diese Vorschrift ist einer der wenigen Änderungsvorschläge, die nicht zu Lasten des Bürgers gehen. Sie ist aber zugleich insoweit von begrenztem Wert, als der Bürger selbst mangels eines konsequenten Auskunftsanspruchs gegenüber den "Sicherheits"-Behörden kaum eine Chance hat, ihn betreffende Daten als falsch zu identifizieren. Diese Regelung stellt eine Verantwortung der übermittelnden Stelle für ihre Datentransaktion her und verpflichtet sie, Empfänger von falschen oder mittlerweile gesperrten (z.B. bestrittenen) Daten von dieser Tatsache zu unterrichten. Der Novellierungsvorschlag beschränkt diese Pflicht auf "regelmäßige" Datenübermittlungen, so daß Einzelfallübermittlungen ausscheiden. Die Realisierung dieser Pflicht setzt voraus, daß die übermittelnde Behörde einzelne Übermittlungsakte und -empfänger protokolliert hat. Dies ist bei "regelmäßigen" Datenübermittlungen immer der Fall, nicht aber bei einzelbezogenen Übermittlungsakten, die bei den Sicherheitsbehörden dominieren.

Hier entstünden bei Ausweitung der Berichtigungspflicht auch auf diesen Bereich neue, wiederum sehr sensible Protokolldateien mit eigenem Erklärungs- und Nutzungswert. Diese Gefahr verhindert zwar die Beschränkung auf "regelmäßige" Übermittlungen, sie legt jedoch das Risiko des Fortbestehens und Benutzens falscher Daten allein dem Bürger auf, der schließlich die Folgen solcher Falschspeicherung zu tragen hat. Welche Bedeutung eine solche Pflicht zur nachträglichen Berichtigung bereits übermittelter Daten insbesondere im Sicherheitsbereich haben kann, ist an dem großen Umfang systematischer Doppel- oder Vielfachsicherungen im Sicherheitsbereich ablesbar.²

Zu § 22:

Verminderung der Kontrollbefugnisse des Bundesdatenschutzbeauftragten

Der Entwurf nimmt die Kontrollbefugnisse des Datenschutzbeauftragten in erheblicher Weise gegenüber der bislang geltenden Gesetzeslage zurück. Die ausdrückliche Festschreibung der Kompetenz des DS-Beauftragten in Abs.1, bei seinen Prüfungen auch auf außerhalb von Dateien gespeichertes Datenmaterial (Akten) zurückgreifen zu können, ist bei

realistischer Sicht nicht als die propagierte Ausdehnung der Kontrollkompetenz zu bewerten. Vielmehr ist mit dieser Regelung zugleich eine - unbenannte - Einschränkung verbunden.

Der Entw. bindet die Überprüfung von Akten an eine besonders begründete Beschwerde eines Betroffenen sowie ausdrücklich auf den "Einzelfall". Die Begr. führt mit aller Deutlichkeit aus, daß mit dieser Beschränkung auf den Einzelfall verhindert werden soll, den DS-Beauftragten "zu einem umfassenden Kontrollorgan" zu machen.

Bisher wurde den DS-Beauftragten in vielen Fällen mit unterschiedlicher Intensität der Zugang zu in Akten gesammeltem Datenmaterial verweigert, obwohl sich nur durch gleichzeitige Prüfung der in den Akten gesammelten Informationen die Zulässigkeit der in den elektronischen Systemen gespeicherten Daten hat überprüfen lassen. Zwar wird den Datenschützern diese Befugnis nun unbestreitbar eingeräumt. Im Gegenzug werden jedoch die Kompetenzen bestritten, systematische Kontrolle von Informationsstrukturen und Praktiken vorzunehmen. Das folgt aus der Gesetzeslogik; die gesetzliche Zulassung nur der Einzelfallkompetenz schließt jede darüberhinausgehende Kompetenz aus. Für die Fälle nur vager Verdachte unzulässiger Datenverarbeitungspraxis, ohne daß der DS-Beauftragte einen bestimmten Betroffenen nennen kann, wird er vor verschlossenen (Akten-) Türen stehen.

Wesentliche Einschränkungen gegenüber der bisherigen Gesetzeslage enthält auch Abs.2. Es werden umfänglichste Datenbereiche der öffentlichen Verwaltung von der Kontrolle dann ausgenommen, "wenn der Betroffene (der Speicherung, d. Red.) der Kontrolle durch den Bundesbeauftragten widerspricht". Das hört sich nach besonderer Respektierung des Rechts auf informationelle Selbstbestimmung an. Tatsächlich verbirgt sich dahinter ein raffiniert gestricktes Muster, das in aller Regel zum gänzlichen Kontrollausschluß des DS-Beauftragten führen wird. In der Begr. heißt es hierzu: "Die Befugnis des Betroffenen, zu widersprechen, setzt voraus, daß er hierzu Gelegenheit hat". Wo aber der Betroffene nichts von seiner Speicherung weiß, und das ist im Geheimbereich die Regel, hat er auch keine Gelegenheit, zu widersprechen; folglich entfällt damit aber auch das Kontrollrecht des Datenschutzbeauftragten.

In der amtl. Begr. heißt es freilich, daß man eine solche Konsequenz nicht wolle. Anstelle aber auf das Prinzip der Vorabewilligung ganz zu verzichten, schlägt die Begr. (nicht der Gesetzestext selbst!) vor, daß in Vollzug des Gesetzes zukünftig "in den Hausnachrichten einer Behörde oder durch eine entsprechende Formularrubrik in den Unterlagen für die Einstellung oder für die Sicherheitsüberprüfung" ein genereller Hinweis auf die Möglichkeit des Widerspruchs aufgenommen werden solle. Wie freilich z.B. vor einer Kontrolle der Rauschgift-Dateien des Bundesfinanzministers die Möglichkeit zum Widerspruch des einzelnen Betroffenen erfolgen kann, bleibt offen. Der einzige Zweck dieser Widerspruchsmöglichkeit scheint zu sein, den betroffenen Behörden erweiterte Möglichkeiten zur Verweigerung datenschutzrechtlicher Kontrolle einzuräumen.

Schließlich verrechtlicht der Entw. zugunsten der Exekutive bisherige Streitfragen um die Kontrollkompetenz der DS-Beauftragten.

Nunmehr ausdrücklich ausgeschlossen wird der DS-Beauftragte von der Kontrolle folgender Datenbereiche:

* Daten, die durch G-10-Abhörmaßnahmen der Geheimdienste gewonnen worden sind. Dies entspricht der Praxis der G-10-Kommission des Bundestages, die dem Datenschutzbeauftragten auch bisher schon die Kontrolle dieser Daten verweigerte.

* Dies gilt gleichermaßen für Steuerdaten. Als Steuerdaten werden auch Daten im Kontext der Rauschgiftfahndung qualifiziert, da Drogenhandel u.a. den Tatbestand der Steuerhinterziehung erfüllt. Auch hier hatte der Bundesfinanzminister dem DS-Beauftragtem schon bisher contra legem den Kontrollzugang verwehrt.

* Schließlich werden als besonders umfängliche Bereiche die sogenannten Personalakten und jene Akten ausdrücklich ausgeschlossen, die bei Sicherheitsüberprüfungen angelegt worden sind.

Auch hier hatten die Bundesbehörden bisher schon den Zugang zum Teil mit Erfolg verweigert.

Zu § 24:

Aufgaben des Bundesdatenschutzbeauftragten

Hervorzuheben ist vor allem Abs.1, also die Änderung des Berichtszeitraumes. Die jährlichen Vorstellungen der Tätigkeitsberichte haben mittlerweile in den Medien einen festen Platz errungen. Die dadurch insbesondere den Sicherheitsbehörden regelmäßig zuteil gewordene Aufmerksamkeit war diesen von Anfang an unbequem und abschaffenswert. Rheinland-Pfalz führte 1983 den Zwei-Jahres-Berichtsrythmus ein, Bayern folgte. Konsequenz: die Informationsfülle der Tätigkeitsberichte halbiert sich, was vor allem auf Kosten der (sonst nirgendwo anders gegebenen) Detailfülle für die Praxis und Probleme sicherheitsbehördlicher Datenverarbeitung geht. Die zukünftige zweijährliche Erscheinungsweise dient ganz eindeutig der Verminderung der öffentlichen Wirkung der Datenschutzkontrollinstanzen.

Jüngst wurde bekannt (FR v. 28.1.89), daß auch die Unionsparteien dem zuvor von der SPD und den Grünen gemachtem Vorschlag folgen wollen, den DS-Beauftragten nicht mehr vom Bundesinnenminister ernennen, sondern vom Bundestag wählen zu lassen: ein untauglicher Versuch, einer Institution Wirkung verschaffen zu wollen, der ihr in ihren Kontrollbefugnissen versagt wird.

3. Resümee:

Die hier kurz beschriebenen, aber wesentlichen Änderungsvorschläge des Entw. für die Datenverarbeitung im Sicherheitsbereich lassen sich auf einen ebenfalls kurzen Nenner bringen: Die Befugnisse zur Verarbeitung von Daten sind erheblich erweitert worden, ebenso die Befugnisse zur Weitergabe. Demgegenüber wurden die Kontrollbefugnisse des Bundesdatenschutzbeauftragten an einigen Stellen unwesentlich erweitert, überwiegend jedoch enger gefaßt.

Die Auskunftsrechte sind noch weiter eingeschränkt worden - obwohl sie bisher schon nahezu bedeutungslos waren. Auf der konzeptionellen Seite ist darauf verzichtet worden, die Mängel einer rein individualrechtlichen Konzeption des Datenschutzes zu beseitigen, indem strukturelle Datenschutzvorschriften aufgenommen werden. Aber nur dadurch ließe sich die gegenwärtig bereits vollzogene und noch zu erwartende Vernetzung der öffentlichen Verwaltung durch übergreifende Verbundsysteme rechtlicher Steuerung überhaupt zugänglich machen. Der Novellierung des BDSG kommt im Hinblick auf die Datenschutzgesetze der Länder Leitfunktion zu. Deren Anpassung an den Entw. des BDSG beschäftigt bereits die Ministerien der Länder.

Anmerkungen:

1 vgl. CILIP Nr.15 zum Referenten-Entw. des Zimmermann-BMI vom 23.6.83; CILIP Nr.18 zum Entw. der SPD-Bundestagsfraktion aus dem Jahre 1984 (BT-Drs.10/1180); CILIP Nr.21 Regierungsentw. vom 14.5.85; CILIP Nr.23 Regierungsentw. 1986 (BT-Drs.10/4737) und CILIP 29, Regierungsentw. vom 5.11.87

2 Zum Ausmaß solcher Doppel- und Vielfachspeicherungen wird auf die Ausführungen zu § 10 f des Musterentwurfs Polizeirecht verwiesen (vgl. CILIP Nr.21) sowie auf den Auszug aus dem 7. Tätigkeitsbericht des Bundesdatenschutzbeauftragten in CILIP Nr.23, S. 98).

PSYCHOLOGIE & GESELLSCHAFTS

KRITIK

49/50

ISBN 3 - 925007 - 49 - 0



Frauen & Psychologie III

INHALT

THEMATISCHE BEITRÄGE

Christiane Schmerl
Die Frau im Mond:
weit entfernt, doch klar sichtbar.
Feministische Psychologie in der BRD

Birgit Rommelspacher
Die Sucht, zu sehr zu lieben:
die neue Krankheit der Frau?

Ruth Großmaß
Nicht die Mutter ist schuld,
sondern „nur“ ihr Geschlecht -
Nancy Chodorova Analyse weiblichen Muttertums

Virginia Davidson
Das namenlose Problem der Psychotherapie -
Sexualität zwischen Therapeuten
und Patientinnen

Renate Kahle
„Frauen ran an die Computer!“?
Technikangst und Technikdistanz
von Frauen in Computerkursen.

Christiane Schmerl
Erfahrungen von Feministinnen
mit dem Psychologiestudium

Kordula Langhof
Alice Rühle-Gerstel (1884 - 1943) - ein Porträt

REZENSIONEN

AKTUALITÄTEN / TERMINE

Eine psychologisch-kritische Zeitschrift für Psychologen, Pädagogen, Sozialwissenschaftler in Theorie und Praxis Einzelheft 1,- DM Doppelheft 1,80 DM Jahresabonnement 40,- DM Student und an. Arbeitslose u.ä. 14,- DM jeweils zzgl. Porto
Erhältlich in jeder guten Buchhandlung oder direkt bei der Redaktion der P & G Bürgerbuschweg 47 D-2100 Oldenburg, Tel. (0441) 919126

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 6. Juni 1988 zur

Neufassung des Bundesdatenschutzgesetzes

Die Datenschutzbeauftragten stellen mit Bedauern fest, daß der vorliegende Entwurf einer Neufassung des Bundesdatenschutzgesetzes im wesentlichen die gleichen Mängel aufweist wie der entsprechende Entwurf der 10. Legislaturperiode des Deutschen Bundestages. Diese Mängel haben die Datenschutzbeauftragten bereits in ihrer Entschließung vom 14. März 1986 aufgezeigt.

Die Datenschutzbeauftragten halten es insbesondere für verfehlt, das allgemeine Datenschutzrecht aufzusplitteln in ein streng auf die Datenverarbeitung in Dateien bezogenes Bundesdatenschutzgesetz und ein den Datenschutz in Akten regelndes Verwaltungsverfahrensgesetz, das weite und wichtige Verwaltungsbereiche (z. B. Finanzverwaltung und Sozialverwaltung) ebensowenig erfaßt wie die Strafverfolgung, und dessen Einhaltung sich überdies weitgehend der Datenschutzkontrolle entzieht.

Die Datenschutzbeauftragten stellen ferner fest, daß bei der Vorbereitung des Entwurfs ihre Empfehlungen sowie die zwischenzeitlich von einigen Bundesländern erlassenen, in wesentlichen Punkten vorbildlichen Neuregelungen des Datenschutzes nahezu unberücksichtigt geblieben sind.

Die Datenschutzbeauftragten verkennen nicht, daß auch der jetzige Entwurf einige Verbesserungen gegenüber dem geltenden Recht aufweist. Insgesamt jedoch werden die in der Begründung des Entwurfs genannten Ziele der beabsichtigten Weiterentwicklung des Bundesdatenschutzgesetzes nicht erreicht:

- Die Anpassung an die Grundsätze des Urteils des Bundesverfassungsgerichts vom 15. 12. 1983 zum Volkszählungsgesetz ist in mehrfacher Hinsicht nicht gelungen: so enthält der Entwurf keine ausdrückliche Regelung der Datenerhebung, obwohl gerade diese den Bürgern unmittelbar belastet; die geplante Regelung im Verwaltungsverfahrensgesetz reicht nicht aus. Auch erfährt der Grundsatz der Zweckbindung zu weitgehende Ausnahmen und die Transparenz der Datenverarbeitung, insbesondere das Recht des Betroffenen auf Auskunft, bleibt hinter verfassungsrechtlichen Anforderungen zurück.
- Dem technologischen Fortschritt auf dem Gebiet der Informations- und Kommunikationstechnik

(z. B. Arbeitsplatzcomputer, neue optische Speichermedien, Videoaufzeichnungen, Telekommunikation und Vernetzung) wird der Entwurf nicht gerecht. Der im Entwurf verwandte Dateibegriff und die Beibehaltung des bisherigen Katalogs technischer und organisatorischer Datensicherungsmaßnahmen vernachlässigen die technische Entwicklung.

- Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird insgesamt eingeschränkt, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und Verwendung personenbezogener Informationen außerhalb von Dateien. Keinesfalls kann eine Einschränkung der Kompetenz der Landesbeauftragten durch den Bundesgesetzgeber hingenommen werden.
- Die Datenschutzvorschriften für den nichtöffentlichen Bereich orientieren sich nicht an dem Grundsatz der Zweckbindung und räumen unvertretbare Verarbeitungsprivilegien ein.

Der Entwurf entspricht daher nicht den Erwartungen an ein zeitgemäßes Datenschutzrecht als Ausprägung des verfassungsrechtlich garantierten Rechts des Bürgers auf informationelle Selbstbestimmung. Dieses Recht ist erst jüngst durch das Bundesverfassungsgericht in seiner Entscheidung vom 9. März 1988 bestätigt worden. Dort heißt es:

„In dieses Recht wird nicht nur dann eingegriffen, wenn der Staat vom einzelnen die Bekanntgabe persönlicher Daten verlangt oder diese der automatisierten Datenverarbeitung zuführt . . . Das Recht auf informationelle Selbstbestimmung schützt vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und ist nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter Sonderregelungen beschränkt.“

Die Konsequenz daraus muß eine möglichst lückenlose und präzise Regelung des Datenschutzes sein, um Rechtssicherheit für Bürger und Verwaltung herzustellen.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 6. Juni 1988 zur

Neufassung des Bundesdatenschutzgesetzes

Die Datenschutzbeauftragten stellen mit Bedauern fest, daß der vorliegende Entwurf einer Neufassung des Bundesdatenschutzgesetzes im wesentlichen die gleichen Mängel aufweist wie der entsprechende Entwurf der 10. Legislaturperiode des Deutschen Bundestages. Diese Mängel haben die Datenschutzbeauftragten bereits in ihrer Entschließung vom 14. März 1986 aufgezeigt.

