grundrechte.ch

Postfach 6948, 3001 Bern, Tel. 031 312 40 30

schnueffelstaat@bluewin.ch

Der Verein grundrechte.ch (Grundrechte Schweiz) ist am 28. Oktober 2006 als Nachfolgeorganisation der Stiftung Archiv Schnüffelstaat Schweiz ASS gegründet worden.

Vernehmlassung BWIS II: Teilrevision Staatsschutzgesetz Stellungnahme von grundrechte.ch

Einleitende Bemerkungen:

Notwendigkeit einer wirklichen Evaluation staatsschützerischer Tätigkeiten

Im Juli 1998 ist das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) in Kraft getreten und bescherte dem Staatsschutz erstmals in seiner bis dahin über hundertjährigen Geschichte eine formelle gesetzliche Grundlage. Auf der Basis dieses Gesetzes bzw. der im Laufe der 90er Jahre vom Bundesrat erlassenen Verordnungen konnte vor allem die eidgenössische Staatsschutzzentrale – früher: Bundespolizei, heute: Dienst für Analyse und Prävention (DAP) – ihre durch den Fichenskandal angekratzte Macht sichern und mehren: Das Gesetz überführte wesentliche Teile der bestehenden Praxis der Überwachung ins Recht. Der DAP konnte seinen Personalbestand nicht nur stabilisieren, sondern ausbauen. Die Zahl der in ISIS, dem Datensystem des DAP, gespeicherten Personen erreichte bereits 2004 einen Bestand von über 60 000.

Der DAP trat mit zum Teil abenteuerlichen Bewertungen der inneren Lage der Schweiz an die Öffentlichkeit.

- Er konnte weiterhin Personen und Organisationen z.B. der Anti-Globalisierungsbewegung als „gewalttätig extremistisch“ desavouieren und etablierte dazu absurde Sprachregelungen („Farbanschlag“).
- Er konnte z.B. in den jährlichen Sicherheitsberichten Organisationen in den Kontext des Terrorismus rücken, ohne diese Fehlinformationen wirklich zu korrigieren.

Bei alledem blieben solche Bewertungen nicht folgenlos:

- Jeweils mehrere hundert Einreisesperren wurden zu den jährlichen Tagungen des WEF in Davos erlassen. Sie stützten sich auf von ausländischen Nachrichtendiensten und Sicherheitsbehörden übernommene Meldungen über angeblich gewalttätige GlobalisierungsgegnerInnen, die die Betroffenen aufgrund des fehlenden Akteneinsichtsrechts nicht korrigieren konnten. Gleiches gilt für die Datenweitergabe des DAP an ausländische Behörden wie etwa vor den Demonstrationen gegen den G8-Gipfel in Genua 2001.
- Der DAP mischte sich mit seinen Bewertungen ausländischer Organisationen und Einzelpersonen in Asylverfahren und in die Visumsvergabe ein.

Schon unter der heutigen Rechtslage sind Rechte des Einzelnen gegenüber dem Staatsschutz praktisch nicht vorhanden. Das Einsichtsrecht in die eigenen Daten ist per Gesetz faktisch abgeschafft. Selbst die im Gesetz vorgesehene nachträgliche Mitteilung an die Betroffenen wurde erst nach der Intervention des Eidgenössischen Datenschutzbeauftragten angegangen.

Eine öffentliche Kontrolle existiert nicht. Die selbst wiederum der Geheimhaltung unterliegende Geschaftsprüfungsdelegation **(**GPDel) der Eidgenössischen Räte erweist sich gerade wegen der fehlenden Öffentlichkeit als ein zahnloses Gremium von „Abnickern**".** Die Kontrolle durch die GPDel krankt zudem am Umstand, dass sie die vom DAP gesammelten Daten in aller Regel nicht auf ihre Richtigkeit hin überprüfen kann, sondern nur dahingehend, ob diese im Sinne des BWIS relevant sind (Terrorismus, verbotener Nachrichtendienst, gewalttätiger Extremismus. etc.). Dasselbe gilt auch für das – ohnehin nicht praxistaugliche – sog. stellvertretende Einsichtsrecht. Der DAP muss im Wesentlichen nur geschickt genug sein, die von ihm gesammelten Daten mit zureichenden Vermutungen über BWIS-relevante Zusammenhänge zu versehen, um vor weiterer Kontrolle sicher zu sein. Damit kann die Kontrolle durch die GPDel kein wirksamer Ersatz für das Einsichtsrecht der Betroffenen sein.

Vor diesem Hintergrund, der hier nur in Stichworten referiert werden kann, braucht es zunächst einmal eine grundsätzliche Evaluation der (Fehl-)Leistungen des Staatsschutzes und der aus diesen präventiven Befugnissen resultierenden Gefahren für die Demokratie.

Statt die Tätigkeit des Staatsschutzes einer eingehenden Überprüfung zu unterziehen und mindestens das Akteneinsichts- bzw. Datenauskunftsrecht wiederherzustellen, hat das EJPD seit den Anschlägen in den USA vom 11. September 2001 den DAP selbst an einer Erweiterung seiner gesetzlichen Befugnisse stricken lassen. Der Leiter des DAP präsidierte die Arbeitsgruppen, die die Gesetzesverschärfungen vorbereiteten. Das Ergebnis war bzw. ist, dass die Wunschlisten des Staatsschutzes in gesetzliche Regelungen bzw. Entwürfe umgebaut werden.

