DJS JDS GDS

Demokratische Juristinnen und Juristen der Schweiz
Juristes Démocrates de Suisse
Giuristi e Giuriste Democratici Svizzeri
Giuristas e Giurists Democratics Svizzers

Schwanengasse 9
3011 Bern
Tel 078 617 87 17
info@djs-jds.ch

Stellungnahme zum Entwurf eines Nachrichtendienstgesetzes, 14.022

(NDG, Entwurf 1, BBl 2014 2237)

z. H. Ständerat (Beratung vom 11.06.2015)

I. Vorbemerkung

In dieser Sommersession wird der Ständerat als Zweitrat den Entwurf eines Nachrichtendienstgesetzes behandeln. Nachdem der Nationalrat den Entwurf – u.E. in grober Verkennung seiner Tragweite für den demokratischen Rechtsstaat – ohne nennenswerte Korrekturen durchgewinkt hat, liegt es nun am Ständerat, die Vorlage mit Bedachtheit und dem erforderlichen Verantwortungsbewusstsein staatspolitisch zu würdigen.

II. Allgemeine Bemerkungen zum Vorhaben

Das Attentat auf Charlie Hebdo hat gezeigt, wie leicht eine freiheitliche Gesellschaftsordnung angreifbar ist. Der Terror hat Europa ins Herz getroffen, die Reaktionen erinnern daran, welch hohen Stellenwert der Meinungsäusserungsfreiheit als Grundpfeiler des Rechtsstaates auch heute noch zugemessen wird. Die Ereignisse zeigen aber auch, dass eine **freiheitliche Gesellschaft** niemals ganz gefeit

ist vor Anschlägen, dass absolute Sicherheit nur zum Preis der Freiheit zu haben ist. Und selbst eine verstärkte Überwachung schützt nicht vor Terror, waren doch die beiden Täter im Schengen-Raum zur verdeckten Beobachtung ausgeschrieben und im Informationssystem der Schengen-Staaten erfasst gewesen (NZZ, 9.1.2015). Bevor nun überhastet nachrichtendienstliche Kompetenzen zum Preis dieser freiheitlichen Grundordnung ausgebaut werden, lohnt es sich deren Nutzen abzuwägen gegen das Misstrauen, das gesät wird und so das rechtsstaatliche Fundament unterwandert.

Gemäss Angaben in der BOTSCHAFT, soll der Entwurf zu einem neuen Nachrichtendienstgesetz «***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 trägt und die veränderten Risiken und Bedrohungen besser berücksichtigt*.» (BOTSCHAFT NDG, BBl 2014, 2106, H.v.Verf.).

Schon eine kursorische Betrachtung des Entwurfs zeigt allerdings, dass das Gegenteil der Fall ist: Mit dem Entwurf werden ganz einseitig die **Kompetenzen des NDB insb. im Bereich der Überwachungsmassnahmen und des Datensammelns massiv ausgebaut**, während der Schutz der Privatsphäre weiter ausgehöhlt wird. Die Erfahrung zeigt zudem, dass ein anfängliches Versprechen von Zurückhaltung im Sicherheitsdiskurs schnell vergessen ist und einer massenhaften, nicht überschaubaren Durchleuchtung zu weichen droht.

Diese Stossrichtung ist darum problematisch, weil sie das wechselseitige **Vertrauen** als Fundament eines liberalen und transparenten Rechtsstaates ersetzt durch etatistische, undurchsichtige und internationalisierte Überwachung, sodass der Staat selbst zunehmend autoritäre Züge anzunehmen droht. Wo das Paradigma der Sicherheit dasjenige der Freiheit verdrängt, verblassen auch juristische Garantien, wie sie in die Bundesverfassung und internationalen Verträge festgeschrieben sind. Doch es bleibt nicht beim eklatanten Einschnitt in die klassischen **Grund- und Menschenrechte**. Hinzu tritt, dass die – zur Prävention – gewonnen Erkenntnisse direkt ins Strafverfahren einfliessen können sollen: Präventiv sollen sehr weitgehende – über die strafprozessualen Zwangsmassnahmen hinaus – Massnahmen ergriffen werden dürfen, auch wenn «die Verdachtslagen teilweise noch nicht [genügen], um strafrechtliche Ermittlungen auszulösen» (Botschaft NDG, BBl 2014, 2163.). Anders als im Strafprozess gelangen die dortigen Schranken der Anordnung, die entsprechenden (grundsätzlich kontradiktorischen) Genehmigungsverfahren und die Beschuldigtenrechte nicht zur Anwendung. Nichtsdestotrotz soll der NDB die so gewonnenen Erkenntnisse an die Strafverfolgungsbehörden weiterleiten dürfen. Damit wird für die nachrichtendienstlichen Bereiche de facto grossflächig das Verbot **unzulässiger Beweisausforschung** (*fishing expedition*) und das damit einhergehende **Verwertungsverbot aufgehoben**. Unterwandert werden damit aufklärerische Maximen des Strafprozesses.

Bereits heute besteht **im Strafrecht eine ganz erhebliche Vorverlagerung der Strafbarkeit** in Form von strafbaren Vorbereitungshandlungen: zu nennen wären etwa die strafbaren Vorbereitungshandlungen hinsichtlich bestimmter Straftaten (Art. 260^{bis} StGB; Art. 226^{ter}), die Beteiligung an einer kriminellen Organisation oder der Unterstützung einer kriminellen Organisation (Art. 260^{ter} StGB), die Terrorismusfinanzierung (Art. $260^{quinquies}$ StGB), die Gefährdung der öffentlichen Sicherheit mit Waffen (Art. 260^{quater} StGB) etc. Hinzu kommen die verselbständigten Beihilfe und Vorbereitungshandlungen bei den Staatsschutzdelikten, insb. beim verbotenen Nachrichtendienst (vgl. Art. 272-274) oder der verbotenen Handlung für einen fremden Staat (Art. 271 StGB). Komplementiert wird das Instrumentarium an Tatbeständen durch zahlreiche mit der eidg. Strafprozessordnung eingeführte weitgehende Zwangsmassnahmen.