Die Datenschutzbeauftragten halten es insbesondere für verfehlt, das allgemeine Datenschutzrecht aufzusplitteln in ein streng auf die Datenverarbeitung in Dateien bezogenes Bundesdatenschutzgesetz und ein den Datenschutz in Akten regelndes Verwaltungsverfahrensgesetz, das weite und wichtige Verwaltungsbereiche (z. B. Finanzverwaltung und Sozialverwaltung) ebensowenig erfaßt wie die Strafverfolgung, und dessen Einhaltung sich überdies weitgehend der Datenschutzkontrolle entzieht.

Die Datenschutzbeauftragten stellen ferner fest, daß bei der Vorbereitung des Entwurfs ihre Empfehlungen sowie die zwischenzeitlich von einigen Bundesländern erlassenen, in wesentlichen Punkten vorbildlichen Neuregelungen des Datenschutzes nahezu unberücksichtigt geblieben sind.

Die Datenschutzbeauftragten verkennen nicht, daß auch der jetzige Entwurf einige Verbesserungen gegenüber dem geltenden Recht aufweist. Insgesamt jedoch werden die in der Begründung des Entwurfs genannten Ziele der beabsichtigten Weiterentwicklung des Bundesdatenschutzgesetzes nicht erreicht:

- Die Anpassung an die Grundsätze des Urteils des Bundesverfassungsgerichts vom 15. 12. 1983 zum Volkszählungsgesetz ist in mehrfacher Hinsicht nicht gelungen: so enthält der Entwurf keine ausdrückliche Regelung der Datenerhebung, obwohl gerade diese den Bürgern unmittelbar belastet; die geplante Regelung im Verwaltungsverfahrensgesetz reicht nicht aus. Auch erfährt der Grundsatz der Zweckbindung zu weitgehende Ausnahmen und die Transparenz der Datenverarbeitung, insbesondere das Recht des Betroffenen auf Auskunft, bleibt hinter verfassungsrechtlichen Anforderungen zurück.
- Dem technologischen Fortschritt auf dem Gebiet der Informations- und Kommunikationstechnik

(z. B. Arbeitsplatzcomputer, neue optische Speichermedien, Videoaufzeichnungen, Telekommunikation und Vernetzung) wird der Entwurf nicht gerecht. Der im Entwurf verwandte Dateibegriff und die Beibehaltung des bisherigen Katalogs technischer und organisatorischer Datensicherungsmaßnahmen vernachlässigen die technische Entwicklung.

- Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird insgesamt eingeschränkt, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und Verwendung personenbezogener Informationen außerhalb von Dateien. Keinesfalls kann eine Einschränkung der Kompetenz der Landesbeauftragten durch den Bundesgesetzgeber hingenommen werden.
- Die Datenschutzvorschriften für den nichtöffentlichen Bereich orientieren sich nicht an dem Grundsatz der Zweckbindung und räumen unvertretbare Verarbeitungsprivilegien ein.

Der Entwurf entspricht daher nicht den Erwartungen an ein zeitgemäßes Datenschutzrecht als Ausprägung des verfassungsrechtlich garantierten Rechts des Bürgers auf informationelle Selbstbestimmung. Dieses Recht ist erst jüngst durch das Bundesverfassungsgericht in seiner Entscheidung vom 9. März 1988 bestätigt worden. Dort heißt es:

„In dieses Recht wird nicht nur dann eingegriffen, wenn der Staat vom einzelnen die Bekanntgabe persönlicher Daten verlangt oder diese der automatisierten Datenverarbeitung zuführt . . . Das Recht auf informationelle Selbstbestimmung schützt vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und ist nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter Sonderregelungen beschränkt.“

Die Konsequenz daraus muß eine möglichst lückenlose und präzise Regelung des Datenschutzes sein, um Rechtssicherheit für Bürger und Verwaltung herzustellen.

Dokumentation:

Drucksache 11/4306

Deutscher Bundestag – 11. Wahlperiode

Artikel 2

Änderung des Verwaltungsverfahrensgesetzes

Das Verwaltungsverfahrensgesetz vom 25. Mai 1976 (BGBl. I S. 1253), geändert durch Artikel 7 Nr. 4 des Gesetzes vom 2. Juli 1976 (BGBl. I S. 1749), wird wie folgt geändert:

.§ 3 a

Erhebung

(1) Erheben ist das Beschaffen von Informationen über persönliche und sächliche Verhältnisse einer natürlichen Person (personenbezogene Informationen) beim Betroffenen oder bei anderen Personen oder Stellen im Rahmen öffentlich-rechtlicher Verwaltungstätigkeit.

(2) Personenbezogene Informationen sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht,
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
 - b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Informationen beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. Werden sie beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 3 b

Geheimhaltung

Die Behörde darf personenbezogene Informationen sowie Betriebs- und Geschäftsgeheimnisse nicht unbefugt offenbaren.

§ 3 c

Zweckbindung

(1) Die Behörde darf von ihr erhobene personenbezogene Informationen verwenden oder übermitteln, soweit dies dem Zweck der Erhebung dient und zur Erfüllung ihrer Aufgaben oder der des Empfängers erforderlich ist. Die Behörde darf ihr übermittelte personenbezogene Informationen für den Zweck verwenden oder übermitteln, zu dessen Erfüllung sie ihr mitgeteilt worden sind.

(2) Das Verwenden oder Übermitteln personenbezogener Informationen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies erlaubt oder anordnet,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, daß es im Interesse des Betroffenen liegt und er in Kenntnis des anderen Zwecks einwilligen würde,
4. die Informationen für den anderen Zweck auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht beim Betroffenen erhoben werden dürfen,
5. die Informationen aus allgemein zugänglichen Quellen entnommen werden können oder die Behörde sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder von Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist oder
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

Das Übermitteln personenbezogener Informationen an andere Personen oder an nicht-öffentliche Stellen ist zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Informationen glaubhaft macht und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Der Empfänger darf die übermittelten Informationen nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt worden sind. In den Fällen der Übermittlung nach Satz 2 unterrichtet die Behörde den Betroffenen von der Übermittlung; dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(3) Eine Verwendung oder Übermittlung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die Behörde dient; dies gilt auch für die Verwendung oder Übermittlung zu Ausbildungs- und Prüfungszwecken durch die Behörde.

(4) Die Behörde darf personenbezogene Informationen, von denen sie auf andere Weise als nach Absatz 1 oder 2 Kenntnis erlangt hat oder die ihr von Personen oder von nicht-öffentlichen Stellen unverlangt mitgeteilt worden sind, verwenden oder übermitteln, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist; im übrigen ist eine Übermittlung unter den Voraussetzungen des Absatzes 2 zulässig.

(5) Sind personenbezogene Informationen, die nach den Absätzen 1 bis 4 übermittelt werden dürfen, mit weiteren personenbezogenen Informationen des Betroffenen oder eines Dritten so verbunden, daß sie nicht oder nur mit unvertretbarem Aufwand voneinander getrennt werden können, darf die Behörde auch diese übermitteln; dies gilt nicht, wenn berechtigte Interessen des Betroffenen oder des Dritten an der Geheimhaltung der Informationen im Einzelfall offensichtlich überwiegen. Unter den Voraussetzungen des Satzes 1 übermittelte weitere Informationen dürfen vom Empfänger nicht verwendet oder übermittelt werden.

§ 3 e

Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag über personenbezogene Informationen, welche die Behörde über ihn besitzt, Auskunft zu erteilen, soweit der Betroffene Angaben macht, die das Auffinden der Informationen ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Auf Verlangen des Betroffenen sind in die Auskunft nach Satz 1 die Herkunft und die Empfänger personenbezogener Informationen einzubeziehen. Über die Form der Erteilung der Auskunft entscheidet die Behörde nach pflichtgemäßem Ermessen; dabei dürfen berechtigte Interessen Dritter nicht beeinträchtigt werden.

(2) Eine Verpflichtung zur Erteilung der Auskunft besteht nicht

1. für die Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung,
2. für die Behörden der Polizei, soweit eine Abwägung ergibt, daß das öffentliche Interesse, die Auskunft nicht zu erteilen, das Interesse des Betroffenen an der Auskunftserteilung überwiegt.

Bezieht sich die Auskunftserteilung auf die Herkunft personenbezogener Daten von in Nummer 1 genannten Behörden, so ist sie nur mit Zustimmung dieser Behörden zulässig; dies gilt auch für die Auskunft über die Übermittlung an diese Behörden. Für die Versagung der Zustimmung gilt Satz 1 Nr. 1 entsprechend. Für die Ablehnung der Auskunftserteilung gilt Absatz 4 Satz 2 entsprechend.

(3) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der Aufgaben der Behörde gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
3. die personenbezogenen Informationen oder die Tatsache, daß die Behörde Kenntnis von ihnen hat, nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf welche die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die Ablehnung der Auskunftserteilung durch die in Absatz 2 Nr. 1 genannten Behörden braucht nicht begründet zu werden.

(5) § 17 Abs. 5 des Bundesdatenschutzgesetzes gilt entsprechend.

§ 3 f

Berichtigung und Sperrung personenbezogener Informationen

(1) Wird festgestellt, daß personenbezogene Informationen unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Personenbezogene Informationen sind zu sperren, wenn die Behörde im Einzelfall feststellt, daß ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Informationen für die künftige Aufgabenerfüllung der Behörde nicht mehr erforderlich sind. Gesperrte Informationen sind mit einem entsprechenden Vermerk zu versehen; sie sollen nicht mehr verwendet oder übermittelt werden."

4. § 26 wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird der Punkt durch ein Semikolon ersetzt und folgender Halbsatz angefügt:

„Die §§ 3a bis 3c und § 3f bleiben unberührt.“

b) Absatz 2 Satz 3 erhält folgende Fassung:

„Eine weitergehende Pflicht, bei der Ermittlung des Sachverhalts mitzuwirken, insbesondere eine Pflicht zum persönlichen Erscheinen, zur Angabe von Informationen, die personenbezogen oder Betriebs- und Geschäftsgeheimnisse sind, sowie zur Aussage, besteht nur, soweit sie durch Rechtsvorschrift besonders vorgesehen ist.“

5. § 30 wird aufgehoben.

Stellungnahme zur "Änderung des Verwaltungsverfahrensgesetzes" - Entwurf vom 6.4.89

BDSG und Verwaltungsverfahrensgesetz

Die vorliegenden Änderungen des Verwaltungsverfahrensgesetzes (VwVfG) sind auf dem Hintergrund des Datenschutzgesetzes zu betrachten. Im BDSG-Entw. hat die Koalition einen restriktiven Dateienbegriff durchgesetzt, der nur die Verarbeitung personenbezogener Daten in automatisierten Dateien, nicht aber in Akten oder manuell geführten Karteien umfaßt. Ausgenommen sind nur diejenigen Akten, die Grundlage von automatisierten Hinweisdateien sind. Das BDSG und der darin festgelegte besondere Schutz für personenbezogene Daten gilt damit für einen großen Bereich der Verwaltungstätigkeit nicht.

Der Umgang der öffentlichen Verwaltung mit Bürgerdaten in Akten und manuellen Karteien soll stattdessen im VwVfG geregelt werden, das allerdings für einen großen Bereich der öffentlichen Verwaltungen nicht gilt, darunter den der Finanz- und Strafverfolgungsbehörden. In den Entwürfen für die Geheimdienstgesetze werden die entsprechenden Regelungen des VwVfG systematisch außer Kraft gesetzt und durch eigenständige Regelungen ersetzt, die vom Datenschutz fast nichts mehr übrig lassen.

Schlechte Fortsetzung der BDSG-Regelungen

Es wäre allerdings irrig anzunehmen, der vorliegende Entwurf würde den Schutz von in Akten enthaltenen Daten, in der Diktion der Gesetzesmacher: Informationen, einfach nur gesetzestechnisch verschieben. Vielmehr werden die Anforderungen für die manuelle Informationsverarbeitung gegenüber den ihrerseits schon eingeschränkten Schutzvorkehrungen des BDSG noch weiter eingeschränkt mit der Begründung, "die erheblichen Unterschiede, die in der Gefährdungslage zwischen automatisierter und herkömmlicher Informationsverarbeitung bestehen", berücksichtigen zu wollen (vgl. allg.Begr.).

Die bereits in der Stellungnahme zum BDSG skizzierten und kritisierten Änderungen werden zum Teil wortgleich ins VwVfG übertragen. Dies gilt insbesondere für die Paragraphen, die die Nutzung, Verarbeitung und Weitergabe von Daten sowie den Auskunftsanspruch von Betroffenen behandeln. Zum anderen werden weitergehende Rechte des Bürgers, die sich aus dem allgemeinen Verwaltungsrecht ergeben, auf das Niveau des BDSG zurückgeschraubt.

Zu einzelnen Regelungen:

Erhebung (§ 3a):

Im BDSG ist keine eigenständige Rechtsgrundlage für die Erhebung enthalten. Aufgrund des restriktiven Dateienbegriffs wird die Erhebung von Daten als eine Form manueller Informationsverarbeitung gefaßt und ins VwVfG eingefügt. Die Erhebung soll grundsätzlich beim Betroffenen

erfolgen. Die Erhebung ohne seine Mitwirkung wird gebunden an das Vorliegen einer Rechtsvorschrift sowie an die Bedingung, daß die Erhebung "keinen unverhältnismäßigen Aufwand erfordern würde", eine Bedingung, die auch an anderen Stellen des Entwurfs wieder auftaucht. Diese - wenn auch eingeschränkte - Bindung an die Erhebung beim Betroffenen ist in den vorliegenden Geheimdienst-Gesetzesentwürfen ausdrücklich aufgehoben worden. Für die anderen gesetzlichen Regelungen des Datenschutzes im sog. Sicherheitsbereich wird diese Aufhebung ebenfalls zu erwarten sein.

Zweckbindung (§ 3c):

Auch hier operiert der Entwurf fast ausschließlich mit den schon kritisierten Regelungen des BDSG-Entw. In Abs.1 wird die Zweckbindung - Daten dürfen nur zu dem Zweck verwendet und weitergegeben werden, zu dem sie erhoben wurden - als Phrase formuliert, auf die dann in Abs.2 die Aufhebung folgt: Entsprechend dem Katalog des § 10 BDSG (Verarbeitung von Daten) wird die Zweckbindung weitgehend eingeschränkt: z.B. wenn es "offensichtlich ist, daß (die Verarbeitung und Übermittlung) im Interesse des Betroffenen liegt und er in Kenntnis des anderen Zwecks einwilligen würde", bei Strafverfolgung, Abwehr von Nachteilen für das Gemeinwohl oder bei Gefahr für die öffentliche Sicherheit etc.

Der Paragraph hat aber auch entscheidende Wirkung auf die geltenden Rechtsvorschriften der Amtshilfe (§ 4ff. des VwVfG). Eine ganz zentrale und sicher gewollte Folge dürfte sein, daß die Restriktionen der Amtshilfe-Regelungen im VwVfG nicht mehr für den Informationsbereich gelten werden.

Auskunftsrecht (§ 3e):

Die Auskunftsregelung entspricht im wesentlichen der des BDSG, d.h. sie schließt Auskunftsansprüche gegenüber den Geheimdiensten vollständig und gegenüber Polizei und Staatsanwaltschaft weitgehend aus. Wird im BDSG vom Antragsteller gefordert, daß er die Art der personenbezogenen Daten näher bezeichnen soll, so geht der vorliegende Paragraph sogar noch weiter. Der Antragsteller muß nicht nur sein Auskunftsinteresse offenlegen, dieses Interesse muß ferner auch so beschaffen sein, daß es der Verwaltung keinen unverhältnismäßigen Aufwand bereitet.

