Vernehmlassungsantwort zum neuen Nachrichtendienstgesetz (NDG) der Swiss Privacy Foundation

1.) Allgemeine Bemerkungen

In seinem Bericht schreibt der Bundesrat unter *«Vorgeschichte»* auf Seite 2, dass die Überführung der nachrichtendienstlichen Teile des Dienstes für Analyse und Prävention (DAP) ins VBS und die anschliessende Zusammenführung des Strategischen Nachrichtendienstes (SND) mit dem DAP zum NDB die Ausarbeitung eines gesamtheitlichen Nachrichtendienstgesetzes erfordere. Der Gesetzesentwurf solle keine Weiterentwicklung der bestehenden Rechtsgrundlagen darstellen, sondern lediglich eine Neukodifikation. Die Rückweisung und die damit verbundenen Auflagen an den Bundesrat von BWIS II durch das eidgenössische Parlament wird fast vollständig ausgeblendet bzw. weiter hinten im Bericht nur kurz angesprochen.

Die neuen Zwangsmassnahmen, welche dem NDB erlaubt sein sollen, sind nach Ansicht der Swiss Privacy Foundation das Kernstück der Vorlage, auch wenn sie leicht übersehbar in ein Gesetz eingebaut sind, welches laut Bericht des Bundesrats ***«keine Weiterentwicklung der bestehenden Rechtsgrundlagen darstellen, sondern eine Neukodifikation, die bestehenden Bedenken und Vorbehalten gegenüber der bisherigen Tätigkeit der Nachrichtendienste in der Schweiz (insbesondere betreffend das Sammeln von Personendaten) weitestmöglich Rechnung tragen soll»***.

Mit dem vorliegenden Gesetzesentwurf werden keine Bedenken, insbesondere solche betreffend das Sammeln und Weitergeben von Personendaten, ausgeräumt. Somit kann die Swiss Privacy Foundation dem vorliegenden Entwurf nichts Positives abgewinnen, im Gegenteil. Statt die Tätigkeit des Staatsschutzes einer eingehenden Überprüfung zu unterziehen und der gefährlichen Anhäufung von sensiblen Daten ein Ende zu bereiten, wie dies die sogenannte zweite Fichenaffäre eigentlich geboten hätte, hält der Bundesrat an den Vorschlägen fest, welche der damalige Dienst für Analyse und Prävention (DAP) nach den Anschlägen in den USA vom 11. September 2001 federführend in diversen Arbeitsgruppen ausarbeiten liess. Das Ergebnis war und ist, dass die Wunschliste des Staatsschutzes in gesetzliche Regelungen umgebaut werden soll. Die eklatanten Schwächen des Staatsschutzes, welche durch die zweite Fichenaffäre offenkundig wurden, wie auch die vom Parlament geltend gemachten Vorbehalte, werden übersehen oder bagatellisiert.

Dies galt schon für die vom Parlament bereits im Dezember 2011 beschlossene erste Revision des BWIS («BWIS II - reduziert»), und dies gilt vor allem auch für den jetzt vorliegenden Entwurf des neuen Nachrichtendienstgesetzes. Der DAP durfte schon im Jahre 2002 kundtun, dass er die einzige wirkliche Grenze im bestehenden Gesetz - das Verbot von strafprozessualen Zwangsmassnahmen - aufgehoben sehen möchte. Grundsätzliche Veränderungen gegenüber der vom Parlament im Jahre 2009 aus grundrechtlichen Bedenken zurückgewiesenen BWIS II Vorlage sind, mit Ausnahme der neu

hinzugekommenen *«Kabelaufklärung»* und der explizit legiferierten Nutzung von Staatsschutzdaten in Strafverfahren, nicht erkennbar. Zentraler Bestandteil des neuen Nachrichtendienstgesetzes sind Befugnisse, die bisher nur im Rahmen eines Strafprozesses als Zwangsmassnahmen möglich sind, welche dort aber mit spezifischen Schranken, Anordnungs- und Genehmigungsverfahren sowie mit weitergehenden Rechten der Angeschuldigten, insbesondere auf Siegelung und Akteneinsicht, verknüpft sind.

An verschiedenen Stellen des Berichts legt der Bundesrat ungeschminkt dar, dass der Nachrichtendienst offenbar als Hilfsdienst der Strafverfolgungsbehörden Ermittlungen tätigen soll, welche den Strafverfolgungsbehörden verwehrt sind, um die Erkenntnisse anschliessend in einem Strafverfahren als Beweis zu verwenden, etwa auf Seite 17 *unter «Abgrenzung von der Tätigkeit der Strafverfolgungsbehörden»* oder im Zweiten Kapitel *«Aufgaben und Zusammenarbeit des NDB»* auf Seiten 20 und 21, ebenso im 4. Abschnitt *«Genehmigungspflichtige Beschaffungsmassnahmen»* auf Seite 38, hier wörtlich: ***«Jedoch sind nicht alle sicherheitspolitisch relevanten Bedrohungen strafrechtlich relevant, bzw. genügen die Verdachtslagen teilweise noch nicht, um strafrechtliche Ermittlungen auszulösen»***.

Anders ausgedrückt: Ist die Verdachtslage ungenügend, um strafrechtliche Ermittlungen auszulösen, kann der NDB ausserhalb eines Strafverfahrens mit Telefonüberwachung, Verwanzung von Räumen, der geheimen Durchsuchung von Datenverarbeitungsanlagen, mit Standortbestimmungen oder mit Kabelaufklärung solange überwachen und Daten sammeln, bis er eventuell etwas findet, was als Anfangsverdacht für ein Strafverfahren genügen könnte und die Angelegenheit anschliessend den Strafverfolgungsbehörden übergeben.

Dass gemäss Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte Überwachungsmassnahmen nur in Frage kommen, wenn tatsächliche Anhaltspunkte für den Verdacht einer Straftat bestehen und wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre (Entscheid des Europäischen Gerichtshofes für Menschenrechte vom 6. September 1978 i.S. Klass und Mitbeteiligte, Publications de la Cour Européenne des Droits de l'Homme, Série A, Volume 28, § 41, in deutscher Übersetzung publiziert in: EuGRZ 1979 S. 278 ff.), aber sogenannte «erkundende» oder allgemeine Überwachung zur Einleitung eines Strafverfahrens unzulässig ist, scheint den Bundesrat nicht zu interessieren. Er zitiert zwar dieses Urteil auf Seite 45 im Bericht ziemlich aus dem Zusammengang gerissen mit *«dass eine nachträgliche Mitteilung den langfristigen Zweck einer Überwachung in Frage stellen und deshalb unter bestimmen Voraussetzungen unterlassen werden dürfe»*, und blendet dabei aus, dass für eine Überwachung tatsächliche Anhaltspunkte für den Verdacht einer Straftat bestehen müssen, aber eine sogenannte «erkundende» oder allgemeine Überwachung als klar unzulässig eingestuft wurde.