Es besteht also in diesem Bereich eine erhebliche Überschneidung strafprozessualer und nachrichtendienstlicher Kompetenzen. Diese **Doppelspurigkeit**, gekoppelt an einen eigentlich unzulässigen, zugleich intransparente Informationsfluss zwischen zwei Behördenzweige gänzlich unterschiedlicher Ausrichtung (Prävention vs. Pönalisierung), führt nicht nur zur Aushöhlung der Beschuldigtenrechte,

indem eine Art **Feindesstrafprozessrecht** geschaffen wird, sondern auch zu **Ineffizienz bei den Bundesbehörden**.
Angesicht der tiefgreifenden Änderungen des Grundwesens des NDB, ist unter demokratischen Gesichtspunkte eine hinreichende Verankerung des Nachrichtendienstgesetzes in der **Verfassung** unabdingbar.

Folgende Ausführungen beschränken sich auf einige ausgewählte Aspekte.

III. Grundsätzliches (1. Kapitel)

Als **Zweck** des Gesetzes nennt Art. 2 zuallererst die «Sicherung der demokratischen und rechtsstaatlichen Grundlagen der Schweiz». Daran werden wir den Entwurf messen. Denn die weiteren Ziele – Schutz von Staatsbürgern, staatlicher Handlungsfähigkeit und internationaler Sicherheitsinteressen können einem jedem Staat – auch einer Diktatur – inhärent sein.

Demokratie und Rechtsstaat, das bedeutet Legitimation durch (zumindest angebliche) politische Gleichberechtigung und einen rechtlichen Rahmen, der Vertrauen in das Staatswesen herstellen soll. Eine Bedrohung der Demokratie oder des Rechtsstaates «im Innern» oder «von unten» impliziert mithin eine Infragestellung seines Menschenbildes, ja überhaupt der *Möglichkeit* einer darauf basierenden **Legitimation**. Wo dieser Staat seine rechtsstaatlich-demokratische *Verfassung* autoritativ und mit Zwang schützen muss, indem er sich über seine Staatsbürger stellt und zum Schutz dieser Verfassung nicht umhin kommt, ebendiese in Teilen aufzugeben, begibt er sich ins Feld einer Diktatur.

Darum darf auch behauptet werden: Ein liberaldemokratischer Rechtsstaat, der nicht in einem schizophrenen Verhältnis zum Staatsschutz steht, krankt. In diesem Punkt stimmt die aktuelle Entwicklung skeptisch: Von Misstrauen gegen Überwachung und Kontrolle ist nichts zu spüren, stattdessen strahlt der Entwurf eine **etatistisch-autoritäre Selbstverliebtheit** aus, wie sie auch offen zugegeben wurde im ERLÄUTERNDEN BERICHT: «*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*.» (ERLÄUTERNDER BERICHT E NDG 2013, S. 16).

Höchst problematisch erscheint in diesem Zusammenhang auch der Art. 3 E-NDG, der dem Bundesrat (via Art. 70 E-NDG) erlaubt, den NDB «in besondere Lagen» uneingeschränkt für **weitere Bereiche** einzusetzen, wobei u.a. eine Ausweitung auf den «Werk-, Wirtschafts- und Finanzplatz Schweiz» genannt wird. Damit wird der NDB zur Waffe in sog. Wirtschaftskriegen umfunktioniert, richtet sich möglicherweise nicht nur gegen Staaten, sondern bald auch schon gegen zivilgesellschaftliche Strukturen (z.B. Whistleblower), die bspw. Praktiken von Schweizer Unternehmungen anprangern.

IV. Aufgaben und Zusammenarbeit (2. Kapitel)

Bei den Aufgaben des NDB wurden als Ziele der Informationsbeschaffung neue, **wenig bestimmte** Vorgaben gemacht, wie die «Feststellung sicherheitspolitisch bedeutsamer Vorgänge im Ausland» (Art. 6 Abs. 1 lit. b) oder die «Wahrung der Handlungsfähigkeit der Schweiz» (Art. 6 Abs. 1 lit. c), aber etwa auch das frühzeitige Erkennen von Bedrohungen ausgehend von «Angriffen auf Informations-, Kommunikations-, Energie-, Transport- und weitere Infrastrukturen» (Art. 6 Abs. 1 lit. a Ziff. 4), wobei

der Begriff dieser *kritischen* Infrastruktur «umfassend» (BOTSCHAFT NDG, BBl 2014, 2143) zu verstehen sei. Damit droht eine erhebliche **Ausweitung** des Handlungsspielraums des NDB.
Die Regel, dass im Bereich der Meinungs-, Versammlungs- und Vereinigungsfreiheit Informationen nur ausnahmsweise beschaffen werden dürfen und zu löschen sind, sobald eine entsprechende terroristische, verbotene nachrichtendienstliche oder gewalttätig-extremistische Tätigkeit ausgeschlossen werden kann (Art. 5 Abs. 6 f. E-NDG), muss dringend ergänzt werden, durch ein **Verbot der Weitergabe** entsprechender Daten.
Die Beteiligung an **internationalen automatisierten Informationssystemen** gemäss Art. 12 Abs. 1 lit. e ist problematisch, da diese als selbstständige völkerrechtliche Verträge des Bundesrates (Art. 69 Abs. 3 E-NDG) der parlamentarischen Genehmigung und damit auch den fakultativen Referendum entzogen sind. Mit Blick auf den Ausschluss der Legislative stellt sich die Frage, wie die Rechtsstaatlichkeit dieser Informationssysteme gewährleistet werden kann.