Berichtigung und Sperrung personenbezogener Informationen (§ 3f):

Die "Gnade des Vergessens", unter dem Begriff des "programmierten Vergessens" als eines der wesentlichen Prinzipien des Datenschutzes anerkannt, wird für die konventionelle Datenverarbeitung außer Kraft gesetzt. In § 3f Abs.2 wird bestimmt, daß Daten, die nicht mehr für die künftige Aufgabenerfüllung erforderlich sind, nicht gelöscht, sondern nur gesperrt werden dürfen und dann auch nur, wenn der Betroffene einen entsprechenden Antrag gestellt hat, in dem er ein "berechtigtes Interesse" nachweist. Selbst wenn als falsch erkannte Informationen sich in den Akten befinden, so soll dies nur in der Akte vermerkt werden, die falsche Information jedoch weiter vorhanden bleiben. In der

Begr. zu § 3f beruft man sich hierfür auf den prinzipiell richtigen Grundsatz der Aktenvollständigkeit, mit dem jederzeit die einzelnen Verwaltungshandlungen nachvollziehbar bleiben sollen. Die Übertragung und Anwendung dieses Grundsatzes auf die manuell geführten Informationen von Sicherheitsbehörden ist jedoch mehr als problematisch, denn der Anspruch auf richtige Daten ist umso wichtiger, wie die Intensität des Eingriffs in Grundrechte steigt. Die vorliegenden Regelungen für die Geheimdienste (vgl. § 9 BVerschG-Entw. und daran anschließend die §§ des MAD- und des BND-Gesetzes) lassen den Anspruch auf Berichtigung nur in Bezug auf Daten in automatisierten Dateien zu, ein Anspruch, der allerdings vom Bürger wegen des Fehlens eines Auskunftrechts kaum umgesetzt werden kann. Solange keine spezialgesetzlichen Regelungen existieren, bliebe damit der § 3f des VwVfG entscheidend.

Fazit

Die Verabschiedung dieses VwVfG würde dem Bürger bereits gegebene Rechtspositionen wieder wegnehmen. Aufgrund der Signalwirkung der Novellierung des VwVfG des Bundes für eine entsprechende Novellierung der VwVfG der Länder würde auch eine Verschlechterung gegenüber den wesentlich umfangreicheren Aktenbeständen der Sicherheitsbehörden der Länder eintreten. Überdies haben die Datenschutzbeauftragten keine generelle Kompetenz zur Überwachung der hier betroffenen konventionellen Informationsverarbeitung.

Libanon

DRINGENDER HILFSAUFRUF

- 500 000 Menschen auf der Flucht
- 300 Tote / 3000 Verletzte
- Vernichtung aller medizinischen Einrichtungen
- Abzug fast aller ausl. Hilfsorganisationen
- Meningitis- (Hirnhautentzündungs-) epidemie in mehreren Palästinenserlagern in Syrien und Nordlibanon

Medico stellt Impfstoff
für 20 000 Menschen zur Verfügung.

WIR BITTEN DRINGEND UM SPENDEN:

Postgiro Köln 6999-508 oder Frankfurter Sparkasse
Kto. 1800 Stichwort: 'Libanon'

Medico international, Obermainanlage 7,
6000 Frankfurt 1, Tel.: 069/ 499 00 41 - 2

III. Die Verpolizeifichung der Strafprozeßordnung

Das Strafverfahrensänderungsgesetz 1988

von Jörn Köhl *

Vorbemerkung der Redaktion

"Ich gehe davon aus", so der damalige rheinland-pfälzische Innenminister Schwarz 1976 im Spiegel (Nr.32, S.29 ff.), "daß der Versuch unternommen wird, die StPO dem Polizeirecht anzupassen." Schwarz äußerte sich seinerzeit zu dem Versuch, die Kontrollstellenregelung des "Musterentwurfs eines einheitlichen Polizeigesetzes" (MEPolG) der 70er Jahre in die StPO einzufügen - ein Versuch, der 1978 mit der Verabschiedung der sog. Raziengesetze im Bundestag mit Erfolg gekrönt wurde. Der Satz hat weitere Aktualität. 1985 beschloß die IMK einen neuerlichen Musterentwurf, mit dem sie auf den vom Volkszählungsurteil des BVerfG ausgehenden Druck zur Verrechtlichung polizeilicher Informationseingriffe reagierte. Dieser Entwurf, der mittlerweile in einer letzten Fassung von 1986 vorliegt (vgl. Cilip 24), beinhaltet rechtliche Regelungen für die polizeiliche Informationstätigkeit allgemein (Erhebung, Speicherung, Verarbeitung, Weitergabe von personenbezogenen Daten) sowie insbesondere für spezifische Fahndungs- und Ermittlungsmethoden opera-

tiver Art, die bis dahin ohne gesetzliche Grundlage betrieben wurden; nämlich: Rasterfahndung, Beobachtende Fahndung, Observation (einschließlich des Einsatzes durch technischer Mittel) sowie verdeckte Ermittlungsmethoden (V-Leute, UCAs u.ä.). Wie schon in den 70er Jahren im Falle der Kontrollstellenregelung geht es auch hier um Eingriffe, die sich nicht nur gegen Störer und Verdächtige richten, sondern deren Sinn gerade in der Anwendung gegen eindeutig unverdächtige Personen besteht.

Wie in den 70er Jahren geht die Umsetzung des neuen MEPolG in die Länderpolizeigesetze nur schleppend voran. Wie damals soll deshalb auch jetzt der Versuch unternommen werden, die StPO mit den noch nicht verabschiedeten Polizeigesetzen zu "harmonisieren" und die rechtlich neuen exekutiven Befugnisse der Polizei auch in der zweiten Rechtsquelle polizeilichen Handelns festzuschreiben. Der gesetzgeberische Weg ging über folgende Schritte:

* ein "Problempapier" aus dem BMJ von 1985, in dem

* Der Autor ist Jurist an der Universität Hannover

es vor allem um die Verrechtlichung der neuen Fahndungsmethoden ging (vgl. CILIP 23, S.118 ff.);

* die Verabschiedung des Schlepptextparagrafen 163 d StPO zusammen mit dem Personalausweisgesetz im Frühjahr 1986 (vgl. CILIP 23, S.29 f.);

* einen "Arbeitsentwurf" aus dem BMJ vom Juli 1986 zu Fragen der elektronischen Fahndung und insbesondere der neuen Fahndungsmethoden, wobei die verdeckten Ermittlungen ausdrücklich noch nicht enthalten waren;

* einen weiteren "Arbeitsentwurf" vom Juli 1987, der vor allem die Umwidmung von Daten aus Straf- und Ermittlungsverfahren zu solchen der präventiven Gefahrenabwehr und "vorbeugenden Verbrechensbekämpfung" zum Gegenstand hatte (beide Entw. in CILIP 29, S. 68 ff.).

Der jetzt vorliegende Referentenentwurf vom November 1988 verzichtet formal auf den Begriff der "vorbeugenden Verbrechensbekämpfung", übernimmt aber nahezu vollständig den Inhalt der entsprechenden Regelungen der "Arbeitsentwürfe". Die verdeckten Ermittlungen, die damals noch fehlten, sind jetzt enthalten. Ergänzt wird er schließlich durch einen Zusatz vom Dezember letzten Jahres über den Aufbau eines zentralen staatsanwaltlichen Informationssystems.

Die Rede, daß die StPO die "magna carta des Beschuldigten" sei, dürfte damit endgültig zu einer Legende geworden sein. Sie ist es bald nicht einmal mehr für den Unbeschuldigten.

I. Datenerhebung mit neuen Ermittlungsmethoden

1. Rasterfahndung

Der Entwurf enthält eine detaillierte Regelung der Rasterfahndung (§§ 98 a ff.). Ihre Zulässigkeit setzt den Verdacht einer der in einem Katalog aufgeführten Straftaten voraus. Dieser Katalog bezieht sich u.a. auf Diebstahl in einem schweren Fall (§ 243 StGB) sowie auf die in § 129 a StGB genannten Straftaten; das bedeutet z.B., daß die Rasterfahndung auch bei dem Verdacht der Zerstörung eines Fahrzeugs der Polizei oder Bundeswehr (§ 305 a StGB) zulässig ist.

Die für den Abgleich (die Rasterung) benötigten Daten sind herauszufiltern und "den Strafverfolgungsbehörden" (d.h. der Polizei oder Staatsanwaltschaft) durch die Herausgabe entsprechender Datenträger zu übermitteln. Können

diese Daten nur mit "unverhältnismäßigem Aufwand" herausgefiltert werden, sind auch Datenträger herauszugeben, auf denen "weitere Daten gespeichert sind"; deren Verwendung ist aber unzulässig. Diese Herausgabepflicht wird durch die Befugnis zur Beschlagnahme von Datenträgern ergänzt.

Der Abgleich wird "auf Verlangen der Staatsanwaltschaft" - also nicht obligatorisch - "unter deren Aufsicht durchgeführt". Er darf nur durch den Richter, bei "Gefahr im Verzug" auch durch die Staatsanwaltschaft, angeordnet werden. Deren Anordnung tritt außer Kraft, sofern nicht binnen drei Tagen eine richterliche Bestätigung ergeht.

2. Polizeiliche Beobachtung

Nach § 163e Entw. darf der Beschuldigte bei dem Verdacht einer Straftat "mit erheblicher Bedeutung" zur Beobachtung an einer Grenze oder zur Beobachtung während einer "zu Zwecken der Strafverfolgung oder der Gefahrenabwehr durchgeführten polizeilichen Kontrolle" (also nicht nur einer Kontrolle nach § 111 StPO) ausgeschrieben werden. Außerdem darf auch das Kennzeichen eines Fahrzeugs ausgeschrieben werden, falls es auf den Beschuldigten zugelassen ist oder von ihm regelmäßig benutzt wird oder wenn anzunehmen ist, daß es - von einem noch unbekanntem Verdächtigen - für eine Straftat "mit erheblicher Bedeutung" benutzt worden ist.

Während der Kontrolle dürfen nicht nur Personalien, Autokennzeichen sowie "Zeit, Ort und mitgeführte Sachen" registriert und der ausschreibenden Stelle gemeldet werden, sondern auch "Erkenntnisse über ... Verhalten, Vor-

Aus der
**SCHRIFTENREIHE
DER
STRAFVERTEIDIGERVEREINIGUNGEN**

aktualisierte Broschüre zum Artikelgesetz zur Änderung der StPO, des StGB, des Versammlungsgesetzes und zur Einführung einer Kronzeugenregelung

Fassung 21.4.89
112 Seiten 6,-- DM

Broschüre zum Referentenentwurf eines Strafverfahrenrechtsänderungsgesetzes -StVAG- 1988-

Gesetzesentwurf, Begründung des BMJ, Stellungnahme der Strafverteidigervereinigungen

Fassung 21.4.89
205 Seiten 9,80 DM

Broschüre zu aktuellen § 129a - Strafverfahren ## 11 Verteidigerinnen und Verteidiger berichten.

86 Seiten 7,-- DM

Bezugsadresse:

Organisationsbüro der
Strafverteidigervereinigungen
Siemensstraße 15
5000 Köln 30
Tel: 0221/ 55 70 26
FAX: 221/ 550 4000

Schecks oder Briefmarken
zzgl. DM 3,80 Porto u. Verpack.

oder Vorabzahlungen auf:
Postgiroamt Köln: Konto
Strafverteidigervereinigungen
Organisationsbüro
c/o RAe Lütkes pp
Nr: 46 41 52 - 502

haben und sonstige Umstände des Antreffens". Diese Informationen dürfen sich auch auf "Begleiter" des Beschuldigten beziehen, darüber hinaus auch auf "andere Personen", von denen aufgrund bestimmter Tatsachen anzunehmen ist, "daß diese mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt werden wird" (§ 163 h).

Zur Anordnung befugt ist der Richter, bei "Gefahr im Verzug" auch die Staatsanwaltschaft; ihre Anordnung muß binnen drei Tagen richterlich bestätigt werden, sonst tritt sie außer Kraft.

3. Observation

Bei dem Verdacht einer Straftat "mit erheblicher Bedeutung" darf eine Observation des Beschuldigten, die länger als 24 Stunden dauern oder an mehr als zwei Tagen stattfinden soll, angeordnet werden (§ 163 f).

Darüber hinaus ist auch eine Observation sog. Kontaktpersonen (nach § 163 h) zulässig. Zur Anordnung befugt ist der Richter, bei "Gefahr im Verzug" auch die Staatsanwaltschaft und ihre Hilfsbeamten (Polizeibeamte bestimmter Dienstgrade); die Eilanordnungen bedürfen einer richterlichen Bestätigung innerhalb von drei Tagen.

Kurzfristige Observations werden durch § 163 f nicht ausgeschlossen; sie dürfen auf eine Generalermächtigung gestützt werden, die in die Strafprozeßordnung eingefügt werden soll (dazu unten 6.).

4. Einsatz technischer Mittel

Auch der Einsatz sog. technischer Mittel wird geregelt (§ 163 g). Danach darf "das nicht öffentlich gesprochene Wort" abgehört und aufgezeichnet werden, falls der

Verdacht einer der in § 100 a StPO genannten Straftaten besteht; auch das Wort sog. Kontaktpersonen (§ 163 h). Der Katalog des § 100a StPO umfaßt etwa 80 Straftaten, darunter das gesamte politische Strafrecht (einschließlich reiner Meinungsdelikte), aber auch Delikte wie einfache Brandstiftung oder Raub.

Das Abhören von Gesprächen in Wohnungen (oder von außerhalb) ist - bei einem Verdacht jener Art - dann erlaubt, wenn es "im Beisein eines nicht offen ermittelnden Beamten" stattfindet. Diese Voraussetzung scheint zu implizieren, daß zusätzlich die Anforderungen für den Einsatz "verdeckter Ermittler" nach § 163 k des Entwurfs - dazu sogleich - erfüllt sein müssen. Doch der Entwurf rechnet - neben den "verdeckten Ermittlungen" im Sinne von § 163 k - mit kurzfristigen "nicht offenen" Ermittlungen, die aufgrund der neuen Generalermächtigung erlaubt sein sollen (unten 6.). Bei einer auf diese Ermächtigung gestützten "nicht offenen" Ermittlung bleibt es also bei jenem Verdacht einer Katalogtat als Voraussetzung eines Lauschangriffs auf Gespräche in Wohnungen.

Bei dem Verdacht einer Katalogtat dürfen außerdem Foto- und Filmaufnahmen "von Personen und Beweismitteln hergestellt werden, die sich in einer Wohnung befinden und für den Beamten offen erkennbar sind". Aufnahmen außerhalb von Wohnungen setzen hingegen keinen spezifischen Verdacht voraus, sie sind also zur Aufklärung jeder Straftat oder zur Ermittlung des Aufenthalts des Beschuldigten zulässig. Die Abhörmaßnahmen sowie die Foto- und Filmaufnahmen in Wohnungen dürfen durch den Richter, bei "Ge-

fahr im Verzug" auch durch die Staatsanwaltschaft und ihre Hilfsbeamten angeordnet werden. Die Foto- und Filmaufnahmen außerhalb von Wohnungen darf jeder Polizeibeamte herstellen, auch ohne "Gefahr im Verzug"; sie stehen unter keinem Richtervorbehalt.

5. Verdeckte Ermittler

Nunmehr soll auch der Einsatz "verdeckter Ermittler" gesetzlich geregelt werden. In einer Legaldefinition heißt es:

"Verdeckte Ermittler sind Beamte des Polizeidienstes, die unter einer ihnen verliehenen Identität (Legende) im Umfeld des Tatverdächtigen und solcher Personen ermitteln, die Erkenntnisse über die Tat oder den Täter haben können."

Der Einsatz von Polizeibeamten, denen keine Legende - für einen gewissen Zeitraum - "verliehen" wird, sondern die gleichsam gelegentlich über ihre Identität und Aufgabe täuschen, soll, wie erwähnt, nach der neuen Generalermächtigung zulässig sein.

Der Einsatz verdeckter Ermittler ist zulässig, wenn der Verdacht besteht, daß eine Straftat "mit erheblicher Bedeutung" auf einem "bestimmten Gebiet" (z.B. BTM- oder Waffenhandels-Delikte, Staatsschutzdelikte, nach Maßgabe der §§ 74a, 120 GVG) oder aber gewerbsmäßig, gewohnheitsmäßig, "von einem Bandenmitglied oder in anderer Weise organisiert" begangen worden ist. Er ist weiterhin zur Aufklärung von "Verbrechen" (d.h. von Taten mit einer Mindeststrafdrohung von einem Jahr) zulässig, "soweit aufgrund bestimmter Tatsachen die Gefahr der Wiederholung besteht". Er ist schließlich zur Aufklärung von Verbrechen zulässig, "wenn die besondere

Bedeutung der Tat den Einsatz gebietet und andere Maßnahmen aussichtslos wären".

