Digitale Gesellschaft
Marktgasse 3
5620 Bremgarten AG

http://digitale-gesellschaft.ch
office@digitale-gesellschaft.ch

VBS
Nachrichtendienst des Bundes
Papiermühlestrasse 20
3003 Bern

28. Juni 2013

Vernehmlassungsantwort zum Nachrichtendienstgesetz (NDG)

Sehr geehrte Damen und Herren

Die *Digitale Gesellschaft* ist ein offener Zusammenschluss von einigen Dutzend netzpolitisch interessierten Gruppen und Einzelpersonen. Mehrheitlich sind wir Experten für technische, rechtliche und systemische Aspekte der gesellschaftlichen Entwicklungen im digitalen Zeitalter.

Im Rahmen der vorliegenden Vernehmlassung haben wir uns mit dem Vorschlag für eine neues Nachrichtendienstgesetz befasst.

Wir sind entsetzt: Statt dass der Gesetzesentwurf die in der heutigen Zeit erhöhten Notwendigkeiten eines sorgfältigen Schutzes von personenbezogenen Informationen umsetzen würde, droht im Fall der Annahme des Entwurfs das Gegenteil: Das unkontrollierte und unkontrollierbare Sammeln und Speichern von personenbezogenen Informationen würde weiter ausgeweitet. So würde das theoretisch von der Bundesverfassung (Artikel 13) und von internationalen Menschenrechtsabkommen geschützte Grundrecht auf Schutz der Privatsphäre, insbesondere auch im digitalen Kontext, weiter ausgehöhlt.

Im Zweckartikel ist völlig richtig der zentrale Punkt „zur Sicherung der demokratischen und rechtsstaatlichen Grundlagen der Schweiz beizutragen“ als Erstes erwähnt. **Damit ein Gesetz „zur Sicherung der demokratischen und rechtsstaatlichen Grundlagen“ beitragen kann, muss aber zuerst einmal sichergestellt werden, dass dieses Gesetz diese demokratischen und rechtsstaatlichen Grundlagen nicht selbst aushebelt!**

Insbesondere müssten folgende Prinzipien sichergestellt werden:

A) Nachgewiesene Verhältnismässigkeit: Da es sich bei jeder Form des staatlichen Beschaffens, Speicherns und Weitergebens von die Privatsphäre betreffenden personenbezogenen Informationen um einen Eingriff in ein Grundrecht handelt, muss die Notwendigkeit der jeweiligen Eingriffe für den Schutz der demokratischen Ordnung und die Verhältnismässigkeit der jeweiligen Regelungen jeweils nachgewiesen sein.

B) Menschenrechtsschutz auch betreffend dem Ausland: Menschenrechte wie das Recht auf Schutz der Privatsphäre gelten nicht nur jeweils innerhalb eines Landes, sondern für alle Menschen

überall. Folglich muss für Massnahmen, bei denen aufgrund der Schwere des Eingriffs in die Privatsphäre im Inland eine gerichtliche Bewilligung und die nachträgliche Information des Betroffenen gefordert sind, dasselbe auch im Hinblick auf das Ausland gelten. Es mag in diesem Zusammenhang nötig sein, eine internationale Institution zu schaffen, die es Betroffenen ermöglicht, ihre Datenschutzrechte international wahrzunehmen.

C) Schutz der freien Meinungsbildung: Es muss sichergestellt sein, dass Aktivitäten des demokratischen Meinungsbildungsprozesses (wozu auch gehört, dass man sich über extremistische Ansichten und die von diesen Ansichten ausgehenden Gefahren informieren können muss) nicht unter die Überwachung fallen.

D) Eingeschränkte Verwendung nachrichtendienstlicher Informationen: Es muss ganz allgemein sichergestellt werden, dass wenn die Beschaffung von Informationen durch die in Artikel 1 aufgeführten Ziele legitimiert wird, diese Informationen nicht (etwa nachdem sie an andere Behörden weitergegeben wurden) für andere Zwecke eingesetzt werden.

E) Respektierung der Schranken für Eingriffe in die Privatsphäre zwecks Strafverfolgung: Insbesondere muss sichergestellt sein, dass die vom Parlament für die Strafverfolgung gesetzten Grenzen betreffend der Mittel zur Informationsbeschaffung nicht auf dem Umweg über das NDG ausgehebelt werden.

F) Verhinderung von indirekten Sanktionen bei kritischer politischer Meinungsäusserung: Folgendes Szenario muss wirksam verhindert werden: Ein politisch interessierter Mensch äussert sich irgendwie kritisch über staatliche Aktivitäten. Daraufhin beschafft der NDB Informationen über ihn. Dabei findet der NDB Hinweise auf strafbare Handlungen durch ihn oder durch Familienmitglieder oder andere Personen in seinem Bekanntenkreis. Der NDB übergibt diese Hinweise der Polizei, die die strafbaren Handlungen daraufhin konsequent verfolgt. Über einen solchen Ablauf würde kritische politische Meinungsäusserung zu strafrechtlichen Sanktionen führen, auch wenn sich die Sanktionen formell nicht auf die politische Meinungsäusserung, sondern auf andere Tatbestände beziehen.

G) Schutz der Freiheit der politischen Meinungsäusserung: Es muss wirksam verhindert werden, dass auch nur die Besorgnis entstehen kann, dass politische Meinungsäusserung zu einem wie oben unter 'F' beschriebenen Ablauf führen kann.

H) Schutz der Menschenrechte von Asylsuchenden: Im Kontext von Menschen, die Asyl beantragt haben oder die solche Personen unterstützen, muss besonders sorgfältig sichergestellt werden, dass nicht Angst vor Informationsbeschaffung durch den NDB und allfälligen Auswirkungen auf die Asylverfahren dazu führt, dass grundlegende Freiheitsrechte nicht mehr voll wahrgenommen werden.

I) Datenschutz bei Auseinandersetzungen zwischen Firmen und Kritikern: Im Fall von politischen Auseinandersetzungen zwischen Kritikern und von ihnen kritisierten Firmen der Privatwirtschaft muss wirksam sichergestellt sein, dass vom NDB beschaffte Informationen über Kritiker nicht dazu missbraucht werden, die betroffenen Firmen in solchen Auseinandersetzungen zu unterstützen.

J) Überwachung nur bei Anhaltspunkten für den Verdacht einer Straftat: Ganz grundsätzlich dürfen 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, EuGRZ 1979 S. 278 ff.)

K) Fairness der Bewilligungsverfahren: Bei der gerichtlichen Bewilligung von Überwachungsmassnahmen ist sicherzustellen, dass nicht aufgrund von einseitig nur von der an der Überwachung interessierten Dienststelle gelieferten Informationen und Argumenten entschieden wird.

L) Recht auf Dateneinsicht und Korrektur: Grundsätzlich sind Menschen und Organisationen, über die der NDB längerfristig Informationen speichert, darüber zu informieren, und in die Lage zu versetzen, die über sie gespeicherten Informationen zu beurteilen und allenfalls zu korrigieren.

M) Recht auf Information über erfolgte Überwachungsmassnahmen: Menschen und Organisationen, die von Überwachungsmassnahmen betroffen sind, müssen innerhalb von wenigen Monaten darüber informiert werden.

N) Recht auf Information bei Weitergabe persönlicher Daten an das Ausland: Menschen und Organisationen, über die der NDB Informationen ans Ausland weitergibt, müssen darüber informiert werden.

