

Demokratische Juristinnen und Juristen Schweiz DJS

Neuengasse 8, 3011 Bern

Tel. 031 312 83 34 / info@djs-jds.ch

www.djs-jds.ch

EJPD

Bundesamt für Polizei - Fedpol

Dienst für Analyse und Prävention DAP

3003 Bern

**Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit BWIS
(Teilrevision BWIS II) – Vernehmlassungsfrist 15. Oktober 2006**

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Gerne nehmen wir die Gelegenheit wahr und unterbreiten Ihnen hiermit unser Stellungnahme zu der von Ihnen vorgeschlagenen Revision des BWIS.

In einem ersten Teil unserer Stellungnahme gehen wir auf Ihren Fragekatalog ein (in französischer Sprache), in einem zweiten Teil unterbreiten wir Ihnen unsere Hauptkritikpunkte im einzelnen und unter Punkt III) ziehen wir ein kurzes Fazit: Zusammenfassend kann festgehalten werden, dass die DJS die vorgesehenen Gesetzesverschärfungen vollumfänglich ablehnen und gegenüber dem Parlament für ein **Nichteintreten** plädieren.

Inhalt der Stellungnahme:

I Stellungnahme zum Fragenkatalog

II Stellungnahme zu einzelnen Bestimmungen

III Fazit aus Sicht der DJS

I Stellungnahme zum Fragenkatalog

1. Gesamteindruck der Vorlage / Impression générale

Notre avis sur ce projet de loi est très négatif. Il s'agit d'une remise en cause des engagements pris par le Conseil fédéral et le Parlement, lorsque ceux-ci ont combattu l'initiative populaire contre la police fouineuse et présenté la LMSI comme contre-projet indirect.

En particulier, l'interdiction des écoutes téléphoniques en matière préventive a été alors un argument majeur des autorités. Maintenant, certes avec une limitation au domaine du « terrorisme », le Conseil fédéral revient sur l'engagement qu'il a pris. Il ouvre ainsi la porte à une pratique policière et politique de l'écoute téléphonique et à l'extension ultérieure de celle-ci à d'autres domaines.

Une remarque analogue peut être faite concernant l'utilisation policière d'agents infiltrés! Les garanties matérielles et juridictionnelles prévues en matière pénale sont largement supprimées. De plus, sur cette question, l'utilisation d'agents infiltrés dans le domaine politique est légalisée et encouragée.

Contrairement à ce que soutient le Conseil fédéral, la limite entre police « préventive » et action pénale « répressive » est plus que floue et donc impossible à maîtriser. Le risque évident du projet de loi est celui d'une double compétence simultanée des autorités de police « préventive » (SAP) et de poursuite pénale (ministère public). Il est d'ailleurs absolument faux de prétendre que les autorités pénales ont une mission répressive uniquement. Au contraire, elles ont aussi une mission d'investigation et, s'agissant des délits en train de se commettre, elles ont l'obligation d'intervenir et de prendre des mesures. Le projet de loi accentue fortement la concurrence entre services fédéraux de police. D'où un risque évident de confusions et de mauvais fonctionnement de la lutte contre le terrorisme.

Selon le projet, le contrôle juridictionnel, quand il se fait, est du ressort du Tribunal administratif fédéral. C'est un très mauvais choix, car il va conduire à des pratiques et des règles très différentes selon que les écoutes, les agents infiltrés ou les perquisitions sur systèmes informatiques seront de « police préventive » ou d'enquête pénale. En matière pénale, le Tribunal pénal fédéral est en effet compétent.

En matière pénale, l'utilisation d'agents infiltrés et la surveillance postale et des télécommunications sont réglées avec des limites et un contrôle judiciaire beaucoup plus stricts que ceux du présent projet de loi. Il s'ensuit une évidente incohérence. Plus le soupçon de la préparation ou d'un crime est concret, moins il est indispensable de mettre des limites empêchant la violation de la sphère privée des personnes; or le projet de loi va exactement en sens contraire! Il facilite les atteintes à la sphère privée, quand les éléments d'un soupçon sont inexistantes ou peu fondés. Le risque du projet de loi est que les garanties de protection des personnes, qui existent dans le droit pénal, deviennent en pratique désuètes et soient finalement abandonnées.