Das gilt sowohl für die vom Parlament bereits beschlossene erste Revision des BWIS („Massnahmen gegen Gewalt bei Sportveranstaltungen" – BWIS I), deren Anlass ursprünglich die Störung der 1.August-Rede des damaligen Bundesrates Kaspar Villiger auf dem Rütli war. Und das gilt umso mehr für den jetzt vorliegenden Entwurf. Hier durfte der DAP schon im Jahre 2002 kundtun, dass er die einzige wirkliche Grenze im bestehenden Gesetz – das Verbot von strafprozessualen Zwangsmassnahmen – aufgehoben sehen möchte. Ähnliche Erklärungen, das geltende Gesetz sei zu liberal, weil es Informationsbeschaffung in der Privatsphäre nicht erlaube, folgten im Extremismusbericht von 2004.

Ein erster Entwurf für eine Revision des BWIS in diesem Sinne wurde 2005 zurückgezogen, nachdem er als „Indiskretion" in die Presse gelangt war. Ein zweiter Entwurf fand sich ohne vorherigen Beschluss des Bundesrates auf der Homepage des BAP. Der nun vorliegende Vernehmlassungsentwurf ist damit der dritte in Serie. Grundsätzliche Veränderungen gegenüber den vorherigen sind nicht erkennbar.

Sein zentraler Bestandteil sind Befugnisse, die bisher nur im Rahmen eines Strafprozesses als Zwangsmassnahmen möglich waren und die dort mit spezifischen Anordnungs- und Genehmigungsverfahren sowie Rechten der Angeschuldigten, insbesondere auf Akteneinsicht, verknüpft sind. Sie werden jetzt

- zu „besonderen Methoden der Informationsbeschaffung": Überwachung der Telekommunikation, technische Überwachung von Privaträumen und geheimes Durchsuchen eines Datenbearbeitungssystems.
- zu Bestandteilen der „allgemeinen Informationsbeschaffung", sofern es den Einsatz „InformantInnen" (richtiger: V-Leuten) und Verdeckten Ermittlern betrifft.

Der Verein grundrechte.ch lehnt dieses Paket insgesamt ab,

- weil es dafür keinen Bedarf gibt. **Seit den 90er Jahren wurde auf eidgenössischer Ebene eine Vielzahl von rechtlichen Regelungen im Sicherheitsbereich erlassen, die sowohl den Staatsschutz im engeren Sinne (BWIS) betrafen als auch die quasi-präventive Tätigkeit im strafrechtlichen Vorfeld erweiterten:** im Strafrecht Einführung des Straftatbestandes der „kriminellen Organisation", im strafprozessualen Bereich (Überwachung der Telekommunikation, verdeckte Ermittlungen u.a.m.), Gesetze und vor allem Verordnungen zum Aufbau von Informationssystemen, das Zentralstellengesetz und darauf aufbauend die „Effizienzvorlage", die die Zuständigkeit des Bundes für Ermittlungen und Vorfeldermittlungen gegen vermutete „kriminelle Organisationen" begründeten. Was eine Erweiterung staatsschützerischer Befugnisse hier noch zusätzlich bringen kann – ausser einem „Krieg der Polizeien" –, ist nicht erkennbar.
- weil es schwerwiegende Eingriffe in Grundrechte und gleichzeitig einen massiven Abbau von Rechtschutzmöglichkeiten und demokratischer Kontrolle zur Folge hat,
- weil damit staatliche Willkür rechtlich verkleidet wird: Der Staatsschutz würde mit dem vorliegenden Entwurf jenes Repertoire an Befugnissen zurück erhalten, das er vor der Fichenaffäre ohne rechtliche Grundlage beansprucht hat. Im Unterschied zur alten Schnüffelpolizei verfügt die neue aber über ausgedehnte technische Mittel – sowohl zur Bearbeitung und Weitergabe von Daten als auch für die hier vorgesehenen „besondere" Informationsbeschaffung.

grundrechte.ch fordert stattdessen, das Einsichtsrecht in Staatsschutzakten wieder herzustellen.

1. „Besondere Informationsbeschaffung" zur Bekämpfung von Terrorismus, verbotenem Nachrichtendienst und Proliferation: Überwachung der Telekommunikation, Einsatz technischer Mittel zur Überwachung von Privaträumen, staatliches Hacken (neues Kapitel 3a, Art. 18 a-m)

Zentraler Bestandteil des Entwurfs ist die Aufhebung des im bisherigen Artikels 14 Abs. 3 enthaltenen Verbots strafprozessualer Zwangsmassnahmen im Rahmen der staatsschützerischen Tätigkeit. An seine Stelle soll ein neues Kapitel 3a treten, das solche Massnahmen – nämlich insbesondere die Überwachung der Telekommunikation, die Überwachung von Privaträumen mithilfe technischer Mittel sowie das Eindringen in private Datenbearbeitungsanlagen (sprich: das staatliche Hacken) – ausdrücklich zulässt. grundrechte.ch lehnt diese Veränderung entschieden ab.