O) Ausnahmen müssen selten sein: Falls es Ausnahmen von der Anwendung der Prinzipien 'M' und 'N' gibt, muss die Anzahl solcher Ausnahmen klein gehalten werden, und die Anzahl der betroffenen Menschen muss regelmässig publiziert werden.

P) Unabhängige Kontrolle und öffentliche Berichterstattung: Für jedes der obigen Prinzipien sind konkrete Massnahmen zur Sicherstellung der Einhaltung des Prinzips und ausserdem die Beobachtung durch eine unabhängige Kontrollinstanz und regelmässige Berichterstattung an die Öffentlichkeit nötig.

Q) Detaillierte Regeln: Als logische Konsequenz der Prinzipien 'A' und 'P' muss jeweils genau geregelt sein, welche Arten von Informationen wie beschafft und wie weiterverwendet werden dürfen.

R) Detaillierte öffentliche Information: Mit mindestens dem Detaillierungsgrad der Regelungen nach 'Q' ist die Öffentlichkeit über Art und Umfang der ergriffenen Massnahmen und der gespeicherten und der weitergegebenen Informationen zu informieren.

Diese Prinzipien sind im vorliegenden Entwurf nicht oder nur ungenügend umgesetzt.

Nach der Einschätzung des Sonderberichterstatters der Vereinten Nationen für das Recht auf Meinungsfreiheit und freie Meinungsäusserung verletzen Staaten ihre Verpflichtungen gemäss den internationalen Menschenrechtsabkommen, wenn der Schutz des Rechts auf freie Meinungsäusserung und das Recht auf Schutz der Privatsphäre bei den Rahmenbedingungen für staatliche Überwachungsmassnahmen nicht im Zentrum stehen: „States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny. In order to meet their human rights obligations, States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks." (Dokument A/HRC/23/40 vom 17. April 2013[1], Absätze 79-80.) Der Bericht des UN-Sonderberichterstatters ist in einer sehr sorgfältigen Sprache verfasst. Dabei sind Empfehlungen mit

1 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

„should“ ausgedrückt. Dass im letzten Satz des zitierten Textteils das stärkere Wort „must“ verwendet wird, drückt aus, dass es sich um eine zwingende Pflicht des Völkerrechts handelt.

Im Hinblick auf die einzelnen Artikel des Gesetzesentwurfs merken wir an:

1. Kapitel: Allgemeine Bestimmungen und Grundsätze der Informationsbeschaffung

zu **Art. 3 Grundsätze der Informationsbeschaffung**

• Minimierung des Eingriffs in die Grundrechte der betroffenen Personen

Im Gesetzesentwurf steht lapidar: „Er wählt jeweils die Beschaffungsmassnahme, die a. am besten geeignet und notwendig ist, um ein bestimmtes Beschaffungsziel zu erreichen; und b. gleichzeitig am wenigsten in die Grundrechte betroffener Personen eingreift. “ (Absatz 3). Offenbar kann hier im Einzelfall zwischen den beiden erwähnten Grundsätzen ein Konflikt bestehen. Es ist nicht akzeptabel, wenn der Gesetzestext so tut, als wäre das nicht der Fall. Darum ist es wichtig, eine unabhängige, direkt dem Parlament verantwortliche Stelle zu schaffen, die verbindliche Richtlinien zum Umgang mit dem Konflikt zwischen diesen beiden Grundsätzen schafft. Dabei ist insbesondere das eingangs erwähnte Prinzip 'A' (nachgewiesene Verhältnismässigkeit) umzusetzen.

Sonst wird es in der Anwendungspraxis so aussehen, dass in aller Regel die Massnahmen ergriffen werden, mit denen sich das Beschaffungsziel am bequemsten erreichen lässt, und Buchstabe b wäre in der Praxis weitgehend wirkungslos.

• Verbot der Beschaffung und Bearbeitung von Informationen über die politischen Aktivitäten

Die Erfahrung zeigt, dass es (auch wenn die Voraussetzungen für eine Ausnahme nicht erfüllt sind) dem NDB nicht einfach fällt, das Verbot der Beschaffung und Bearbeitung von Informationen über die politische Betätigung und die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit einzuhalten. Siehe auch die eingangs erwähnten Prinzipien 'F' (Verhinderung von indirekten Sanktionen bei kritischer politischer Meinungsäusserung), 'G' (Schutz der Freiheit der politischen Meinungsäusserung) und 'H' (Schutz der Menschenrechte von Asylsuchenden).

Es reicht darum nicht, dies im Grundsatz zu verbieten und dann ausnahmsweise doch wieder zu erlauben, wenn nicht gewährleistet ist, dass die Bewilligung solcher Ausnahmen objektiv und unabhängig, durch einen Richter, erfolgen muss. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung von Überwachungen anzustreben.

Darüber hinaus muss im Jahresbericht des NDB nachträglich dokumentiert werden, über welche Gruppierungen in Anwendung der Ausnahmeregelung Informationen über politische Tätigkeiten beschafft wurden. Auch die genaue Zahl der in diesem Zusammenhang überwachten Personen ist öffentlich zu machen.

• Löschungen von personenbezogen erhobenen Daten

Absatz 7: Das Prinzip der unverzüglichen Löschung von personenbezogen erhobenen Daten, die eigentlich gar nicht beschafft hätten werden sollen, ist selbstverständlich grundsätzlich richtig. Es fehlen hier aber die notwendigen flankierenden Massnahmen, die die darüber hinausgehenden Rechte der betroffenen Personen sicherstellen würden, etwa (a) im Hinblick auf Löschung von

allfälligen Kopien der Informationen in anderen Datenbanken, (b) im Hinblick auf das Korrigieren von an andere Behörden weitergegebenen fehlerhaften Informationen, und (c) im Hinblick auf das Recht, gerichtlich feststellen zu lassen, ob die Informationsbeschaffung widerrechtlich erfolgt ist. (Siehe das eingangs erwähnte Prinzip 'L': Recht auf Dateneinsicht und Korrektur.) Ausserdem fehlt die Erwähnung von wirksamen Mechanismen, um daraus zu lernen, dass eine Informationsbeschaffung erfolgt ist, die sich im Nachhinein als nicht gerechtfertigt erwiesen hat. Beim Prozess der Datenlöschung ist darauf zu achten, dass die für solche Lernprozesse relevanten Informationen in nicht-personenbezogener Form dokumentiert werden, bevor die zugrundeliegenden personenbezogenen Daten gelöscht werden.

2. Kapitel: Aufgaben und Zusammenarbeit des NDB

zu **Art. 4 Aufgaben des NDB**

• Bedrohungen von Informations- und Kommunikations-Infrastrukturen

Absatz 1, Buchstabe a, Punkt 5: Was genau ist gemeint mit „Bedrohungen der inneren und äusseren Sicherheit, die ausgehen von… Angriffen auf Informations-, Kommunikations-,… Infrastrukturen“?

Dies ist so unklar, dass es die Befürchtung nährt, dass es sich hier um einen „Gummiparagraphen“ handeln könnte, mit dem im Laufe der Zeit immer weitgehendere Eingriffe etwa zur Überwachung des Internet-Verkehrs zur Abwehr solcher „Bedrohungen“ gerechtfertigt würden. (Siehe das eingangs erwähnte Prinzip 'A': nachgewiesene Verhältnismässigkeit.)