Auf Seite 64 wird dann mit Art. 55 *«Weitergabe von Personendaten an inländische Behörden»* die Katze endgültig aus dem Sack gelassen. Hier schreibt der Bundesrat***: «Namentlich die Weitergabe von Daten aus genehmigungspflichtigen***

Beschaffungsmassnahmen erfordert weitere Schutzmassnahmen. Damit soll verhindert werden, dass z.B. bei Fernmeldeüberwachungen festgestellte, geringfügige Straftaten den Strafverfolgungsbehörden gemeldet werden. Das Strafprozessrecht enthält eine vergleichbare Regelung für solche sogenannten Zufallsfunde (Art. 278 StPO). Das NDG übernimmt deshalb in Absatz 3 den Grundsatz, dass nur Erkenntnisse bezüglich Straftaten verwendet werden dürfen, für deren Verfolgung auch die vergleichbare strafprozessrechtliche Überwachungsmassnahme hätte angeordnet werden dürfen.»

Nicht nur soll also auf einen Anfangsverdacht verzichtet werden, vielmehr sollen ohne Anfangsverdacht noch einschneidendere Mittel als die, welche die Strafverfolgungsbehörden zur Verfügung haben, zur verdeckten Ermittlung im Geheimbereich von Personen zulässig sein, um eventuell strafprozessuale Beweise zu beschaffen. Art. 55 NDG ist nichts anderes als eine Legalisierung von «Fishing Expeditions» als Grundlage im Strafverfahren und somit klar verfassungswidrig, vgl. BGE 6B_849/2010 vom 14. April 2011 (Badenfahrt) und andere, er widerspricht auch der EMRK resp. deren Auslegung durch den EGMR (Urteil Klass). In Verbindung mit Art. 29 NDG, nach welchem der NDB die Mitteilung über die durchgeführte *«genehmigungspflichtige Beschaffungsmassnahme»* aufschieben oder von ihr absehen kann, wenn dies notwendig ist, um eine laufende Beschaffungsmassnahme oder ein laufendes rechtliches Verfahren nicht zu gefährden, kann ein Angeschuldigter bis zu seiner rechtskräftigen Verurteilung aufgrund von Beweisen, welche von den Strafverfolgungsbehörden aufbauend auf Erkenntnissen des NDB nachträglich erhoben wurden, und sogar darüber hinaus, über das verdachtsunabhängige Eindringen in den Privat- und Geheimbereich im Unwissen gelassen bleiben und so seiner Verteidigungsrechte beraubt werden. Die Aufschiebung der Mitteilung bis zum Abschluss des Strafverfahrens heisst, dass Betroffene auch während des Strafverfahrens nicht erfahren, aus welcher Quelle Informationen stammen. Faktisch wird die Verteidigung in solchen Fällen wohl nur die übliche Floskel «Amtlich wurde bekannt … » erhalten. Eine Verteidigung ist so nicht möglich. Das ist eine Verletzung des Prinzips der Waffengleichheit im Strafprozess.

Begründet werden die diversen gewünschten verdeckten Ermittlungen im Privat- und Geheimbereich damit, dass Terroristen und Verbrecher die neuesten Techniken benutzen würden und daher der Staat nachziehen müsse. Dem ist entgegenzuhalten, dass schon lange vor der Internetzeit geheime Besprechungen in privaten Räumen durchgeführt wurden, aber eine rückwirkende Erfassung nie möglich war. Erst mit der Einführung digitaler Telefonzentralen in den 1980er-Jahren und später bei Internetdiensten war eine systematische Speicherung von Verbindungsdaten möglich. Nur dadurch konnte und kann die Frage «wer hat wann mit wem für wie lange kommuniziert» für die gesamte Bevölkerung in die Vergangenheit schauend beantwortet werden. Seit diese Daten vorhanden sind, wurden sie in der Schweiz zur Strafverfolgung genutzt, zuerst auf kantonaler gesetzlicher Basis, dann ab 2002 gestützt auf das BÜPF, ohne dass Terroristen und Verbrecher durch die digitalen Telefonzentralen einen entscheidenden Vorteil gehabt hätten. Es war also der Staat, der die neue Technik ausnutzte, und nicht umgekehrt, wie vom Bundesrat in den Unterlagen zum NDG behauptet wird.

Noch einen Schritt weiter geht die Überwachung für Personen, welche ständig ein Mobiltelefon auf sich tragen. Der Standort des Telefons wird regelmässig erfasst, und so lassen sich von jedem beliebigen Abonnenten eines mobilen Telefons alle seine Bewegungen innerhalb der Schweiz für ein halbes Jahr und mehr in die Vergangenheit zurückverfolgen. Mit Antennensuchläufen und IMSI-Catchern können die Aufenthaltsorte von beliebigen Personen ermittelt werden, was zur Zeit der guten alten Telefonkabinen ebenfalls nicht möglich war.

Auf Seite 13 schreibt der Bundesrat, dass er pro Jahr mit etwa 10 Fällen genehmigungspflichtiger Beschaffungsmassnahmen rechne, auf Seite 14 geht er von rund 16 zusätzlichen Stellen aus, welche dafür benötigt werden. Es obliegt der parlamentarischen Aufsicht, dieses Verhältnis in Frage zu stellen, sollten die zusätzlichen Stellen tatsächlich genehmigt werden.

Weiter fällt auf, dass im Gegensatz zu James Bond und anderen Agenten aus dem Kino, welche jeweils im Ausland Spionen nachjagen, der NDB vornehmlich innerhalb der Schweiz verdeckte Beschaffungsmassnahmen ausführen soll. Dazu schreibt der Bundesrat auf Seite 16 des Berichts*: «Die Informationsbeschaffung im Ausland soll deshalb nur erfolgen, wenn die zur Gefahrenabwehr benötigten Informationen im Inland nicht beschafft werden können»*. Weiter auf Seite 10*: «Sollen Informationen bezüglich verbotenem Nachrichtendienst gesammelt werden, so sind nach geltendem Recht nicht allgemein zugängliche Orte (z.B. Hotelzimmer) generell jeder Bedrohungsabklärung entzogen. Spione nutzen diese Lücke bewusst aus; sie stehen vielfach unter diplomatischer Immunität und sind geschult, unter Tarnung Informationen zu beschaffen. Hinzu kommen Abklärungen internationaler Ermittlungsbüros, die nicht selten in (getarntem) staatlichem Auftrag handeln. Die Folge der heutigen Rechtslage ist, dass beispielsweise auch die Spionageabwehr grundsätzlich an der «Tür zum privaten Raum» endet. Dadurch entstehen gewichtige Lücken im Abwehrdispositiv.» und auf Seite 39: «Beispiel: Ein sich in der Schweiz unter operativer Tarnung aufhaltender ausländischer Nachrichtendienstoffizier versucht, menschliche Quellen zu rekrutieren und von diesen illegal Informationen aus sensiblen Bereichen zu beschaffen. Es ist dem NDB bekannt, dass der Offizier für die Führung der menschlichen Quellen Mobiltelefonanschlüsse benutzt. Insgesamt hat er vier Prepaid-Abonnemente für Mobiltelefone in der Schweiz gekauft. Um festzustellen, zu welchen Personen er mit diesen Telefonen Kontakt hat, ist es notwendig, die Verbindungsnachweise oder Randdaten dieser Mobiltelefonanschlüsse zu erheben.»* Wie der britische Abhördienst Government Communications Headquarters (GCHQ) während des G20-Gipfels 2009 in London soll der NDB also den Telefon- und Email-Verkehr von Personen, welche unter diplomatischer Immunität stehen, abhören und womöglich ein verwanztes Internet-Café einrichten. Die vom Bundesrat konstruierten Beispiele sind realitätsfremd und nicht überzeugend. Auch im Lichte der bundesrätlichen Praxis, zufällig erwischte Spione ungeschoren laufen zu lassen (2006 «Tom» in Bern, US-Agenten im Fall Tinner, Bespitzelung von Bundesrätin Calmy Rey in Lausanne), erscheint die Argumentation fadenscheinig. Unter dem Vorwand, fremde Agenten im Land enttarnen zu wollen, soll mit den neuen *«genehmigungspflichtigen*