V. Informationsbeschaffung (3. Kapitel)

1. Genehmigungsfreie Beschaffungsmassnahmen

Die Kritik an den bisherigen bzw. den genehmigungsfreien Überwachungsmassnahmen bleibt unverändert. Besonders schädlich halten wir den **Einsatz bezahlter Spitzel** (Art. 15 E-NDG). Die neue Massnahme der **Personen- und Sachfahndungsausschreibung** ist ein einschneidendes Kontrollinstrument; es ist daher unabdingbar, die Voraussetzungen der Anordnung einschränken und nicht einfach generell auf Art. 6 Abs. 1 lit. a zu verweisen.

2. Legendierungen und Tarnidentitäten

Die Ausstattung mit **Legendierungen und Tarnidentitäten** – gar für kantonale Vollzugsbehörden und HUMINT – halten wir für problematisch.

3. Auskunfts- und Meldepflichten

Die Auskunftspflichten – gekoppelt an die Geheimhaltungspflichten gegenüber Dritten – gehen ausserordentlich weit. Kantonale und Bundesbehörden, Organisationen, die öffentliche Aufgaben wahrnehmen und auch Private werden so letztlich zum **verlängerten Arm des Nachrichtendienstes**. Das unterminiert nicht nur das gesellschaftliche und staatliche Vertrauensverhältnis, sondern droht darüber hinaus in der Umgehung der Genehmigungspflicht zu münden.

Art. 19 Abs. 1 sieht für einen – wie in der BOTSCHAFT selbst zugegeben – «**breit gefasste[n] Adressatenkreis**» (BOTSCHAFT NDG, BBl 2014, 2159) eine Auskunftspflicht vor, namentlich auch für Organisationen, die öffentliche Aufgaben wahrnehmen. Der Begriff der öffentlichen Aufgaben umfasst ein enorm weites Feld, zuzurechnen sind ihm gemäss der Lehre etwa: Tätigkeit des amtlichen Verteidigers; Lehrertätigkeit; Betreiben von Spitälern; Tätigkeit des SRK; Familienausgleichskassen; Versorgung mit elektrischer Energie; Betreiben eines Flughafens etc. (vgl. BOSCHUNG, Der bodengebundene Rettungsdienst, Diss. FR, 2010, 117). Dringend erforderlich ist nicht nur eine klare Einschränkungen dieses Adressatenkreises, sondern auch die Schaffung von Transparenz hinsichtlich dieser Auskunftspflicht.
Zudem ist der Kreis der Bedrohungen, die eine Auskunftspflicht auslösen, zu weit gezogen. Insbesondere kann es nicht genügen, dass allein schon das diffuse «**befürworten**» von Gewalttaten (Art. 19 Abs. 2 lit. e) zu einer Kategorisierung als «gewalttätig-extremistisch» führt.

Die Bestimmungen zur **Identifikation und Befragung** von Personen (Art. 22 ff.) ist problematisch, zumal wo entsprechende Daten strafrechtlich relevant sind oder sein könnten, greift doch der NDB da-

mit in den Bereich des Strafprozessrechts ein, ohne die dortigen Garantien zu berücksichtigen. Derartige Massnahmen müssen den Angehörigen der ordentlichen Polizeikorps bzw. den Strafverfolgungsbehörden vorbehalten bleiben.
Die Massnahmen nach Art. 24 stellen **schwerwiegende Eingriffe** in die Persönlichkeitsrechte und Privatsphäre dar. Insbesondere bei der Auskunftspflicht von privaten Betreibern einer Sicherheitsinfrastruktur (Abs. 1 lit. b) droht eine Umgehung genehmigungspflichtiger Massnahmen. Sie sind daher abzulehnen, sollten aber zumindest als **genehmigungspflichte Massnahme** ausgestaltet werden.
Höchst problematisch ist der Generalverweis auf Art. 14 BÜPF in Abs. 2. Einerseits fehlt die **ausdrückliche Einschränkung**, dass dies (analog zu Abs. 1) nur im Einzelfall und nur zum «Erkennen, Verhindern oder Abwehren einer konkreten Bedrohung nach Artikel 19 Absatz 2» erlaubt ist. Andererseits wird mit der Inpflichtnahme (privater) Internetanbieter der Bogen weit überspannt, zumal diese gemäss Bundesgericht (vgl. BGer, I. ÖRA, 22.1.2013, 1B_481/2012) ohne zeitliche Beschränkung auskunftspflichtig sein sollen. Derartige Massnahmen sind abzulehnen bzw. mindestens einer vorgängigen Genehmigungspflicht zu unterstellen. Solange dies nicht gewährt ist, ist auch der Entzug der aufschiebenden Wirkung von Rechtsmittel gegen entsprechende Verfügungen (Art. 79 Abs. 2) entschieden abzulehnen.