• Schutz von Mitarbeitern und Infrastruktur ist Mittel zum Zweck, nicht Aufgabe des NDB

Absatz 7: Dieser Absatz ist hier fehl am Platz, der Schutz von Mitarbeitern und Infrastruktur des NDB ist doch nicht Teil vom Zweck des NDB. Sicher ist nicht beabsichtigt, es zu einer Aufgabe des NDB erklären, eigennützig für die eigenen Interessen zu schauen!
Dieser Absatz ist ausserdem redundant, da das Thema umfassend in Artikel 5 behandelt wird. Er sollte daher ersatzlos gestrichen werden.

zu **Art. 5 Schutz- und Sicherheitsmassnahmen**

• sollen ausschliesslich die Gewährleistung des gesetzlichen Auftrags des NDB bezwecken

Es fehlt hier eine Klarstellung, dass es sich ausschliesslich um Schutz- und Sicherheitsmassnahmen mit dem Ziel der Gewährleistung des gesetzlichen Auftrags des NDB geht.

Auf keinen Fall darf es bei Massnahmen zur Geheimhaltung darum gehen, die Art oder den Umfang von Aktivitäten des NDB vor der Bevölkerung zu verstecken.

Das Problem ist, dass der Artikel in der jetzigen Form zu einer Erschwerung oder Verhinderung des Aufdeckens und Korrigierens von Missständen innerhalb des NDB missbraucht werden kann. (Siehe das eingangs erwähnte Prinzip 'P': unabhängige Kontrolle und öffentliche Berichterstattung .)

zu **Art. 7 Kantonale Vollzugsbehörden**

• Auch in dringenden Fällen können Aufträge schriftlich formuliert werden

Absatz 2: Die Möglichkeit, Aufträge an kantonale Vollzugsbehörden in dringenden Fällen mündlich zu übermitteln, ist wohl ein Relikt aus der Zeit, als schriftlich formulierte Aufträge nur auf dem im

Vergleich zum Telefon viel langsameren Postweg übermittelt werden konnten. Mit den heutigen technischen Mitteln können die Aufträge ohne nennenswerte Verzögerung etwa mit verschlüsseltem Mail kommuniziert werden. Allenfalls kann telefonisch nachgedoppelt werden, um sicherzustellen, dass das verschlüsselte Mail unverzüglich geöffnet wird und dass sich die zuständige Amtsstelle des Auftrags sofort annimmt. Aber es gibt keinen Grund, die für die Ausführung des Auftrags bestimmenden Informationen und Anweisungen nicht schriftlich zu formulieren. Das dient der Sicherstellung der präzisen Ausführung des Auftrags und auch der Kontrollierbarkeit. (Siehe das eingangs erwähnte Prinzip 'P': unabhängige Kontrolle und öffentliche Berichterstattung.)

zu **Art. 10 Zusammenarbeit mit dem Ausland**

• Beteiligung an internationalen automatisierten Informationssystemen

Absatz 1(e) - Dieser Punkt über die „Beteiligung an internationalen automatisierten Informationssystemen “ muss unbedingt durch eine Referenz auf einen (noch hinzuzufügenden) Artikel ergänzt werden, der regelt

- wie der NDB sicherstellt, dass Daten, die er mittels solcher Informationssysteme international zur Verfügung stellt, auch von den Behörden anderer Länder nur im Einklang mit den schweizerischen gesetzlichen Regelungen (insbesondere im Hinblick auf die Abwägung zwischen Schutz der Privatsphäre und dem Schutz der Allgemeinheit vor schwerwiegenden Bedrohungen) genutzt werden (siehe die eingangs erwähnten Prinzipien 'A': nachgewiesene Verhältnismässigkeit , 'B': Menschenrechtsschutz auch betreffend dem Ausland und 'D': eingeschränkte Verwendung nachrichtendienstlicher Informationen),
- wie der NDB sicherstellt, dass der Erfolg der Umsetzung dieses Prinzips durch eine unabhängige Stelle kontrolliert werden kann (siehe das eingangs erwähnte Prinzip 'P': unabhängige Kontrolle und öffentliche Berichterstattung),
- wie es Betroffenen möglich ist, ihre Datenschutzrechte international wahrzunehmen (siehe das eingangs erwähnten Prinzipien 'B': Menschenrechtsschutz auch betreffend dem Ausland und 'L': Recht auf Dateneinsicht und Korrektur),
- dass die Information von Betroffenen über die Weitergabe von personenbezogen Daten an das Ausland (siehe das eingangs erwähnte Prinzip 'N': Recht auf Information bei Weitergabe persönlicher Daten an das Ausland) informiert werden,
- welche Arten von Daten in solche Informationssysteme eingespeist werden dürfen und was die genauen Voraussetzungen der Einspeisung von Mitteilungen und anderen Informationen in solche internationalen Informationssysteme sind (siehe das eingangs erwähnte Prinzip 'Q': detaillierte Regeln).

Ein solcher Artikel könnte sinnvoll etwa nach Artikel 56 des vorliegenden Entwurfs eingefügt werden.

3. Kapitel: Informationsbeschaffung

zu **Art. 13 Menschliche Quellen**

• Einsatz von bezahlten Spitzeln

Der Einsatz von bezahlten Spitzeln ist ein extrem schwerwiegender Eingriff. Es ist unbedingt notwendig, durch sorgfältige Regelungen (die im vorliegenden Gesetzesentwurf leider fehlen) sicherzustellen, dass

- diese Massnahme - wenn überhaupt - nur bei schwerwiegenden Bedrohungen eingesetzt wird (siehe das eingangs erwähnten Prinzip 'A': nachgewiesene Verhältnismässigkeit),
- der Erfolg der Umsetzung dieses Prinzips der Verhältnismässigkeit durch eine unabhängige

Stelle kontrolliert werden kann (siehe das eingangs erwähnte Prinzip 'P': Unabhängige Kontrolle und öffentliche Berichterstattung),
- die Öffentlichkeit über den Umfang der Einsatzes dieser Massnahme und die damit jeweils verfolgten Ziele informiert wird (siehe das eingangs erwähnte Prinzip 'R': Detaillierte öffentliche Information).

Aufgrund der Schwere dieses Eingriffs muss das Gesetz unbedingt eine richterliche Entscheidung als Voraussetzung für den Einsatz von Spitzeln vorschreiben. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung von Überwachungen anzustreben.

• Steuerbefreite verdeckte Zahlungen an Spitzel

Es fehlt eine klare Regelung, wer im Einzelfall entscheidet, ob „es für den Quellenschutz oder die weitere Informationsbeschaffung notwendig ist“, dass die Entschädigungen weder als steuerbares Einkommen noch als Einkommen im Sinne des AHV-Gesetzes gelten sollen. Solange dies nicht klar geregelt ist, werden in Verletzung des Prinzips der Rechtsstaatlichkeit praktisch alle solchen Einkünfte als nicht steuerbar und nicht AHV-pflichtig behandelt werden, auch wenn die im Gesetz dafür vorgesehene Voraussetzung nicht erfüllt ist.

