Rainer J. Schweizer*

Ein neues Staatsschutzgesetz?

Die Sicherung der freien Kommunikation der Menschen geht jetzt der Stärkung der Machtmittel der Geheimdienste vor

Der Bundesrat beabsichtigt, der Bundesversammlung ein völlig neues «Nachrichtendienstgesetz» vorzulegen, das das Bundesgesetz über die Wahrung der inneren Sicherheit (BWIS) von 1997 ablösen soll. Nach diesem Gesetzesvorhaben soll der Aufgabenkreis des Schweizer Staatsschutzes erheblich ausgeweitet und dessen Datenbeschaffung um zahlreiche geheim einsetzbare Instrumente ergänzt werden. Der Beitrag zeichnet die Entwicklung des Staatsschutzrechtes nach und erhebt gewisse Einwendungen gegen die geplanten Neuerungen. Er stellt anschliessend die Grundsatzfrage, ob nach den neuesten Erkenntnissen über die Tätigkeiten der NSA und anderer Geheimdienste und der mit diesen zum Teil zusammenarbeitenden grossen IT-Unternehmen nicht zuerst wesentliche Klärungen über all die öffentlich gewordenen illegalen, demokratiefeindlichen Praktiken erfolgen sowie neue, wirksame Sicherungen für die Freiheitsrechte der Bürgerinnen und Bürger vorgesehen werden müssen, bevor die Kompetenzen des Nachrichtendienstes gestärkt werden.

Le Conseil fédéral a l'intention de soumettre à l'Assemblée fédérale une «loi sur les services de renseignement» entièrement nouvelle, qui doit remplacer la loi fédérale sur le maintien de la sécurité intérieure de 1997 (LMSI). Selon ce projet de loi, les tâches des services de renseignements suisses devraient être considérablement élargies, et la manière dont ils se procurent des données complétée par de nombreux instruments pouvant être utilisés en secret. La contribution retrace le développement du droit de la protection de l'État et émet certaines objections à l'encontre des nouveautés prévues. Elle pose ensuite la question de principe de savoir si, au vu des dernières informations sur les activités de la NSA et d'autres services secrets et celles de grandes entreprises IT travaillant en partie ensemble, il ne faudrait pas d'abord procéder à des éclaircissement sur toutes les pratiques antidémocratiques illégales devenues publiques, et prévoir de nouvelles garanties efficaces pour les libertés individuelles des citoyennes et des citoyens avant de renforcer les compétences du service de renseignements.

Inhalt

I. Die Frage ist: Brauchen wir jetzt das geplante neue Nachrichtendienstgesetz?

Das Bundesgesetz über die Wahrung der inneren Sicherheit (BWIS) vom 21. März 1997[1] wurde seit dem Inkrafttreten am 1. Januar 1999 mehrfach und besonders eingehend in den Jahren 2007–2011 einer Revision unterzogen. Die Änderungen vom 23. Dezember 2011 wurden vom Bundesrat zum grösseren Teil auf den 16. Juli 2012 in Kraft gesetzt. Doch weniger als ein Jahr später hat das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) am 8. März 2013 ein Vernehmlassungsverfahren über ein völlig neues *Nachrich-*

* Prof. Dr. iur., em. Professor für öffentliches Recht, Europa- und Völkerrecht an der Universität St. Gallen (HSG).

[1] SR 120.