4. Genehmigungspflichtige Beschaffungsmassnahmen

Die neuartigen, genehmigungspflichtigen Massnahmen **gehen weit über eine defensive Gefahrenabwehr hinaus**. Vorgesehen sind insbesondere: die Überwachungsmassnahmen gemäss BÜPF, also den Zugang zu Vorratsdaten der Telekommunikation (mit der Verschärfung des BÜPF: bis zu 12 Monaten zurückliegend); Verwendung von Ortungsgeräten (IMSI-Catchern); der Einsatz von Überwachungsgeräten an nicht öffentlichen Orten; das Eindringen in Computersysteme und –netzwerke (inkl. Einsatz von Bundestrojanern und Cyberwar-Massnahmen) sowie Durchsuchungsmassnahmen.
Diese Massnahmen stellen **gravierende Eingriffe** in die verfassungsmässigen Grund- und Menschenrechte dar. Zu beobachten ist ein eigentlicher Paradigmenwechsel: So soll der Nachrichtendienst über neue Beschaffungsmassnahmen verfügen, die – teilweise gar über die strafprozessualen Zwangsmassnahmen hinausgehend – sehr weitgehende Eingriff in die Privatsphäre erlauben sollen.
Dass von diesen genehmigungsbedürftigen Massnahmen der **gewalttätige Extremismus** ausgenommen bleibt, vermag die Bedenken nicht auszuräumen und ist wohl primär dem politischen Spektrum im Parlament geschuldet. Abgesehen davon bedarf es gerade mal der Änderung eines Buchstabens, um diesen Sachverhalt zu ändern, und es ist möglicherweise nur eine Frage der Zeit, wann dies geschehen wird.
Hinzu kommt, dass Daten aus genehmigungspflichtigen Beschaffungsmassnahmen via Art. 57 Abs. 2 E-NDG möglicherweise doch auch für den Bereich des gewalttätigem Extremismus gesammelt und weiterverwertet werden. Liest man die BOTSCHAFT genau, so können die dortigen kryptischen Ausführungen dahingehend gedeutet werden, dass «Informationen […], die nichts mit dem Aufklärungsziel zu tun haben» möglicherweise als «für die Zwecke des Auftrags notwendige Daten […] zur weiteren Auswertung in die entsprechenden Informationssysteme des Verbunds» eben doch weiterverwendet werden (BOTSCHAFT NDG, BBl 2014, 2192 f.). Damit würde sich Art. 57 Abs. 2 E-NDG als **Trojanisches Pferd** entpuppen.
Im Rahmen des Genehmigungsverfahrens erscheint dringend nötig, dass jedenfalls Fälle von besonderer Bedeutung **zwingend dem Bundesrat vorgelegt** werden (vgl. Art. 29 Abs. 1 i.F.v. E/NR-NDG). Eine allfällige Schriftlichkeit des Konsultationsverfahrens (Abs. 2) darf nicht Vorwand sein für die leichtfertige Anwendung eines **Dringlichkeitsverfahrens**. Im Falle eines solchen muss nebst dem Chef VBS zwingend auch das BVGer die Beschaffungsmassnahme mit sofortiger Wirkung beenden können.
Die **Mitteilungspflicht** nach Art. 32 E-NDG ist tatsächlich eher eine Geheimhaltungserlaubnis (vgl. Abs. 2), was eine undurchsichtige und ausufernde Anwendungspraxis der Massnahmen begünstigt.

Voraussetzung für eine effektive justizielle Kontrolle ist ausserdem eine detailliertere Auskunftspflicht, die sich nicht auf Grund, Art und Dauer der Überwachung beschränkt.

5. Information über Vorgänge im Ausland

Art. 35 impliziert den Vollzug sogar von eigentlich genehmigungspflichtigen (Zwangs)massnahmen im Ausland (Abs. 5), was ohne jeden Zweifel die **Souveränität anderer Staaten verletzt** (vgl. in der Schweiz Art. 271 StGB). Das ist völkerrechtlich nicht haltbar; zugleich entzieht es der Kritik am Treiben fremder Geheimdienste in der Schweiz die Grundlage und delegitimiert letztlich auch das schweizerische nachrichtendienstliche und strafrechtliche Dispositiv zum Schutz vor fremder Spionage – mithin den NDB selbst.

Dass ausserdem die justiziellen Garantien (Genehmigungspflicht) im Ausland gemäss Abs. 2 *e contrario* nicht zur Anwendung gelangen (ebenso BOTSCHAFT NDG, BBl 2014, 2174), droht auch ein eklatanter Eingriff in **grundrechtliche Positionen** und letztlich auch eine Ungleichbehandlung für Personen ausserhalb der Schweiz.

6. Cyberwar

Art. 36 Abs. 1 E-NDG, der das Eindringen in Computersysteme und –netzwerke im Ausland vorsieht, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen, geht weit über eine Abwehrmassnahme und ist in seinen Konsequenzen als Instrument des Cyberwars hoch delikat und letztlich unberechenbar. Auch Abs. 2, der die Informationsbeschaffung auf demselben Wege vorsieht, ist gefährlich, zumal ein solches Verhalten völkerrechtswidrig sein dürfte und erhebliches (diplomatisches) Sprengpotential hat, dem die Schweiz möglicherweise nicht gewachsen sein wird.

Geradezu fahrlässig erscheint die Möglichkeit, den Entscheid über derartige völkerrechtlich unzulässige Handlungen an den Vorsteher des VBS oder an den Direktor des NDB zu **delegieren** (so aber Art. 36 Abs. 1 E/NR-NDG). Will man internationales Recht brechen, so sollte dies immerhin (als genehmigungspflichtige Massnahme) einer richterlichen Prüfung unterliegen.