Es ist daher vorzusehen, dass für die Gewährung der Steuer- und AHV-Befreiung vorgängig eine richterliche Entscheidung nötig sein muss.

zu **Art. 14 Ausschreibung von Personen und Fahrzeugen zwecks Aufenthaltsfeststellung**

Dies ist ein extrem schwerwiegender Eingriff in die Persönlichkeitsrechte der betroffenen Personen. Es ist unbedingt notwendig, durch sorgfältige Regelungen (die im vorliegenden Gesetzesentwurf leider fehlen) sicherzustellen, dass
- diese Massnahme - wenn überhaupt - nur bei schwerwiegenden Bedrohungen eingesetzt wird (siehe das eingangs erwähnten Prinzip 'A': nachgewiesene Verhältnismässigkeit),
- der Erfolg der Umsetzung dieses Prinzips der Verhältnismässigkeit durch eine unabhängige Stelle kontrolliert werden kann (siehe das eingangs erwähnte Prinzip 'P': unabhängige Kontrolle und öffentliche Berichterstattung),
- die Öffentlichkeit über den Umfang der Einsatzes dieser Massnahme und die damit jeweils verfolgten Ziele informiert wird (siehe das eingangs erwähnte Prinzip 'R': detaillierte öffentliche Information).

Aufgrund der Schwere dieses Eingriffs muss das Gesetz unbedingt eine richterliche Entscheidung als Voraussetzung für den Einsatz dieser Massnahme vorschreiben. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung von Überwachungen anzustreben.

zu **Art. 17 Auskunftspflicht bei einer konkreten Bedrohung**

• „Angriffe“ auf Informations- und Kommunikations-Infrastrukturen

Absatz 2, Buchstabe d: Analog zu den Ausführungen zu Artikel 4 erfordert der Begriff eines „Angriffs“ auf kritische Infrastrukturen eine präzise Definition, insbesondere wenn es um Informations- und Kommunikations-Infrastrukturen geht. Im Internet gibt es fortwährend sehr viele Versuche, auf alle möglichen Computersysteme (und damit auch solche der kritischen Infrastruktur)

unautorisiert zuzugreifen, mit dem Ziel der zweckentfremdeten unautorisierten Verwendung. Wenn solche Angriffe gelingen, können sie (häufig vom Angreifer unbeabsichtigt) sehr erheblichen Schaden verursachen. Bei angemessen gesicherten Computersystemen sind aber die allermeisten solcher Angriffe chancenlos und nicht der Rede wert.

Es ist also präzise zu regeln, wo genau die Schwelle eines „Angriffs“ ist, der diese Auskunftspflicht auslöst.

• zu weit gefasster Begriff „gewalttätiger Extremismus“

Absatz 2, Buchstabe e: Wahrheitsgemäss von „gewalttätigem Extremismus“ kann nur dann gesprochen werden, wenn tatsächlich Gewalttaten stattfinden. Wenn jemand zwar Gewalttaten befürwortet, aber aufgrund der Umstände dadurch das reale Stattfinden von Gewalttaten nicht gefördert wird, dann ist keine konkrete Bedrohung der inneren oder äusseren Sicherheit gegeben . Die Worte „verüben, fördern oder befürworten “ am Ende dieses Buchstabens sind daher durch „verüben oder fördern “ zu ersetzen.

• Pflicht zum Stillschweigen über Anfragen und Auskünfte

Absatz 3: Die allgemeine Pflicht zum Stillschweigen über Anfragen und Auskünfte ist unverhältnismässig. (Siehe das eingangs erwähnte Prinzip 'A': nachgewiesene Verhältnismässigkeit.) Wenn im Einzelfall eine Geheimhaltung solcher Anfragen und Auskünfte angebracht ist, dann aufgrund von Erfordernissen der konkreten Situation und nur für eine begrenzte Zeit. Aufgrund der Schwere des Eingriffs in das Öffentlichkeitsprinzip muss das Gesetz unbedingt eine richterliche Entscheidung als Voraussetzung für diese Schweigepflicht vorschreiben. Allenfalls könnte das Gesetz eine solche Pflicht zum Stillschweigen über Anfragen des NDB und diese betreffende Auskünfte vorsehen, die nach zwei Wochen automatisch erlischt, wenn nicht bis dann eine richterliche Entscheidung betreffend einer Verlängerung vorliegt.

zu **Art. 18 Besondere Auskunfts- und Meldepflicht**

• Auskunftspflicht von Behörden, die für den Betrieb von Informatiksystemen zuständig sind

Absatz 1, Buchstabe i: Es fehlt die Klarstellung, dass sich diese Auskunftspflicht nur auf den Aufgabenbereich des Betriebs der Informatiksysteme, nicht jedoch auf alle in den Informatiksystemen gespeicherten Informationen bezieht. Für die Bearbeitung von Auskunftsbegehren, die sich auf in den Informatiksystemen gespeicherte oder durch sie übermittelte Informationen beziehen, muss die jeweils inhaltlich zuständige Behörde verantwortlich sein. Dies muss auch im Gesetz ganz klar und unmissverständlich festgehalten sein, sonst ist die Gefahr der Verletzung dieses Prinzips der Rechtsstaatlichkeit gross und der schweizerische Staat ist nicht vertrauenswürdig. Siehe auch die eingangs erwähnte Prinzipien 'A': nachgewiesene Verhältnismässigkeit, 'G': Schutz der Freiheit der politischen Meinungsäusserung, 'H': Schutz der Menschenrechte von Asylsuchenden, 'P': Unabhängige Kontrolle und öffentliche Berichterstattung, 'Q': Detaillierte Regeln.

• Pflicht zum Stillschweigen über Anfragen und Auskünfte

Absatz 2: Die allgemeine Pflicht zum Stillschweigen über Anfragen und Auskünfte ist unverhältnismässig. (Siehe das eingangs erwähnte Prinzip 'A': nachgewiesene Verhältnismässigkeit.) Wenn im Einzelfall eine Geheimhaltung solcher Anfragen und Auskünfte angebracht ist, dann aufgrund von Erfordernissen der konkreten Situation und nur für eine begrenzte Zeit. Aufgrund der Schwere des Eingriffs in das Öffentlichkeitsprinzip muss das Gesetz unbedingt eine richterliche Entscheidung als Voraussetzung für diese Schweigepflicht vorschreiben. Allenfalls könnte das Gesetz eine solche

Pflicht zum Stillschweigen über Anfragen des NDB und diese betreffende Auskünfte vorsehen, die nach zwei Wochen automatisch erlischt, wenn nicht bis dann eine richterliche Entscheidung betreffend einer Verlängerung vorliegt.

• Nichtöffentliche Liste über unaufgefordert zu meldende Vorgänge und Feststellungen

Absatz 4: Die vorgesehene nichtöffentliche Liste verletzt das Öffentlichkeitsprinzip und die eingangs erwähnten Prinzipien 'A': nachgewiesene Verhältnismässigkeit , 'H': Schutz der Menschenrechte von Asylsuchenden, 'J': Überwachung nur bei Anhaltspunkten für den Verdacht einer Straftat, 'L': Recht auf Dateneinsicht und Korrektur, 'P': unabhängige Kontrolle und öffentliche Berichterstattung, 'R': detaillierte öffentliche Information.

Falls eine solche Liste notwendig ist, muss sie öffentlich gemacht werden.

zu **Art. 21 Besondere Auskunftspflichten Privater**

• Auskunftspflicht von Transportdienstleistern

Es sollte im Gesetzestext deutlicher gemacht werden, dass (gemäss den Ausführungen im „erläuternden Bericht“) hier in erster Linie an gewerbliche Personentransporte gedacht ist.

Dann muss eine richterliche Bewilligung klar zur Voraussetzung erklärt werden, damit solche Auskünfte eingeholt werden dürfen. Schliesslich stellen personenbezogenen Auskünfte im Bereich der Personenbeförderung einen sehr erheblichen Eingriff in die Privatsphäre dar. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung von Überwachungen anzustreben.