tendienstgesetz (NDG) eröffnet.[2] Am 23. Oktober 2013 hat der Bundesrat gemäss Medienmitteilung «vom Ergebnis des Vernehmlassungsverfahrens über das Nachrichtendienstgesetz Kenntnis genommen»; er «sieht die grundsätzliche Stossrichtung des Nachrichtendienstgesetzes bestätigt und hat das VBS mit der weiteren Ausarbeitung der Botschaft bzw. des Gesetzesentwurfs beauftragt»[3]. Mit diesem neuen NDG sollen nicht nur das BWIS und das weitgehend organisationsrechtliche, kurze Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) vom 3. Oktober 2008[4] abgelöst werden, sondern vor allem soll der zivile Nachrichtendienst (ND) der Schweiz einen erheblich grösseren Aufgabenbereich erhalten sowie im In- und Ausland weitreichende, geheime Datenbeschaffungsbefugnisse bekommen, wie sie die Bundesversammlung bei der letzten Revision des BWIS 2009/11 noch abgelehnt hatte und wie sie den Kriminalpolizeidiensten von Bund und Kantonen nach der Strafprozessordnung (StPO) nie zustehen.[5] Der Zug mit einem grundlegend neu ausgerichteten Staatsschutzgesetz kommt jetzt auf die Schienen. Ob die «Reise» mit diesem Gesetz *jetzt sachlich notwendig, rechtsstaatlich korrekt sowie mit der Bundesverfassung und dem Völkerrecht konform ist, das ist noch nicht vertieft untersucht* und diskutiert worden. Die folgenden Gedanken wollen dazu einige Hinweise geben, wobei auch das in den letzten Jahren völlig veränderte Umfeld der internationalen digitalen Kommunikation mit den massiven Spionagetätigkeiten befreundeter Nachrichtendienste sowie einem vielfach rechtswidrigen Gebaren der grossen ausländischen IT-Unternehmen unbedingt in Rechnung gestellt werden muss.

II. Das geplante NDG: Ein völlig neues Konzept der rechtlichen Ausrichtung des Staatsschutzes

1. Die bisherige Entwicklung des Staatsschutzrechtes

1.1 Das BWIS von 1997

Um die Tragweite der neuen Vorschläge zu beurteilen, ist es empfehlenswert, sich kurz die Anliegen und das System des bisherigen Rechts des Staatsschutzes bzw. der Nachrichtendienste zu vergegenwärtigen. Das BWIS von 1997 zog bekanntlich die Konsequenzen aus der 1989/90 untersuchten Fichen-Affaire im Schweizer Staatsschutz und sollte zugleich eine Antwort auf die Volksinitiative «S.o.S. Schweiz ohne Schnüffelpolizei» sein[6]. Die *konzeptionellen Leitgedanken* waren, dass sich der *Inland*nachrichtendienst auf die präventive Abwehr von den sog. *Staatsschutzdelikten*, also von Straftaten nach dem Dreizehnten Titel des Strafgesetzbuches (StGB)[7] betreffend Verbrechen und Vergehen gegen den Staat und die Landesverteidigung (Art. 265–278 StGB) sowie nach dem Zwölften Titel des StGB betreffend Verbrechen und Vergehen gegen den öffentlichen Frieden (Art. 258–263 StGB), konzentrieren sollte.[8] Dementsprechend ging es darum, präventive Informationstätigkeiten für eine Vorbeugung von «Gefährdungen durch Terrorismus, verbotenen Nachrichtendienst, gewalttätigen Extremismus und organisiertes Verbrechen» sowie von «verbotenem Handel mit Waffen und radioaktivem Materialien und verbotenem Technologietransfer» (Art. 2 Abs. 1 Entwurf BWIS von 1994) zu regeln.[9] Dabei sollten die Informationen,[10] soweit sie nicht von Amtsstellen und durch Auskünfte erhältlich waren, im Wesentlichen durch Auswertung öffentlich zugänglicher Quellen erfolgen – ein Wirkungsfeld nota bene, das durch das nachfolgend aufblühende Internet unerwartet stark an Breite und Tiefe gewonnen hatte. Jegliche Zwangsmassnahmen waren der Kriminalpolizei oder anderen spezialisierten Verwaltungsstellen vorbehalten, an welche der Staatsschutzdienst seine Erkenntnisse über bestimmte kritische Vorgänge zu liefern hatte.[11] Angesichts des Umstandes, dass dieser Nachrichtendienst *weitgehend nur mit Vermutungen oder Verdächtigungen* arbeitet, die häufig gegen die verfassungs- und menschenrechtliche Unschuldsvermutung (Art. 32 Abs. 1 Bundesverfassung, BV, Art. 6 Abs. 2 Europäische Menschenrechtskonvention, EMRK, und Art. 14 Abs. 2 UNO PAKT II)[12] verstossen und eigentlich kaum rechtsstaatlich faire Rechtsschutzverfahren zulassen, sollten seine Informationsbearbeitungen von anderen Sicherheitsbehörden strikt abgeschottet bzw. organisatorisch getrennt sein. Daher wurde für den Dienst durch das Bundesgesetz selbst ein separates «Bundesamt für Sicherheit» vorgesehen, das allerdings schliesslich nicht er-

[2] Vgl. Bericht des VBS zum Entwurf eines Nachrichtendienstgesetzes (NDG) vom 8. März 2013 und Entwurf Nachrichtendienstgesetz (NDG) vom 8. März 2013.