Le projet ne concerne pas seulement le terrorisme. **Certaines mesures sont clairement applicables au domaine politique:**

- exploration radio (art 14 a);
- informateurs et agents infiltrés (art 14 b-c-d);
- mesures d'interdiction d'activités (art 18 n).

Pour les raisons qui précèdent, nous refusons d'entrer en matière sur cette révision.

2. Total- oder Teilrevision / Révision totale ou partielle ?

Nous pensons que les dépenses du SAP sont inutiles et incontrôlables. Il serait adéquat de réduire massivement les ressources affectées au SAP, ce qui permettrait d'affecter utilement des moyens en personnel, infrastructures et matériel aux autorités judiciaires pénales.

3. Auskunftspflicht / Devoir de renseigner

Dans la loi actuelle, l'extension de la liste des organismes obligés de renseigner est toujours limitée dans le temps. Cette limite doit être maintenue, car elle oblige le Conseil fédéral à réexaminer le bien-fondé de la liste en vigueur. Nous ne sommes donc pas favorable au projet sur cette question aussi.

L'obligation de renseigner des transporteurs aériens est déjà en vigueur en pratique. Pourquoi l'introduire comme règle en faveur du SAP? N'y a-t-il pas double emploi avec des renseignements donnés à d'autres services de police?

Pourquoi un devoir de renseigner, non soumis au contrôle du juge, pour les transporteurs par rail, par cars, par camions, y compris les marchandises? Cela va beaucoup trop loin, s'agissant d'investigations préventives n'impliquant pas le soupçon concret de la commission d'une infraction.

4. „Besondere Mittel“ zur Informationsbeschaffung / Champ d'application des « moyens spéciaux »

La réglementation actuelle est suffisante et le projet est donc disproportionné. En particulier, si une personne ou un groupe sont concrètement soupçonnés de menacer la sécurité intérieure ou extérieure ou l'intégrité physique d'autres personnes, il faut alors qu'une enquête judiciaire pénale soit mise en oeuvre et non une simple démarche préventive comme le prévoit l'art 18'b, al1 lettre a) du projet.

Ce projet est disproportionné et crée en plus une situation de confusion des compétences.

Nous sommes catégoriquement opposés à l'introduction dans la loi de « moyens spéciaux » d'investigation. S'agissant de domaines d'activités criminelles particulièrement graves (terrorisme, prolifération d'armes, espionnage), un soupçon de commission ou de préparation d'un crime doit absolument conduire à la mise en oeuvre de la police judiciaire et du juge. Les règles de la procédure pénale doivent alors s'appliquer et ces règles permettent à la fois un contrôle judiciaire efficace et une activité efficace de l'investigation policière par une surveillance téléphonique, des télécommunications, voire par des agents infiltrés.

Pour les raisons qui précèdent, la loi actuelle est parfaitement suffisante, tout en ménageant une certaine protection de la sphère intime contre les intrusions disproportionnées ou injustifiées.

5. Anordnungs- und Genehmigungsverfahren / Procédures proposées pour le projet

Nous constatons que cette procédure donne plus de latitude au SAP de prendre des mesures de surveillance clandestine que la procédure pénale n'en donne aux autorités judiciaires. Comme expliqué plus haut, cette différence de traitement est injustifiée et surtout incohérente.

Il est faux par ailleurs de donner au Tribunal fédéral administratif la tâche de contrôle. Tout ce qui concerne la surveillance postale et des télécommunications ainsi que les agents infiltrés doit faire l'objet d'une réglementation unique et être attribué à une instance juridictionnelle unique au courant de l'appréciation juridique dans ces domaines: le Tribunal pénal fédéral de Bellinzone.