• unklare Definition von „Sicherheitsinfrastrukturen“

In der digitalen Welt gibt es überall Sicherheitsinfrastrukturen im weiteren Sinn, und praktisch alle Menschen und Firmen sind somit im weiteren Sinn Betreiber und Betreiberinnen von Sicherheitsinfrastrukturen. Das ist sicher hier nicht gemeint. Des Gesetzestext muss also durch eine präzise Umschreibung der gemeinten Kategorie von Sicherheitsinfrastrukturen ergänzt werden. Sonst ist das eingangs erwähnten Prinzip 'A' (nachgewiesene Verhältnismässigkeit) verletzt.

Beim jetzigen Stand der technischen Entwicklung ist (gemäss den Ausführungen im „erläuternden Bericht“) wohl nur an Einrichtungen der Zugangskontrolle und der Videoüberwachung gedacht. Das sollte dann auch genau so in den Gesetzestext geschrieben werden. Sonst handelt es sich (insbesondere da keine gerichtliche Bewilligungspflicht vorgesehen ist) um einen Gummiparagraphen, der die Vertrauenswürdigkeit des Schweizer Staats massiv untergraben würde.

• Sicherheitsinfrastrukturen im Bereich der Privatsphäre

Nach dem vorliegenden Entwurf hat der NDB, ohne auch nur eine Bewilligung einholen zu müssen, Zugriff auf auch alle Daten von Sicherheitsinfrastrukturen, die private Bereiche betreffen oder mit betreffen. Dies verletzt in eklatanter Weise die eingangs erwähnten Prinzipien 'A': nachgewiesene Verhältnismässigkeit, 'J': Überwachung nur bei Anhaltspunkten für den Verdacht einer Straftat, 'L': Recht auf Dateneinsicht und Korrektur, 'Q': Detaillierte Regeln.
Das Gesetz muss darum vorsehen, dass vor dem Einholen von Auskünften von Betreibern von Sicherheitsinfrastrukturen eine richterlicher Bewilligung eingeholte werden muss. Der Richter muss insbesondere beurteilen, ob die gewünschten Daten private Bereiche betreffen oder mit betreffen, und ob gegebenenfalls der Zugriff auf die Aufzeichnungen unter Auflagen zu gestatten oder gar nicht zu gestatten ist. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem

Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung von Überwachungen anzustreben.

Wenn es Personen gibt, die sicher oder mit einer erheblichen Wahrscheinlichkeit in ihrer Privatsphäre betroffen sind, müssen sie wenigstens nachträglich informiert werden.

• Video-Aufzeichnungen von legitimen politischen und religiösen Versammlungen

Nach dem vorliegenden Entwurf hat der NDB, ohne auch nur eine Bewilligung einholen zu müssen, Zugriff auf Überwachungs-Videos mit denen sich etwa mittels Gesichtserkennungs-Technologien viele der Teilnehmer etwa von politischen oder auch religiösen Versammlungen identifiziert werden könnten. Dies betrifft nicht nur bewusst öffentliche Veranstaltungen wie Demonstrationen, sondern auch nichtöffentliche Veranstaltungen, wenn die Teilnehmer auf dem Weg zu der Veranstaltung oder im Anschluss von einer Überwachungskamera erfasst werden. Dies verletzt in eklatanter Weise die eingangs erwähnten Prinzipien 'A': nachgewiesene Verhältnismässigkeit, 'C': Schutz der freien Meinungsbildung, 'F': Verhinderung von indirekten Sanktionen bei kritischer politischer Meinungsäusserung, 'G': Schutz der Freiheit der politischen Meinungsäusserung, 'H': Schutz der Menschenrechte von Asylsuchenden, 'J': Überwachung nur bei Anhaltspunkten für den Verdacht einer Straftat, 'Q': detaillierte Regeln.

Das Gesetz muss darum vorsehen, dass vor dem Einholen von Auskünften von Betreibern von Sicherheitsinfrastrukturen eine richterlicher Bewilligung eingeholt werden muss. Der Richter muss insbesondere beurteilen, ob die gewünschten Daten politische oder religiöse Veranstaltungen betreffen oder mit betreffen, und ob gegebenenfalls der Zugriff auf die Aufzeichnungen unter Auflagen zu gestatten oder gar nicht zu gestatten ist. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung von Überwachungen anzustreben.

Die Veranstaltern von betroffenen Veranstaltungen müssen wenigstens nachträglich informiert werden.

• Auskünfte nach BÜPF Art. 14

Absatz 2: Von der Möglichkeit für nicht genehmigungspflichtigen Beschaffungsmassnahmen sind die Auskünfte nach BÜPF Art. 14 Absatz 4 auszunehmen. Dort geht es um das Internet betreffende Auskünfte, die erlauben, zu einer über das Internet erfolgten Kommunikation die Person, die kommuniziert hat, zu identifizieren. Wenn ausserhalb vom Kontext einer konkreten, über das Internet verübten Straftat (das ist in BÜPF Art. 14 Absatz 4 die Voraussetzung) und ausserhalb von genehmigungspflichtigen Beschaffungsmassnahmen solche Auskünfte eingeholt werden können, untergräbt das die Möglichkeit, anonym über das Internet zu kommunizieren. Wie wichtig diese Möglichkeit der anonymen Kommunikation über das Internet ist, wird in dem bereits eingangs zitierten Bericht des UN-Sonderberichterstatters nachdrücklich betont: „The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization.“ (Absatz 25.) Auskünfte nach BÜPF Art. 14 Absatz 4, die aufgrund der gemäss BÜPF Art. 15 Abs. 3 gespeicherten Daten erfolgen, sind folglich als schwerwiegende Eingriffe die Grundrechte zu betrachten, die höchstens ausnahmsweise, im Rahmen von genehmigungspflichtigen Beschaffungsmassnahmen, erlaubt werden dürfen.

zu **Art. 22 Arten von genehmigungspflichtigen Beschaffungsmassnahmen**

Diese Massnahmen verletzen Grundprinzipien der Rechtsstaatlichkeit in eklatantester Weise, insbesondere auch, weil die Massnahmen nicht auf Personen eingeschränkt ist, für die ein dringender Tatverdacht betreffend einer Straftat besteht.

• Beträchtliche Erweiterungen der erlaubten Massnahmen

Absatz 1: Hier werden gegenüber der bisherigen Rechtslage erhebliche zusätzliche Formen von Eingriffen in die Privatsphäre erlaubt, insbesondere:

- der Zugriff auf die Vorratsdaten (Buchstabe c)
- der Einsatz von IMSI-Catchern u.ä. (Buchstabe e)
- der Einsatz von Überwachungsgeräten (Buchstabe f)
- die Verwendung von Trojanern (noch über die Möglichkeiten der Strafverfolgungsbehörden gemäss E-BÜPF hinaus) (Buchstabe g. 1)
- Cyberwar-Massnahmen (Buchstabe g. 2)

In dem bereits eingangs zitierten Bericht des UN-Sonderberichterstatters führt dieser detailliert die Bedingungen aus, unter denen seiner Einschätzung nach Eingriffe in das Grundrecht auf Achtung der Privatsphäre unter den internationalen Menschenrechtsabkommen nur erlaubt sind: „In this regard, the Special Rapporteur takes the position that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, as elucidated in General Comment 27.15. The test as expressed in the comment includes, inter alia, the following elements:
(a) Any restrictions must be provided by the law (paras. 11-12);
(b) The essence of a human right is not subject to restrictions (para. 13);
(c) Restrictions must be necessary in a democratic society (para. 11);
(d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);
(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim (para. 14);
(f) Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected (paras. 14-15). ” (Absatz 29)

Konkret im Hinblick auf die hier vorgeschlagene Ausweitung der Einschränkungen des Rechts auf Wahrung der Privatsphäre sind die Punkte (c) und (e) relevant: Solange die vorgeschlagenen Eingriffe nicht strikt notwendig sind, damit die demokratischen Ordnung der Schweiz erhalten werden kann, muss die vorgeschlagene Ausweitung der Massnahmen schon aus Menschenrechtsgründen abgelehnt werden.