Beschaffungsmassnahmen», in BWIS II noch *«besondere Mittel der Informationsbeschaffung»* genannt, durch den NDB vorab die eigene Bevölkerung überwacht werden. Es wird vornehmlich erneut die politische Opposition und MigrantInnen-Organisationen treffen, wobei letztere oft auch von ihren «eigenen» Nachrichtendiensten in der Schweiz ausspioniert werden.

Der vorliegende Entwurf des NDB bringt entgegen den Aussagen des Berichts keine signifikante Verbesserung der Qualität. Wenn der Bundesrat auf Seite 54 schreibt: *«Während die Datenbearbeitung beispielsweise im Bereich Spionageabwehr, Nonproliferation oder Schutz kritischer Infrastrukturen kaum jemals zu Kritik Anlass gab, hat sich die Datenbearbeitung im Bereich des gewalttätigen Extremismus immer wieder als politisch und datenschutzrechtlich besonders sensibel erwiesen»* geht er offenbar davon aus, dass die Datenbearbeitung im Bereich Spionageabwehr, Nonproliferation oder Schutz kritischer Infrastrukturen keiner Qualitätssteigerung bedürfe und übersieht, dass derartige Daten bisher noch niemand zu Gesicht bekommen und entsprechend kommentiert hat. Die einzige wirkliche Qualitätskontrolle besteht darin, dass verzeichnete Organisationen und Personen ihre eigenen Fichen studieren und bewerten.

In den letzten Jahren fanden derartige wirkliche Qualitätskontrollen nur im Bereich des gewalttätigen Extremismus statt, und das Ergebnis ist ernüchternd. Wenn der Bundesrat auf Seite 56 weiter schreibt *«die Einrichtung einer internen Qualitätssicherungsstelle im NDB hat sich bewährt»*, ist dem entgegenzuhalten, dass der Berg von sinnlosen Daten, welche der NDB innert weniger Jahren angehäuft hat, nur auf öffentlichen Druck hin und erst per Ende 2012 angeblich abgebaut wurde. Gemäss Jahresbericht 2012 der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation der eidgenössischen Räte sind aber rund 100 als eigenständige Objekte registrierte Medien noch nicht gelöscht, obwohl das Bundesverwaltungsgericht am 18. März 2009 die Löschung sämtlicher diesbezüglicher Einträge verlangt hat. Auch mit dem neuen NDG bleibt das Datensammelmotto des NDB «Quantität statt Qualität». Wenn dieses Prinzip grundlegend geändert werden soll, ist eine wirkungsvolle Kontrolle vor, und nicht nach der Datenerhebung durch den NDB anzusetzen. Insbesondere sind Datenfluten auslösende Bestimmungen wie etwa die Aushebelung des Verbots der Beschaffung und Bearbeitung von Informationen über die politische Betätigung und die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit, die besondere Auskunfts- und Meldepflicht von Amtsstellen, die besonderen Auskunftspflichten Privater, die Beobachtungsliste und das Verzeichnis der Gruppierungen, die als gewaltextremistisch einzustufen sind, entweder ersatzlos zu streichen oder so auszugestalten, etwa mit einem Richtervorbehalt, dass der Sammeltätigkeit ein effizienter Riegel geschoben wird.

Von Staatsschutzbehörden gesammelte Daten, ob richtig oder unrichtig (siehe Art. 39, Weiterbearbeitung von unrichtigen Daten) sind immer eine grosse Gefahr für unbescholtene Bürgerinnen und Bürger, da diese Daten meist mit anderen Behörden im In- und Ausland ausgetauscht werden. So ist etwa denkbar, dass - zusätzlich zur bereits thematisierten Verwendung in Strafverfahren - ein Einreisevisum nicht erteilt, ein Asylgesuch nicht bewilligt

oder eine Bewerbung zur Besetzung einer Arbeitsstelle im öffentlichen Dienst nicht berücksichtigt wird, nur weil eine Person, aus was für Gründen auch immer, in einer Staatsschutzdatenbank verzeichnet ist.

Auch ist nicht ersichtlich, weshalb die Daten, welche in den Datenbanken des NDB abgelegt werden, unterschiedlichen Qualitätsstandards genügen sollen, zumal sie nach ihrer Erfassung frei in den Datenbanken des NDB hin- und herkopiert werden können und dabei auch ihren Charakter ändern, indem sie etwa das Attribut einer Erkenntnis aus einer bewilligungspflichtigen Beschaffungsmassnahme verlieren. Wie aus diesem Tohuwabohu brauchbare Produkte hergestellt werden können sollen, bleibt wohl vorerst ein Geheimnis des NDB und des Bundesrats.

Aus diesen Gründen lehnt die Swiss Privacy Foundation das vorliegende Nachrichtendienstgesetz vollumfänglich ab. Wir schliessen uns den Argumenten der Minderheit der nationalrätlichen Rechtskommission (Rückweisung BWIS II, 20. Juni 2008) an. Das Strafrecht und die Strafprozessordnungen bieten bereits eine genügende und sehr weitreichende Handhabe, auch für präventive Ermittlungen. Die mit dem NDG vorgesehenen Eingriffe in die Privatsphäre sind unverhältnismässig.

2.) Anmerkungen zu einzelnen Artikeln

1. Kapitel: Allgemeine Bestimmungen und Grundsätze der Informationsbeschaffung

Art. 3 Grundsätze der Informationsbeschaffung

In der Vergangenheit hat sich der NDB regelmässig nicht an die Schranken von Art. 3 Abs. 5 NDG gehalten, welcher die Beschaffung und Bearbeitung von Informationen über die politische Betätigung und die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit untersagt. Wiederholt wurden z. B. Personen, welche um die Bewilligung einer Demonstration nachsuchten, fichiert. Die jüngste derartige Fiche, welche vorliegt, ist ein Bewilligungsgesuch vom 25. Januar 2010 für eine Anti-WEF-Demo. Ein Grund dafür dürften die Beobachtungsliste und die Liste der Gruppierungen, die als gewaltextremistisch einzustufen sind, sein, welche auf Antrag der Staatschützer durch eine leichtfertige breite Fächerung durch den Bundesrat die Schranken von Art. 3 Abs. 5 NDG vollständig aushebeln. Weitere Fichen, welche vorliegen und die Aushebelung der Schranken von Art. 3 Abs. 5 NDG illustrieren, betreffen z. B. Besucher einer öffentlichen Gerichtsverhandlung in Basel vom 30. Oktober 2007 gegen vier Störer des Länderspiels Schweiz - Israel, die friedlich verlaufene Spontandemo *«Gegen den Überfall der israelischen Armee auf die internationale Freiheits-Flotte»* vom 5. Juni 2010 in Basel oder ein Solidaritäts-Konzert in der Villa Rosenau Basel vom 12. Juni 2010.