Das Verbot strafprozessualer Zwangsmassnahmen ist der einzige Punkt, an dem sich das derzeit geltende Gesetz von der staatsschützerischen Praxis vor dem Fichenskandal unterscheidet. Solche Massnahmen sind – wenn überhaupt – nur im Rahmen des Strafprozesses hinnehmbar. Schon in diesem Rahmen hat sich die Zahl der Telekommunikationsüberwachungen seit den 90er Jahren massiv erhöht. **Bereits im Jahre 1992 stellte die Geschäftsprüfungskommission des Nationalrates fest, dass sich diese (strafprozessualen) Überwachungen in ihrem Charakter grundsätzlich gewandelt haben – von einem Instrument zur Erhärtung eines bestehenden Verdachts, von einer strafprozessualen Zwangsmassnahme im eigentlichen Sinne also, zu einer Methode der Ausforschung des Umfeldes eines Angeschuldigten. Derartige Überwachungsmassnahmen haben also bereits heute einen quasi-präventiven Charakter, was sich vor allem an der Masse der (rückwirkenden) Teilnehmeridentifizierungen (rund 5 000 pro Jahr) zeigt.**

Vor einer neuerlichen Ausweitung der Überwachungen – nunmehr in den definitiv präventivpolizeilichen oder besser: geheimdienstlichen Bereich – wäre erwartbar gewesen, dass der Bundesrat hier Transparenz schafft und die Praxis der Überwachungen, das Genehmigungsverfahren und die Folgen der Überwachungen im Strafprozess untersucht, sowohl was ihre Kosten und ihr Nutzen für im Strafverfahren als auch was die Konsequenzen für die Rechte der BürgerInnen betrifft. Das ist jedoch nicht passiert. Eine Statistik der Überwachungen, die diesen Namen verdient, gibt es nicht. Der Dienst für besondere Aufgaben des UVEK, der eine technische Vermittlerrolle zwischen den Strafverfolgungsbehörden und den Dienste-Anbietern einnimmt, gibt nur die Zahl der von ihm jährlich bearbeiteten Überwachungsdossiers bekannt.

- Staatsschützerische Befugnisse zur Telekommunikationsüberwachung nicht erforderlich

Schon aufgrund der bestehenden Rechtslage wird aber deutlich, dass eine Ausweitung von Überwachungsbefugnissen in den geheimdienstlich-präventiven Bereich nicht erforderlich ist. Nach dem vorliegenden Entwurf sollen die „besonderen" Mittel der Informationsbeschaffung bei einer „konkreten Gefahr für die innere oder äussere Sicherheit der Schweiz" eingesetzt werden können, insbesondere wenn diese vom „Terrorismus" ausgeht.

Alle bekannten Versuche, den Begriff Terrorismus zu definieren, beziehen sich entweder auf Straftaten, die (unter bestimmten Bedingungen) als terroristisch gelten, oder auf terroristische Organisationen bzw. Vereinigungen, bei denen es sich wiederum um Gruppierungen handelt, die spezifische Straftaten begehen oder planen.[1]

In beiden Fällen ist auch in der Schweiz heute bereits eine Überwachung möglich. Der Straftatenkatalog des „Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs" (BÜPF) umfasst nicht nur die gemeinhin als terroristisch bezeichneten Straftaten selbst – von der Brandstiftung bis zur vorsätzlichen Tötung –, sondern auch

- den Art. 260bis StGB, der bereits die Vorbereitung solcher Straftaten unter Strafe stellt, und
- den Art. 260ter, der die Beteiligung an einer kriminellen Organisation mit Strafe bedroht. Strafbar sind danach auch solche Gruppierungen, deren Zweck die Begehung von Straftaten im Ausland ist. Die Straftaten selbst müssen noch nicht begangen worden sein.

Das BÜPF schliesst zwar die vor seinem Inkrafttreten möglichen Überwachungen zur „Verhinderung von Straftaten" bewusst aus, erlaubt jedoch Überwachungen im Vorfeld, weil dieses Vorfeld selbst kriminalisiert ist. Das BÜPF geht damit bereits heute nahe an die Grenzen dessen, was in einem demokratischen Rechtsstaat tolerierbar ist.

Ausgeschlossen sind Überwachungen nur dann, wenn tatsächlich weder konkrete Vorbereitungshandlungen noch konkrete Anzeichen für die Existenz einer kriminellen (terroristischen) Organisation absehbar sind. Wo solche Anzeichen nicht vorhanden sind, kann auch keine konkrete Gefahr bestehen. Zusätzliche staatsschützerische Überwachungen sind vor diesem Hintergrund nicht erforderlich.

- Scheintatbestände als Eingriffsvoraussetzungen

Die Loslösung von Überwachungsbefugnissen selbst von diesen weit ins Vorfeld gehenden Straftatbeständen muss notwendigerweise dazu führen, dass die Eingriffsvoraussetzungen nicht mehr klar be-

[1] vgl. die Terrorismusdefinition der EU, Amtsblatt L 164 v. 22.6.2002

nannt werden können bzw. dass Scheintatbestände konstruiert werden, die eine Bestimmtheit nur vorgaukeln.
Dies ist hier der Fall. Die „konkrete Gefahr für die innere oder äussere Sicherheit der Schweiz“, die den Einsatz „besonderer“ Überwachungsmethoden rechtfertigen soll, ist eben nicht zu verwechseln mit der „konkreten Gefahr“ des Polizeirechts. Letztere bezeichnet eine unmittelbar bevorstehende und deshalb in ihren Dimensionen und Folgen absehbare Schädigung eines geschützten Rechtsgutes, im Normalfall: das Bevorstehen einer Straftat. Im Polizeirecht beinhaltet dieser Begriff also immer eine Dimension der zeitlichen Nähe. Die zeitliche Nähe ist die Voraussetzung dafür, dass der polizeiliche Einsatz erforderlich, verhältnismässig und angemessen sein kann. Dementsprechend müssen die Massnahmen zur Abwehr einer solchen Gefahr immer dringliche Massnahmen sein.