• Notwendigkeit, die Betroffenen detailliert zu informieren

Falls aber solche Massnahmen doch wirklich notwendig sind, müssen die betroffenen Personen wenigstens im Nachhinein nicht nur informiert werden, dass eine Überwachung stattgefunden hat (wie in Artikel 29 vorgesehen), sondern auch über die konkreten Massnahmen informiert werden. Die Betroffenen müssen die Möglichkeit haben, wenigstens im Nachhinein die Angemessenheit der Massnahmen in einem Gerichtsverfahren zu bestreiten. In dem Fall, dass sich solche Massnahmen des NDB als nicht gerechtfertigt herausstellen, ist den betroffenen Personen eine Entschädigung zuzusprechen. Falls durch das Eindringen in Räumlichkeiten oder in Computersysteme ein Sachschaden entsteht, müssen die Betroffenen Anspruch auf Schadensersatz haben.

Siehe auch die eingangs erwähnten Prinzipien 'A': nachgewiesene Verhältnismässigkeit,

'E': Respektierung der Schranken für Eingriffe in die Privatsphäre zwecks Strafverfolgung, 'J': Überwachung nur bei Anhaltspunkten für den Verdacht einer Straftat, 'K': Fairness der Bewilligungsverfahren, 'L': Recht auf Dateneinsicht und Korrektur, 'M': Recht auf Information über erfolgte Überwachungsmassnahmen.

zu **Art. 25 Genehmigungsverfahren**

• Vertretung der Interessen der in ihren Grundrechten betroffenen Personen

Es fehlt die Sicherstellung einer wirksamen Vertretung des Interesses am Schutz der Privatsphäre. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem Bundesverwaltungsgericht nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung von Überwachungen anzustreben.

• Statistiken über die Genehmigungsverfahren

Im Anbetracht von Berichten aus dem Ausland (z.B. USA[2], Deutschland[3]), wo über längere Zeit Bewilligungen für Überwachungsmassnahmen in praktisch jedem Fall erteilt worden sind (offensichtlich ohne echte Prüfung), ist es wichtig, Statistiken über die gerichtliche Prüfung zu veröffentlichen, die mindestens folgendes dokumentieren:

- die Anzahl der gestellten Anträge für bewilligungspflichtige Beschaffungsmassnahmen
- wie viele der Anträge vollständig bewilligt wurden
- wie viele der Anträge teilweise bewilligt wurden
- wie viele der Anträge gar nicht bewilligt wurden
- wie viele der Anträge zurückgezogen wurden
- wie lange sich die Richter durchschnittlich mit den einzelnen Anträgen befasst haben (Hier geht es nicht um die Zeit zwischen der Einreichung des Antrags und der Beantwortung, sondern um die Anzahl der auf die Feststellung und Beurteilung des Sachverhalts verwendeten Arbeitsstunden.)

zu **Art. 29 Mitteilungspflicht**

Es gibt in diesem Entwurf betreffend der Mitteilungspflicht so viele Ausnahmen, dass der Sinn des Artikels damit fast völlig ausgehöhlt ist.

Nur Nicht-Erreichbarkeit der betroffenen Personen und Notwendigkeit weiterer, aktuell laufender Überwachungsmassnahmen (die durch die Mitteilung gefährdet wären) sind legitime Gründe für einen Aufschub der Mitteilung.

Es ist sehr beunruhigend, dass „ein laufendes rechtliches Verfahren nicht zu gefährden“ überhaupt als Grund für Ausnahme von der Mitteilungspflicht vorgeschlagen worden ist. Was kann denn im Zusammenhang von „laufenden rechtlichen Verfahren“ (wohl strafrechtlicher Art) der Grund sein, berechtigte Überwachungsmassnahmen seitens des NDB zu verschweigen? Die Verfahren sind durch eine Mitteilung doch nur gefährdet, wenn sie sich auf Erkenntnisse abstützen, die ausserhalb der rechtsstaatlichen Grenzen für Ermittlungen in Strafverfahren gewonnen wurden!

Siehe auch die eingangs erwähnten Prinzipien 'A': nachgewiesene Verhältnismässigkeit, 'D': Schutz der freien Meinungsbildung, 'E': Respektierung der Schranken für Eingriffe in die Privatsphäre zwecks Strafverfolgung, 'J': Überwachung nur bei Anhaltspunkten für den Verdacht einer Straftat, 'L': Recht auf Dateneinsicht und Korrektur, 'M': Recht auf Information über erfolgte Überwachungsmassnahmen .

2 http://en.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court
3 http://gutjahr.biz/2013/04/bestandsdatenauskunft/

zu **Art. 32 Allgemeine Bestimmungen (über die Beschaffung von Informationen über Vorgänge im Ausland)**

• Schutz der Grundrechte von Personen ausserhalb der Schweiz

Im „erläuternden Bericht“ ist lapidar vermerkt: „Im Spannungsfeld zwischen den Sicherheitsinteressen der Schweiz und dem Schutz der Grundrechte ausländischer Staatsangehöriger, bzw. von Personen im Ausland, überwiegt nach dem Konzept dieser Vorlage grundsätzlich das Sicherheitsinteresse. Der Grundrechtsschutz von Personen im Ausland soll gegenüber demjenigen von Personen im Inland weniger umfassend berücksichtigt werden. “ Das ist in dieser Form nicht akzeptabel. Die Gültigkeit der Menschenrechte endet doch nicht an den Grenzen der Schweiz! (Siehe das eingangs erwähnte Prinzip 'B': Menschenrechtsschutz auch betreffend dem Ausland.) Zwar sind die Argumente zutreffend, dass der Grundrechtsschutz im Zusammenhang von Auslandseinsätzen schwieriger ist als im Zusammenhang mit der Informationsbeschaffung im Inland. Aber die erhöhte Schwierigkeit darf nicht verringerte Bemühung zur Folge haben! Falls vorgängige Prüfung zwecks Bewilligung durch einen Richter nicht möglich ist, so muss die Informationsbeschaffung wenigstens im Nachhinein durch einen Richter beurteilt werden. Dabei ist dem Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung von Grundrechtseingriffen im Ausland anzustreben. Der NDB ist zu verpflichten, aus allfälligen Rügen des Richters angemessene Konsequenzen zu ziehen, und die Aufsichtsorgane sind ausdrücklich zu verpflichten, dies zu kontrollieren.

• Cyberwar

Zu Massnahmen, die im Ausland als elektronische Kriegsführung (Cyberwar) interpretiert werden können, darf der NDB wegen der Gefahr einer unkontrollierbaren Eskalation auf keinen Fall ermächtigt werden!