Aus diesem Grund ist es zwingend notwendig, entweder Art. 3 Abs. 8 NDG ersatzlos zu streichen oder zumindest die Beobachtungsliste und die Liste der Gruppierungen, die als gewaltextremistisch einzustufen sind, sowie jeden Eingriff in den Gehalt von

Art. 3 Abs. 5 NDG einem Richtervorbehalt zu unterstellen. Noch besser wäre, wenn alle diese Listen künftig öffentlich wären oder zumindest im Jahresbericht des NDB nachträglich ausgewiesen wird, welche Gruppierungen überwacht wurden bzw. Auskunft gegeben wird über die genaue Zahl der überwachten Personen. Im Bericht des Deutschen Bundesamtes für Verfassungsschutz finden sich jährlich sogenannte Strukturangaben. Diese umfassen sowohl die Zahl der im nachrichtendienstlichen Informationssystem gespeicherten Personen als auch Angaben über das Personal und den Stellenetat des Inlands-Geheimdienstes.

2. Kapitel: Aufgaben und Zusammenarbeit des NDB

Art. 4 Abs. 7 Aufgaben des NDB und Art. 5 Schutz- und Sicherheitsmassnahmen
Offensichtlich wurden Art. 4 Abs. 7 und Art. 5 NDG kurzfristig in den Gesetzesentwurf eingefügt, als Reaktion auf den Mega-Datendiebstahl von 2012 durch einen Mitarbeiter des Geheimdienstes. Derartige Bestimmungen gehören aber u. E. nicht in dieses Gesetz resp. sollten eigentlich selbstverständlich sein für einen Dienst, der in derart heiklem Umfeld tätig ist. Sofern mit Art. 4 Abs. 7 NDG allerdings dem NDB alle Kompetenzen dieses Gesetzes gegeben werden sollen, um seine Mitarbeiterinnen und Mitarbeiter, seine Einrichtungen, seine Quellen und die von ihm bearbeiteten Daten zu schützen, ist er ebenfalls abzulehnen. Die Beobachtungsliste beispielsweise wurde schon der Sonntagszeitung zugespielt, welche dann darüber berichtet hat. Der NDB könnte neu gestützt auf Art. 4 Abs. 7 NDG eine ähnliche Aktion starten wie der Bundesnachrichtendienst (BND) in Deutschland, welcher aufgrund eines vergleichbaren Vorfalls den Journalisten-Skandal lostrat. Bei dieser im Jahre 2005 aufgeflogenen Überwachung wurden in der Zeit von 1993 bis mindestens 1998 verschiedene kritisch über den Geheimdienst berichtende Journalisten systematisch observiert, um das Datenleck zu finden. Für derartige Massnahmen sind aber ganz klar die Strafverfolgungsbehörden zuständig, welche genügend gesetzliche Grundlagen haben.

Was für Art. 4 Abs. 7 NDG gilt, gilt uneingeschränkt auch für den gesamten Art. 5 NDG. In eigenen Geschäftsräumen kann jeder Betrieb ohne gesetzliche Grundlage ein Sicherheitsregime aufziehen. Derartige Bestimmungen können in einer Verordnung oder gar einem Reglement erlassen werden. Gemäss Art. 34 Abs. 1ter FMG regelt der Bundesrat, unter welchen Voraussetzungen Polizei- und Strafvollzugsbehörden im Interesse der öffentlichen Sicherheit eine störende Fernmeldeanlage erstellen, in Betrieb nehmen oder betreiben können. Diese Norm ist allenfalls durch «Staatsschutzbehörden» zu ergänzen. Allenfalls Abs. 2 dieses Artikels ergibt einen Sinn.

3. Kapitel: Informationsbeschaffung

Art. 13 Menschliche Quellen
«Spitzel» oder «bezahlte Denunzianten» würde den Inhalt dieses Artikels besser umschreiben als *«Menschliche Quellen»*. Der Begriff vertuscht die Tatsache, dass es sich hier um ganz verschiedene Rollen handeln kann. Vom einmaligen Informationsgeber, dem bewussten Denunzianten oder CD-ROM-Anbieter, über den regelmässigen Informanten bis

hin zum gesteuerten V-Mann. Kennzeichnend insbesondere für die letzte Gruppe ist, dass diese Personen auch ihre eigenen Interessen mit einbringen, wie das u.a. deutlich geworden ist rund um den NSU in Deutschland. Gemäss Bericht des Bundesrats verlangen Spitzel insbesondere im Ausland vielfach Geld für die Weitergabe ihrer Informationen. Es ist nicht nachvollziehbar, weshalb aus diesem Grund Spitzel auch in der Schweiz bezahlt werden sollen, wie dies mit «BWIS II - reduziert» leider bereits eingeführt wurde - damals allerdings gemäss Art. 14a Abs. 3 BWIS nur *«Soweit es für den Quellenschutz oder die weitere Informationsbeschaffung notwendig ist»*. Es besteht die grosse Gefahr, dass Spitzel im Sinne eines Geschäftsmodells entweder Phantasie-Meldungen oder zumindest tatsachenwidrige Dramatisierungen an den NDB verscherbeln werden. Etwas surreal mutet im Zusammenhang mit der jüngsten Gesetzgebung betreffend den Finanzplatz Schweiz an, dass die Zahlungen in Form von Schwarzgeld erfolgen sollen. Sofern an der Bezahlung von Spitzeln in der Schweiz festgehalten wird, ist jede einzelne Zahlung einem Richtervorbehalt zu unterstellen. Die Zahlungen müssen mindestens AHV- bzw. steuerpflichtig sein (in der Höhe gem. den entsprechenden rechtlichen Grundlagen über den Nebenerwerb) und die GPDel muss jährlich über die einzelnen Zahlungen informiert werden.

Art. 14 Ausschreibung von Personen und Fahrzeugen zwecks Aufenthaltsfeststellung
Es sollen Personen zwecks Aufenthaltsfeststellung ausgeschrieben werden, wenn begründete Anhaltspunkte vorliegen, welche diese Personen mit einer Bedrohungen der inneren oder äusseren Sicherheit in Zusammenhang bringen. Das Spektrum der möglichen Bedrohungen geht von Terrorismus über verbotenen Nachrichtendienst, die Weiterverbreitung von nuklearen, chemischen und biologischen Waffen, den illegalen Handel mit radioaktiven Substanzen und Kriegsmaterial etc. bis hin zu gewalttätigem Extremismus. Um einen Missbrauch des NDB und somit ein Ausufern der Ausschreibungen zu verhindern, ist der Katalog von zulässigen Bedrohungen, welche die Aufenthaltsfeststellung von Personen erlauben, zwingend zusammenzustreichen. Alle Ausschreibungen sind zudem einem Richtervorbehalt zu unterstellen.