In dem hier vorliegenden Entwurf geht diese zeitliche Dimension notwendigerweise verloren. Eine konkrete Gefahr kann nicht durch eine Überwachung abgewehrt werden, die im Normalfall ein halbes, bei Verlängerung ein ganzes Jahr dauern oder gar danach durch eine neue Bewilligung um denselben Zeitraum ausgedehnt werden kann. Es geht in diesem Entwurf nicht um eine konkrete Gefahr, sondern um eine allgemeine Gefahrenvermutung.
Typischerweise werden die potenziell Betroffenen auch nicht wie im Polizeirecht als „Störer“ bezeichnet, sondern als „mutmassliche Gefährder“. Darunter will der Entwurf in Art. 18b Bst. a Personen, Organisationen oder Gruppierungen verstanden wissen, die „verdächtigt (werden), die innere oder äussere Sicherheit der Schweiz konkret zu gefährden“. Diese Formulierung ist erstens weitgehend tautologisch: Worin die Gefahr konkret bestehen soll, benennt weder der vorgeschlagene Gesetzestext selbst noch die Erläuterung. Zweitens macht diese Formulierung deutlich, dass nicht eine konkrete Handlung oder ein organisatorischer Zusammenhang den „Gefährder“ zum „Gefährder“ macht, sondern der „Verdacht“, den die Staatsschützer gegen diese Person hegen. „Da die Warnungen der Nachrichtendienste möglichst frühzeitig erfolgen sollen“, so heisst es auf Seite 8 der Erläuterungen, „müssen sie mit ihren Erhebungen vor dem Zeitpunkt einsetzen können, in welchem die entsprechenden Gefährdungen konkret und unmittelbar bevorstehen oder gar der Verdacht einer kriminellen Handlung besteht.“ Anders ausgedrückt: die „Gefahr für die innere und äussere Sicherheit der Schweiz“, die künftig die Voraussetzung zum Beispiel einer Telefonüberwachung oder der Verwanzung einer Wohnung sein soll, ist noch weniger als ein strafrechtlicher Anfangsverdacht**.** Dies macht der Bericht auch an anderer Stelle deutlich: Im Zusammenhang mit der Frage, ob den Bedürfnissen des DAP mit einem Ausbau des Strafrechts Genüge getan werden könnte, führt der Bericht auf S. 20 aus: „Nach heutigem Recht setzt repressives Tätigwerden einen hinreichenden Verdacht auf Begehung einer strafbaren Tat voraus. Gerade daran mangelt es jedoch typischerweise beim Beginn von nachrichtendienstlichen Abklärungen. In einer ersten Phase bestehen bloss Annahmen und vage Hinweise. Hinzu kommt, dass Gefahren für die innere Sicherheit häufig auf den ersten Blick kaum als solche erkennbar und einschlägige Handlungen (noch) nicht strafrechtlich fassbar sind.“ **Daraus wird deutlich, dass nicht ein irgendwie gearteter konkreter Verdacht notwendig sein soll, um jemanden zum „Gefährder“ zu machen. Als Basis für diese Qualifizierung sollen vielmehr vage Vermutungen und Annahmen ausreichend sein.**
Damit werden aber auch alle anderen Eingriffsvoraussetzungen in Art. 18b zur blossen Schaumschlägerei: Die Art und Schwere der Gefährdung lässt sich zu diesem Zeitpunkt noch gar nicht absehen.

Kriterien der Verhältnismässigkeit und Angemessenheit greifen nicht, da es keine Handlung, kein Ereignis und keinen (strafbaren) organisatorischen Zusammenhang gibt, mit dem der staatliche Eingriff in die Rechte der BürgerInnen ins Verhältnis gesetzt werden können. Als Voraussetzung bleibt dann einzig, dass alle anderen (allgemeinen) Ausforschungsmassnahmen nichts gebracht haben. Anders ausgedrückt: die Tatsache, dass nichts Wirkliches gegen eine Person oder Organisation vorliegt, wird zur Voraussetzung dafür, dass einschneidende Eingriffe in ihre Rechte und Freiheiten vorgenommen werden dürfen. Je weniger Verdacht, desto mehr Überwachung. Das Ergebnis der vorgeschlagenen Besitmmungen wäre, dass nicht nur Terroristen, sondern auch völlig unbescholtene Menschen Ziel der vorgeschlagenen Überwachungsmassnahmen werden können.

- Berufsgeheimnis faktisch aufgehoben (Art. 18c)

Angesichts der Tatsache, dass schon der Kreis der eigentlichen Zielpersonen kaum abgegrenzt ist, ist es umso weniger akzeptabel, dass auch Dritte in die Überwachung miteinbezogen werden können. Dies ist umso gravierender, wenn es dabei um Personen geht, die durch ein Berufsgeheimnis geschützt sind. Zwar sieht der Entwurf im Normalfall vor, dass eine Kammer des Bundesverwaltungsgerichts die durch die Überwachung bei Ärzten, Anwälten oder Priestern erzielten Daten vorher triagiert. Aber auch hier lässt der Entwurf ein Hintertürchen offen: **Der Staatsschutz soll auch Daten erhalten, die unter das jeweilige Berufsgeheimnis fallen, wenn er annimmt, dass die „Gefährdung der Sicherheit … gezielt unter dem Vorwand des Berufsgeheimnisses“ erfolge. Damit ist das Berufsgeheimnis faktisch aufgehoben.**

- Verwertbarkeit im Strafverfahren

Spätestens an diesem Punkt zeigt sich, dass die neuen staatsschützerischen Überwachungsbefugnisse nicht nur unnötig und gefährlich, sondern für die Strafverfolgung kontraproduktiv sind. Der bestehende Art. 17 Abs. 1 BWIS verpflichtet zwar die Staatsschutzorgane, Informationen, die der Strafverfolgung dienen können, „unverzüglich“ an die Strafverfolgungsbehörden weiterzugeben. Die Frage ist allerdings, wie diese Informationen genutzt werden könnten.