[3] http://www.news.admin.ch/message/index.html?lang=de&print_style=yes&msg-id=5…24. Oktober 2013.

[4] SR 121. Das ZNDG diente der von der Bundesversammlung 2008 beschlossenen Fusion des Inland-Staatsschutzes (damals: Dienst für Analyse und Prävention DAP im Bundesamt für Polizei) mit dem bisherigen Strategischen Nachrichtendienst.

[5] Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0). Vgl. auch das die elektronische Überwachung deutlich begrenzende Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1). Der Entwurf des NDG vom 8. März 2013 sieht auch vor, dem Militärischen Nachrichtendienst zusätzliche Mittel zu geben (vgl. Änderung des bisherigen Rechts, Ziff. 9).

[6] Vgl. Botschaft des Bundesrates vom 7. März 1994, BBl 1994 II, 1127 ff.

[7] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0).

[8] Näheres zum BWIS von 1997: Reto Patrick Müller, Innere Sicherheit Schweiz, Rechtliche und tatsächliche Entwicklungen im Bund seit 1848, Diss. Basel, Egg bei Einsiedeln 2009, 434 ff.

[9] BBl 1994 II, 1203.

[10] «Informationen» umfassen Personendaten i.S. von Art. 2 Abs. 2 Bst. a Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (SR 235.1) sowie Sachdaten (z.B. über ausländische Militäranlagen).

[11] Das wurde jetzt, unter Vorbehalt gesetzlicher Ausnahmen, in Art. 17 Abs. 1bis i.d.F. vom 23. Dezember 2011 klargestellt.

[12] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101); Konvention zum Schutze der Menschenrechte und Grundfreiheiten, abgeschlossen in Rom am 4. November 1950 (SR 0.101); Internationaler Pakt über bürgerliche und politische Rechte, abgeschlossen am 16. Dezember 1966 in New York (SR 0.132.2).

richtet wurde, weil dessen Aufgaben dem Dienst für Analyse und Prävention (DAP) im Bundesamt für Polizei (BAP)[13] zugewiesen worden waren.[14] Wichtige konzeptionelle Entscheide waren auch, die Aktivitäten des *Auslands*nachrichtendienstes nicht zu normieren – weil international angeblich nicht üblich –[15], im Inland umgekehrt den Staatsschutzorganen *besondere Schranken* zur Sicherung einer offenen Demokratie zu setzen (vgl. Art. 3 BWIS[16]) sowie mit den Art. 19–21 BWIS die *Personensicherheitsprüfungen* zu einer von den Nachrichtendiensten getrennten, ordentlichen und weitestgehend offenen Verwaltungspolizeiaufgabe zu erheben.

1.2 2007: Der Kampf gegen Hooligans als Staatsschutzaufgabe

Vor dem von der Schweiz und Österreich betreuten europäischen Fussballereignis EURO 2008[17] wurde auf Initiative des Bundesrates[18] am 24. März 2006 eine Änderung des BWIS beschlossen[19], welche *polizeiliche Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen* regeln wollte und auf den 1. Januar 2007 in Kraft gesetzt wurde (vgl. die Art. 24*a*–24*h* BWIS).[20] Sachlich hatte diese Novelle nichts mit dem Staatsschutz zu tun, und verfassungsrechtlich muss sie als ein Irrläufer bezeichnet werden, weil der Bund nach BV gar nicht zuständig ist, Polizeikompetenzen der Kantone im Bereich der öffentlichen Sicherheit und Ordnung zu bestimmen.[21]

1.3 Das BWIS II (reduziert) von 2011

Die nächste einschneidende Revision des BWIS wurde vom Bundesrat ab 2007 angegangen, indem er für den Nachrichtendienst ein *Paket von zusätzlichen Befugnissen zu vorwiegend geheimen Informationsbeschaffungen* einforderte.[22] Die Revision kann als ein Ausläufer der internationalen, von den USA seit 2001 vorangetriebenen vielfältigen, eigentlich kriegsrechtlichen Massnahmen im Kampf gegen den islamistisch motivierten Terror angesehen werden, denn die Botschaft zur Revision übernimmt im Wesentlichen deren Argumentation und Regelungsideen.[23] Gefordert wurden *umfassende Auskunftspflichten* von praktisch allen Behörden und Verwaltungsstellen des Bundes und der Kantone sowie als *zusätzliche Mittel* zur Informationsbeschaffung Befugnisse zur Überwachung des Post- und Fernmeldeverkehrs, zum Beobachten von Personen an nicht allgemein zugänglichen Orten (auch mittels technischen Überwachungsgeräten) sowie zum geheimen Untersu-

---

[13] Vgl. FN 4.