Soweit es für die Legende "unerläßlich" ist, dürfen "entsprechende Urkunden hergestellt werden". Der Ermittler darf unter der Legende "am Rechtsverkehr teilnehmen". Er darf das Einverständnis zum Betreten einer Wohnung "nicht durch ein über die Nutzung der Legende hinausgehendes Täuschen, namentlich Vortäuschen einer Berechtigung, herbeiführen". (Nach der Begründung des Entwurfs ist auch eine Legende selbst verboten, die "darauf angelegt" ist, diese Berechtigung vorzutäuschen.) Heimliche Durchsuchungen sind unzulässig.

Die Identität des Beamten darf nicht nur nach Maßgabe von § 96 StPO ("zum Wohl des Bundes oder eines deutschen Landes") oder zu seinem Schutz geheimgehalten werden, sondern auch dann, "wenn die Offenbarung die Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers gefährden würde". Damit dürfte die Sperrung des V-Manns in der Hauptverhandlung zur Regel werden.

Der Einsatz des "Verdeckten Ermittlers" setzt die "Zustimmung" der Staatsanwaltschaft voraus, außer bei "Gefahr im Verzug". Bestimmte Einsätze (gegen namentlich bekannte Beschuldigte, falls Wohnungen betreten werden sollen oder falls die Maßnahme über drei Monate dauern soll) bedürfen darüber hinaus der "Zustimmung" des Richters, außer bei "Gefahr im Verzug". Bei polizeilichen Eilanordnungen sind die je relevanten Zustimmungen binnen drei Tagen nachzuholen.

6. Generalmächtigungen

Der Entwurf sieht die Einführung von Generalmächtigungen vor, d.h. von Befugnissen zum Eingriff in Grundrechte in Form von Generalklauseln - und zwar einerseits für die Staatsanwaltschaft und die in ihrem Auftrag handelnden Polizeibeamten (§ 161), andererseits für selbständige Ermittlungen der Polizei (§ 163). Damit unterstellt der Entwurf, daß eine strafprozessuale Generalbefugnis dem verfassungsrechtlichen Gebot, die gesetzlichen Voraussetzungen für Grundrechtseingriffe präzise zu bestimmen, genügt. Er hält es außerdem implizit für zulässig, daß der Gesetzgeber darauf verzichtet, Befugnisse nach Maßgabe der Eingriffsintensität sowie in Relation zu der Aufgabe, zu deren Erfüllung sie dienen sollen, auszugestalten. Beide Prämissen sind arg zweifelhaft; darüber hinaus sind die Rückwirkungen einer Generalmächtigung auf den Geltungsbereich der Spezialbefugnisse zu beachten.

Für das Verhältnis von Spezialbefugnissen zu einer Generalmächtigung (z.B. in Polizeigesetzen) gilt der Grundsatz, daß auf die Generalmächtigung nicht zurückgegriffen werden darf, wenn im Einzelfall spezielle Eingriffsvoraussetzungen nicht erfüllt sind. Ohne dieses Postulat wären die Spezialbefugnisse in Wahrheit aufgehoben und durch die Generalmächtigung ersetzt. Die Begründung wiederholt einerseits diesen Grundsatz, andererseits dementiert sie ihn: indem sie es für zulässig erklärt, eine "nicht offene" Ermittlung auf die Generalmächtigung zu stützen, wenn die speziellen Voraussetzungen für "verdeckte Ermittlungen" nicht erfüllt sind. Vermutlich ist dieser Widerspruch in der Struktur

der Befugnis zu verdeckten Ermittlungen begründet; aufgrund dieser Struktur (die weitgehend offen läßt, wozu der Beamte im einzelnen befugt ist,) werden die Bedingungen der Anwendbarkeit jenes Grundsatzes diffus.

II. Zweckentfremdung durch Umwidmung von Daten

So wichtig die Voraussetzungen für die Erhebung der Informationen, so wichtig sind die Regeln für deren Verwendbarkeit. Nach dem Entwurf sind die erhobenen Informationen auch zu anderen - als den mit der Erhebung verfolgten - Zwecken verwendbar. Die Regelung dieser Zweckentfremdung von Informationen ist nicht gerade durchsichtig; fünf Typen von Regeln sind dabei zu berücksichtigen.

1. Nutzung in anderen Strafverfahren

An einige der neuen Erhebungsbefugnisse sind Verwertungsregeln geknüpft, die sich auf die Nutzung der Information in anderen Strafverfahren (als dem, in dem sie erhoben wurde) beziehen; das gilt für die Rasterfahndung, das Abhören privater Gespräche, für Foto- und Filmaufnahmen in Wohnungen und verdeckte Ermittlungen. In diesen Fällen setzt die Verwertbarkeit der Information wiederum den Verdacht einer Katalogtat voraus, d.h. sie ist an den Katalog gebunden, der auch für die Erhebung der Information maßgeblich ist. Die Verwertbarkeit der aus verdeckten Ermittlungen stammenden Daten geht insofern darüber hinaus, als die generalklauselartige Zulässigkeitsvoraussetzung - Verbrechen mit "besonderer Bedeutung" - auch für die Verwendung der Daten gilt.

Allemaal ist aber zu beachten, daß

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
und der Datenschutzkommission Rheinland-Pfalz vom 14./15. März 1988 in Mainz**

Polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen

Eines der dringendsten datenschutzrechtlichen Anliegen ist die Schaffung bereichsspezifischer Grundlagen für die Datenverarbeitung der Sicherheitsbehörden. Dies gilt ebenso für die Nachrichtendienste. Schon seit Jahren haben die Datenschutzbeauftragten entsprechende Forderungen erhoben. Spätestens seit dem „Volkszählungsurteil“ des Bundesverfassungsgerichts vom 15. 12. 1983 ist das gesetzliche Regelungsdefizit offenbar. So hat der Bayerische Verfassungsgerichtshof in einer Entscheidung vom 9. 7. 1985 bezogen auf die polizeiliche Datenverarbeitung hervorgehoben, es sei geboten, daß der Gesetzgeber die Materie regelt, die bisher Gegenstand der „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS)“ ist.

Mit der Erhebung, Speicherung und Weitergabe personenbezogener Daten greift die Polizei in die Grundrechte der Betroffenen ein, ohne daß dafür immer die verfassungsrechtlich gebotenen gesetzlichen Grundlagen vorhanden sind. So haben schon einige Gerichte die polizeiliche Datenverarbeitung zum Zwecke vorbeugender Straftatenbekämpfung bis zum Erlaß bereichsspezifischer gesetzlicher Grundlagen für unzulässig erklärt. Gleichwohl kommen die gesetzgeberischen Initiativen zur Behebung dieses Zustandes nur äußerst schleppend voran.

Allerdings hat das Bundesverfassungsgericht dem Gesetzgeber in der Vergangenheit Übergangsfristen zur Beseitigung von Regelungsdefiziten zugebilligt, wenn damit eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden werden kann, die der verfassungsmäßigen Ordnung noch fernstünde als der bisherige Zustand.

Dabei ist auf folgendes hinzuweisen:

1. Übergangsfristen können ihrer Natur nach nicht unbegrenzt in Anspruch genommen werden. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, daß sie dann nicht mehr anerkannt werden können, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert.
2. Während der Übergangsfrist reduziert sich die Befugnis zu Eingriffen auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebes“ unerlässlich ist. Es ist mithin unzulässig und mit den vom Bundesverfassungsgericht festgestellten reduzierten Befugnissen unvereinbar, bereits bestehende Datenverarbeitungsabläufe noch auszuweiten, etwa durch den Aufbau neuer Datenbanken oder die Ausschöpfung neuer technischer Möglichkeiten, soweit die Eingriffe in die Rechte der Betroffenen damit eine neue Qualität erreichen.
3. Besondere Zurückhaltung hat sich die Polizei dort aufzuerlegen, wo Eingriffe in das informationelle Selbstbestimmungsrecht noch weitere Grundrechte betreffen.
 - 3.1 Die Feststellungen von Personalien, damit verbundene Datenabgleiche und Speicherungen sowie Film- und Videoaufnahmen sind anlässlich von öffentlichen Versammlungen während der Übergangszeit nur dann als zulässig anzusehen, wenn Anhaltspunkte dafür vorliegen, daß strafbare Handlungen begangen werden.
 - 3.2 Die Nutzung technischer Hilfsmittel zur verdeckten Datenerhebung durch Lauschangriffe in Wohnungen muß grundsätzlich ausgeschlossen sein.
4. Der Einsatz von verdeckten Ermittlern und V-Leuten sowie langfristige Observationen und polizeiliche Beobachtung dürfen nur zugelassen werden, wenn konkrete Anhaltspunkte für bestimmte schwere Straftaten bestehen. Es muß festgelegt werden, wer diese Maßnahmen anordnen darf, wie die anfallenden Erkenntnisse verwertet werden dürfen und wann die Betroffenen zu unterrichten sind.
5. Im Hinblick auf die von den Verfassungsgerichten für die Übergangszeit geforderte Beschränkung auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebs“ unerlässlich ist, erinnern die Datenschutzbeauftragten an ihre früheren Beschlüsse zur polizeilichen Datenverarbeitung. Danach sind künftig insbesondere folgende Datenverarbeitungsvorgänge zu unterlassen:
 - Speicherung diskriminierender personenbezogener Hinweise in polizeilichen Informationssystemen;
 - Speicherung (ehemals) verdächtiger Personen zu Zwecken vorbeugender Straftatenbekämpfung ohne verantwortbare kriminologische Prognose;
 - Speicherung von Daten über Personen, bei denen eine Anklageerhebung mangels öffentlichen Interesses abgelehnt wurde;
 - Speicherung von Daten über Kinder, die der Begehung einer Straftat verdächtig werden;
 - Weitergabe von Informationen, die mit speziellen polizeilichen Befugnissen erhoben wurden, an andere als Polizeidienststellen.

diese Einschränkungen der Verwertbarkeit (auf die Erklärung von Katalogtaten bzw. von Verbrechen mit "besonderer Bedeutung") nur gelten, sofern die Informationen "zu Beweis Zwecken" verwendet werden, d.h. soweit sie selbst als Beweismittel dienen. Werden sie hingegen zum Anlaß genommen, neue Ermittlungen aufzunehmen, ohne später die Rolle eines Beweismittels zu übernehmen, dann dürfen sie auch verwendet werden, wenn die Ermittlungen sich auf Taten beziehen, die in dem Katalog nicht genannt sind. Der Entwurf orientiert sich mit dieser Entscheidung an der Rechtsprechung zur Verwertbarkeit sog. Zufallserkenntnisse bei der Telefonüberwachung.

2. Nutzung zu präventiven Zwecken

In den eben erwähnten Verwertungsregeln findet sich immer derselbe Vorbehalt: "unbeschadet § 478". Mit dieser Bestimmung wird die Verwendung von in Strafverfahren gewonnenen Informationen zum Zweck der Gefahrenabwehr zugelassen. Sie ist an - mehr oder minder - qualifizierte Gefahren einschätzungen geknüpft, sofern die Information mit einer der neuen Erhebungsmethoden gewonnen wurde. So ist die Verwendung von Informationen aus Lauschangriffen nur zur "Abwehr einer gegenwärtigen Gefahr für Leib und Leben einer Person" oder zur Verhütung einer in § 100 a StPO genannten Straftat zulässig. In den übrigen Fällen (Rasterfahndung, sog. polizeiliche Beobachtung, Observation, verdeckte Ermittlung) setzt sie eine "erhebliche" Gefahr für die öffentliche Sicherheit voraus. Die Verwendung von Ermittlungsdaten zur Gefahrenabwehr ist im

Übrigen nicht ausgeschlossen, wenn der Beschuldigte freigesprochen, die Eröffnung des Hauptverfahrens abgelehnt oder das Verfahren eingestellt worden ist.

3. Dateiregelungen für "Strafverfolgungsbehörden"

Die Polizei ist - über § 478 hinaus - auch im Rahmen der neuen Dateiregelungen des Entwurfs berücksichtigt, unter dem Titel "Strafverfolgungsbehörde", den sie mit der Staatsanwaltschaft teilt. Diese Regelungen betreffen nicht nur die Speicherung, sondern auch die Veränderung und Nutzung von in Strafverfahren gewonnenen Informationen.

Nach § 481 des Entwurfs ist die Speicherung und Verwendung personenbezogener Informationen durch "Strafverfolgungsbehörden", Gerichte und Vollstreckungsbehörden "für Zwecke des Strafverfahrens" (also des Verfahrens, in dem sie erhoben wurden) erlaubt. Diese Zweckbestimmung wird sodann, soweit es um die Verwendung geht, in zwei Hinsichten erweitert: die Daten dürfen auch "für andere Strafverfahren" verwendet werden. Dabei wären aber die zuvor erwähnten Verwertungsregeln, siehe unter 1., zu beachten, sofern spezifische Formen der Erhebung vorauszusetzen sind. Sie dürfen des weiteren genutzt werden, soweit dies durch besondere gesetzliche Bestimmungen zugelassen ist. Zu diesen Bestimmungen gehört auch - der unter 2. erwähnte - § 478. Das bedeutet: auch die in Dateien gespeicherten Informationen aus Strafverfahren dürfen zum Zweck der Prävention verwendet werden. Es darf sich im übrigen um "zentrale Dateien" handeln; die Begründung verweist auf Dateien des BKAs.

Nach § 482 dürfen "Strafverfolgungsbehörden" zur "Vorsorge für künftige Strafverfolgung" personenbezogene Informationen aus Strafverfahren speichern, auch in zentralen Dateien. Diese Informationen dürfen dann künftig zur Aufklärung von Straftaten verwendet werden (insofern "Vorsorge"). Dieser Begriff tritt an die Stelle der in den Arbeitsentwürfen 1986/87 noch enthaltenen "vorbeugenden Verbrechensbekämpfung". Informationen über den Beschuldigten dürfen gespeichert werden, wenn zu erwarten ist, daß er "eine weitere Straftat" begehen wird. Diese Prognose wird - nach dem Entwurf - nicht dadurch ausgeschlossen, daß der Beschuldigte freigesprochen wird, die Eröffnung des Hauptverfahrens abgelehnt oder das Verfahren eingestellt wird. Informationen über andere Personen (u.a. über "Kontakt- und Begleitpersonen, Hinweisgeber und sonstige Auskunftspersonen") dürfen gespeichert werden, "soweit dies zur Vorsorge für künftige Strafverfolgung wegen einer Straftat mit erheblicher Bedeutung unerlässlich ist; die Speicherdauer darf drei Jahre nicht überschreiten."

Daneben gilt - wie bei Speicherrungen nach § 481 - die allgemeine Öffnungsklausel für weitere Nutzungen nach "besonderen gesetzlichen Bestimmungen"; das bedeutet, daß jene Daten nach Maßgabe von § 478 auch für Zwecke der Prävention genutzt werden dürfen.

Die nach §§ 481, 482 gespeicherten Daten dürfen "für Zwecke eines Strafverfahrens" auch im online-Verfahren von Polizeibehörden, Staatsanwaltschaften und Strafgerichten abgerufen werden.

4. Staatsanwaltliches Informationssystem

Obwohl die Staatsanwaltschaften an den eben erwähnten Dateien partizipieren können, sieht der Entwurf - in einer Ergänzung vom 22. Dezember 1988 - ein spezielles, länderübergreifendes staatsanwaltschaftliches Informationssystem vor. Es soll zu einer Konzentration von Ermittlungen gegenüber Beschuldigten verhelfen, denen gleichzeitig Straftaten an verschiedenen Orten zur Last gelegt werden. In dieser Datei dürfen nur spezifische Ermittlungsdaten gespeichert werden (u.a. Personaldaten, Tatzeiten und -vorwürfe, Erledigungsart), sie dürfen nur von Staatsanwaltschaften "für andere Strafverfahren einschließlich der Vollstreckung" verwendet werden. Die Abrufbarkeit der Daten im online-Verfahren darf eingerichtet werden.

5. Auskünfte aus Strafverfahren

Schließlich sind - unter dem Gesichtspunkt der Zweckentfremdung von Informationen aus Strafverfahren - noch Vorschriften über Auskünfte aus Strafakten sowie über Akteneinsicht in diesen Überblick einzubeziehen. Behörden dürfen nach dem Entwurf Auskünfte - u.U. auch Akteneinsicht - erhalten, soweit dies "zur Erfüllung einer bestimmten ihnen obliegenden Aufgabe erforderlich" ist, und sofern keine besonderen Verwendungsregelungen, "Zwecke der Strafverfolgung" oder "überwiegende schutzwürdige Interessen des Beschuldigten oder anderer" entgegenstehen.