7. Funk- und insb. Kabelaufklärung

Gerade mal zwei Jahre nach Beginn der Enthüllungen Edward Snowdens und der politischen Empörungen über die amerikanische Spionagetätigkeit, will der Bund mit der Kabelaufklärung dem NDG ein Instrument geben, das dem amerikanischen Programm PRISM nicht unähnlich ist. Damit wird der **Funkaufklärung**, an sich bereits ein zweifelhaftes Instrument, das erst spät überhaupt legalisiert wurde (BWIS II, Art. 4a), ein weiteres Aushorch-Instrument neuer Quantität und Quantität zur Seite gestellt.
Gestützt auf Art. 38 E-NDG soll die Beschaffung von Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland sowie zur Wahrung weiterer wesentlicher Landesinteressen, also auch zum Schutz des Werk-, Wirtschafts- und Finanzplatzes, grenzüberschreitende Signale aus leitungsgebundenen Netzen erlaubt werden. Nicht nur Betreiber von leitungsgebundenen Netzen, sondern auch Anbieter von Telekommunikationsdienstleistungen, sollen verpflichtet werden, dem durchführenden Dienst (ZEO) die Daten zu liefern und allfällige Verschlüsselungen zu entfernen (Art. 42). Dieses systematische Überwachen immenser Datenströme basierend auf Suchbegriffen und die damit zusammenhängende Verpflichtung von Netzbetreiberinnen und Telekommunikationsdienstleistern, stellen einen eigentlichen **Paradigmenwechsel** dar.
Dabei dürfte es ganz wesentlich auch darum gehen, **Partnerdienste** mit Informationen zu versorgen bzw. entsprechende Kontrollmassnahmen souverän und in legalisierter Weise vorzunehmen. Es stellt sich damit auch die Frage, inwiefern die Schweiz ihre immer wieder betonte **Neutralität** durch die Hintertür aufweicht. Unter den Begriff der «sicherheitspolitisch bedeutsamen Vorgängen im Ausland»

lässt sich praktisch alles subsumieren. Es gibt berechtigte Gründe anzunehmen, dass künftig auch ausländische Partnerdienste bei der Stichwortliste (Selektoren) mitbestimmen werden. So wurde etwa in Deutschland im Rahmen der NSA-Untersuchung bekannt, dass der amerikanische Dienst rund 800'000 Selektoren einspeisen wollte (vgl. http://www.zeit.de/digital/datenschutz/2015-04/ueberwachung-bnd-half-nsa-wirtschaftsspionage-europa), wovon 40'000 als problematisch bewertet wurde (etwas weil sie sich auf europäische Politiker und Unternehmen bezogen), wobei gemäss Spiegel über die Hälfte dieser tatsächlich aktiviert wurde (vgl. http://www.spiegel.de/politik/deutschland/spiegel-bnd-affaere-weitet-sich-aus-a-1033881.html). Droht auch der Schweiz bald der Vorwurf der Wirtschaftsspionage vonseiten der ihrer europäischen Nachbarn?
Nach Art. 38 Abs. 2 sind Daten zu vernichten, wenn sich **sowohl der Sender als auch der Empfänger in der Schweiz** befindet. Das erweckt vorab den Eindruck, dass für Personen im Ausland, deren Datenverkehr die Schweiz überwacht, nicht die selben grundrechtlichen Standards gelten sollen, was doch erstaunt. In Deutschland hat sich ausserdem gezeigt, dass ein entsprechender Filter, der Daten von deutschen Staatsbürgern hätte aussondern sollen, nie richtig funktioniert hat (vgl. https://netzpolitik.org/2014/eikonal-wie-der-bnd-der-nsa-zugang-zum-internetknoten-de-cix-schenkte).

Bei genauer Betrachtung zeigt sich aber – was weit gravierender ist –, dass sich erstens bei grenzüberschreitenden Leitungen **kaum je Sender und Empfänger in der Schweiz befinden** (vgl. Cloud, Emailserver etc.). Zweitens leitet gemäss Botschaft das ZEO nicht nur Daten gemäss einem Suchauftrag an den NDB weiter, sondern sämtliche «Hinweise auf eine Gefährdung der inneren oder äusseren Sicherheit», BOTSCHAFT NDG, BBl 2014, 2179). Es besteht daher die Gefahr, dass zahlreiche Informationen als «Drittdaten» via Art. 57 Abs. 2 E-NDG doch abgelegt und weiterverarbeitet werden, wenn sie «für die Erfüllung der Aufgaben nach Artikel 6 Absatz 1 benötigt werden» (vgl. oben).

Unabdingbar – aber nicht vorgesehen – ist im Bereich der Kabelaufklärung eine umfassende **Aufsicht**, die angesichts der Datenmenge und der Komplexität wird diese ressourcenmässig erheblich über diejenige der Funkaufklärung hinausgehen müssen.

VI. Datenbearbeitung und Archivierung (4. Kapitel)

1. Allgemeines

Zu bedauern ist vorweg, dass hinsichtlich sämtlicher relevanten Daten *nicht* das Datenschutzgesetz, sondern ein **Sonderrecht** gilt (Art. 62 Abs. 2 E-NDG).
Mit Art. 43 Abs. 2 (Weiterbearbeitung von Des- und Falschinformationen, s.a. Art. 44 Abs. 4 in fine) drohen die **Schranken der Datenbearbeitung neutralisiert** zu werden, indem unzulässig bearbeitete Daten nicht gelöscht, sondern einfach als falsche Informationen gekennzeichnet werden.
Nicht erhebliche **Drittdaten** müssen dringend ausgesondert oder anonymisiert werden. Mit dem Vorschlag des Nationalrates, «Meldungen, die mehrere Personendaten enthalten» als Ganzes zu beurteilen, droht genau dies umgangen zu werden (vgl. Art. 44 Abs. 1 E/NR-NDG).
Mit Blick auf die Vielzahl von Informationssystemen und die Möglichkeit der Mehrfachspeicherung fragt sich, inwiefern eine **effektive Qualitätssicherung** möglich ist. Erschwert, ja verunmöglicht wird damit das Auskunfts-, bzw. Korrekturrecht der Betroffenen und es droht eine Umgehung der Aufbewahrungsdauer.
Bezüglich der Lösung des Problems verweisen wir auf den Vorschlag der *Digitalen Gesellschaft* (vgl. deren Stellungnahme v. 28.6.2013, 14): Die Menge der beschafften Daten ist massiv einzuschränken, mehrfach relevante Daten sind zentral zu speichern und dann **nicht via Kopien, sondern via Referen-**