In Art. 18k Abs. 4 neu heisst es zwar, dass die Bestimmungen des BÜPF auch hinsichtlich der Verwertung von Zufallsfunden sinngemäss gelten sollen. Nähme man diese Bestimmung, die in den Erläuterungen nicht näher ausgeführt wird, ernst, so würde das heissen, dass die für die Genehmigung einer strafprozessualen Telekommunikationsüberwachung zuständigen RichterInnen jeweils prüfen müssten, ob die Voraussetzungen einer Überwachung gemäss dem BÜPF auch in dem Verfahren erfüllt wären, in dem sie als Beweismittel eingeführt werden sollen (Art. 9 Abs. 2 und 3 BÜPF). Sie müssten also feststellen, ob eine Katalogstraftat gegeben ist und ob ein dringender Tatverdacht gegen die betroffene Person vorgelegen hat. Letzteres wird aber in der Regel nicht der Fall sein, weil die staatsschützerische Überwachung nach dem vorliegenden Entwurf einen solchen Verdacht eben gerade nicht erfordert. Eine rechtmässige Verwendung der in der staatsschützerischen Überwachung gefundenen Ergebnisse in ein strafrechtliches Verfahren wäre damit eigentlich ausgeschlossen.
grundrechte.ch befürchtet daher, dass die Übertragung von Informationen aus staatsschützerischen Überwachungen in Strafverfahren unter Umgehung der Vorschriften für die Verwertung von Zufallsfun-

den stattfinden wird. Ein „Waschen“ von Informationen, das Verwischen ihrer Herkunft durch die Konstruktion angeblicher anderer Informationswege, mag verlockend sein, ist aber für ein rechtsstaatliches Strafverfahren untragbar. Die Verwendung von Informationen aus geheim(dienstlich)en Überwachungen ohne Angabe der Herkunft macht aus einem Strafprozess ein Kasperle-Theater.
Der geheimdienstliche Quellenschutz und das Unmittelbarkeitsprinzip im Strafprozess schliessen einander aus. Befugnisse zur Anwendung „besonderer“ Überwachungsmethoden steigern deshalb nicht die Effizienz des Strafverfahrens, sondern gefährden sie. In diesem Zusammenhang ist es irreführend, wenn der Bericht auf S. 10 festhält, durch das Nebeneinander von Repression und Prävention würden sich Mehrwerte ergeben und es würde keine nachteiligen Folgen zeitigen, wenn der gegenseitige Informationsaustausch spielt. Zumindest dann, wenn die rechtsstaatlichen Regelungen eingehalten werden – was man doch eigentlich müsste voraussetzen können – stimmt dies nicht. Aktuelle Beispiele von Verfahren gegen mutmassliche Terroristen in Deutschland und in Grossbritannien zeigen im Übrigen, dass die Gefahr, dass ein Strafverfahren durch Geheimdienstinformationen kontaminiert und dadurch gefährdet wird, real ist und dass zwischen Prävention und Repression deutliche Zielkonflikte zu Tage treten können.
Die Problematik liegt dabei insbesondere darin, dass Geheimdienste regelmässig NICHT bereit sind, die Quellen ihrer Informationen offen zu legen oder einer Überprüfung zugänglich zu machen. Zudem besteht die Möglichkeit, dass Aussagen, die von einem Geheimdienst gewonnen worden sind, auf unzulässige Verhörmethoden, allenfalls sogar Folter, zurückgehen. Das führt dazu, dass in einem Strafverfahren auf Informationen, die von einem inländischen oder ausländischen Geheimdienst stammen, regelmässig nicht abgestellt werden kann.

- Kontrolle durch das Bundesverwaltungsgericht

Der Entwurf lässt keinen Zweifel daran, dass das ganze Verfahren der Überwachung von der Exekutive (vom DAP selbst sowie vom Departementsvorsteher und allenfalls vom Gesamtbundesrat) dominiert werden soll. Das Bundesamt, konkret also der DAP, stellt den Antrag und kann im Dringlichkeitsfalle gleich mit der Überwachung beginnen. Den Entscheid trifft das EJPD in Zusammenarbeit mit dem VBS oder bei Streitigkeiten zwischen den Departementsvorstehern der Gesamtbundesrat.
An der Dominanz der Exekutive ändert auch die Tatsache nichts, dass eine spezielle Kammer des Bundesverwaltungsgerichts eine Stellungnahme abgeben muss. Eine richterliche Überprüfung ist generell nie mehr wert als das Prüfungsprogramm, das ihr vom Gesetz vorgegeben wird. Bereits aus dem Bereich der strafprozessualen Überwachungsmassnahmen ist bekannt, dass die genehmigenden Richter – dort in der Regel die Anklagekammern – kaum eine Überwachung ablehnen. Im Falle der staatsschützerischen Überwachung wird diese Schwäche der Justiz gegenüber der Exekutive noch deutlicher. Diese Kammer des Bundesverwaltungsgerichts hat für ihre Stellungnahme nur 72 Stunden Zeit. Sie ist von den Informationen abhängig, die der DAP ihr liefert, ohne jede Möglichkeit, diese Informationen auf ihre Stichhaltigkeit zu überprüfen. Und sie muss ihre Stellungnahme auf der Grundlage völlig unspezifischer Eingriffsvoraussetzungen treffen, die sich einer griffigen justiziellen Handhabung zwangsläufig entziehen. Das Bundesverwaltungsgericht kann vor diesem Hintergrund nur das justizielle Alibi für die Entscheidung der Exekutive liefern. Eine wirkliche Begrenzung kann aus diesem Verfahren nicht erwachsen.