Auch Privatpersonen dürfen unter engen Voraussetzungen über einen Rechtsanwalt Auskünfte bzw. Akteneinsicht erhalten. Schließlich werden Aktenauskunft und -ein-

sicht für wissenschaftliche Zwecke geregelt.

In den Dateiregelungen wird dann auf diese Vorschriften verwiesen: soweit "Akteneinsicht oder Auskunft aus den Akten gewährt werden könnte, kann stattdessen Auskunft aus einer Datei erteilt werden."

6. Verwandlung in Strafverfahrensdaten

Bisher wurden nur Vorschriften des Entwurfs berücksichtigt, die die Zweckverwandlung von Daten aus Strafverfahren zulassen. Am Ende sei noch auf Regeln für den umgekehrten Fall hingewiesen: der Verwendung von andernorts erhobenen Informationen zum Zweck der Strafverfolgung.

Der Entwurf beläßt es bei der allgemeinen Befugnis der Staatsanwaltschaft, zum Zweck der Strafverfolgung "von allen öffentlichen Behörden Auskunft zu verlangen" (§ 161 StPO). Neu hingegen ist eine Vorschrift, die die Verwendung von Daten betrifft, die mit polizeirechtlichen Befugnissen zum Zweck der Gefahrenabwehr erhoben wurden: sofern es sich um eine - polizeigesetzlich geregelte - Rasterfahndung, Abhörmaßnahme oder verdeckte Ermittlung handelt, ist die Verwendung "zu Beweiswecken" nur zur Aufklärung einer in § 98 a (Rasterfahndung) des Entwurfs genannten Straftat erlaubt. Der Entwurf unterstellt also die Einführung jener Befugnisse in den Polizeigesetzen.

Die Polizei ist nach dem Entwurf befugt, "von allen öffentlichen Behörden Auskunft" - nun nicht zu verlangen, sondern - "zu erbitten" (§ 163).

Eine Bitte um Auskunft ohne gesetzliche Grundlage: das ginge nun in der Tat zu weit.



Roland Appel, Dieter Hummel,
Wolfgang Hippe

DIE NEUE SICHERHEIT
Vom Notstand zur sozialen
Kontrolle

230 S., franz. br., 24,80 DM

Roland Appel/Dieter Hummel: Die Republik nach der Volkszählung

Theo Schiller: Von der Notstandsbewegung zum Bürgerprotest

Jürgen Seifert: Politische Ausgrenzung in der Geschichte der BRD

Roland Appel: Zur Geschichte der Sicherheitsgesetzgebung

Karin Heuer: Zeig mir deine Sozialversicherungsnummer und ich sag' dir wer du bist

Volker Beck/Günter Dworek: Der AIDS-Staat

Eckart Riehle: Die Verpolizeilichung der Prävention

Wolfgang Hippe: Kulturpolitik als Innenpolitik

Claus Eurich: Auf dem Weg in die Bilderautokratie

Ulrich Beck: Wissenschaft und Sicherheit

Roland Roth: Menschenrecht - eine noch immer aktuelle politische Utopie

Peter Brückner: Der soziale Friede als wirklicher Traum der Revolution

Thomas Blanke: Der Präventionsstaat in der Risikogesellschaft

Wilhelm Steinmüller: Volkszählung in einer informatisierten Gesellschaft

Volksblatt Verlag

Postfach 250 405, 5 Köln 1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (Strafverfahrensänderungsgesetz vom 03.11.1988)

Die Konferenz begrüßt, daß ein Entwurf zur Regelung des Datenschutzes im Strafverfahrensrecht vorgelegt worden ist und daß darin für die besonderen Ermittlungs- und Fahndungsmethoden eigenständige Befugnisnormen vorgesehen sind sowie Regelungen zur Verarbeitung personenbezogener Daten und zur Akteneinsicht in die Strafprozeßordnung aufgenommen werden sollen.

Die im Entwurf vorgesehenen Datenschutzregelungen sind an den verfassungsrechtlichen Grundsätzen der Verhältnismäßigkeit und Normenklarheit zu messen. Weil im Bereich der Grundrechtsausübung nach der Rechtsprechung des Bundesverfassungsgerichts alle wesentlichen Entscheidungen vom Gesetzgeber selbst zu treffen sind, ist die gesamte Informationsverarbeitung wegen ihres Eingriffscharakters in der Strafprozeßordnung präzise und umfassend gesetzlich zu regeln.

Der vorliegende Entwurf entspricht den sich aus dem Recht auf informationelle Selbstbestimmung ergebenden Anforderungen noch nicht; er ist im übrigen unvollständig. Die Datenschutzkonferenz hebt deshalb unter gleichzeitiger Bezugnahme auf ihren Beschluß vom November 1986 folgende Kritikpunkte hervor:

1. Zu den Regelungen über die Ermittlungs- und Fahndungsmethoden

* Die Erhebung und Weiterverarbeitung personenbezogener Daten durch Strafverfolgungsorgane greift empfindlich in das Persönlichkeits-

recht der Bürger ein. Umso wichtiger ist es, nach dem Grad der Betroffenheit im Gesetz Abstufungen vorzunehmen. Zwischen dem Beschuldigten, dem Verdächtigen, dem von Vorfeldermittlungen Betroffenen und dem erkennbar nicht Verdächtigen (z.B. Geschädigten, Zeugen) sollte daher unterschieden werden. Vor allem die Regelungen über "Kontakt- und Begleitpersonen", "andere Personen" und "Dritte" werden dem nicht gerecht.

* Es muß klargestellt werden, daß die Ermittlungsgeneralklausel keine Eingriffe gestattet, die in ihrer Eingriffstiefe den besonders geregelten gleichkommen. So wären z.B. die Voraussetzungen des Einsatzes von V-Leuten besonders zu regeln. Auch weiterentwickelte "besondere Fahndungs- und Ermittlungsmethoden" dürfen nicht auf die Ermittlungsgeneralklausel gestützt werden. In die Strafprozeßordnung sind Verfahrensregelungen aufzunehmen, die eine Information etwa der zuständigen Parlamentsausschüsse über die beabsichtigte Anwendung vorsehen. Vor dem Einsatz qualitativ neuer Methoden müssen auf jeden Fall gesetzliche Regelungen geschaffen werden.

* Der Entwurf betont zu Recht, daß bei jeder einzelnen Ermittlungs- und Datenverarbeitungsmaßnahme der Grundsatz der Verhältnismäßigkeit zu beachten ist. Dies muß bereits in einzelnen Befugnisnormen zum Ausdruck kommen. Die bislang vorgesehenen Straftatenkataloge sind mit dem Ziel einer Einschränkung zu überprüfen;

die bloße Anknüpfung an den Begriff der "Straftat mit erheblicher Bedeutung" ohne weitere Differenzierung reicht nicht aus.

* Die Anordnung von Ermittlungs- und Fahndungsmethoden, die besonders stark in das Recht auf informationelle Selbstbestimmtheit eingreifen, ist dem Richter vorzubehalten. Gleiches gilt, wenn mit solchen besonderen Methoden erhobene Daten für andere Strafverfahren oder für andere - polizeiliche - Zwecke verwendet werden sollen.

* Wegen der Tiefe der Eingriffe bei besonderen Ermittlungs- und Fahndungsmethoden darf der Richtervorbehalt - von besonderen Eilfällen abgesehen - nicht durch Entscheidungen der Staatsanwaltschaft oder der Polizei ersetzt werden. Soweit ausnahmsweise die Staatsanwaltschaft oder die Polizei eine Anordnung treffen muß, dürfen erlangte Daten nicht weiter verwendet werden, wenn die richterliche Bestätigung ausbleibt; erhobene Daten sind zu löschen.

* Die Verwendung von durch besondere Ermittlungs- oder Fahndungsmethoden erlangten Daten für polizeiliche Zwecke muß neben dem Richtervorbehalt voraussetzen, daß das Polizeirecht vergleichbare Eingriffe gestattet oder daß die Daten zur Abwehr einer gegenwärtigen Gefahr für Leib und Leben erforderlich sind.

2. Zu den besonderen Regelungen über die Datenverarbeitung

Regelungen über die Datenverarbeitung im Strafverfahren setzen eine Gesamtkonzeption über die Informationsverarbeitung bei den Strafverfolgungsbehörden voraus. Notwendig sind insbesondere klare Bestimmungen über die Zusammenarbeit zwischen Staatsanwalt-

schaft und Polizei. Der vorliegende Entwurf läßt den hierzu notwendigen Konsens jedoch nicht erkennen.

* Der Gesetzgeber sollte möglichst genau regeln, welche Arten von Daten für "Zwecke des Strafverfahrens", für Zwecke anderer Strafverfahren oder für die Aufklärung künftiger Straftaten in automatisierten Dateien landes- oder bundesweit zur Verfügung stehen sollen und in welchem Verhältnis hierzu das Bundeszentralregister steht.

* Der Gesetzgeber muß, auch um Doppelspeicherungen zwischen staatsanwaltschaftlichen und polizeilichen Informationssystemen zu vermeiden, eindeutig festlegen, wem die Entscheidungsbefugnis über die bei der Strafverfolgung angefallenen Daten zusteht und für welche Zwecke sie verwendet werden dürfen.

* Daten, die für bloße Tätigkeitsnachweise gespeichert werden (Vorgangsverwaltung), dürfen für andere Zwecke nicht verwendet werden und müssen nach kurzen Fristen gelöscht werden.

* Die vorgesehene Speicherung von Daten über Personen, die "bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen", oder die "Opfer einer Straftat werden könnten", gibt zu Bedenken Anlaß, weil das Anlegen von Dateien über besondere Personengruppen wie z.B. Prostituierte, Homosexuelle und ausländische Gastwirte als erlaubt angesehen werden könnte.

* Die Datenspeicherung über Personen, die mangels hinreichendem Tatverdacht freigesprochen worden sind oder bei denen das Ermittlungsverfahren eingestellt oder die Anklage nicht zugelassen worden ist, darf nur unter engeren Voraussetzungen erfolgen.

3. Zur Akteneinsicht

Strafakten sind wegen ihres teilweise sehr sensiblen Inhalts geheimzuhalten. Sie dürfen deshalb auch anderen öffentlichen Stellen nur unter engeren Voraussetzungen zugänglich sein. Nicht am Strafverfahren beteiligte Personen dürfen auch über Rechtsanwälte allenfalls in besonderen Ausnahmefällen Einsicht oder Auskunft aus Strafakten erhalten.

4. Fehlende Regelungen

Regelungsbedürftig sind vor allem:

- * die engere Feststellung der Zulässigkeit erkennungsdienstlicher Behandlungen und der Voraussetzungen für den Fahndungsabgleich sowie die weitere Verwendung der dabei gewonnenen Daten,
- * die Verbesserung des Schutzes der Persönlichkeitsrechte bei der Erhebung persönlicher Daten von Angeklagten und Zeugen im Strafverfahren,
- * der allenfalls begrenzte Einsatz der Genomanalyse im Strafverfahren.

blätter des iz3w

Informationszentrum dritte welt - iz3w

Gen- und Blotechnologie in der Landwirtschaft und Auswirkungen in der „Dritten Welt“

Be-
zug:
blätter
des iz3w
Postf. 5328

Febr. 1989
Nr. 155
60 S.

7800 Freiburg

Buchhandel:

Prolit, Pf, 63 Gießen

8 mal im Jahr für 40/30 Mark
Einzelheft 5 DM + 1,50 DM Porto

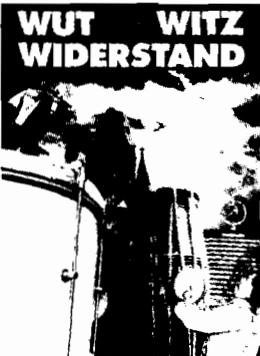
»I-W-F – Mördertreff« Fotoband

Büro für ungewöhnliche Maßnahmen und Bundeskongress Entwicklungspolitischer Aktionsgruppen/BUKO (Herausgeber)

Wut, Witz, Widerstand

Berlin, September 1988. Die Herren der Welt hatten geladen ... und alle, alle kamen. Am geladesten waren wohl die GegnerInnen von IWF und Weltbank.

Der Fotoband »Wut, Witz, Widerstand« beschreibt die politische Aktion der Gegenöffentlichkeit in der BRD 1988, zu der sich unzählige Gruppierungen in dem »breitesten außerparlamentarischen Oppositionsspektrum seit Bestehen der BRD« (Spiegel) zusammenfanden.



Schmetterling Vg., Holzhauser Str. 31, 7 Stuttgart 80, ISBN 3-926369-59-0, 128 S., A4, Kunstdruckpapier, ca. DM 19,80. Ober **Buchhandel** bzw. **Büro für ungewöhnl. Maßnahmen**, c/a FDGO im Kerngehäuse, Curvstr. 20, 1 Berlin 36, Tel. 030 / 611 94 04 (gegen Vorkasse, Scheck o.ä., zzgl. DM 3.-Porto)

**Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
und der Datenschutzkommission Rheinland-Pfalz vom 14./15. März 1988 in Mainz**

Polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen

Eines der dringendsten datenschutzrechtlichen Anliegen ist die Schaffung bereichsspezifischer Grundlagen für die Datenverarbeitung der Sicherheitsbehörden. Dies gilt ebenso für die Nachrichtendienste. Schon seit Jahren haben die Datenschutzbeauftragten entsprechende Forderungen erhoben. Spätestens seit dem „Volkszählungsurteil“ des Bundesverfassungsgerichts vom 15. 12. 1983 ist das gesetzliche Regelungsdefizit offenbar. So hat der Bayerische Verfassungsgerichtshof in einer Entscheidung vom 9. 7. 1985 bezogen auf die polizeiliche Datenverarbeitung hervorgehoben, es sei geboten, daß der Gesetzgeber die Materie regelt, die bisher Gegenstand der „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS)“ ist.

Mit der Erhebung, Speicherung und Weitergabe personenbezogener Daten greift die Polizei in die Grundrechte der Betroffenen ein, ohne daß dafür immer die verfassungsrechtlich gebotenen gesetzlichen Grundlagen vorhanden sind. So haben schon einige Gerichte die polizeiliche Datenverarbeitung zum Zwecke vorbeugender Straftatenbekämpfung bis zum Erlaß bereichsspezifischer gesetzlicher Grundlagen für unzulässig erklärt. Gleichwohl kommen die gesetzgeberischen Initiativen zur Behebung dieses Zustandes nur äußerst schleppend voran.

Allerdings hat das Bundesverfassungsgericht dem Gesetzgeber in der Vergangenheit Übergangsfristen zur Beseitigung von Regelungsdefiziten zugebilligt, wenn damit eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden werden kann, die der verfassungsmäßigen Ordnung noch fernstünde als der bisherige Zustand.

Dabei ist auf folgendes hinzuweisen:

1. Übergangsfristen können ihrer Natur nach nicht unbegrenzt in Anspruch genommen werden. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, daß sie dann nicht mehr anerkannt werden können, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert.
2. Während der Übergangsfrist reduziert sich die Befugnis zu Eingriffen auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebes“ unerlässlich ist. Es ist mithin unzulässig und mit den vom Bundesverfassungsgericht festgestellten reduzierten Befugnissen unvereinbar, bereits bestehende Datenverarbeitungsabläufe noch auszuweiten, etwa durch den Aufbau neuer Datenbanken oder die Ausschöpfung neuer technischer Möglichkeiten, soweit die Eingriffe in die Rechte der Betroffenen damit eine neue Qualität erreichen.

3. Besondere Zurückhaltung hat sich die Polizei dort aufzuerlegen, wo Eingriffe in das informationelle Selbstbestimmungsrecht noch weitere Grundrechte betreffen.

3.1 Die Feststellungen von Personalien, damit verbundene Datenabgleiche und Speicherungen sowie Film- und Videoaufnahmen sind anlässlich von öffentlichen Versammlungen während der Übergangszeit nur dann als zulässig anzusehen, wenn Anhaltspunkte dafür vorliegen, daß strafbare Handlungen begangen werden.

3.2 Die Nutzung technischer Hilfsmittel zur verdeckten Datenerhebung durch Lauschangriffe in Wohnungen muß grundsätzlich ausgeschlossen sein.

4. Der Einsatz von verdeckten Ermittlern und V-Leuten sowie langfristige Observationen und polizeiliche Beobachtung dürfen nur zugelassen werden, wenn konkrete Anhaltspunkte für bestimmte schwere Straftaten hestehen. Es muß festgelegt werden, wer diese Maßnahmen anordnen darf, wie die anfallenden Erkenntnisse verwertet werden dürfen und wann die Betroffenen zu unterrichten sind.