Darum ist klar festzuhalten, dass der NDB auf keinen Fall Angriffe (Massnahmen nach Artikel 22 Absatz 1 Buchstabe g sind Angriffe!) auf Computersysteme und Computernetzwerke im Ausland durchführen darf. (Der zweite Satz von Artikel 32 Absatz 2 wird damit hinfällig.)

zu **Art. 34-38 Kabelaufklärung**

• Schutz der Grundrechte von Personen ausserhalb der Schweiz

Es fehlen konkrete Regelungen zum Schutz der Grundrechte von Personen ausserhalb der Schweiz. (Siehe das eingangs erwähnte Prinzip 'B': Menschenrechtsschutz auch betreffend dem Ausland.) Die Regelung von Artikel 32 Absatz 3 ist völlig ungenügend, sie verwirklicht weder das Prinzip der Gewaltentrennung noch werden den betroffenen Personen irgendwelche Möglichkeiten eingeräumt, ihre Rechte zu verteidigen.

In Anbetracht dessen, dass nicht klar ist, ob die „Kabelaufklärung“ überhaupt irgend einen wesentlichen Nutzen erzielen kann (dafür müssen ja wesentliche dafür relevante internationale Datenströme in unverschlüsselter Form durch die Schweiz fliessen) und zumal für das Problem der Verletzung der Grundrechte von Personen ausserhalb der Schweiz laut dem „erläuternden Bericht“ keine Lösung möglich ist, ist die „Kabelaufklärung“ aus Gründen der Verhältnismässigkeit (siehe das eingangs erwähnte Prinzip 'A': nachgewiesene Verhältnismässigkeit) grundsätzlich abzulehnen.

Dazu kommt im Kontext des PRISM-Skandals, dass es dem Ansehen der Schweiz im Ausland schadet, wenn die Schweiz dasselbe tut oder auch nur versucht.

• Schutz der Grundrechte von Personen in der Schweiz

Im Fall der Anwendung von Art. 37(3) können die an den NDB gelieferten Daten auch personenbezogene Informationen über Personen in der Schweiz enthalten. Diesem Absatz wäre daher eine klare Bestimmung hinzuzufügen, dass die betroffenen Personen informiert werden müssen, falls der NBD diese Daten in personenbezogener Weise auswertet.

• Information der Bevölkerung

Es fehlen Regelungen zur Information der Bevölkerung über den Umfang von derartigen ergriffenen Massnahmen. Siehe das eingangs erwähnte Prinzip 'R': detaillierte öffentliche Information .

• unabhängige Kontrollinstanz

Es fehlt eine unabhängige Kontrollinstanz analog zu der unabhängige Kontrollinstanz für die Funkaufklärung gemäss Art. 67

4. Kapitel: Datenbearbeitung und Archivierung

zu **Art. 39, 40, 42-52 Grundsätze, Qualitätssicherung, Informatiksysteme**

Die Vielzahl der Informatiksysteme und die resultierenden Duplizierungen von Informationen machen eine effektive Qualitätssicherung (einschliesslich die Wahrnehmung des Rechts der Betroffenen auf Auskunft über die Datenspeicherung und die Korrektur von falschen Informationen) unmöglich. Bei der vorgeschlagenen Architektur mit der Vielzahl von Informatiksystemen ist es geradezu vorprogrammiert, dass es zu einem Wildwuchs von nicht immer konsistenten Daten kommt, die allzu häufig den gesetzlich geforderten Zeitpunkt der Löschung überdauern. Diese Einschätzung entspricht der tatsächlich beobachteten Situation, wie sie in einem Teilbereich von der Geschäftsprüfungsdelegation des Parlaments beschrieben wird: http://www.parlament.ch/d/organe-mitglieder/delegationen/geschaeftspruefungsdelegation/isis-inspektion/Documents/nachkontrolle-isi-gpdel-2012-d.pdf

Der einzige Weg zu einer echten Lösung dieser Probleme ist wohl, von vornherein die Menge der Daten, die beschafft werden, im Vergleich zu dem heute Üblichen massiv einzuschränken und dann eine zentrale Stelle zur Datenpflege einzuführen. Daten, die für mehrere der im Gesetzesentwurf erwähnten Informatiksysteme relevant sind, sind in ein zentrales Informationssystem zu überführen, wo sie zentral gepflegt werden können. Die anwendungsgebiets-spezifischen Datensammlungen sollen nicht Kopien dieser Daten enthalten, sondern Referenzen auf den jeweiligen Eintrag im zentralen Informationssystem. (Das ist so zu implementieren, dass jeder, der Zugang zu mindestens einer der anwendungsgebiets-spezifischen Datensammlungen hat, damit automatisch auch Zugang zu den in abgerufenen Datensätzen referenzierten Einträgen im zentralen Informationssystem erhält). Diese zentrale Stelle für Datenpflege (und nicht die für Informationsbeschaffung verantwortlichen Dienststelle) sollte auch für die gesetzeskonforme Löschung von Daten und für den Kontakt zur Bevölkerung betreffend Ausübung der Datenschutzrechte verantwortlich sein.

Eine solche zentrale Stelle für Datenpflege ersetzt nicht die Art. 40 vorgesehene Qualitätssicherungsstelle. Jedoch sollte die Qualitätssicherungsstelle unter anderem die Qualität der Prozesse zur Datenpflege (einschliesslich Löschung von Daten) überwachen. Daraus folgt, dass die Qualitätssicherungsstelle für diese Prozesse nicht selber verantwortlich sein sollte.

zu **Art. 54 Überprüfung vor der Weitergabe**

Es fehlt jeglicher Hinweis darauf, wie das unzweifelhaft aus rechtsstaatlichen Grundsätzen wichtige Ziel „Der NDB stellt vor jeder Weitergabe von Personendaten oder Produkten sicher, dass die Personendaten den rechtlichen Vorgaben nach diesem Gesetz genügen und ihre Weitergabe rechtlich vorgesehen und im konkreten Fall notwendig ist“ realisiert werden soll. So ist zu befürchten, dass dies weitgehend ein frommer Wunsch bleiben könnte bzw. eigentlich ein Etikettenschwindel. Es fällt jedenfalls auf, dass weder das Sicherstellen dieses wichtigen Grundprinzips noch eine auch nur stichprobenhafte Kontrolle, dass das Prinzip eingehalten wird, zu den in Art. 40 aufgelisteten Aufgaben der „internen Qualitätssicherungsstelle“ gehört.

zu **Art. 55 Weitergabe von Personendaten an inländische Behörden**

• Einschränkung der Weitergabe an inländische Behörden

Es fehlen geeignete Regelungen zum Schutz der eingangs erwähnten Prinzipien 'A': Nachgewiesene Verhältnismässigkeit, 'C': Schutz der freien Meinungsbildung, 'D': eingeschränkte Verwendung nachrichtendienstlicher Informationen, 'E': Respektierung der Schranken für Eingriffe in die Privatsphäre zwecks Strafverfolgung, 'F': Verhinderung von indirekten Sanktionen bei kritischer politischer Meinungsäusserung, 'G': Schutz der Freiheit der politischen Meinungsäusserung, 'H': Schutz der Menschenrechte von Asylsuchenden, 'J': Überwachung nur bei Anhaltspunkten für den Verdacht einer Straftat .