[14] Erst 2008 wurde durch die Fusion des inländischen Staatsschutzdienstes mit dem Auslandsnachrichtendienst ein selbständiges Bundesamt geschaffen (vgl. Art. 2 ZNDG). Zudem verpflichtet Art. 15 Abs. 4 BWIS i.d.F. vom 23. Dezember 2011 jetzt den NDB, «das Informationssystem wird getrennt von den übrigen Informationssystemen der Polizei und der Verwaltung geführt»; das muss wohl für alle vom NDB geführten Datenbanken gemäss Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes (ISV-NDB) vom 4. Dezember 2009 (SR 121.2) gelten.

[15] Erste Teilregelungen der Aufgaben und Befugnisse des *Auslandsnachrichtendienstes* enthalten heute die Art. 1, 4*a* und 4*b* ZNDG, sowie bes. die Art. 11–14 und 20 der Verordnung über den Nachrichtendienst des Bundes (V-NDB) vom 4. Dezember 2009 (SR 121.1) sowie die Verordnung über die elektronische Kriegführung und die Funkaufklärung (VEKF) vom 17. Oktober 2012 (AS 2012, 5527; SR 510.292). Näheres zu den vielfältigen Aktivitäten und Mitteln des Auslandsnachrichtendienstes der Schweiz bei Tatjana Rothenbühler, Völkerrechtliche Aspekte nachrichtendienstlicher Tätigkeit am Beispiel der mit dem Ausland betrauten Dienststellen des Nachrichtendienstes des Bundes (NDB), Diss. Freiburg, Zürich 2012, passim (dazu die Rezension von Reto Müller in Sicherheit & Recht 1/2013, 53 ff.). Spezifisch zu den Rechtsfragen des Einsatzes des Funkaufklärungssystems ONYX: unten FN 41).

[16] Betr. besondere Garantien für die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit sowie das Verbot der Verletzung des Stimm-, Petitions- und Statistikgeheimnisses.

[17] Dazu das Schwerpunktheft EURO 2008, Sicherheit & Recht 3/2008, 1 ff.

[18] Vgl. Botschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Massnahmen gegen Gewaltpropaganda und gegen Gewalt anlässlich von Sportveranstaltungen) vom 17. August 2005 (BBl 2005, 5613 ff.).

[19] AS 2006, 3703 ff.

[20] Vgl. Robert Soos/Christoph Vögeli, BWIS-Massnahmen gegen Gewalt an Sportveranstaltungen: Top oder Flop? Das Rayonverbot und die Meldeauflage in der Praxis, Sicherheit & Recht 3/2008, 156 ff.

[21] Zur Begründung hatte sich der Bundesrat auf die «inhärente Kompetenz» des Bundes berufen, «im Innern und im Äussern die notwendigen Massnahmen zu seinem Schutz bzw. zum Schutz seiner Interessen und Organe zu treffen. Diese Zuständigkeit des Bundes ist im Bestand des gesamtschweizerischen Gemeinwesens als solchem begründet». (Botschaft Ziff. 5.1, BBl 2005, 5637). Wie Fussballrowdies den Bestand des Landes gefährden oder bedrohen können, bleibt offen. Die Mehrheit der Kantone wollte prophylaktisch die Kompetenzen aus diesem Massnahmegesetz vor der EURO 2008. Seither haben sich die Kantone aber auf das Konkordat über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen vom 15. November 2007/2. Februar 2012 (vgl. Webseite der KKJPD/CCDJP/CDDGP) geeinigt. Zu den enormen verfassungs- und kompetenzrechtlichen Problemen des Bundes in der Sicherheitsgesetzgebung *mangels einer Verfassungskompetenz für besondere Polizeiaufgaben* s. Näheres bei Markus H.F. Mohler, Sicherheitsrecht und Rechtssicherheit bei Sportveranstaltungen (staatliche Sicherheitsmassnahmen, Umfang und Grenzen), in: Oliver Arter/Margareta Baddeley (Hrsg.), Sport und Recht, Sicherheit im Sport, Bern 2008, 73 ff., *90 f.* m.w.H.; Ders., Grundzüge des Polizeirechtes der Schweiz, Basel 2012, 73 ff., bes. Rz. 200 ff.; Ders., Ungenügende Polizeibestände, Lösungsansatz unter Respektierung der verfassungsrechtlichen Kompetenzordnung, Sicherheit & Recht 2/2013, 69 ff.; Rainer J. Schweizer, St. Galler Kommentar zur BV, 2. Aufl., Zürich/St. Gallen 2008, Art. 57 BV, Rz. 7 ff.; Ders., Bundesstaatliche Kompetenzverteilung im Polizei- und Sicherheitsrecht, Sicherheit & Recht 3/2012, 185 ff., je mit weiteren Hinweisen.