5. Im Hinblick auf die von den Verfassungsgerichten für die Übergangszeit geforderte Beschränkung auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebs“ unerlässlich ist, erinnern die Datenschutzbeauftragten an ihre früheren Beschlüsse zur polizeilichen Datenverarbeitung. Danach sind künftig insbesondere folgende Datenverarbeitungsvorgänge zu unterlassen:

- Speicherung diskriminierender personenbezogener Hinweise in polizeilichen Informationssystemen;
- Speicherung (ehemals) verdächtiger Personen zu Zwecken vorbeugender Straftatenbekämpfung ohne verantwortbare kriminologische Prognose;
- Speicherung von Daten über Personen, bei denen eine Anklageerhebung mangels öffentlichen Interesses abgelehnt wurde;
- Speicherung von Daten über Kinder, die der Begehung einer Straftat verdächtig werden;
- Weitergabe von Informationen, die mit speziellen polizeilichen Befugnissen erhoben wurden, an andere als Polizeidienststellen.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (Strafverfahrensänderungsgesetz vom 03.11.1988)

Die Konferenz begrüßt, daß ein Entwurf zur Regelung des Datenschutzes im Strafverfahrensrecht vorgelegt worden ist und daß darin für die besonderen Ermittlungs- und Fahndungsmethoden eigenständige Befugnisnormen vorgesehen sind sowie Regelungen zur Verarbeitung personenbezogener Daten und zur Akteneinsicht in die Strafprozeßordnung aufgenommen werden sollen.

Die im Entwurf vorgesehenen Datenschutzregelungen sind an den verfassungsrechtlichen Grundsätzen der Verhältnismäßigkeit und Normenklarheit zu messen. Weil im Bereich der Grundrechtsausübung nach der Rechtsprechung des Bundesverfassungsgerichts alle wesentlichen Entscheidungen vom Gesetzgeber selbst zu treffen sind, ist die gesamte Informationsverarbeitung wegen ihres Eingriffscharakters in der Strafprozeßordnung präzise und umfassend gesetzlich zu regeln.

Der vorliegende Entwurf entspricht den sich aus dem Recht auf informationelle Selbstbestimmung ergebenden Anforderungen noch nicht; er ist im übrigen unvollständig. Die Datenschutzkonferenz hebt deshalb unter gleichzeitiger Bezugnahme auf ihren Beschluß vom November 1986 folgende Kritikpunkte hervor:

1. Zu den Regelungen über die Ermittlungs- und Fahndungsmethoden

* Die Erhebung und Weiterverarbeitung personenbezogener Daten durch Strafverfolgungsorgane greift empfindlich in das Persönlichkeits-

recht der Bürger ein. Umso wichtiger ist es, nach dem Grad der Betroffenheit im Gesetz Abstufungen vorzunehmen. Zwischen dem Beschuldigten, dem Verdächtigen, dem von Vorfeldermittlungen Betroffenen und dem erkennbar nicht Verdächtigen (z.B. Geschädigten, Zeugen) sollte daher unterschieden werden. Vor allem die Regelungen über "Kontakt- und Begleitpersonen", "andere Personen" und "Dritte" werden dem nicht gerecht.

* Es muß klargestellt werden, daß die Ermittlungsgeneralklausel keine Eingriffe gestattet, die in ihrer Eingriffstiefe den besonders geregelten gleichkommen. So wären z.B. die Voraussetzungen des Einsatzes von V-Leuten besonders zu regeln. Auch weiterentwickelte "besondere Fahndungs- und Ermittlungsmethoden" dürfen nicht auf die Ermittlungsgeneralklausel gestützt werden. In die Strafprozeßordnung sind Verfahrensregelungen aufzunehmen, die eine Information etwa der zuständigen Parlamentsausschüsse über die beabsichtigte Anwendung vorsehen. Vor dem Einsatz qualitativ neuer Methoden müssen auf jeden Fall gesetzliche Regelungen geschaffen werden.

* Der Entwurf betont zu Recht, daß bei jeder einzelnen Ermittlungs- und Datenverarbeitungsmaßnahme der Grundsatz der Verhältnismäßigkeit zu beachten ist. Dies muß bereits in einzelnen Befugnisnormen zum Ausdruck kommen. Die bislang vorgesehenen Straftatenkataloge sind mit dem Ziel einer Einschränkung zu überprüfen;

die bloße Anknüpfung an den Begriff der "Straftat mit erheblicher Bedeutung" ohne weitere Differenzierung reicht nicht aus.

* Die Anordnung von Ermittlungs- und Fahndungsmethoden, die besonders stark in das Recht auf informationelle Selbstbestimmtheit eingreifen, ist dem Richter vorzubehalten. Gleiches gilt, wenn mit solchen besonderen Methoden erhobene Daten für andere Strafverfahren oder für andere - polizeiliche - Zwecke verwendet werden sollen.

* Wegen der Tiefe der Eingriffe bei besonderen Ermittlungs- und Fahndungsmethoden darf der Richtervorbehalt - von besonderen Eilfällen abgesehen - nicht durch Entscheidungen der Staatsanwaltschaft oder der Polizei ersetzt werden. Soweit ausnahmsweise die Staatsanwaltschaft oder die Polizei eine Anordnung treffen muß, dürfen erlangte Daten nicht weiter verwendet werden, wenn die richterliche Bestätigung ausbleibt; erhobene Daten sind zu löschen.

* Die Verwendung von durch besondere Ermittlungs- oder Fahndungsmethoden erlangten Daten für polizeiliche Zwecke muß neben dem Richtervorbehalt voraussetzen, daß das Polizeirecht vergleichbare Eingriffe gestattet oder daß die Daten zur Abwehr einer gegenwärtigen Gefahr für Leib und Leben erforderlich sind.

2. Zu den besonderen Regelungen über die Datenverarbeitung

Regelungen über die Datenverarbeitung im Strafverfahren setzen eine Gesamtkonzeption über die Informationsverarbeitung bei den Strafverfolgungsbehörden voraus. Notwendig sind insbesondere klare Bestimmungen über die Zusammenarbeit zwischen Staatsanwalt-

schaft und Polizei. Der vorliegende Entwurf läßt den hierzu notwendigen Konsens jedoch nicht erkennen.

* Der Gesetzgeber sollte möglichst genau regeln, welche Arten von Daten für "Zwecke des Strafverfahrens", für Zwecke anderer Strafverfahren oder für die Aufklärung künftiger Straftaten in automatisierten Dateien landes- oder bundesweit zur Verfügung stehen sollen und in welchem Verhältnis hierzu das Bundeszentralregister steht.

* Der Gesetzgeber muß, auch um Doppelspeicherungen zwischen staatsanwaltschaftlichen und polizeilichen Informationssystemen zu vermeiden, eindeutig festlegen, wem die Entscheidungsbefugnis über die bei der Strafverfolgung angefallenen Daten zusteht und für welche Zwecke sie verwendet werden dürfen.

* Daten, die für bloße Tätigkeitsnachweise gespeichert werden (Vorgangsverwaltung), dürfen für andere Zwecke nicht verwendet werden und müssen nach kurzen Fristen gelöscht werden.

* Die vorgesehene Speicherung von Daten über Personen, die "bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen", oder die "Opfer einer Straftat werden könnten", gibt zu Bedenken Anlaß, weil das Anlegen von Dateien über besondere Personengruppen wie z.B. Prostituierte, Homosexuelle und ausländische Gastwirte als erlaubt angesehen werden könnte.

* Die Datenspeicherung über Personen, die mangels hinreichendem Tatverdacht freigesprochen worden sind oder bei denen das Ermittlungsverfahren eingestellt oder die Anklage nicht zugelassen worden ist, darf nur unter engeren Voraussetzungen erfolgen.

3. Zur Akteneinsicht

Strafakten sind wegen ihres teilweise sehr sensiblen Inhalts geheimzuhalten. Sie dürfen deshalb auch anderen öffentlichen Stellen nur unter engeren Voraussetzungen zugänglich sein. Nicht am Strafverfahren beteiligte Personen dürfen auch über Rechtsanwälte allenfalls in besonderen Ausnahmefällen Einsicht oder Auskunft aus Strafakten erhalten.

4. Fehlende Regelungen

Regelungsbedürftig sind vor allem:

- * die engere Feststellung der Zulässigkeit erkennungsdienstlicher Behandlungen und der Voraussetzungen für den Fahndungsabgleich sowie die weitere Verwendung der dabei gewonnenen Daten,
- * die Verbesserung des Schutzes der Persönlichkeitsrechte bei der Erhebung persönlicher Daten von Angeklagten und Zeugen im Strafverfahren,
- * der allenfalls begrenzte Einsatz der Genomanalyse im Strafverfahren.

blätter des iz3w

Informationszentrum dritte welt - iz3w

Gen- und Biotechnologie in der Landwirtschaft und Auswirkungen in der „Dritten Welt“

Be-
zug:
blätter
des iz3w
Postf. 5328

Febr. 1989
Nr. 155
60 S.

7800 Freiburg

Buchhandel:

Prolit, Pf, 63 Gießen

8 mal im Jahr für 40/30 Mark
Einzelheft 5 DM + 1,50 DM Porto

»I-W-F – Mördertreff« Fotoband

**Büro für ungewöhnliche
Maßnahmen und Bundes-
kongress Entwicklungs-
politischer Aktionsgruppen/
BUKO (Herausgeber)**

Wut, Witz, Widerstand

Berlin, September 1988. Die Herren der Welt hatten geladen ... und alle, alle kamen. Am geladesten waren wohl die GegnerInnen von IWF und Weltbank.

Der Fotoband »Wut, Witz, Widerstand« beschreibt die politische Aktion der Gegenöffentlichkeit in der BRD 1988, zu der sich unzählige Gruppierungen in dem »breitesten außerparlamentarischen Oppositionsspektrum seit Bestehen der BRD« (Spiegel) zusammenfanden.

**WUT WITZ
WIDERSTAND**



Schmetterling Vg., Holzhauser Str. 31, 7 Stuttgart 80, ISBN 3-926369-59-0, 128 S., A4, Kunstdruckpapier, ca. DM 19,80. Über **Buchhandel** bzw. **Büro für ungewöhnl. Maßnahmen**, c/o FDGO im Kerngehäuse, Curvyrstr. 20, 1 Berlin 36, Tel. 030 / 611 94 04 (gegen Vorkasse, Scheck o.ä., zzgl. DM 3.-Porto)

IV. Verabschiedet:

Das Artikel-Gesetz zum Demonstrationsrecht, zur Kronzeugenregelung etc.

Nach anderthalb Jahren hat es die Bonner Koalition am 21.4.89 geschafft. Der Bundestag verabschiedete in 2. und 3. Lesung den Abbau des Demonstrationsrechts, die Kronzeugenregelung und weitere Strafrechtsverschärfungen sowie eine im letzten Augenblick nachgeschobene Befugnis für Ton- und Bildaufnahmen bei und in Zusammenhang mit öffentlichen Versammlungen.

1. Zum Gesetzgebungsverfahren

Nachdem die Ermordung von Braunmühls 1986 als Rechtfertigung für das "Gesetz zur Bekämpfung des Terrorismus" gedient hatte, boten die Schüsse an der Startbahn West des Frankfurter Flughafens, denen am 2. November 1987 zwei hessische Polizeibeamte zum Opfer gefallen waren, die Gelegenheit, erneut ein Paket von Repressionsparagrafen einzubringen. Um den angeblichen "Handlungsbedarf" zu decken, brachte die Koalition den Entwurf eines Artikelgesetzes ein, der eine Vielzahl von Rechtsänderungen zusammenfaßte (Dokumentation und Kritik in CILIP 29, S.134 ff.). Er enthielt folgende Punkte:

1. Einen § 130b des StGB, der die "Befürwortung von Gewalt" unter Strafe stellen sollte, angelehnt an den 1981 wieder abgeschafften § 88a. Dieser Zensurparagraf sollte den im Dezember 1986 im "Gesetz über die Bekämpfung des Terrorismus" eingeführten § 130a - Anleitung zu Straftaten - ergänzen;
2. Eine Erhöhung des Strafrahmens für erpresserischen Menschenraub (§ 239a), Geiselnahme (§ 239b), Diebstahl von Waffen und Sprengstoff (§ 243) sowie die Einführung eines besonders schweren Falls der

Störung öffentlicher Betriebe (§ 316b StGB).

3. Die Einfügung des schweren Landfriedensbruchs in den Katalog der Straftaten des § 112a StPO, der eine Verhängung von U-Haft bei Wiederholungsgefahr zuläßt.

4. Mehrere Verschärfungen im Versammlungsrecht:

- * die Pflicht zur Teilnahme an Vorbereitungsgesprächen zwischen Demonstrationsanmeldern und Polizei (§ 14 a)

- * das strafbewehrte Verbot des Aufrufs zu einer aufgelösten oder verbotenen Versammlung (§ 23)

- * die Ausweitung und Strafbewehrung des sog. Vermummungsverbots bei Demonstrationen (§ 17a und 29), das 1985 als Ordnungswidrigkeit ins Versammlungsgesetz eingeführt worden war.

5. Die Einführung einer Kronzeugenregelung für Terrorismus-Verfahren, die 1986 im "Gesetz über die Bekämpfung des Terrorismus" gescheitert war.

Der Bundesrat stimmte am 8.7.88 dem Gesetz mit Ausnahme von § 130b zu, woraufhin die Bundesregierung im August 1988 den Entwurf als Bundestagsdrucksache (Drs. Nr. 11/2834) vorlegte - einschließlich des inkriminierten Zensurparagrafen.

2. Die am 21. April d.J. verabschiedete Fassung

Sie folgte weiteren Änderungsanträgen der Koalitionsparteien. Verglichen mit der Drucksache vom August 1988 wurde vom Bundestag folgende Schlußfassung verabschiedet, die damit Rechtskraft erhalten hat:

Entfallen sind:

* Der Zensurparagraph 130 b des Entw.

* § 14a Versammlungs-G (Entw.), der die Anmelder einer Demonstration unter Androhung eines Bußgeldes zur Teilnahme an einem Vorgespräch mit der Polizei zwingen sollte.

Modifiziert wurde:

* Die Kronzeugenregelung. Der Entw. sah vor, daß der Generalbundesanwalt bei diesem Deal sich der Zustimmung des Ermittlungsrichters beim BGH versichern mußte; beschlossen wurde die von der FDP favorisierte Fassung, nach der der Generalbundesanwalt für einen Kronzeugendeal die Zustimmung eines Strafsenats des BGHs bedarf.

Geblichen sind:

* Die Anhebung der Vermummung und der sog. passiven Bewaffnung von einer Ordnungswidrigkeit zur Straftat

* Die Inkriminierung der "Zusammenrottung" in Verbindung mit Vermummung und "passiver Bewaffnung"

* Die Bestrafung des Aufrufs zu einer verbotenen Demonstration

* Die Erhöhung des Strafrahmens bei verschiedenen Delikten (§§ 239a und b, 243 und 316b), wenn auch mit kleinen Veränderungen.

* Der Haftgrund Wiederholungsgefahr in Fällen des Verdachts des schweren Landfriedensbruchs, ohne daß der Beschuldigte zuvor für eine solche Straftat verurteilt sein

müßte.

Neu eingeführt und verabschiedet wurde:

* Ein § 12a VersG, der die Polizei zu Bild- und Tonaufnahmen **bei und in Zusammenhang mit** öffentlichen Versammlungen ermächtigt. Auf diese kurzfristig im Handstreich neu eingeführten Regelung ins VersG lohnt es sich, genauer einzugehen. Ansonsten gilt unsere Kritik in CILIP 29, S.158 ff.

3. Videos und Wanzen bei Demonstrationen und ihrer Vorbereitung

Diese Frage ist seit 1986 Gegenstand der Diskussion um die Neuordnung der Polizeigesetze gewesen. Der "Musterentwurf eines einheitlichen Polizeigesetzes" (ME-PolG) der IMK von 1986 sieht dazu den § 8b "Datenerhebung bei öffentlichen Veranstaltungen, Ansammlungen und Versammlungen" vor, der in ähnlicher Form auch in den bereits vorliegenden Länderpolizeigesetz-Entwürfen übernommen worden ist. Zum Teil haben die Länder in dieser Frage aber durchaus liberalere Vorschläge präsentiert (z.B. NRW, vgl. CILIP 30, S. 32). Mit der Verabschiedung dieses § 12a VersG werden alle Hoffnungen, daß einzelne Länder zu liberaleren Lösungen, die dem Schutz des staatsfreien Demonstrationsrechts besser gerecht würden, schlicht und einfach begraben. Die Länderhoheit im Polizeirecht wird durch diesen Coup einfach ausgehoben.