Im NDG muss klar festgehalten werden, dass die Weitergabe von nachrichtendienstlich gewonnen Informationen nur statthaft ist, wenn damit das Verhindern von unmittelbar bestehenden Bedrohungen der inneren und äusseren Sicherheit gemäss Art. 4(1)a bezweckt wird.

In jedem anderen Kontext ist die Verwendung von nachrichtendienstlich gewonnen Informationen etwa zur Strafverfolgung als Menschenrechtsverletzung zu betrachten, wie in der Darlegung der Prinzipien am Anfang dieser Vernehmlassungsantwort deutlich gemacht wurde.

• Verhinderung einer indirekten Weitergabe an Privatfirmen

Wenn nachrichtendienstlich gewonnene Informationen etwa an andere Behörden weitergegeben werden, muss sichergestellt sein, dass diese die Informationen auf keinen Fall an Privatfirmen weitergeben. (Siehe das eingangs erwähnte Prinzip 'I': Datenschutz bei Auseinandersetzungen zwischen Firmen und Kritikern.)

zu **Art. 56 Weitergabe von Personendaten an ausländische Behörden**

• Beachtung der grundlegenden Prinzipien bei der Weitergabe von Personendaten

Dieser Artikel muss unbedingt durch eine Referenz auf einen (noch hinzuzufügenden) Artikel ergänzt werden, der regelt

- wie der NDB sicherstellt, dass Daten, die er ausländischen Behörden zur Verfügung stellt, auch von den Behörden anderer Länder nur im Einklang mit den schweizerischen gesetzlichen Regelungen (insbesondere im Hinblick auf die Abwägung zwischen Schutz der Privatsphäre und dem Schutz der Allgemeinheit vor schwerwiegenden Bedrohungen) genutzt werden (siehe die eingangs erwähnten Prinzipien 'A': nachgewiesene Verhältnismässigkeit, 'B': Menschenrechtsschutz auch betreffend dem Ausland und 'D': Eingeschränkte Verwendung nachrichtendienstlicher Informationen),
- wie der NDB sicherstellt, dass der Erfolg der Umsetzung dieses Prinzips durch eine unabhängige Stelle kontrolliert werden kann (siehe das eingangs erwähnte Prinzip 'P': unabhängige Kontrolle und öffentliche Berichterstattung),

- wie es Betroffenen möglich ist, ihre Datenschutzrechte international wahrzunehmen (siehe das eingangs erwähnten Prinzipien 'B': Menschenrechtsschutz auch betreffend dem Ausland und 'L': Recht auf Dateneinsicht und Korrektur),
- dass die Information von Betroffenen über die Weitergabe von personenbezogen Daten an das Ausland informiert werden (siehe das eingangs erwähnte Prinzip 'N': Recht auf Information bei Weitergabe persönlicher Daten an das Ausland),
- welche Arten von Daten in internationale Informationssysteme eingespeist werden dürfen und was die genauen Voraussetzungen der Einspeisung von Mitteilungen und anderen Informationen in solche internationalen Informationssysteme sind (siehe das eingangs erwähnte Prinzip 'Q': detaillierte Regeln).

• Keine nachrichtendienstliche Informationsbeschaffung für gewöhnliche Strafverfolgung

Auch bei der Weitergabe von Personendaten an ausländische Behörden muss auf jeden Fall sichergestellt werden, dass aus genehmigungspflichtigen Beschaffungsmassnahmen stammende Erkenntnisse nur zur Abwehr von bestehenden Bedrohungen der inneren und äusseren Sicherheit gemäss Art. 4(1)a genutzt werden. An Länder, die dies nicht gewährleisten, dürfen gar keine aus genehmigungspflichtigen Beschaffungsmassnahmen im Sinne des NDG stammenden Erkenntnisse weitergegeben werden.

Für allgemeine Kriminalitätsbekämpfung gibt es internationale polizeiliche Zusammenarbeit. Die Schweiz darf nicht Hand dazu leisten, mittels nachrichtendienstlich gewonnenen Erkenntnissen die Rechtsstaatlichkeit in anderen Ländern auszuhebeln. Siehe das eingangs erwähnten Prinzip 'B': Menschenrechtsschutz auch betreffend dem Ausland.

Absatz 2 Buchstabe a ist folglich ersatzlos zu streichen.

Der Text vom jetzigen Buchstaben e in Absatz 2 ist dahingehend zu ergänzen, dass es bei den „erheblichen Sicherheitsinteressen“ nur um die Abwehr von Bedrohungen der inneren und äusseren Sicherheit gemäss Art. 4(1)a gehen darf.

• Schutz der Rechte des Betroffenen bei Anfragen an ausländische Behörden

Der Text von jetzigen Buchstaben b in Absatz 2 ist dahingehend zu ergänzen, dass eine solche Informationsübermittlung, wenn sie nicht zweifelsfrei im Interesse des Betroffenen ist, vorgängig durch einen Richter bewilligt worden sein muss. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung der Informationsweitergabe an das Ausland anzustreben.

zu **Art. 57 Weitergabe von Personendaten an Dritte**

• Schutz der Rechte des Betroffenen bei Anfragen an Privatfirmen

Der Text von jetzigen Buchstaben b in Absatz 2 ist dahingehend zu ergänzen, dass eine jegliche Informationsübermittlung, die über Name und Adresse und Adressierungselemente der Telekommuniation wie Telefon-Nummer, Email-Adresse, IP-Nummer hinausgeht, vorgängig durch einen Richter bewilligt worden sein muss, wenn sie nicht zweifelsfrei im Interesse des Betroffenen ist. Aufgrund des Prinzips 'K' (Fairness der Bewilligungsverfahren) ist dem Richter nicht nur der Antrag des NDB, sondern auch eine Replik vorzulegen, die von einer unabhängigen Amtsperson verfasst wurde, deren Aufgabe es ist, die Minimierung der Informationsweitergabe an Privatfirmen anzustreben.

zu **Art. 58 Auskunftsrecht**

Das Auskunftsverfahren muss unbedingt wesentlich vereinfacht und bürgerfreundlich gestaltet werden. Insbesondere ist es nicht angebracht, eine Empfehlung des EDÖB zur Voraussetzung zu erklären, damit überhaupt eine rasche Auskunft erteilt wird. Auskunftsbegehren sind immer sofort und umfassend zu beantworten, wenn dies die innere und äussere Sicherheit nicht gefährdet. Wenn eine solche Auskunft verweigert wird, muss es möglich sein, den EDÖB als eine bisher noch nicht in das Verfahren involvierte, unabhängige Instanz anzurufen.

6. Kapitel: Politische Steuerung, Kontrolle sowie Rechtsschutz

zu **Art. 61 Politische Steuerung durch den Bundesrat**

• Beobachtungsliste

Absatz 1: Die Beobachtungsliste muss öffentlich sein. Nur so ist eine effektive öffentliche Kontrolle von diesem gravierenden Eingriff in die Grundrechte erreichbar.

• völkerrechtliche Verträge

Absatz 3: Völkerrechtliche Verträge, die eine Beteiligung an internationalen Informationssystemen für personenbezogene Daten vorsehen, greifen in Grundrechte ein. Solche völkerrechtlichen Verträge dürfen darum nicht der alleinigen Kompetenz des Bundesrats unterstellt werden.

Fazit: Im vorliegenden Gesetzesentwurf ist der Schutz der Grundrechte völlig ungenügend und muss unbedingt systematisch verbessert werden!

Mit freundlichen Grüssen

N. Bollow

Norbert Bollow
für die *Digitale Gesellschaft*