[22] Botschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) (Besondere Mittel der Informationsbeschaffung) vom 15. Juni 2007 (BBl 2007, 5037 ff.), mit Gesetzesentwurf (BBl 2007 5139 ff.). Näheres bei Müller (FN 8), 443 ff.

[23] In der «Übersicht» zur Botschaft schrieb der Bundesrat: «Die Sicherheits- und Gefahrenlage der Schweiz hat sich in den letzten Jahren namentlich durch die erhöhte Wahrscheinlichkeit von islamistischen Terrorschlägen sukzessive verschlechtert» (BBl 2007, 5038). Die Schweiz hat seit dem Anschlag in Kloten auf eine Maschine der Swissair durch die PFPL von 1969 über Schiessgefechte von Grenzwächtern mit RAF-Terroristen 1977 bis zu Brandanschlägen durch die PKK auf türkische Geschäfte in der Nordwestschweiz 2006/08 eine ganze Reihe von terroristischen Anschlägen erlebt (vgl. Sicherheit Schweiz, Lagebericht 2013 des Nachrichtendienstes des Bundes, Bern 2013, 36 ff.). Allerdings lag die Bewältigung dieser Anschläge durchwegs bei den zuständigen Kriminalpolizeien.

chen von Datenbearbeitungssystemen. Allerdings wurden auch Vorschläge zur Verbesserung des Rechtsschutzes gemacht.[24]

Sowohl in der Vernehmlassung wie in der Bundesversammlung stiessen die Vorschläge auf erhebliche Kritik.[25/26] Nachdem das Parlament mit dem Entscheid des Ständerates als Zweitrat die Vorlage im Frühjahr 2009 unter Auflagen zurückgewiesen hatte,[27] unterbreitete der Bundesrat am 27. Oktober 2010 eine als Übergangslösung bezeichnete, stark verschlankte Vorlage,[28] der die Bundesversammlung mit der Änderung des BWIS vom 23. Dezember 2011 im grossen Ganzen zustimmte.[29] Die wichtigste Neuerung für das Wirken des Nachrichtendienstes des Bundes (NDB) im In- und im Ausland ist die *Ordnung des Einsatzes von «Informantinnen und Informanten»*, inkl. von Massnahmen zu deren Schutz.[30] Damit hatte der ND wieder die Fähigkeit erlangt, welche der Staatsschutz vor der Fichen-Affaire (ohne Gesetzesgrundlage) allzu vielfältig wahrgenommen hatte. Neben dieser sehr heiklen Datenbeschaffungsmethode wurden dem NDB im BWIS neu einige (1997 abgelehnte) *besondere exekutive Kompetenzen* zum Verbot einer terroristischen oder gewalt-extremistischen Propaganda und anderen Tätigkeit (Art. 9)[31], zur Sicherstellung, Beschlagnahme und Einziehung von Propagandamaterial (Art. 13a) sowie zum Einsatz von Dienstwaffen (Art. 5a) eingeräumt.[32]