Zu den Regelungen im einzelnen (vgl. auch den Brief des Hamburgerischen Datenschutzbeauftragten Schapper an den Innensenator der Hansestadt, abgedruckt in der TAZ, 21.4.89):

1. Bild- und Tonaufnahmen sollen

Artikel 3

Änderung des Versammlungsgesetzes
und des Strafgesetzbuches

(1) Das Versammlungsgesetz in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1789), zuletzt geändert durch ... (BGBl. I S. ...), wird wie folgt geändert:

1. Nach § 12 wird eingefügt:

„§ 12 a

(1) Die Polizei darf Bild- und Tonaufnahmen von Teilnehmern bei oder in Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von ihnen erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Die Unterlagen sind nach Beendigung der öffentlichen Versammlung oder zeitlich und sachlich damit unmittelbar in Zusammenhang stehender Ereignisse unverzüglich zu vernichten, soweit sie nicht benötigt werden

1. für die Verfolgung von Straftaten von Teilnehmern oder
2. im Einzelfall zur Gefahrenabwehr, weil die betroffene Person verdächtig ist, Straftaten bei oder im Zusammenhang mit der öffentlichen Versammlung vorbereitet oder begangen zu haben, und deshalb zu besorgen ist, daß von ihr erhebliche Gefahren für künftige öffentliche Versammlungen oder Aufzüge ausgehen.

Unterlagen, die aus den in Satz 1 Nr. 2 aufgeführten Gründen nicht vernichtet wurden, sind in jedem Fall spätestens nach Ablauf von drei Jahren seit ihrer Entstehung zu vernichten, es sei denn, sie würden inzwischen zu dem in Satz 1 Nr. 1 aufgeführten Zweck benötigt.

(3) Die Befugnisse zur Erhebung personenbezogener Informationen nach Maßgabe der Strafprozeßordnung und des Gesetzes über Ordnungswidrigkeiten bleiben unberührt.“

angefertigt werden dürfen, wenn "tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß (von den Teilnehmern) erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen" (Abs.1). Von erheblichen Gefahren kann aber bereits ausgegangen werden, wenn Gefahren für "nicht unwesentliche Vermögenswerte" vorliegen. Tatsächliche Anhaltspunkte für eine solche Gefahr könnten bereits vorliegen, wenn ein wortradikales Flugblatt vor einer Demonstration auftaucht.

2. In diesem Falle sind Aufnahmen aber nicht nur bei der Demonstration selbst möglich. Die Formulierung "bei oder im Zusammenhang mit öffentlichen Versammlungen" läßt vielmehr auch Mitschnitte bei Vorbereitungstreffen und nicht-öffentlichen Versammlungen im Vorfeld einer Demonstration zu. Es geht also auch um das "nicht-öffentlich gesprochene Wort", um den Lauschangriff, der dann wohl durch Polizeibeamte in Zivil erfolgen wird. Damit wird nicht nur die Freiheit der Demonstration eingeschränkt, sondern auch die Unverletzlichkeit der Wohnung.

3. Von den Aufnahmen dürfen auch andere Personen betroffen sein, von denen keine Gefahr ausgeht, also auch eindeutig friedliche Demonstranten.

4. Grundsätzlich sollen die entsprechenden Daten nach der Demonstration unverzüglich vernichtet bzw. gelöscht werden. Weiterbenutzt werden dürfen diejenigen Unterlagen und Daten, die für die Strafverfolgung (Abs.2, Nr.1), aber auch zu präventiv-polizeilichen Zwecken (Nr.2) "benötigt" werden. Während die Daten für Strafverfolgungszwecke von der Polizei unbefristet gehalten werden dürfen, dürfen sie zu präventiven

Zwecken zunächst über drei Jahre aufbewahrt werden. Die Dauer der Speicherung verlängert sich jeweils, wenn die entsprechende Voraussetzung der Aufbewahrung, die im folgenden beschriebene Gefahrenvermutung, erneut erfüllt wird.

Diese besteht zum einen darin, "daß die Person verdächtig ist, Straftaten bei oder im Zusammenhang mit der öffentlichen Versammlung vorbereitet oder begangen zu haben". Bereits der Verdacht einer nicht strafbaren Vorbereitung reicht also für eine Speicherung über einen längeren Zeitraum aus.

Die Formulierung in Abs.2 Nr.2 knüpft die Weiterverwendung der Unterlagen zum anderen an eine Gefahrenprognose: wenn eine Person verdächtigt wird, bei oder im Zusammenhang der entsprechenden Demonstration Straftaten begangen oder geplant zu haben, dann ist "deshalb (auch) zu besorgen (...), daß von ihr erhebliche Gefahren für künftige öffentliche Versammlungen oder Aufzüge ausgehen".

Fazit

Die Geschichte dieses Gesetzes belegt eindrücklich den Umgang der Regierenden mit zentralen demokratischen Grundrechten. Jeder beliebige Anlaß ist recht, das ewige Mißtrauen vor einer autonomen bürgerlichen Äußerung ohne staatliche Einmischung und Kontrolle erneut in Gesetze umzusetzen. Es ist deshalb auch kein Zufall, daß der CDU-Abgeordnete Stark bei der Verabschiedung des Gesetzes nicht mehr an die Schüsse an der Startbahn erinnert, sondern nunmehr auf die Demonstrationen und Aktionen im Zusammenhang des Hungerstreiks der

RAF-Häftlinge verweist. Bei der Beliebigkeit der Anlässe darf jetzt bereits auf das nächste Artikelgesetz gewartet werden. Vielleicht schafft es die CDU dann, den alten Landfriedensbruch-Paragrafen, für dessen Wiedereinführung sie sich seit seiner Abschaffung 1970 stark gemacht hat, wieder durchzusetzen.

Die Gegenstimmen aus den Reihen der FDP sind zwar zu begrüßen. Solange sie aber ihren Widerstand danach kalkulieren, daß die Nein-Stimmen nicht den Koalitionsbeschluß und die Parteidisziplin gefährden, werden die liberalen FDP-Abgeordneten nur halbe Glaubwürdigkeit verlangen können.

Chronologie der Ereignisse:

Dezember 88

14.12. Im Zusammenhang mit der Affäre um die Ermordung des Studenten Schmücker im Berliner Grunewald 1972, verdichten sich die Hinweise, daß dem V-Mann Weingruber vom Bundesamt für Vfs "Schweigegehd" in Höhe einer sechsstelligen Summe gezahlt worden ist.

Es bestätigt sich, daß der Berliner Vfs das Mitglied der PKK Pätzold (SPD) bespitzeln ließ.

Das Berliner LG hält die Genomanalyse grundsätzlich für ein gültiges Beweismittel.

16.12. Das Regensburger VG erklärt ein Demonstrationsverbot für rechtswidrig, das damit begründet worden war, daß die Teilnahme von Kindern den Tatbestand der "passiven Bewaffnung" erfülle.

Artikel 3

Änderung des Versammlungsgesetzes
und des Stragesetzbuches

(1) Das Versammlungsgesetz in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1789), zuletzt geändert durch ... (BGBl. I S. ...), wird wie folgt geändert:

1. Nach § 12 wird eingefügt:

„§ 12 a

(1) Die Polizei darf Bild- und Tonaufnahmen von Teilnehmern bei oder in Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Die Unterlagen sind nach Beendigung der öffentlichen Versammlung oder zeitlich und sachlich damit unmittelbar in Zusammenhang stehender Ereignisse unverzüglich zu vernichten, soweit sie nicht benötigt werden

1. für die Verfolgung von Straftaten von Teilnehmern oder
2. im Einzelfall zur Gefahrenabwehr, weil die betroffene Person verdächtig ist, Straftaten bei oder im Zusammenhang mit der öffentlichen Versammlung vorbereitet oder begangen zu haben, und deshalb zu besorgen ist, daß von ihr erhebliche Gefahren für künftige öffentliche Versammlungen oder Aufzüge ausgehen.

Unterlagen, die aus den in Satz 1 Nr. 2 aufgeführten Gründen nicht vernichtet wurden, sind in jedem Fall spätestens nach Ablauf von drei Jahren seit ihrer Entstehung zu vernichten, es sei denn, sie würden inzwischen zu dem in Satz 1 Nr. 1 aufgeführten Zweck benötigt.

(3) Die Befugnisse zur Erhebung personenbezogener Informationen nach Maßgabe der Strafprozeßordnung und des Gesetzes über Ordnungswidrigkeiten bleiben unberührt.“

angefertigt werden dürfen, wenn "tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß (von den Teilnehmern) erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen" (Abs.1). Von erheblichen Gefahren kann aber bereits ausgegangen werden, wenn Gefahren für "nicht unwesentliche Vermögenswerte" vorliegen. Tatsächliche Anhaltspunkte für eine solche Gefahr könnten bereits vorliegen, wenn ein wortradikales Flugblatt vor einer Demonstration auftaucht.

2. In diesem Falle sind Aufnahmen aber nicht nur bei der Demonstration selbst möglich. Die Formulierung "bei oder im Zusammenhang mit öffentlichen Versammlungen" läßt vielmehr auch Mitschnitte bei Vorbereitungstreffen und nicht-öffentlichen Versammlungen im Vorfeld einer Demonstration zu. Es geht also auch um das "nicht-öffentlich gesprochene Wort", um den Lauschangriff, der dann wohl durch Polizeibeamte in Zivil erfolgen wird. Damit wird nicht nur die Freiheit der Demonstration eingeschränkt, sondern auch die Unverletzlichkeit der Wohnung.

3. Von den Aufnahmen dürfen auch andere Personen betroffen sein, von denen keine Gefahr ausgeht, also auch eindeutig friedliche Demonstranten.

4. Grundsätzlich sollen die entsprechenden Daten nach der Demonstration unverzüglich vernichtet bzw. gelöscht werden. Weiterbenutzt werden dürfen diejenigen Unterlagen und Daten, die für die Strafverfolgung (Abs.2, Nr.1), aber auch zu präventiv-polizeilichen Zwecken (Nr.2) "benötigt" werden. Während die Daten für Strafverfolgungszwecke von der Polizei unbefristet gehalten werden dürfen, dürfen sie zu präventiven

Zwecken zunächst über drei Jahre aufbewahrt werden. Die Dauer der Speicherung verlängert sich jeweils, wenn die entsprechende Voraussetzung der Aufbewahrung, die im folgenden beschriebene Gefahrenvermutung, erneut erfüllt wird.

Diese besteht zum einen darin, "daß die Person verdächtig ist, Straftaten bei oder im Zusammenhang mit der öffentlichen Versammlung vorbereitet oder begangen zu haben". Bereits der Verdacht einer nicht strafbaren Vorbereitung reicht also für eine Speicherung über einen längeren Zeitraum aus.

Die Formulierung in Abs.2 Nr.2 knüpft die Weiterverwendung der Unterlagen zum anderen an eine Gefahrenprognose: wenn eine Person verdächtig wird, bei oder im Zusammenhang der entsprechenden Demonstration Straftaten begangen oder geplant zu haben, dann ist "deshalb (auch) zu besorgen (...), daß von ihr erhebliche Gefahren für künftige öffentliche Versammlungen oder Aufzüge ausgehen".

Fazit

Die Geschichte dieses Gesetzes belegt eindrücklich den Umgang der Regierenden mit zentralen demokratischen Grundrechten. Jeder beliebige Anlaß ist recht, das ewige Mißtrauen vor einer autonomen bürgerlichen Äußerung ohne staatliche Einmischung und Kontrolle erneut in Gesetze umzusetzen. Es ist deshalb auch kein Zufall, daß der CDU-Abgeordnete Stark bei der Verabschiedung des Gesetzes nicht mehr an die Schüsse an der Startbahn erinnert, sondern nunmehr auf die Demonstrationen und Aktionen im Zusammenhang des Hungerstreiks der

RAF-Häftlinge verweist. Bei der Beliebigkeit der Anlässe darf jetzt bereits auf das nächste Artikelgesetz gewartet werden. Vielleicht schafft es die CDU dann, den alten Landfriedensbruch-Paragrafen, für dessen Wiedereinführung sie sich seit seiner Abschaffung 1970 stark gemacht hat, wieder durchzusetzen.

Die Gegenstimmen aus den Reihen der FDP sind zwar zu begrüßen. Solange sie aber ihren Widerstand danach kalkulieren, daß die Nein-Stimmen nicht den Koalitionsbeschluß und die Parteidisziplin gefährden, werden die liberalen FDP-Abgeordneten nur halbe Glaubwürdigkeit verlangen können.

Chronologie der Ereignisse:

Dezember 88

14.12. Im Zusammenhang mit der Affäre um die Ermordung des Studenten Schmücker im Berliner Grunewald 1972, verdichten sich die Hinweise, daß dem V-Mann Weingruber vom Bundesamt für Vfs "Schweigegehd" in Höhe einer sechststelligen Summe gezahlt worden ist.

Es bestätigt sich, daß der Berliner Vfs das Mitglied der PKK Pätzold (SPD) bespitzeln ließ.

Das Berliner LG hält die Genomanalyse grundsätzlich für ein gültiges Beweismittel.

16.12. Das Regensburger VG erklärt ein Demonstrationsverbot für rechtswidrig, das damit begründet worden war, daß die Teilnahme von Kindern den Tatbestand der "passiven Bewaffnung" erfülle.

21.12. Die Ermittlungen wegen des Bombenanschlags auf die Berliner Diskothek "La Belle" werden eingestellt.

22.12. Das bayerische OLG verurteilt eine 23jährige Frau wegen Unterstützung einer terror. Vereinigung zu zehn Monaten Haft mit vierjähriger Bewährungsfrist. Sie hatte 1986 eine Veranstaltung zur "Situation der politischen Gefangenen in der BRD" organisiert.

Januar 89

5.1. Das Abhören von Telefongesprächen in West-Berlin soll künftig auch bundesdeutschen Dienststellen gestattet werden. Nach dem Willen der Alliierten sollen auf Wunsch des Berliner CDU/FDP-Senats die entsprechende Bundesgesetze übernommen werden.

9.1. Die Datenschutzbeauftragte von Baden-Württemberg legt ihren Bericht vor und erhebt schwere Vorwürfe gegen die Sicherheitsbehörden, weil das LKA 354 Personen des öffentlichen Lebens unzulässig in der Staatschutzdatei APIS gespeichert hat.

17.1. Das Hamburger OLG verurteilt den 39jährigen Physiklehrer Storim wegen Unterstützung einer terror. Vereinigung zu einem Jahr Haft ohne Bewährung.

18.1. Das Stuttgarter OLG verurteilt R. Prauss und A. Sievering zu neun Jahren Gefängnis, wegen Beteiligung an dem Sprengstoffanschlag auf die Firma Dornier.

19.1. Nach Ansicht des BVerwG kann der Staat die Bewaffnung des Werkschutzes für Atomkraftwerke mit Faustfeuerwaffen zwingend vorschreiben.

20.1. Das Düsseldorf OLG verurteilt vier Angeklagte wegen Mitgliedschaft in einer terror. Vereinigung und Beteiligung an einem Sprengstoffanschlag zu Haftstrafen

zwischen 4 und 9 Jahren.

24.1. Prozeßbeginn vor dem Frankfurter OLG gegen zwei junge Männer wegen Mitgliedschaft und Unterstützung einer terror. Vereinigung (§129a).

29.1. Berliner Abgeordnetenhauswahl. Es beginnen Koalitionsverhandlungen zwischen SPD und AL, die zu einem "Rot-Grünen" Senat führen.

Februar 89

1.2. 28 RAF-Häftlinge beginnen einen Hungerstreik, mit dem Ziel der Zusammenlegung aller "Politischen Gefangenen".

2.2. Die Hamburger Bürgerschaft beschließt die Einführung eines kommunalen Ausländerwahlrechts.

15.2. Prozessbeginn vor dem OLG Düsseldorf gegen Ingrid Strobl wegen Mitgliedschaft in einer terror. Vereinigung und Beteiligung an einem Bombenanschlag.

In einem Strafverfahren in Berlin wird zum zweiten Mal der genetische Fingerabdruck als Beweismittel verwendet.

21.2. Der Berliner Innensenator Kewenig verweigert zwei Beamten des VfS die Aussagegenehmigung vor dem parlamentarischen Untersuchungsausschuß.

27.2. Der neue Innenminister von Schleswig-Holstein Bull hebt den Erlaß zur Einführung des Reizgases "CS" für die Polizei auf.