La mise en oeuvre de « moyens spéciaux » implique toujours, en fin de procédure, une décision en opportunité du chef du DFJP, voire du Conseil fédéral. Ce faisant, la loi donne un poids politique très lourd aux décisions qui seront prises, qu'il s'agisse d'accepter ou de refuser une « mesure spéciale ». Mais simultanément, la décision restes secrète et le chef du Département ou le Conseil fédéral n'aura aucun compte à rendre publiquement. Cette formule manque de transparence et est de nature à porter préjudice au crédit du gouvernement.

6. Tätigkeitsverbot / Mesures d'interdiction d'activité

Il s'agit d'une réglementation nouvelle que le projet entend appliquer aussi dans le domaine politique.

Nous nous opposons à cette réglementation, qui donne des pouvoirs exorbitants au chef du Département de justice et police. En particulier, les exemples donnés par le message évoquent par avance les abus qui pourraient être commis. Ainsi, le soutien moral ou financier des mouvements de résistance contre les dictatures pourrait être interdit d'un trait de plume par M. BLOCHER.

La compétence donnée au chef du Département- et non au Conseil fédéral comme actuellement- est inadmissible. Ce genre de décision doit absolument rester exceptionnel. La création d'une base légale aux contours excessivement flous et la compétence donnée à un seul Conseiller fédéral risquent de produire des décisions liberticides et arbitraires. Certes, un recours juridictionnel est prévu, mais l'efficacité de ce recours est sujette à caution dans un système constitutionnel où le Tribunal fédéral ne revoit pas la constitutionnalité des lois fédérales.

II Stellungnahme zu einzelnen Bestimmungen

1. „Besondere Informationsbeschaffung“ zur Bekämpfung von Terrorismus, verbotenem Nachrichtendienst und Proliferation: Überwachung des Post- und Fernmeldeverkehrs, Einsatz technischer Mittel zur Überwachung von Privaträumen, geheimes Durchsuchen eines Datenverarbeitungssystems (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 staatschützerischen 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 geheime Eindringen in private Datenbearbeitungsanlagen (sprich: das staatliche Hacken) – ausdrücklich zulässt.

Das Verbot strafprozessualer Zwangsmassnahmen ist der einzige und zentrale Punkt, an dem sich das derzeit geltende Gesetz von der staatschützerischen Praxis von vor dem Fichenskandal unterscheidet. Solche Massnahmen sind nach Ansicht der JDS – 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.

Der Bundesrat hat es bisher unterlassen, in diesem enorm sensiblen Bereich Transparenz zu schaffen und die Praxis der Überwachungen, das Genehmigungsverfahren und die Folgen der Überwachungen im Strafprozess im Detail zu untersuchen – sowohl was die Kosten und der Nutzen für im Strafverfahren betrifft als auch was die Konsequenzen für die Rechte der BürgerInnen sind. Es gibt keine zuverlässige und aussagekräftige Statistik der Überwachungen und 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.

Wiedereinführung Telekommunikationsüberwachung

Bereits aufgrund der bestehenden Rechtslage wird 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.

In beiden Fällen ist auch in der Schweiz seit längerem 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 staatschützerische 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 benannt werden können und folglich 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 Bestehen 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 „verdächtig (werden), die innere oder äussere Sicherheit der Schweiz konkret zu gefährden“.

Worin die Gefahr konkret bestehen soll, benennt allerdings weder der vorgeschlagene Gesetzestext selbst noch die Erläuterung. Vielmehr 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.“

Dies hat zur Folge, dass die Tatsache, dass nichts Wirkliches gegen eine Person oder Organisation vorliegt, zur Voraussetzung dafür wird, dass einschneidende Eingriffe in ihre Rechte und Freiheiten vorgenommen werden dürfen. **Je weniger Verdacht, desto mehr Überwachung.** Damit würden unweigerlich nicht nur mutmassliche „Terroristen“, sondern auch völlig unbescholtene Menschen Ziel dieser anvisierten Überwachungsmassnahmen.

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 jederzeit in die Überwachung miteinbezogen werden

können. Dies ist umso gravierender, wenn es Personen betrifft, 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, was für die DJS völlig unhaltbar ist.