Art. 16 Tarnidentitäten
Tarnidentitäten innerhalb des NDB wurden mit «BWIS II - reduziert» bereits Ende 2011 eingeführt. Der entsprechende Artikel 14c BWIS ist erst seit dem 16. Juli 2012 in Kraft, trotzdem soll dieses Mittel bereits erweitert werden, indem Tarnidentitäten nach 5 Jahren um jeweils 3 Jahre verlängert werden können. Ebenso sollen Tarnidentitäten neu benutzt werden können zur Informationsbeschaffung bei jeder konkreten *«Gefährdung der inneren oder äusseren Sicherheit der Schweiz»* im Sinne von Art. 4 Abs. 1 NDG. Ebenfalls neu sollen auch Spitzel im Rahmen einer bestimmten Operation bis zu 12 Monaten eine Tarnidentität annehmen können. Es ist nicht ersichtlich, weshalb sich nach so kurzer Zeit bereits eine Ausweitung dieser Bestimmung aufdrängt. **Wie Beispiele aus anderen Ländern zeigen, sind insbesondere *«menschliche Quellen»* im Rahmen einer bestimmten Operation», versehen mit einer Tarnidentität, schnell nicht mehr kontrollierbar. Der NDB sollte vom Parlament gezwungen werden, über die bisherige Praxis Rechenschaft abzulegen, bevor überhaupt über eine Erweiterung nachgedacht wird.** Gerade wenn mit Tarnidentitäten versehene Personen für die Informationsbeschaffung, die bisher ohne dieses

Mittel erfolglos war, eingesetzt werden sollen, müsste die Übung eigentlich abgebrochen und nicht noch mit Massnahmen ausgebaut werden, die äusserst heikel sind bzw. lebensgefährlich werden können.

Art. 17 Auskunftspflicht bei einer konkreten Bedrohung

Dieser Artikel bewirkt ähnlich wie die Beobachtungsliste und die Liste der Gruppierungen, die von den Behörden als gewaltextremistisch eingestuft werden, einen Automatismus, welcher lediglich zu einer Ansammlung von Unmengen nicht relevanter Daten führen, aber keinen Nutzen erzielen wird. Die Vergangenheit hat dies mehrfach gezeigt. Gemäss Art. 17 Abs. 2 lit. e NDG ist eine konkrete Bedrohung der inneren oder äusseren Sicherheit gegeben, wenn ein bedeutendes Rechtsgut wie Leib und Leben betroffen ist und die Bedrohung ausgeht von gewalttätigem Extremismus im Sinne von Bestrebungen von Organisationen, die die demokratischen und rechtsstaatlichen Grundlagen ablehnen und zum Erreichen ihrer Ziele Gewalttaten verüben, fördern oder befürworten. Dienststellen und Organisationen können sogar unaufgefordert Meldung erstatten. Mit dem Begriff *«Gewalttaten befürworten»* ist praktisch alles abgedeckt, was in einer hitzigen Diskussion gesagt wird. **Art. 17 Abs. 2 lit. e NDG ist daher zu streichen.** Auch das deutsche Bundesverfassungsgericht in Karlsruhe hat in seinem Urteil vom 24. April 2013 betreffend die «Anti-Terror-Datei», welche mit den Datenbanken des NDB vergleichbar ist, erkannt, dass das blosse Befürworten von Gewalt nicht ausreiche, um die Daten eines Menschen in der Datensammlung zu speichern.

Art. 18 Besondere Auskunfts- und Meldepflicht

Auch diese Bestimmung bewirkt einen Automatismus, welcher lediglich zu einer Unmenge nicht relevanter Daten führen, aber keinen Nutzen erzielen wird. Mit Art. 18 Abs. 1 lit. i NDG, wonach *«Behörden, die für den Betrieb von Informatiksystemen zuständig sind, zur Auskunft verpflichtet sind»*, erhält der NDB uneingeschränkt Einsicht in alle Geschäfte, Verfahren und Daten von kommunalen, kantonalen und nationalen Behörden, weil heute alle Verwaltungen elektronisch arbeiten. In jeder Verwaltungsbehörde gibt es eine Stelle, die für den Betrieb der Informatikdienste zuständig ist. Die schwammige Definition zeigt einmal mehr die Problematik der gesamten Vorlage. Zudem ist Art. 18 Abs. 3, wonach *«unaufgefordert Meldung zu erstatten ist, wenn eine konkrete und schwere Bedrohung der inneren oder äusseren Sicherheit festgestellt wird»*, ein weiterer Freibrief zur Denunziation per Gesetz und es ist zu befürchten, dass die so unter Druck gestellten Behörden unhinterfragt Personendaten liefern, weil sie dazu unaufgefordert verpflichtet sind, wenn sie eine kaum definierbare *«konkrete und schwere Bedrohung der inneren oder äusseren Sicherheit feststellen»*. Diese Bestimmung ist zu streichen.

Art. 21 Besondere Auskunftspflichten Privater

Wie schon in Art. 17 und 18 würden durch die vage Definition einer konkreten Bedrohung der inneren oder äusseren Sicherheit zahllose kaum verwertbare Einträge aufgrund von Daten gewerbsmässiger Transporteure und Sicherheitsdienstleister generiert. Ebenso soll der NDB durch die neue Bestimmung von Art. 21 Abs. 1 lit. b NDG Zugriff auf sämtliche Videoüberwachungsbilder von Privaten haben. Mit der zunehmenden Ausbreitung von Videoüberwachung wächst potenziell auch das, was der NDB an Informationen zur

Verfügung hat, ohne dass aber Qualitätsstandards oder Einschränkungen für private Videoüberwachungen bestehen. Diese Bestimmung ist zu streichen.

Ebenfalls sollen durch den NDB Auskünfte nach Artikel 14 des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs eingeholt werden können. Hier kommt zum Tragen, dass bei Straftaten, welche über das Internet begangen wurden, ein Eingriff ins Fernmeldegeheimnis ohne Richtervorbehalt möglich wäre, was prinzipiell nicht zu gestatten ist. **Auskünfte auf Randdaten, die aufgrund Art. 15 Abs. 3 BÜPF vorgehalten werden, müssen den selben Einschränkungen und Voraussetzungen unterworfen sein, wie die genehmigungspflichtigen Beschaffungsmassnahmen.**

Art. 22 Arten von genehmigungspflichtigen Beschaffungsmassnahmen
Der NDB soll neu alles dürfen, was Strafverfolgungsbehörden bei einem begründeten Tatverdacht mit richterlicher Genehmigung auch erlaubt ist, allerdings sollen die Kompetenzen bedeutend weiter gehen. Bei der Überwachung des Fernmeldeverkehrs ist die rückwirkende Auswertung von Rechnungs- und Verbindungsdaten gemeint. Hier ist anzumerken, dass die «Vorratsdatenspeicherung» bisher von allen Verfassungsgerichten europäischer Staaten, welche sie beurteilt haben, als verfassungswidrig beurteilt wurde. Auch vor dem EGMR in Strassburg sind diverse Verfahren in dieser Angelegenheit hängig. Erschwerend kommt hinzu, dass mit der Revision des BÜPF (Telefonüberwachungsgesetz) die Speicherpflicht von Rechnungs- und Verbindungsdaten von 6 auf 12 Monate ausgedehnt werden soll. Zudem erlaubte das Bundesgericht auch den Zugriff auf Daten, welche viel älter sind als die vom Gesetz bestimmte Zeit von 6 Monaten (BGE 1B_481/2012 vom 22. Januar 2013). Gemäss Art. 14 Abs. 4 BÜPF ist eine rückwirkende Überwachung in gewissen Fällen (Teilnehmeridentifikation bei Straftaten, welche über das Internet begangen wurden) sogar ohne richterliche Genehmigung möglich.