23.2. Der Prozeß um die Politistenmorde v. 2.11.87 an der Startbahn West beginnt.

26.2. Nach Informationen der TAZ und des SPIEGELS ist ein Grüner Bremer Bürgerschaftsabgeordneter vom amerikanischen Geheimdienst (NSA) überwacht und abgehört worden.

28.2. Sieben Telefonanschlüsse von AKW-Gegnern sollen vom LfV Niedersachsen illegal abgehört worden sein.

März 89

2.3. Die Verwaltung der besetzten Häuser in der Hamburger Hafentrasse wird der Lawaetz-Stiftung durch einen Bürgerschaftsbeschluss entzogen und zukünftig der senatseigenen Verwaltungsgesellschaft "Hafenrand mbH" übertragen.

Der Berliner Untersuchungsausschuß zu den Aktivitäten des VfS bestätigt, daß die TAZ seit ihrer Gründung bespitzelt worden ist.

Der zuständige Staatsanwalt beim LG Amberg stellt die Ermittlungen gegen Beamte der Berliner Sondereinheit EbLT wegen Körperverletzungen bei einer Anti-WAA-Demonstration ein.

Die EbLT wird mit sofortiger Wirkung aufgelöst.

12.3. Bundespräsident Richard v. Weizsäcker begnadigt die ehemalige RAF-Angehörige Angelika Speitel.

Der Juwelier Rene Düe wird endgültig vom Vorwurf freigesprochen, einen Millionenraub in seinem Geschäft vorgetäuscht und Versicherungsbetrug begangen zu haben. Maßgeblich beteiligt an der Konstruktion diese Vorwurfs war der Versicherungsdetektiv Werner Mauss.

14.3. Der bayerische Landtag verabschiedet eine Verschärfung des Polizeiaufgabengesetzes, wonach der Unterbringungsgewahrsam für mutmaßliche Störer von 48 Stunden auf 2 Wochen ausgedehnt wird.

15.3. Der frühere Bundesdatenschutzbeauftragte und jetzige Innenminister von Schleswig-Holstein, Bull, unterliegt in einem Rechtsstreit dem früheren Präsidenten des BKA, Horst Hehold, der sich durch eine Publikation von Bull in seinen

Persönlichkeitsrechten verletzt gefühlt hatte.

Große Bundestagsdebatte über den "Deutschen Herbst" 1977.

Der Leiter des Berliner VfS Wagner wird vom neuen Innensenator Pätzold entlassen.

24.3. Das Bremer VG urteilt, daß die Polizei aus verfassungsrechtlichen Gründen eine Demonstration grundsätzlich nicht in einem sogenannten Wanderkessel einschließen darf. Gleichzeitig bezeichnen die Richter eine erfolgte umfassende Foto- und Videoüberwachung der Demonstranten als rechtswidrig (4 A 226/86).

Der BGH hebt das 3. Urteil im Schmücker-Prozeß wegen Verfahrensfehler auf. Es muß zum vierten Mal verhandelt werden.

April 89

16.4. Neuer Bundesinnenminister wird der bisherige Kanzleramtsminister Wolfgang Schäuble.

18.4. Nach der Fußballkatastrophe in Sheffield will Premierministerin Thatcher den Kennkartenzwang für Fußballzuschauer einführen.

Bei dem Versuch, eine Bombe zu entschärfen, wird ein Beamter des BKA getötet.

20.4. Der Bundestag verabschiedet das Poststrukturgesetz, das u.a. neue Befugnisse zur Überwachung der technischen Kommunikationsformen enthält (vgl. diese Ausgabe).

21.4. Der Bundestag verabschiedet ein Artikelgesetz mit einer Regelung für die strafrechtliche Behandlung von Kronzeugen und einschneidenden Eingriffen in das Demonstrationsrecht u.a. (vgl. diese Ausgabe).

24.4. Der Hamburger Senat kündigt die Mietverträge mit der Hafenstraße fristlos.

Summary:

This is once more an edition which is devoted exclusively to internal security legislation in the Federal Republic of Germany. Strong public pressure forced the coalition of Christian Democrats and Free Democrats to change earlier drafts of the legislation from 1985. In this issue we publish the following revised drafts that were introduced into the West German parliament in April 1989:

- the law concerning the cooperation between the federal and state internal intelligence agencies
- * the Military intelligence service act (MAD)
- * the Federal espionage service act (BND)
- * the Federal data protection act
- * the public service procedure act
- regulating the handling of personal data in public service agencies.

Besides these drafts which are introduced into parliament as a single set of measures, we also present other laws and drafts that are concerned with the handling of data by internal security agencies:

- * a draft for a criminal procedure act which regulates the dataprocessing of public prosecution agencies
- * a new law which has been passed by the legislator in April that allows the police and intelligence agencies to survey all new technological means of communication (telefax etc.) and requires that private companies in the communication sector assist the police and intelligence agencies in its surveillance of private communication
- * a new law, also recently passed, that allows the police not only to

survey demonstrations but also the preparation process with audio and video means. Additionally we document legislation regulating

- * the constitutional right of public demonstrations
- * the introduction of chief witnesses in trials against so-called terrorists.

We add materials and legislation acts to this issue that we think to be important in giving a full picture of the present state of internal security laws in the FRG.

The editorial discusses the meaning of this new legislative effort for the constitutional rights of citizens and tries to highlight the political and sociological background of the law making process. In the Seventies the structure, the tactical concepts and technical means of the police and the intelligence agencies in the FRG were undergoing rapid changes. Two important developments correspond to those changes: On the one hand a new political activism with different goals and strategies, on the other a decisive change in the policing strategies of the state, brought about by the Social Democrats. Risk and crisis prevention being their objective, they aimed at a general modernization of the state bureaucracy. "Information" became one of the main resources of state policing - supported by new technological means and computerization.

One immediate result of those policies was a ruling passed down by the German Supreme Court in 1983 (the so-called public census decision), in which strict rules were set for the collection and processing of information of citizens and new legislation was called for. After the CDU/FDP coa-

lition came into power in 1982 they started to draw up new legislation since fall 1985 (see CILIP No. 21). Under insistent public pressure revised drafts were presented in the course of the last years (see CILIP No. 21, 23, 29, 31).

Summarizing our evaluation of these drafts and, partly already, laws, we come to the following conclusions:

* Formally at least they meet the demands of the Supreme Court decision by providing a legislative basis for state datacollection and processing

* In their substance most of the proposals and laws contradict the principles set by the Supreme Court as well as constitutional rights of citizens in this country

* One of the major new developments enforced by this legislation is the granted right to the police to adopt intelligence measures such as the deployment of undercover agents and video surveillance of the population

* An uncontrollable flow of data can be set up between the police and intelligence and secret service agencies. Additionally intelligence agencies are given the right to pass on information to private agencies and foreign governmental agencies.

* Social security agencies as well as semi-state organizations like the TÜV are forced to open their computer based information systems on request of the security agencies. Not the "owner" of the information but the requesting agency has to decide on the legality of the request.

So far public protest has managed to delay the quick passing of certain legislation measures. CILIP

wants to support this protest with information and critical reasoning.

Wieviel INFORMATION braucht der Mensch?



Robert Jungk:

Die Blätter haben für mich
in der weitgehend unrichti-
schen, mächtiggehobenen
deutschen Medienland-
schaft einen ganz beson-
deren Stellenwert

*
*
* Wir können an dieser
* Stelle schreiben.
* Die Blätter sind die auf-
* sagenstärkste und meist-
* abonnierte politisch-
* wissenschaftliche
* Monatszeitschrift in
* deutscher Sprache

*
* Wir finden es besser,
* wenn Sie sich selber Ihr
* Urteil bilden.

*

Blätter für deutsche und internationale Politik

ANFORDERUNGSCOUPON

Ich habe kein Surimi, bitte mich kostenloses Probestampfen vollständig unverändert zu verschicken

Ich möchte die abonnieren. Zum Preis von jährlich 52,- DM (Schüler/Studenten DM 63,-) und Versandkosten

Name (Nachname)

Strasse

PLZ, Wohnort

Datum (monat/jahr)

Vorname (Nachname) (Bitte nicht
verändern) (Bitte nicht ändern)
Ich will die Blätter für meine Mitbestim-
mung, meine Meinung, meine Haltung
äußern

Datum (monat/jahr)

Aus dem Inhalt der letzten Hefte

Bürgerrechte & Polizei Nr.27

- * Verfassungsschutz:
Organisation - EDV - Personalentwicklung und Kosten
- * Die Männer vom Amt - Zur Personalpolitik
- * Zum Trennungsgebot:
Polizei und Geheimdienste: Sicherheitspolitische "Wiedervereinigung"?
- * Verfassungsschutz und Volkszählung
- * Das "Celler Loch" - "Terrorbekämpfung" und die Kontrolle des Verfassungsschutzes
- * Sicherheitsüberprüfung:
Politischer Ariernachweis als Regelanfrage gegen Jedermann

Bürgerrechte & Polizei Nr. 28

- * Verfassungsschutz-Skandale:
Eine Chronik
- * Schmücker-Prozeß: Der VfS als Herr des Strafverfahrens
- * Baden-Württemberg: Parlamentarische Kontrolle des Verfassungsschutzes
- * Bewußtseinspolizei - Öffentlichkeitsarbeit eines Geheimdienstes
- * Der Auskunftsanspruch gegenüber VfS-Behörden und Polizei

* Beobachtungsobjekt Verfassungsfeind: Vom KPD-Verbot bis zur Sammlung extremistischer Äußerungen

* Der Verfassungsschutz im Spiegel der Literatur

Bürgerrechte & Polizei Nr. 30

- * EbLT: Ein Spezialbataillon der Berliner Verwaltung
- * Von Interpol zu TREVI - Polizeiliche Zusammenarbeit in Europa
- * Die Verrechtlichung operativer Polizeiarbeit
- * Sammelrezension Polizeigeschichte
- * SPUDOK-Prozesse

Bürgerrechte & Polizei Nr.31

- * Dokumentation & Kritik:
 - Entw. BKA-Gesetz
 - Entw. Ausländerzentralregister-G
- * Fallstudie: Polizeiaktionen während der IWF-Tagung
- * Polizeiliche Schußwaffeneinsatz 87
- * Polizeiliche Entwicklungshilfe - Ein Betrag zur "Befriedigung staatlicher Grundbedürfnisse" in der 3. Welt

Bestellungen an:

Kirschkern Buchversand, Hohenzollerndamm 199, 1000 Berlin 31.
Bei Abschluß eines Abonnements sind einmalig zurückliegende Hefte zum Abo-Preis von je DM 7,- (plus Versandkosten) beziehbar.

Albrecht Funk

Polizei und Rechtsstaat

Entstehungsgeschichte der preu-
Bischen Polizei 1848 – 1914
1986. 406 S., DM 88,-
ISBN 3-593-33524-7

Nicht wachsende Kriminalität
und neu entstehende Ordnungs-
probleme der bürgerlichen Ge-
sellschaft sind es, die Entstehung
und Ausbau einer polizeilichen
Exekutivgewalt im 19. Jahrhun-
dert prägen und bestimmen, son-
dern der Konflikt um die Form
der staatlichen Herrschaftsge-
walt. In der Entstehungsges-
chichte der Polizei spiegelt sich
diese Auseinandersetzung in be-
sonders scharfer Weise wider.
Worum es in diesem Konflikt um
die Staatsgewalt ging, in welchen
Kompromissen zwischen monar-
chischem Staat und Bürgertum
dieser mündete und wie sich dies
im Aufbau und den Strukturen
der deutschen Polizei nieder-
schlug, wird aus den Akten der
preußischen Ministerien heraus-
gearbeitet. Die historische Ana-
lyse schärft dabei den Blick für
eine auch heute noch aktuelle
Frage: In welcher Form und mit
welchen Mitteln kann die Polizei
gesellschaftlich so eingebunden
werden, daß die direkte Kon-
trolle der Bürger über die staatliche
Zwangsgewalt erhalten und die
bürgerlichen Freiheiten unan-
getastet bleiben?

Die aktuellen Veränderungen der
Polizei (vgl. dazu Busch, Funk
u.a., *Die Polizei in der Bundesre-
publik*, Campus 1985) sind kaum
zu verstehen, wenn man die histo-
rischen Wurzeln des Polizeisys-
tems nicht kennt.

Autor: Albrecht Funk ist Privat-
dozent am Fachbereich 15 der
Freien Universität Berlin.

Campus Verlag

Bockenheimer Landstraße 100
6000 Frankfurt/Main 1
Tel. (069) 7401 12-16
Telefax: (069) 7401 17

Heiner Busch
Albrecht Funk,
Udo Kauß,
Wolf-Dieter Narr,
Falco Werkentin
**Die Polizei
in der
Bundesrepublik**

1985. 508 S., DM 68,-
ISBN 3-593-33413-5

Welche Rolle spielt die Poli-
zei in der Bundesrepublik? Wie
ist sie auf Länder- und Bundes-
ebene organisiert? Wofür wird sie
von den staatlichen Instanzen ein-
gesetzt? Mit welchen Waffen und
Informationstechnologien ist sie
ausgerüstet? Aber auch: Wie läßt
sie sich kontrollieren? Wie kann
der Bürger sich gegen sie wehren?

**Neu:
Studienausgabe
DM 38,-**

Falco Werkentin
**Die Restauration
der deutschen
Polizei**

Innere Rüstung von 1945 bis zur
Notstandsgesetzgebung
252 S., 14,8 × 21 cm,
DM 39,-, November 1984
ISBN 3-593-33426-7

Die Polizei ist
mehr, als sich aus Verfassungsn-
ormen und offiziellen Bekun-
dungen ableiten läßt. Ihre wirkliche
Funktion in der politischen
Struktur einer Gesellschaft wird
bestimmt durch die Form ihrer
Organisation, ihrer Rekrutierung,
Ausbildung und Ausrüstung. Unter
diesem Gesichtspunkt zeichnet
der Autor Entstehung, Tradition
und Wandel der westdeutschen
Polizei nach.

Autor: Falco Werkentin ist Mit-
herausgeber des Informations-
dienstes „Bürgerrechte und Polizei
(CILIP)“. Co-Autor von Funk
u. a., *Verrechtlichung und Ver-
drängung*, Opladen 1984 und von
Busch u. a., *Die Polizei in der
Bundesrepublik*, Campus 1984

Udo Kauß

Der suspendierte Datenschutz bei Polizei und Geheimdiensten

Ca. 350 S., 14,8 × 21 cm,
ca. DM 58,-, Oktober 1988
ISBN 3-593-34051-8

Die Kontrolleure zu kontrollieren:
das ist die Aufgabe der Daten-
schützer in Bund und Ländern.
Dieses Buch nun analysiert Insti-
tution und Wirksamkeit des Daten-
schutzes – und kommt zu Ergeb-
nissen, die alles andere als beru-
hend sind.

Die Datenschutzbeauftragten ha-
ben sich überwiegend in die Rolle
eines Organs regierungsamtlicher
Akzeptanzbildung drängen lassen.
Sie konnten immer nur die Rand-
niemals jedoch die Kernbereiche
exekutiver Informationsgier be-
einflussen. Sie konnten Daten-
schutz nur dort verwirklichen, wo
er die Effizienz der Sicherheitsbe-
hörden zu steigern versprach.

Der Autor leistet jedoch mehr als
»bloß« eine Wirkungsanalyse der
Institution des Datenschutzbeauf-
tragten. Er bietet zugleich eine
materialreiche Einführung in die
Praxis und die Probleme der Si-
cherheitsbehörden und legt das
Labyrinth der sicherheitsbehördli-
chen Datenströme frei.

Deutlich wird, daß alle Kontroll-
probleme unlösbar bleiben müs-
sen, solange die bestehenden
Strukturen unangetastet bleiben
und ihnen der Datenschutz nur
»vorgeschaltet« wird. Denn ohne
eigene Eingriffsmöglichkeiten
sind die Datenschutzbeauftragten
auf den guten Willen der Si-
cherheitsbehörden angewiesen. Mit
ihrem einzigen echten Machtmittel,
der öffentlichen Anprange-
rung kritikwürdiger DV-Praxis,
gehen sie allzu sparsam und behör-
denfreundlich um. Der Daten-
schutz als Bürgerrecht droht dabei
auf der Strecke zu bleiben.

Autor: Udo Kauß lebt als Rechts-
anwalt in Freiburg. Er ist Mitglied
des Bundesvorstandes der Huma-
nistischen Union, Mitherausgeber
von *Bürgerrechte und Polizei* und
Mitautor von *Die Polizei* (Campus
1985).