- Mitteilungspflicht – die Ausnahme als Regel

Angesichts der in Art. 18 1 Abs. 2 formulierten Ausnahmen wird die in Abs. 1 formulierte Mitteilungspflicht praktisch entwertet. Hier zeigt sich deutlich der Unterschied zwischen strafprozessualen und staatsschützerischen Überwachungen. Ein strafrechtliches Ermittlungsverfahren endet entweder mit der Einstellung, dem Freispruch oder einem Schuldspruch. Danach kann in der Regel eine Mitteilung an die Betroffenen erfolgen, sofern sie nicht bereits im Strafverfahren selbst von der Überwachung erfahren haben.

Eine staatsschützerische Überwachung hat aber nicht zum Ziel, Beweise für die Schuld oder Unschuld einer Person zu erbringen. Sie ist nicht Teil eines Verfahrens, das mit einer Ungefährlichkeitsbescheinigung endet. Unter diesen Umständen kann eine Zielperson auch nach dem Ende einer „besonderen" Informationsbeschaffung nicht damit rechnen, ganz aus dem Visier der Staatsschützer zu verschwinden. Die in Bst. a und b aufgelisteten Gründe, von der Mitteilung abzusehen, wären damit fast immer gegeben und würden die Mitteilung in der Praxis fast immer verhindern. Akzeptabel kann deshalb allenfalls ein Aufschub bis zum Abschluss eines allfälligen Strafverfahrens sein. Danach muss sie aber zwingend erfolgen.

Bst. d ist ganz zu streichen. Die Argumentation, eine Person sei nicht erreichbar, dient heute schon als Ausrede dafür, die Mitteilungspflicht nach einer strafprozessualen Telekommunikationsüberwachung auf kaltem Wege entfallen zu lassen.

2. „Allgemeine" Informationsbeschaffung – erweitere Befugnisse für die Staatsschutztätigkeit insgesamt

Während die Bestimmungen über „besondere Informationsbeschaffung" auf die „Bekämpfung" von Terrorismus, verbotenem Nachrichtendienst und Proliferation beschränkt sein sollen, beziehen sich die erweiterten Regelungen über „allgemeine Informationsbeschaffung" auf den gesamten Tätigkeitsbereich des Staatsschutzes. Sie beziehen sich mithin auch auf das, was im Gesetz als „gewalttätiger Extremismus" bezeichnet wird und was in der Praxis nichts anderes darstellt als den Umgang mit politischen und sozialen Bewegungen.

2.1. InformantInnen, Tarnidentitäten: Haupt- und nebenamtliche Spitzel (Art. 14b-d)

grundrechte.ch lehnt die hier vorgesehene ausdrückliche Zulassung von „InformantInnen" und Verdeckten ErmittlerInnen generell ab.

Bereits die bisher in Art. 14 Abs. 2 Bst. d enthaltene Befugnis zur „Entgegennahme und Auswertung von Meldungen" erweist sich als gefährlich. Ging es doch hier auch um die Meldungen privater Personen, sprich: DenunziantInnen, die im Schutze der Anonymität und häufig getrieben durch übersteigertes Geltungsbedürfnis oder undurchschaubare (politische) Motive Angaben über Bekannte oder gar Verwandte machen. Eine solche anonyme Meldung an den Staatsschutz ist etwas grundsätzlich anderes als die Anzeige einer Straftat, bei der die Angeschuldigten anschliessend die Möglichkeit haben, sich zu verteidigen. Schon bisher hat der Staatsschutz für solche „Meldungen" einen Judaslohn gezahlt.

Der vorliegende Entwurf geht weit darüber hinaus. Er regelt nicht nur die passive Entgegennahme von Informationen. Die Erläuterung zu Art. 14b Abs. 1 macht deutlich, dass es dem Entwurf um den Einsatz von „InformantInnen“ geht. Wenn Drittpersonen zur heimlichen Ausforschung anderer eingesetzt werden und dazu einen bezahlten (!) Auftrag erhalten, sind sie aber nicht mehr blosse „InformantInnen“, sondern V-Leute. Dies gilt umso mehr, wenn sie dafür mit einer Tarnidentität ausgestattet werden und mit staatlich gefälschten Urkunden an Rechtsgeschäften teilnehmen.

Die Ausstattung von Privatpersonen oder eigenen MitarbeiterInnen mit Tarnidentitäten würde nun im staatsschützerischen Bereich dieselben Befugnisse schaffen, wie sie im Strafverfahren mit dem Bundesgesetz über verdeckte Ermittlungen eingeführt wurden. Während dort geheime Ermittlungsmethoden immerhin noch an einen Straftatverdacht gebunden sind, sollen diese Methoden hier ohne jegliche weitere Voraussetzung eingesetzt werden dürfen. Da sie als „allgemeine“ Methoden der Informationsbeschaffung vorgesehen sind, würde das bedeuten, dass sie in sämtlichen Bereichen staatsschützerischer Tätigkeit einsetzbar wären.