Seit 2007 haben Telekom- und Internetprovider in Dänemark die Pflicht, alle Daten ein Jahr lang aufzubewahren. Die gelagerten Mengen sind enorm. Allein im Jahr 2012 wurden 900 Milliarden Daten gespeichert, das waren 145 000 Daten pro Däne. Jeder der rund fünf Millionen Bewohner des Landes wurde jeden Tag im Durchschnitt fast 400-mal registriert. Der Geheimdienst PET stellt nun fest, dass die Einholung derartiger Informationen *«in sehr geringem Ausmass»* für die Ermittlungen relevant sein könne. Für die Terrorfahndung spielte sie bisher überhaupt keine Rolle.

Vor diesem Hintergrund müsste, wenn überhaupt, über Schranken bei den Strafverfolgungsbehörden diskutiert werden und sicher nicht über eine Erweiterung der Rechte des NDB.

Besonders auch der Einsatz von Ortungsgeräten, um den Standort und die Bewegung von Personen festzustellen, und der Einsatz von Überwachungsgeräten, um das nicht öffentlich gesprochene Wort abzuhören oder aufzuzeichnen oder um Vorgänge an nicht öffentlichen oder nicht allgemein zugänglichen Orten zu beobachten oder aufzuzeichnen, dringen viel zu stark in die Intimsphäre von Personen ein, um sie einem im geheimen und im Vorfeld

agierenden Nachrichtendienst zu gewähren.

Das Eindringen in Computersysteme und Computernetzwerke soll mit der Revision des BÜPF auch den Strafverfolgungsbehörden erlaubt werden, allerdings gemäss Botschaft nur, um den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs in unverschlüsselter Form abzufangen und auszuleiten. Der Entwurf des NDG sieht aber vor, dass der NDB in ein Computersystem eindringen und sämtlich vorhandene Informationen beschaffen und verwenden darf. Theoretisch sind damit auch Manipulationen der Daten durch die Staatsschützer möglich. Um Trojaner via Internet auf Computer installieren zu können, muss der NDB mit dem Internet Service Provider der Zielperson zusammenarbeiten. Die Personen, welche angeblich ausspioniert werden sollen, besitzen aber als getarnte Diplomaten keinen Internetzugang über einen schweizerischen Provider. Durchsuchungen von Räumen durch die Staatsschützer werden - im Gegensatz zu Durchsuchungen durch Strafverfolgungsbehörden - verdeckt durchgeführt. Die davon betroffenen Personen haben keine Möglichkeit, eine Siegelung zu verlangen oder bei der Sichtung beschlagnahmter Schriftstücke anwesend zu sein. Die geheime Durchsuchung von Räumen wird zwangsläufig dazu führen, dass die Geheimdienste sich mit nicht legalen Massnahmen Zugang zu den Räumlichkeiten verschaffen müssen.

Der NDB soll sogar befugt werden, zum Eindringen in Computernetzwerke, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen falls diese für Angriffe auf kritische Infrastrukturen verwendet werden. **Diese Ermächtigung zu Cyberattacken ist unverständlich und gefährlich.**

Aus all diesen Gründen, weil Polizei- und Geheimdienstdaten grundsätzlich zu trennen sind und wegen der geplanten Verquickung von Staatsschutzaktivitäten mit Strafverfahren, lehnt die Swiss Privacy Foundation diese genehmigungspflichtigen Beschaffungsmassnahmen für den NDB kategorisch ab.

Art. 25 Genehmigungsverfahren
Wie bei anderen Artikeln des vorliegenden Entwurfs entsteht auch hier der Eindruck, dass der Bundesrat mit etwas Kosmetik der allgemeinen Kritik am Staatsschutz entgegenwirken will.

Die vorgeschlagene Regelung widerspricht der Gewaltentrennung. Es ist nicht Aufgabe des Bundesrats, Entscheide von Gerichten zu prüfen und entweder als gut zu befinden oder aber zu verwerfen. Die Rechtsmittelinstanz des Bundesverwaltungsgerichts ist das Bundesgericht. Zudem erlässt der Bundesrat die Beobachtungsliste und wäre bei einer genehmigungspflichtigen Beschaffungsmassnahme gegenüber einer auf der Beobachtungsliste figurierenden Organisation oder Person in Personalunion Auftraggeber und Genehmigungsstelle. Auch besteht die grosse Gefahr, dass der Richter in der Annahme, dass der Bundesrat schon ordentlich prüfen werde, alle Gesuche bewilligt, und dass anschliessend der Bundesrat in der Annahme, ein Richter habe ja bereits alles gründlich geprüft, jedes Gesuch wohlwollend abnickt. Einen wirkungsvollen Schutz gegen

unverhältnismässige Bewilligungen von genehmigungspflichtigen Beschaffungsmassnahmen bietet diese Regelung auf jeden Fall nicht.

Generell sollte für vom NDB beantragte verdachtsunabhängige genehmigungspflichtige Informations-Beschaffungsmassnahmen eine höhere Hürde gelten als für vergleichbare Massnahmen nach der Strafprozessordnung: Auch Art. 197 Abs. 3 StPO verlangt für Zwangsmassnahmen, die in die Grundrechte nicht beschuldigter Personen eingreifen, dass sie besonders zurückhaltend eingesetzt werden. Denkbar und sinnvoll wäre eine Regelung analog zur richterlichen Triage von gesiegelten Dokumenten von Personen, welche einem Berufsgeheimnis unterstehen. Dem NDB dürften nur Daten ausgehändigt werden, welche einen Bezug zum im Gesuch zur genehmigungspflichtigen Beschaffungsmassnahme genannten Zweck haben.

Art. 29 Mitteilungspflicht
Mit der Möglichkeit, Mitteilungen aufzuschieben oder von ihnen abzusehen, wenn dies notwendig ist, um ein laufendes rechtliches Verfahren nicht zu gefährden, werden angeschuldigte Personen sämtlicher Verteidigungsrechte beraubt. Hier ist explizit zu legiferieren, dass Erkenntnisse aus genehmigungspflichtigen Beschaffungsmassnahmen einem absoluten strafrechtlichen Verwertungsverbot unterstehen, weil diese Erkenntnisse ohne jeden Anfangsverdacht erhoben wurden. Auch das deutsche Bundesverfassungsgericht in Karlsruhe hat in seinem Urteil vom 24. April 2013 betreffend die «Anti-Terror-Datei», welche mit den Datenbanken des NDB vergleichbar ist, erkannt, dass Polizei- und Geheimdienstdaten grundsätzlich zu trennen seien.