Verwertbarkeit im Strafverfahren

An diesem Punkt (Art. 18k Abs. 4) zeigt sich unmissverständlich, 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 praktisch nie 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. Es ist vielmehr davon auszugehen, dass die Übertragung von Informationen aus staatsschützerischen Überwachungen in Strafverfahren unter Umgehung der Vorschriften für die Verwertung von Zufallsfunden 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 eine Farce.

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 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 es zwischen Prävention und Repression deutliche Zielkonflikte geben kann.

Alibi-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) in einer Art und Weise dominiert werden soll, die nach Ansicht der DJS eine **unhaltbare Verwischung der Gewalten darstellt**. Das Bundesamt, konkret also der DAP, stellt den Antrag und kann im Dringlichkeitsfalle gleich selbst 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 und keine Möglichkeit, diese Informationen auf ihre Stichhaltigkeit zu überprüfen. 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. 18i 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 ganz offensichtlich nicht zum Ziel, Beweise für die Schuld oder Unschuld einer Person zu erbringen. So kann eine Zielperson auch nach dem Ende einer „besonderen“ Informationsbeschaffung nicht damit rechnen, ganz aus dem Visier der Staatsschützer zu verschwinden. Die in Art 18i, Abs 2 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 und in jedem Fall 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 – erweiterte Befugnisse für die Staatsschutzfähigkeit insgesamt beim Bund und in den Kantonen

Während die Bestimmungen über „besondere Informationsbeschaffung“ auf die „Bekämpfung“ von Terrorismus, verbotenen Nachrichtendienst und Proliferation beschränkt sein sollen, beziehen sich die erweiterten Regelungen der „allgemeinen 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.

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

Bereits die bisher in Art. 14 Abs. 2 Bst. d enthaltene Befugnis zur „Entgegennahme und Auswertung von Meldungen“ geht schon sehr weit und ist kaum kontrollierbar: Meldungen privater Personen, sprich: DenunziantInnen, die im Schutze der Anonymität und häufig getrieben durch übersteigertes Geltungsbedürfnis oder aus undurchschaubaren (politischen) Motiven Angaben über Nachbarn, Arbeitskollegen, 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. Der vorliegende Entwurf geht nun 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 gezielten 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 eigentliche V-Leute. Dies gilt umso mehr, wenn sie dafür mit einer Tarnidentität ausgestattet werden und mit staatlich gefälschten Urkunden an Rechtsgeschäften teilnehmen sollen.

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 zwielfichtigen Methoden im Staatsschutzbereich ohne jegliche weitere Voraussetzung eingesetzt werden dürfen. **Da sie als „allgemeine“ Methoden der Informationsbeschaffung vorgesehen sind, muss davon ausgegangen werden, dass sie künftig in sämtlichen Bereichen staatsschützerischer Tätigkeit einsetzbar wären, womit die Schweiz auf dem besten Weg rückwärts zum Spitzel- und Schnüffelstaat wäre.**

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**, sowie die Anwerbung von Medienschaffenden als V-Personen. Beides hat der deutsche Bundesnachrichtendienst seit den 90er Jahren permanent prakti-

ziert. Diese Praxis ist seit Sommer 2006 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 verummten 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.

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 daher ersatzlos zu streichen.

Auskunftspflichten (Art 13-13d)

Die DJS lehnen die hier vorgesehene Ausdehnung der Auskunftspflicht - die ein eigentlicher Zwang zur Auskunft ist - 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“ ausdehnt. Bereits die bestehenden Auskunftspflichten und Melderechte sind nicht akzeptabel. Um eine datenschutzrechtliche Überprüfung möglich zu machen und Denunziationsgelüste zu beschränken, müsste generell gelten, dass die Weitergabe von Informationen an den Staatsschutz schriftlich protokolliert werden.

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 zudem neu auch **private Transportunternehmen** in Dienst genommen werden. Damit könnte theoretisch jeder Taxifahrer dazu gezwungen werden, als Staatsschutzinformant zu agieren.

Der Zugang zu Daten von Transportunternehmen muss auf das Strafverfahren beschränkt bleiben und darf - wenn überhaupt - nur auf richterliche Anordnung erfolgen.