Der Entwurf verzichtet hier generell auf Vorkehrungen zum Schutz von BerufsgeheimnisträgerInnen. Nach dem bisherigen Text wäre es problemlos möglich, z.B. Sekretariatspersonal von Anwaltskanzleien als Spitzel anzuwerben, wie das beispielsweise der deutsche Verfassungsschutz diverse Male getan hat (im Fall des heutigen grünen Bundestagsabgeordneten Hans-Christian Stroebele oder auch bei den Verteidigern im „Schmücker-Verfahren“). Ebenfalls möglich wäre die Ausforschung von Medienschaffenden durch V-Personen, womit der vom Bundesgericht mehrfach bekräftigte Informantenschutz im Medienrecht ausgehebelt würde, und die Anwerbung von Medienschaffenden als V-Personen. Beides hat der deutsche Bundesnachrichtendienst seit den 90er Jahren praktiziert. Diese Praxis ist derzeit einer der Gegenstände eines Parlamentarischen Untersuchungsausschusses des Deutschen Bundestages.

Auch beim Einsatz von haupt- oder nebenamtlichen Spitzeln zeigt sich, dass der geheimdienstliche Quellenschutz dem Strafverfahren zuwider läuft. Eine Verwendung der so erlangten Informationen im Strafverfahren führt unweigerlich zu einer Verunstaltung des Strafverfahrens. Es ist kaum anzunehmen, dass der Staatsschutz ohne weiteres einer Aussage von InformantInnen oder eigenen verdeckt agierenden BeamtInnen vor Gericht zustimmen wird. Aussagen von V-Mann-Führern, d.h. Zeugen vom Hörensagen, von vermummten ZeugInnen, beschränkte Aussagegenehmigungen u.ä. werden die Folgen sein.

Schutzprogramme darf es nur für gefährdete ZeugInnen in Strafverfahren geben. Sie müssen dort allerdings gewährleisten, dass eine persönliche Einvernahme durch die Verteidigung in der Hauptverhandlung gesichert ist. Alles andere ist nicht akzeptabel.

2.2. Lagedarstellung (Art. 10a)

Der DAP hat bereits bisher bei interkantonalen Polizeieinsätzen als Lagezentrale fungiert und dabei eine problematische Rolle wahrgenommen. Die Lagedarstellung ist eine strategische Aufgabe und darf nicht mit der Sammlung und Auswertung personenbezogener Daten vermischt werden. Die Bearbeitung personenbezogener Daten in dem neuen Datensystem ist deshalb auf freiwillig überlassene Daten zu beschränken. Ein Zugang privater Personen oder Sicherheitsdienste zu einer Lagedarstellung ist abzulehnen. Art. 10a Abs. 4 ist ganz zu streichen.

2.3. Auskunftspflichten (Art 13-13d)

grundrechte.ch lehnt die hier vorgesehene Ausdehnung der Auskunftspflicht und des Melderechts grundsätzlich ab. Seit Oktober 2001 bedient sich der DAP bereits einer Verordnung, die gestützt auf den bestehenden Art. 13 Abs. 3 BWIS die Auskunftspflichten und Melderechte über das Normalmass ausdehnte. Bereits die bestehenden Auskunftspflichten und Melderechte sind nicht akzeptabel. Um eine datenschutzrechtliche Überprüfung möglich zu machen und Denunziationsgelüste zu beschränken, ist hier generell vorzusehen, dass die Weitergabe von Informationen an den Staatsschutz schriftlich protokolliert wird.

Mit dem vorliegenden Entwurf sollen die **Auskunftspflichten,** die bisher in der Verordnung vorgesehen sind, generell für die Bekämpfung von Terrorismus, verbotenem Nachrichtendienst und Proliferation **erlaubt und erweitert werden.** Nach Art. 13a Abs. 1 neu sind – ähnlich wie bisher per Verordnung – nicht nur staatliche Stellen zur Weitergabe von Informationen an den Staatsschutz verpflichtet und ermächtigt, sondern auch „Organisationen, die öffentliche Aufgaben erfüllen". Darunter fallen z.B. kulturelle Organisationen, die Leistungsverträge mit einer kantonalen Verwaltung geschlossen haben, Spitäler, oder Hilfswerke, die Asylsuchende betreuen, etc. Sie alle haben im Normalfall ein besonderes Vertrauensverhältnis zu ihren KlientInnen, das zu missbrauchen sie nun gezwungen werden können.

In Art. 13c sollen nun auch **private Transportunternehmen** in Dienst genommen werden. Damit wird theoretisch jeder Taxifahrer dazu gezwungen, als Staatsschutzinformant zu agieren.

grundrechte.ch lehnt diese Vorschläge grundsätzlich ab. Der Zugang zu Daten von Transportunternehmen muss auf das Strafverfahren beschränkt bleiben und darf nur auf richterliche Anordnung erfolgen.

2.4. Funkaufklärung: Elektronische Kriegsführung

Der DAP nutzt seit Jahren die „grossen Ohren" des Militärs für seine Zwecke mit. Was diese Funküberwachung gebracht hat, wurde weder für den Strategischen Nachrichtendienst im VBS noch für die Zwecke des Staatsschutzes dargelegt. Zahlenmaterial ist nicht vorhanden, Evaluationen gibt es nicht.

Die bisherige Praxis wurde rechtswidrig als „Beobachtung von Vorgängen an öffentlich zugänglichen Orten" verkauft. Über Satellit vermittelte Telekommunikation ist aber nicht öffentlich, sondern wird nur durch die Entschlüsselung zugänglich. grundrechte.ch fordert diese Praxis zu unterbinden.