7. Abschnitt: Kabelaufklärung
Im erläuternden Bericht wird darauf hingewiesen, dass dieser Abschnitt einem Gesetz in Schweden nachgebildet ist. Wichtige Fragen diesbezüglich bleiben aber unbeantwortet, etwa wie Kabelaufklärung zu bewerkstelligen sei, was die Aufgaben und Kosten der privaten Anbieter sein könnten, wie viele Stellen innerhalb der Armee und innerhalb des NDB benötigt werden und was es bezüglich entstehender Kosten bedeutet. Bevor 5 Artikel auf knapp 2 Seiten zum Gesetz erhoben werden, muss vorher geklärt werden, was überhaupt möglich ist, was der Nutzen ist - etwa wenn Angaben über schweizerische natürliche oder juristische Personen als Suchbegriffe nicht zulässig sind -, welche personellen Ressourcen benötigt werden und was schliesslich die gesamten Kosten sind.

Aufgrund der zusätzlichen Kosten, welcher der Bundesrat den Anbietern von Fernmeldediensten im Zusammenhang mit der Revision des BÜPF, vor allem durch Beschaffung und Unterhalt von Infrastruktur, aber auch durch Personal, welches rund um die Uhr abrufbereit sein muss, aufbürden will, kann erahnt werden, dass mit der Kabelaufklärung nochmals enorme Kosten zusätzlich auf die Anbieter von Fernmeldediensten zukommen werden, die nur ungenügend abgegolten werden.

Zudem soll die Kabelaufklärung nicht nur Betreiberinnen von leitungsgebundenen Netzen (also diejenigen, welche Kabel ins Ausland besitzen) betreffen, sondern auch Anbieterinnen

von reinen Telekommunikationsdienstleistungen. Damit könnten - wie im US-Überwachungsprogramm Prism - auch Anbieterinnen von Cloud-Diensten (E-Mail, Foren, Chat-Räume, Online-Speicher, Office-Programme etc.) und Hosting-Provider zur Ausleitung von Daten gezwungen werden.

Wie bei der Funkaufklärung soll bei der Kabelaufklärung der Fernmeldeverkehr aller Teilnehmer aufgezeichnet und ausgewertet werden. Im Gegensatz zur Funkaufklärung, welche ausschliesslich Signalquellen im Ausland abdeckt, betrifft die Kabelaufklärung einerseits ausschliesslich schweizerische Fernmeldeanbieter, andererseits neben hier nicht interessierendem Transitverkehr auch ausschliesslich Sender oder Empfänger, welche sich in der Schweiz befinden. Das Fernmeldeverhalten einer Person in der Schweiz geniesst aber den uneingeschränkten Schutz des Fernmeldegeheimnisses, unabhängig davon, ob mit einer Gegenstelle in der Schweiz oder im Ausland kommuniziert wird. Das nachträgliche Herausfiltern von Inhalten, welche aus der Schweiz an einen Empfänger in der Schweiz gesandt wurden, ändert nichts daran. Auch aus diesem Grund ist die Kabelaufklärung abzulehnen.

4. Kapitel: Datenbearbeitung und Archivierung

Art. 39 Grundsätze

Der Grundsatz gemäss Art. 39 Abs. 3 NDG, wonach der NDB dieselben Daten in mehrere Informationssysteme überführen kann und mit der Überführung die Vorgaben des jeweiligen neuen Informationssystems gelten, ist unseriös. In der Grafik auf Seite 55 des Berichts wird lediglich abgebildet, nach welchem Muster neue Daten erfasst werden. Sind die Daten aber erst einmal im System, sind alle Grenzen aufgehoben und unterschiedlichste Daten, z. B. solche aus öffentlichen Quellen und solche aus genehmigungspflichtigen Massnahmen, sind plötzlich gleichwertig und können von jedermann eingesehen und weiterkopiert bzw. weitergeleitet werden. Auch Daten aus den geschützten Datenbehältern können in Produkte des NDB einfliessen und landen so noch vor der Erstellung eines Berichts im System IASA NDB, welches den heutigen Systemen ISIS und ISAS entspricht. Auf Daten in IASA NDB haben alle Mitarbeitenden des NDB direkt und alle anderen Zugriffsberechtigten via INDEX NDB Zugriff. Werden Daten, welche aus geschützten Datenbehältern ins IASA NDB kopiert wurden im Bericht verwendet, landen sie zusätzlich noch in GEVER NDB, wo alle Mitarbeiterinnen und Mitarbeiter des NDB im Abrufverfahren Zugriff haben. Mit dem Kopieren in ein anderes System ändern Informationen auch ihre Attribute, z. B. die Fristen für die periodischen Überprüfungen oder die maximale Aufbewahrungsdauer.

Ein derartiges «Data Management By Chaos» widerspricht einer eisernen Regel der Datenbank-Modellierung, wonach eine Information nur einmal im System resp. im Systemverbund abgelegt werden darf. Sobald ein und dieselbe Information mehrfach vorhanden ist, verändert sich diese Information aufgrund von Mutationen unterschiedlich, über kurz oder lang entsteht zwingend eine inkonsistente Datenbank. Auch kann dem Argument des Bundesrats, wonach *«in Abweichung zu den üblichen Datenschutzauflagen der NDB als unrichtig erkannte und entsprechend bewertete Daten aufbewahren dürfen*

muss», nicht gefolgt werden. Unrichtige Daten sind selbstverständlich umgehend zu löschen. Wenn es denn sein muss, können Erkenntnisse über Desinformation und Falschinformationen problemlos in einer neuen, nicht fehlerbehafteten Meldung erfasst werden.

Weiter ist anzumerken, dass Daten aus der Kabelaufklärung nicht in den Restdatenspeicher, sondern auch in geschützte Datenbehälter gehören, weil sie in der Schweiz unter Missachtung des Fernmeldegeheimnisses beschafft wurden.

Art. 40 Qualitätssicherung

Aufbauend auf die obenstehenden Anmerkungen zu Art. 39 kann festgehalten werden, dass sich eine Diskussion über Qualitätssicherung erübrigt, solange vom Design her eine inkonsistente Datenbank vorliegt. Wenn der Bundesrat im Bericht von *«differenzierter Regelung der Datenhaltung»* und *«einheitlich hoher Standard der Datenbearbeitungsqualität»* spricht und wenig später anmerkt, dass *«Daten oft für die Auftragserfüllung in ein anderes System überführt werden müssen»* und mit *«Die Daten können somit zwischen den Systemen kopiert werden und unterstehen den jeweiligen Vorgaben der verschiedenen Informationssysteme»* schliesst, hinterlässt das viele Fragezeichen. Eine effiziente Qualitätssicherung hat auf Gesetzesstufe so zu erfolgen, dass das nach wie vor gültige Motto des NDB «Quantität statt Qualität» durch rigorose Einschränkungen der Sammeltätigkeit verunmöglicht wird.