2. Die Neuausrichtung von 2013

Die *Motive des NDB für die Neuregelung* sind u.a., dass erstens die letzte Revision des BWIS die gewünschten weitreichenden geheimen Datenbeschaffungsmittel nicht gebracht hat, zweitens die Fusion der Dienste zu diversen Schwierigkeiten und Unklarheiten führte und drittens sich der Nachrichtendienst in der fundamental veränderten Welt der heutigen Informations- und Kommunikationsmedien neu positionieren sollte. Nach der Vernehmlassungsvorlage vom 8. März 2013 soll der NDB neu nicht nur wie bisher die demokratischen und rechtsstaatlichen Grundlagen der Schweiz sichern helfen (so Art. 1 BWIS), sondern *auch für Aufgaben zur Wahrung anderer «wesentlicher Landesinteressen»* eingesetzt werden können.[33] Für solche weiteren wesentlichen Landesinteressen ist es dem Bundesrat sogar erlaubt, «in besonderen Lagen» dem NDB besondere Aufträge und zusätzliche Befugnisse von Zwangsmassnahmen, wie Funkaufklärung im Inland[34] sowie Kabelaufklärung einzuräumen.[35] Der Begriff der «besonderen Lagen» ist staatsrechtlich neu und völlig offen; er bildet keinesfalls eine Schwelle wie die «ausserordentlichen Lagen», die nach Art. 58 Abs. 2 BV allein einen Assistenzdienst der Armee rechtfertigen, noch lässt er sich vergleichen mit der «schweren Störung der öffentlichen Ordnung oder der inneren oder äusseren Sicherheit», die allein eine sicherheitspolitische Massnahme des Bundesrates nach Art. 185 Abs. 3 BV rechtfertigt![36]

Richtig besehen werden hier besondere gesetzliche «Notrechtskompetenzen» geschaffen, die der Bundesrat ohne Beachtung der qualifizierten Vorgaben von Art. 184 und 185 sowie von Art. 173 Abs. 1 Bst. a–d BV wahrnehmen können soll. Der NDB soll sich also zum einen um die bisherigen, klassischen Aufgaben des Staats- bzw. Verfassungsschutzes kümmern. Zum anderen soll er sich *neu*, ohne irgend eine Begrenzung, auch mit den «Angriffen auf kritische Informations-, Kommunikations-, Energie-, Transport- und weitere Infrastrukturen, die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind (kritische Infrastrukturen)» sowie mit nicht bestimmten weiteren, ihm vom Bundesrat zugewiesenen Aufträgen befassen. Während das BWIS bisher den Zweck verfolgt, *gegenüber spezifischen Bedrohungen* die Grundlagen der demokratischen Verfassungsordnung der Schweiz zu sichern und die Freiheitsrechte der Bevölkerung zu schützen, soll der NDB inskünftig *generell* «zur Wahrung der Handlungsfähigkeit der Schweiz» und «weiterer wesentlicher Landesinteressen» Informationen beschaffen und bearbeiten können.[37]

---

[24] Vgl. namentlich Art. 13*b* Entwurf Änderung BWIS von 2007 (BBl 2007 5141) sowie Art. 13*b* BWIS i.d.F. vom 23. Dezember 2011.

[25] Der bundesrätliche Entwurf wurde 2009 eingehend begutachtet: Giovanni Biaggini, Verfassungsrechtliche Abklärung betreffend die Teilrevision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Vorlage «BWIS»), in: VPB 4/2009 Nr. 14, 238–330. Namentlich bei den geheimen Beschaffungsmitteln stellte Biaggini erheblichen Nachbesserungsbedarf fest: 258 ff., bes. 282/283.

[26] Vgl. z.B. Lucien Müller/Nina Widmer/Rainer J. Schweizer, Staatsschutzgesetzgebung auf Abwegen, Zur Reform des Bundesgesetzes zur Wahrung der inneren Sicherheit, NZZ, Nr. 294 vom 16. Dezember 2008, 15.

[27] Entscheid des Nationalrates vom 17. Dezember 2008 und des Ständerates vom 3. März 2009, vgl. AB S 2009, 19 ff.

[28] Siehe Zusatzbotschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit («BWIS II reduziert») vom 27. Oktober 2010 (BBl 2010, 7841 ff.) mit Gesetzesentwurf (BBl 2010, 7895 ff.).

[29] Siehe BBl 2012, 91 ff.

[30] Vgl. Art. 14*b* und bezüglich der Tarnidentitäten Art. 14*c* BWIS sowie Art. 7 ZNDG.

[31] Dazu Biaggini (FN 25), VPB 4/2009 Nr. 14, 284 ff.