zen im jeweiligen spezifischen Informationssystem zu implementieren. Nicht die für die Informationsbeschaffung zuständige Stelle, sondern eine zentrale Stelle soll für die Datenpflege zuständig sein. Die Qualitätssicherungsstelle (Art. 44 Abs. 44) ihrerseits sollte diesen Prozess überwachen, im Sinne einer Supervision über die zentrale Stelle für Datenpflege.
Ganz generell ist das **massive Datensammeln** weder zielführend noch im Sinne rechtsstaatlicher Prinzipen. Abzulehnen ist insbesondere die stigmatisierende und präventive Überwachung, wie sie das System Quattro P vorsieht, das erhebliche Datenmengen im Zusammenhang der Ein- und Ausreise «bestimmter Kategorien ausländischer Personen» produziert (gemäss ISV-NDB wurden allein im Jahr 2013 über eine halbe Million Personen überprüft, NZZaS, 1.2.2015, 13). Nicht weniger problematisch ist der sog. Restdatenspeicher; es ist gänzlich unklar, welche Daten hier gespeichert werden und wie die Rechtmässigkeit, aber auch die Datenqualität sichergestellt werden soll. Nicht ausgeschlossen ist, dass dieser zu einer unkontrollierten Datenkrake wird. Angesicht dessen ist eine Aufbewahrungsdauer der Daten über 20 Jahre (so Art. 56 Abs. 4 E/NR-NDG) vehement abzulehnen.

2. Datenweitergabe

Die Datenweitergabe an inländische Behörden ist **zu allgemein formuliert**. Die Datenweitergabe ans Ausland geht trotz der Anlehnung ans DSG und der Schutzklausel in Art. 60 Abs. 3 zu weit, weil im nachrichtendienstlichen Bereich sowohl die datenschutzrechtlichen **Rechtsmittel fehlen** und auch die Einhaltung der **Schutzgarantien (Abs. 3) nicht gewährleistet** werden kann. Zudem fehlt eine Garantie, dass die entsprechenden Daten – im Sinne des Spezialitätsprinzips – nicht an andere Dienste **weitergeleitet** werden, von denen möglicherweise eine Bedrohung ausgeht.

3. Datenweitergabe an Strafverfolgungsbehörden insbesondere

Art. 59 Abs. 2 E-DGB sieht die Weitergabe von Personendaten an inländische Behörden vor, auch an Strafverfolgungsbehörden. Ähnlich sieht Art. 60 sieht die Weitergabe an ausländische Behörden u.a. zwecks Strafverfolgung vor.

In Anbetracht der Tatsache, dass «die Informationsbearbeitung bereits zu einem Zeitpunkt erfolgen [muss], zu dem **noch kein rechtsgenügender Verdacht** auf die Vorbereitung oder das Vorliegen einer Straftat besteht», der NDB also «aktiv nach diesen Bedrohungen suchen und sie im Verbund mit den anderen Behörden abwehren» muss (BOTSCHAFT NDG, BBl 2014, 2181, H.v.Verf.), ist diese Datenweitergabe in höchstem Masse fragwürdig.

Bedenkt man das Instrumentarium und die Engmaschigkeit der Netze, mit denen diese Daten teils ohne jeglichen Anfangsverdacht gewonnen werden, so handelt es sich – aus strafrechtlicher Perspektive – um nichts anderes als eine **unzulässige Beweisausforschung**, zumal faktisch planlos Beweisaufnahmen getätigt werden, also Zwangsmassnahme ohne hinreichenden Tatverdacht durchgeführt werden. Damit werden die strafprozessualen Voraussetzungen (Art. 196 ff. StPO) umgangen. Nach Rechtsprechung des Bundegerichts sind die Ergebnisse einer «**fishing expedition**» nicht verwertbar. Nimmt man rechtsstaatliche Grundsätze ernst, muss für so erhobene Daten ein absolutes Verwertungsverbot gelten (vgl. auch VETTERLI, ZStrR 2012, 455 f.; BSK StPO-GFELLER/THORMANN, Art. 243 N 39 ff.). Diese ausgebaute geheimpolizeiliche Überwachung ist daher mit Blick auf strafprozessuale Grundsätze hoch problematisch, selbst wenn man die Datenweitergabe an Strafverfolgungsbehörden beschränken würde auf die Möglichkeit einer Anzeigeerstattung, die bei hinreichendem Tatverdacht strafprozessuale Zwangsmassnahme auslösen könnte.

Bereits heute besteht im Strafrecht eine ganz erhebliche Vorverlagerung der Strafbarkeit und das Strafprozessrecht kennt zahlreiche (auch geheime) Überwachungsmassnahmen. Somit droht eine **Doppelspurigkeit**, die nicht nur eine Art **Feindesstrafprozessrecht** schafft, sondern **Ineffizienz und**

Undurchsichtigkeit schaffen wird (siehe oben).