Art. 55 Weitergabe von Personendaten an inländische Behörden

Dieser Artikel widerspricht dem Trennungsprinzip der Daten von Nachrichtendiensten und Polizeibehörden. Daten aus genehmigungspflichtigen Beschaffungsmassnahmen unterliegen dem Verwertungsverbot von Art. 277 StPO, weil sie aus strafprozessual nicht genehmigten Überwachungen stammen. Da sie ohne Anfangsverdacht erhoben wurden, käme ihre Verwendung einer «Fishing Expedition» gleich, was mit der Rechtsprechung des EGMR (Urteil Klass) nicht vereinbar ist. Es besteht kein Raum für eine Zufallsfunde-Regelung analog zu Funden aus strafprozessualer Überwachung des Fernmeldeverkehrs.

Art. 56 Weitergabe von Personendaten an ausländische Behörden

Auch bei der Weitergabe von Personendaten an ausländische Behörden ist auf jeden Fall sicherzustellen, dass aus genehmigungspflichtigen Beschaffungsmassnahmen stammende Erkenntnisse einem absoluten Verwertungsverbot im Sinne von Art. 277 StPO unterstehen.

Art. 58 Auskunftsrecht

Das indirekte Auskunftsrecht, wie dies in BWIS vorgesehen war und wie dies auch in «BWIS II - reduziert» leider weitergeführt wurde, hat sich als untauglich und als reine Schikane erwiesen. Auskunft erhielt nur, wer mit viel Geduld und Geld den Rechtsweg beschritt. Der einzige Fall, den das Bundesgericht bisher beurteilt hat (BGE 1C_289/2009 vom 2. November 2011) begann am 11. August 2008 mit dem Schreiben des beauftragten Rechtsvertreters an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und endete via Bundesverwaltungsgericht mehr als 3 Jahre später mit der

Feststellung des Bundesgerichts, dass der EDÖB *«im Sinne der Erwägungen»* Auskunft zu erteilen habe. Aufgrund der zeitlichen und finanziellen Strapazen wird kaum jemand diesen Weg beschreiten, so dass heute faktisch kein Auskunftsrecht besteht.

Das Auskunftsrecht muss endlich entsprechend dem DSG gestaltet werden, so wie dies der Bundesrat in der Botschaft zu «BWIS II - reduziert» tatsächlich noch beantragt hatte. Nur so besteht eine minimale öffentliche Kontrolle über die geheimen Tätigkeiten des Nachrichtendienstes.

Bleibt es bei dem hier vorgeschlagenen Vorgehen, muss der NDB zumindest in jedem Fall dazu verpflichtet werden, der gesuchstellenden Person nach DSG Auskunft zu geben, sobald das Geheimhaltungsinteresse dahingefallen ist resp. nach Ablauf der Aufbewahrungsdauer. Die in Abs. 8 festgehaltene Einschränkung, dass dies nur gewährt wird, sofern es nicht mit übermässigem Aufwand verbunden ist, muss ersatzlos gestrichen werden.

Art. 61 Politische Steuerung durch den Bundesrat / Art. 63 Beobachtungsliste

Wenn der Bundesrat lediglich alle vier Jahre dem NDB einen geheim zu haltenden strategischen Grundauftrag erteilt, kann dies eigentlich nur bedeuten, dass der NDB in dieser Zeit praktisch nicht kontrolliert werden soll. Die in diesem Grundauftrag spezifizierten thematischen und regionalen Prioritäten müssen zwingend dem parlamentarischen Kontrollorgan (GPDel) unterbreitet werden. Nur so kann das Kontrollorgan tatsächlich sicherstellen, dass die ihm jährlich unterbreitete Beobachtungsliste nicht dem Grundauftrag widerspricht. Dasselbe gilt für die vom Bundesrat jährlich bestimmten Gruppierungen, die unter Beobachtung gestellt werden sollen. Auch diese Informationen müssen der GPDel - zusammen mit der Beobachtungsliste - unaufgefordert zugestellt werden. Nur so kann einigermassen gewährleistet werden, dass mit der Beobachtungsliste und der Bestimmung der Gruppierungen, die als gewaltextremistisch einzustufen sind, nicht erneut unsinnig viele, teils unsicherer oder gar falsche Daten gesammelt und verarbeitet werden. Ein weiteres Mittel, um dies zu verhindern, ist hier einzubauen: Die Beobachtungsliste und die Bestimmung der Gruppierungen, die als gewaltextremistisch einzustufen sind, sind einem Richtervorbehalt zu unterstellen, ebenso alle Aktivitäten des NDB, welche die Beschaffung und Bearbeitung von Informationen über die politische Betätigung und die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit betreffen.

Art. 64 Tätigkeitsverbot

Mit «BWIS II - reduziert» wurde dem Bundesrat bereits die Kompetenz erteilt, einer natürlichen Person, Organisation oder Gruppierung eine Tätigkeit zu verbieten, die die innere oder äussere Sicherheit konkret bedroht. Dieser unnötige und unverhältnismässige, präventive Eingriff in die demokratischen Freiheiten muss ersatzlos gestrichen werden. Je nach politischer Zusammensetzung des Bundesrates kann eine solche Bestimmung schnell missbraucht werden. Zudem zeigt sie reell kaum Wirkung, wie Beispiele aus anderen Ländern deutlich machen.

3.) Fazit

Das neue NDG erlaubt dem Staatsschutz ohne jeglichen Tatverdacht weitgehende strafprozessuale Zwangsmassnahmen einzusetzen. Die Erkenntnisse aus diesen Zwangsmassnahmen sollen als Beweise in Strafverfahren einfliessen. Die Datenhaltung mit der gewollten Redundanz von Daten und den unterschiedlichen Qualitätsanforderungen an die Erfassung der Daten bei gleichzeitiger totaler Durchlässigkeit der verschiedenen Datenbanken ist inakzeptabel. Die viel gepriesenen Qualitätskontrollen sind reine Kosmetik. Sie verhindern keine ausufernde Erfassung von nutzlosen Daten. Die Aushebelung des Verbots der Beschaffung und Bearbeitung von Informationen über die politische Betätigung und die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit, die besondere Auskunfts- und Meldepflicht von Amtsstellen, die zwingenden Auskunftspflichten Privater, das Sammeln von Informationen durch bezahlte Spitzel und Informanten, die Beobachtungsliste und das Verzeichnis der Gruppierungen, die alleine vom Bundesrat als gewaltextremistisch eingestuft werden, sind alles Massnahmen, die faktisch ein schrankenloses Sammeln von Daten auf Gesetzesstufe vorgeben. Das Auskunftsrecht hingegen bleibt ein reines Alibi. Es verhindert ein immer wieder einverlangtes unbürokratisches und mit vertretbarem Aufwand verbundenes Vorgehen, um das Grundrecht auf Einsicht in die Datensammlungen - hier diejenigen des NDB - wahrnehmen können.

Aus all diesen Gründen lehnt die Swiss Privacy Foundation das NDG in dieser Form ab.