Hinter ihr verbirgt sich eine absurde Auslegung des Fernmeldegeheimnisses, nach der ein Telefonanruf im Landesinnern zwar von dem Grundrecht geschützt wird, aber ein Anruf oder Fax aus dem Inland ins Ausland jederzeit ohne jeglichen Verdacht herausgefiltert und abgefangen werden darf. Grundrechte sind Rechte von Personen. Sie hören nicht einfach auf zu existieren, wenn diese Personen mit anderen im Ausland in Verbindung treten. Diese absurde Interpretation mag international anerkannt sein. Das zeigt aber nur, wie gering der Wert der Grundrechte in der „Staatengemeinschaft" veranschlagt wird.

3. Betätigungsverbote (Art. 18n)

1998, kurz vor Inkrafttreten des BWIS hat der Bundesrat die aus dem Kalten Krieg stammenden Beschlüsse über das Propagandaverbot (und die Beschlagnahme von „Propaganda" ohne Verfahren)

sowie über das Redeverbot, aufgehoben, weil sie offensichtlich der Europäischen Menschenrechtskonvention widersprachen. Der Propagandabeschluss ist inzwischen durch die erste Revision des BWIS nunmehr in gesetzlicher Form wieder eingeführt worden (Art. 13a BWIS). Mit dem hier vorgesehenen Art. 18n soll das Verbotsinstrumentarium um nicht näher bestimmte Betätigungsverbote ausgeweitet werden.
Derartige Verbote kann derzeit nur der Bundesrat gestützt auf Art. 184 der Bundesverfassung erlassen. So hat er u.a. tamilischen Organisationen das Sammeln von Spenden bei ihrer jährlichen Demonstration untersagt. Schon die bestehende Rechtslage erweist sich als äusserst problematisch, da sie exekutive Eingriffe in die Rechte und Freiheiten von Personen zulässt, ohne dass gegen diese Personen ein strafrechtlicher Verdacht existiert und ohne dass gegen sie ein strafrechtliches Verfahren geführt würde. Immerhin handelt es sich hierbei um eine Notstandsbefugnis, die nur im Einzelfall anwendbar ist.
Das ausdrückliche Ziel des jetzigen Entwurfs ist es, den Notstand in den Alltag einzuführen. grundrechte.ch lehnt diese Normalisierung ab, zumal an keiner Stelle des Entwurfs vermerkt ist, welche Tätigkeiten im Einzelnen verboten werden dürfen. Es kann nicht zugelassen werden, dass der Staat Personen, die nicht strafrechtlich verurteilt sind und damit als unschuldig zu gelten haben, fünf Jahre oder länger die Wahrnehmung von Grundrechten versagt.

Allein der EJPD-Vorsteher soll nach diesem Entwurf einer „Person, Organisation oder Gruppierung“ eine Tätigkeit verbieten können, die „mittelbar oder unmittelbar dazu dient, terroristische oder gewaltextremistische Umtriebe zu propagieren, zu unterstützen oder in anderer Weise zu gefährden und die die innere oder äussere Sicherheit der Schweiz konkret gefährdet“. Als Beispiel dafür führt der Bericht nur Geldsammlungen von Exilorganisationen an, die dabei erpresserisch vorgehen oder für humanitäre Zwecke bestimmte Gelder in den Kauf von Waffen umlenken könnten. Der Bericht betont, dass sich dafür „oft kaum ein direkter Beweis erbringen“ lasse. Das Fehlen von Beweisen wird in diesem Entwurf nun als Beleg für die Notwendigkeit von präventiven Massnahmen gewertet. Anders ausgedrückt: weil keine Beweise erbracht werden können, soll der Departementsvorsteher ohne Beweise handeln dürfen.

Bei genauerer Betrachtung würde diese Vorschrift aber auch erheblich weiter gehende Massnahmen zu: Denkbar wäre u.a., einer als „gewaltextremistisch“ eingestuften Organisation das Führen einer Website oder die Herausgabe einer Zeitung zu verbieten oder einem Drucker, das Herstellen einer Zeitung zu untersagen, die zu Protesten gegen das Davoser WEF aufruft. Dass die „konkrete Gefahr für die innere und äussere Sicherheit der Schweiz“ ein äusserst dehnbarer Begriff ist, der nicht ansatzweise an die konkrete Gefahr im Polizeirecht oder an den konkreten Verdacht im Strafprozessrecht heranreicht, haben wir bereits oben dargestellt.

Die Beschwerdemöglichkeit beim Bundesverwaltungsgericht macht dieses Vorgehen nicht besser. Sie bedeutet eine Umkehr der Beweislast. Nicht der Staat müsste den Betroffenen nachweisen, dass sie eine Straftat begangen haben. Die jeweiligen Personen oder Organisationen müssten nachweisen, dass sie mit ihrer Tätigkeit die Sicherheit der Schweiz nicht gefährden. Dies ist umso schwieriger, als sie keine Einsicht in die Daten haben, die der Staatsschutz über sie gesammelt hat.

Stattdessen ist darauf hinzuwirken, dass die bisherigen Notstandsbefugnisse des Bundesrates einer richterlichen Kontrolle unterworfen werden, bei der in jedem Falle die entsprechenden Staatsschutz-Informationen offen zu legen sind.

4. Einsichts- und Auskunftsrecht

grundrechte.ch fordert die Wiederherstellung des Einsichtsrechtes in die eigenen Unterlagen. Dieses Recht ist die minimale Voraussetzung für eine wirkliche Kontrolle des Staatsschutzes und für das Funktionieren des Datenschutzes. Eine wirksame Alternative dazu gibt es – wie eingangs dargelegt – nicht.

Bern, den 12. Oktober 2006
grundrechte.ch