Zwar sieht Art. 57 Abs. 1bis E/NR-NDG nunmehr vor, dass «aus genehmigungspflichtigen Beschaffungsmassnahmen stammende Personendaten, die keinen Bezug zur spezifischen Bedrohungslage aufweisen, nicht verwendet werden und spätestens 30 Tage nach Beendigung der Massnahme vernichtet werden.» Allerdings nicht klar, wozu diese Personen «nicht verwendet» werden, namentlich inwiefern damit ein (über Personendaten hinausgehendes) generelles **Verbot der Weitergabe an Strafbehörden** gemeint ist.

Eine weitere Beschränkung betrifft Daten aus nicht genehmigungspflichtigen Massnahmen, namentlich Privater und öffentlicher Auskunftspflicht. Diese Erkenntnisse sollen nunmehr den Strafverfolgungsbehörden nur zur Abklärung «**schwerer Straftaten**» zur Verfügung gestellt werden (Art. 19 Abs. 6 E/NR-NDG und Art. 24 Abs. 3 E/NR-NDG). Dies ist pure **Augenwischerei**: Die Umgehung des Verbot der unzulässigen Beweisausforschung kann nicht relativiert werden, nur weil «schwere» Taten betroffen sind. Nebenbei sei angemerkt, dass als schwere Straftat etwa nach N-SIS-V Art. 33 Abs. 5 selbst ein Diebstahl gilt (verwiesen wird auf Art. 286 Abs. 2 StPO).

4. Auskunftsrecht

Nach wie vor ist das Auskunftsrecht **rechtsstaatlich problematisch und undurchsichtig** ausgestaltet. Mit dem Vorschlag, verschlimmert durch den E/NR (Art. 63 Abs. 2, der eine vollkommen nichtssagende Auskunft vorsieht), wird das sog. «Auskunftsrecht» pulverisiert.
Das **Erteilen von Auskunft** bei erheblichen, nicht wiedergutzumachenden Schäden ohne Gefährdung der inneren oder äusseren Sicherheit ist nicht als Ausnahme, sondern als **Regel** auszugestalten und zwar bereits bei Anfragen an den NDG. Ungenügend ist ausserdem, dass der EDÖB hierzu nur Empfehlungen abzugeben hat; ausdrücklich festzuhalten ist ausserdem in Art. 64 Abs. 1, dass auch bzgl. der Empfehlung der ausnahmsweisen sofortigen Auskunftserteilung (Art. 63 Abs. 5) eine Prüfung des Vollzuges durch das BVGer offensteht.
Hinsichtlich Verfügung zur Fehlerbehebungen des BVGer (Art. 64 Abs. 2 E-NDG) ist klarzustellen, dass nicht nur dem NDB, sondern auch dem **EDÖB**, der Weg ans Bundesgericht offensteht.
Wichtig erscheint zudem, dass den entsprechenden Prüfinstanzen (EDÖB, BVGer, ggf. BGer) direkte **Einsicht in die Akten** gewährt wird. Nur so können sie sich ein unabhängiges Bild machen, wie es von einer justiziellen Behörde zu erwarten ist.
Der **explizite Ausschluss von Rechtsmitteln** (Art. 65) ohne Nennung eines Vorbehaltes i.S. der völkerrechtlich verbrieften Gegenausnahme erscheint einmal mehr müssig. Das höchste Schweizer Gericht hat vor kurzem in BGE 138 I 6 die Anfechtbarkeit der Mitteilung des Abteilungspräsidenten des Bundesverwaltungsgerichts anerkannt. Im Entscheid wurde insbesondere darauf hingewiesen, dass der EGMR in mehreren Beschwerdefällen einen Anspruch auf gerichtliche Beurteilung bzgl. geheimer Überwachung, Aufzeichnung von Personendaten und deren Verwendung unter dem Gesichtswinkel von Art. 8 und Art. 13 EMRK anerkannt hat (E. 1.3.2). Weiter wurde festgehalten: «*Ein Bedürfnis nach einer Überprüfung kann nicht verneint werden. Insoweit ist nicht von Bedeutung, dass die Mitteilung des Beauftragten nach Art. 18 Abs. 2 BWIS [künftig Art. 65 NDG, H.v.Verf.] ausdrücklich keiner Beschwerde unterliegt und die Mitteilung des Abteilungspräsidenten daher keinen eigentlichen Rechtsmittelentscheid darstellt.*» (E. 1.2).

VII. Steuerung, Kontrolle, Rechtsschutz (6. Kapitel)

Vgl. hierzu die verschiedenen Hinweise bei den einzelnen Massnahmen/Bestimmungen.
Hinsichtlich des Rechtsschutzes sind Konstellationen durchwegs problematisch, in denen das **BVGer** sowohl im Vorfeld Genehmigungsinstanz ist als auch später Beschwerdeinstanz; hier droht ein erheb-