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 je transparent dargelegt. Zahlenmaterial ist nicht vorhanden, Evaluationen gibt es nicht, dem Parlament werden jegliche Auskünfte im Zusammenhang mit entsprechenden Budgetanträgen verweigert.

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. Hinter dieser Praxis 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.

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 neuen Art. 18n soll das Verbotsinstrumentarium um nicht näher bestimmte Betätigungsverbote ausgeweitet werden.

Derartige Verbote kann **derzeit nur der Gesamt-Bundesrat** gestützt auf Art. 184 der Bundesverfassung erlassen. So hat er u.a. tamilischen Organisationen das Sammeln von Spenden bei ihrer jährlichen Demonstration untersagt. Bereits 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 und aus der bisherigen Verantwortlichkeit des Gesamt-Bundesrates herauszulösen. Die DJS lehnen diese Änderung entschieden ab, zumal an keiner Stelle des Entwurfs vermerkt ist, welche Tätigkeiten im Einzelnen verboten werden dürfen. Es kann nicht zugelassen werden, dass **ein einzelner Bundesrat** Personen, die nicht strafrechtlich verurteilt sind und damit als unschuldig zu gelten haben, fünf Jahre oder länger die Wahrnehmung von Grundrechten versagt: **Neu soll es in der Kompetenz des Vor-**

stehers des EJPD liegen, 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 zulassen: 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 endlich die bisherigen Notstandsbefugnisse des Gesamtbundesrates einer richterlichen Kontrolle unterworfen werden, bei der in jedem Falle die entsprechenden Staatsschutz-Informationen offen zu legen sind.

Einsichts- und Auskunftsrecht

Seit Inkrafttreten des BWIS im Juli 1998 verlangen die DJS die Wiederherstellung des Einsichtsrechtes in die eigenen Staatsschutz-Unterlagen. Die bisherige Regelung ist eine Farce. Das Einsichtsrecht in die vom DAP gesammelten Personendaten 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.

III Fazit aus Sicht der DJS

Bevor das BWIS überhaupt einer derart einschneidenden Verschärfung unterzogen wird, besteht nach Ansicht der DJS dringend die Notwendigkeit einer wirklichen Evaluation staatschützerischer Tätigkeiten seit Inkrafttreten des BWIS im Juli 1998.

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. Bedauerlicherweise sind genaue Zahlen nicht erhältlich, bzw. werden gegenüber der Öffentlichkeit geheim gehalten.

Eine öffentliche Kontrolle der im geheimen operierenden Staatsschützer existiert nicht. Die selbst wiederum der Geheimhaltung unterliegende Geschäftsprüfungsdelegation (**GPDel**) der Eidgenössischen Räte erweist sich gerade wegen der fehlenden Öffentlichkeit als ungenügend. Die Kontrolle durch die GPDel stösst nicht zuletzt an enge Grenzen, weil sie die vom DAP gesammelten Daten in aller Regel nicht auf ihre Richtigkeit hin überprüfen kann, sondern allenfalls 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. Die Kontrolle durch die GPDel kann kein wirksamer Ersatz für das Einsichtsrecht der Betroffenen sein.

Es braucht nach Ansicht der DJS zunächst einmal eine grundsätzliche Evaluation der Tätigkeit des Staatsschutzes und der aus diesen präventiven Befugnissen resultierenden Gefahren für die Demokratie. **Es braucht zudem zwingend eine vertiefte Analyse über die Tauglichkeit der zahlreichen Gesetzgebungen, Verordnungen und weiteren Zwangs-Massnahmen, die im gesamten Bereich der inneren Sicherheit und speziell im Rahmen der „Bekämpfung des Terrorismus“ in der Schweiz in Kraft sind**, wie z.B.: die Einführung des Straftatbestandes der „kriminellen Organisation“, zusätzliche Gesetze 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“ (*Massnahmen zur Verbesserung der Effizienz und der Rechtsstaatlichkeit in der Strafverfolgung*), die die Zuständigkeit des Bundes für Ermittlungen und Vorfeld-Ermittlungen gegen vermutete „kriminelle Organisationen“ begründeten.

Bern, den 16. Oktober 2006