licher **Interessenkonflikt**. Das BVGer hat dies selbst bemängelt im Vernehmlassungsverfahren und vorgeschlagen, das **BStGer** solle entscheiden (BOTSCHAFT NDG, BBl 2014, 2207). Doch auch hier droht möglicherweise ein Konflikt, indem das BStGer in einem späteren Strafverfahren selbst angeordnete Massnahmen dem Vorwurf der unberechtigten Beweisausforschung ausgesetzt sehen könnte.
Sofern völkerrechtliche Verträge personenbezogene Daten betreffen, müssen diese aufgrund der Schwere des grundrechtlichen Eingriffs vom **Parlament abgesegnet** werden und dem **fakultativen Referendum** unterstellt werden (Art. 69 Abs. 3 E-NDG).
Die Wirksamkeit von **Tätigkeitsverboten** wird angezweifelt, stattdessen droht ein je nach Konstellation eine Missbrauchsgefahr und unverhältnismässige Eingriffe in die Grundrechte. Diese Tätigkeitsverbote sollen nunmehr nach dem Willen des Nationalrates mit einem Organisationsverbot ergänzt werden (Art. 72a E/NR-NDG). Es erscheint nicht grundsätzlich falsch, bisher auf exekutives Notrecht abgestützte **Organisationsverbote** auf eine formellgesetzliche Grundlage zu stellen. Die nunmehr offene, gegenüber Art. 184 und Art. 185 BV weniger strikte Formulierung, droht allerdings in einer inflationären Anwendung gegen politisch nicht genehme Gruppierungen zu münden – daher ist darauf zu verzichten. Zu verlangen wäre mit Blick auf den grundrechtlichen Eingriff mindestens eine unmittelbare, schwere Bedrohung von fundamentalen Rechtsgütern. Gemäss dem schwammigen Gesetzestext soll hingegen bereits ausreichen, dass eine Organisation die innere oder äussere Sicherheit konkret bedroht und auch bloss «mittelbar» dazu dient, gewalttätige Aktivitäten zu fördern. Unnötig ist die Bestimmung (wie bereits die vorangehenden Noterlasse) auch darum, weil solche Verbote zur Bekämpfung von Gruppierungen wie dem IS oder Al-Kaïda untauglich und unnötig sind, zumal ein umfangreiches strafrechtliches Instrumentarium besteht. Besonders problematisch ist auch der **Ausschluss des Rechtsweges**, wie der Nationalrat vorschlägt (Art. 79 Abs. 1^{bis} E/NR-NDG)
Ganz generell sollten die Aufsichtsmechanismen **konkreter** formuliert werden und Prüfungsinstrumente **effizienter** ausgestaltet werden. Insbesondere ist der direkte Zugang zu Akten und Unterlagen ohne Einschränkung zu gewähren.
Insgesamt muss die **Aufsicht** über den NDG ganz erheblich gestärkt und ausgebaut werden. Im Allgemein sollten die Aufsichtsmechanismen im Gesetz **konkreter** formuliert werden und Prüfungsinstrumente **effizienter** ausgestaltet werden, insbesondere hinsichtlich des Zugangs zu Akten und Unterlagen.
Prüfenswert erscheint der Vorschlag der SiK-S zur Schaffung einer Schaffung einer selbständigen und **unabhängigen nachrichtendienstlichen Aufsicht;** diese sollte aber gänzlich unabhängig von VBS sein (ebenso Prof. Schefer, in: http://www.computerworld.ch/news/it-branche/artikel/der-ndb-braucht-eine-unabhaengige-aufsicht-67533). Diese muss mit umfassenden Aufsichts-, Auskunfts- und Einsichtsrechte ausgestattet sein und vor allem über die nötigen Ressourcen verfügen. Daneben sollte die Aufsicht und Kontrolle durch den **Bundesrat** verbindlicher und konkreter festgehalten werden.
Schliesslich muss die **GPDel** in ihrer Aufsicht gestärkt werden. Es bestehen doch Zweifel, dass eine Handvoll Parlamentarier die Aufgabe der legislativen Kontrollen erfüllen kann. Es würde sich lohnen, sich jetzt darüber Gedanken zu machen, als in 5 Jahren einen NDB-Untersuchungsausschuss zu installieren.

VIII. Öffentlichkeit und Transparenz

Ein Nachrichtendienst, der dem demokratischen Rechtsstaat zudienen soll, ist gut beraten, seine Arbeit öffentlich zu dokumentieren. Bei allem Verständnis für bestimmte Geheimhaltungsinteressen ist dafür zu sorgen, dass **grösstmögliche Transparenz** hergestellt wird, etwa durch Bericht und Publikation (oder Ermöglichung von Einsichtnahmen) von detaillierten Statistiken bzgl. Genehmigungsverfahren, Einträge in Informationssystemen, Listen (z.B. Art. 20 Abs. 4, Art. 71), u. dergl.

Nicht nachvollziehbar ist in diesem Zusammenhang auch **die Ausnahme vom Öffentlichkeitsprinzip** (Art. 66), zumal das BGÖ in Art. 7 spezifische und zugeschnittene Ausschlussgründe kennt. Dies würde dafür sorgen, dass nur vertraulich behandelt wird, was tatsächlich vertraulich ist, ohne dass die Geheimhaltungsinteressen tangiert würden (so auch SCHEFER, in: http://www.computerworld.ch/news/it-branche/artikel/der-ndb-braucht-eine-unabhaengige-aufsicht-67533).

IX. Schlussbemerkung

Zusammengefasst erweist sich die Bemerkung, dass mit dem Entwurf «keine Weiterentwicklung der bestehenden Rechtsgrundlagen» vorgenommen wird, als grosser Trugschluss ist. Das Gegenteil ist der Fall. Ohne die bisherige Staatsschutztätigkeit gutheissen zu wollen – die 900'000 Fichen aus dem Kalten Krieg und die weiteren 200'000 (vgl. GPDel Bericht vom 30. Juni 2010) sind Warnung genug – ist doch unzweifelhaft, dass der Nachrichtendienst mit vorliegendem Entwurf eine völlig neue Funktion erhalten soll: Von einer defensiven Gefahrenabwehr hin zum **offensiven Geheimpolizeiapparat**. Solange das nicht zugegeben wird, kann **keine öffentliche Diskussion** geführt werden über das Verhältnis von Sicherheit/Kontrolle zur Freiheit – eine Diskussion, wie sie sich gerade angesichts der sich rasch verändernden europa- und weltpolitischen Lage einem jeden demokratischen Rechtsstaat aufdrängt.

DJS / Bern, 4. Juni 2015