[32] Vgl. Art. 14*a*–14*e* V-NDB. Unklar ist, nach welchen Regeln sich der Gebrauch der verschiedenen zugelassenen Waffen, der auf Notwehr und Notstand beschränkt ist (Art. 5*a* Abs. 2 BWIS), richtet ; vermutlich nach dem Bundesgesetz über die Anwendung polizeilichen Zwangs und polizeilicher Massnahmen im Zuständigkeitsbereich des Bundes (Zwangsanwendungsgesetz, ZAG) vom 20. März 2008 (SR 364) und der Verordnung über die Anwendung polizeilichen Zwangs und polizeilicher Massnahmen im Zuständigkeitsbereich des Bundes (Zwangsanwendungsverordnung, ZAV) vom 12. November 2008 (SR 364.3).

[33] Dazu zählen etwa nach Art. 1 Abs. 2 Bst. c Entwurf NDG, Handlungsfähigkeit der Schweiz zu unterstützen, sowie nach Art. 1 Abs. 3 in besonderen Lagen etwa «die Unterstützung der schweizerischen Aussenpolitik und der Schutz des Werk-, Wirtschafts- und Finanzplatzes Schweiz» (sic!).

[34] Die bisher mindestens auf Verordnungsstufe ausgeschlossen ist: vgl. Art. 5 VEKF (FN 15).

[35] Vgl. bes. Art. 1 Abs. 3, Art. 4 Abs. 1 Bst. b, c. und d, sowie Art. 62 i.V.m. Art. 33 Abs. 2 Bst. b und Art. 34–38, Entwurf NDG.

[36] Vgl. Mohler, Grundzüge (FN 21), 240 ff. Rz. 733 ff.; Schweizer, Bundesstaatliche Kompetenzverteilung (FN 21), 190/191.

[37] So Art. 4 Abs. 1 Entwurf Nachrichtendienstgesetz (NDG) vom 8. März 2013.

Neben der Festlegung des sachlichen Aufgabenbereichs ist entscheidend, welche Befugnisse zur Informationsbeschaffung und -verarbeitung der NDB zukünftig haben soll. Geplant ist, dass der NDB ähnlich wie heute schon Meldungen zahlreicher Behörden und selbstverständlich alle öffentlichen Medien nutzen soll, aber auch «menschliche Quellen» – wie geheime Informanten oder private Anzeiger abschöpfen (HUMINT, Human Intelligence genannt)[38] – sowie von vielen öffentlichen, ja sogar von privaten Stellen mit Sicherheitsaufgaben spezielle Auskünfte verlangen kann. Am wichtigsten ist aber, dass der NDB *neu geheime Zwangsmassnahmen*, vom Abhören von Wohnungen, über die Auswertung von GPS bis zum Eindringen in Computersysteme (sog. Trojaner)[39] oder zum Eindringen in Räumlichkeiten, einsetzen können soll (vgl. die Grafik S. 135).[40] Dazu braucht es allerdings eine Genehmigung einer Abteilungspräsidentin oder eines Abteilungspräsidenten des Bundesverwaltungsgerichts sowie die Unterrichtung des Sicherheitsausschusses des Bundesrates und die Zustimmung der Chefin oder des Chefs des VBS.[41] Zudem soll eine solche geheime Beschaffungsmassnahme – diverse Ausnahmen vorbehalten – der betroffenen Person nachträglich mitgeteilt werden, die dann ein Beschwerderecht hat.[42] Der die offene Demokratie schützende Art. 3 BWIS wird allerdings nur in verkürzter Form im NDG weiterbestehen.[43]

All diese Instrumente soll der NDB *auch gegen Personen und Organisationen im Ausland nutzen* können. Dazu zählen namentlich besondere, im Nachrichtendienstwesen verbreitete Kompetenzen für Eingriffe in die Telekommunikation, so mittels der schon bestehenden Funkaufklärung (COMINT Communication Intelligence)[44] und *neu* mittels der Kabelaufklärung (ELINT Electronic Intelligence)[45]. Indessen sind für diese Aktivitäten (abgesehen von der Kabelaufklärung in der Schweiz über Vorgänge im Ausland) keine gerichtliche Genehmigung, keine nachträgliche Mitteilung und kein Rechtsschutz vorgesehen.[46]

3. Zu den Problemen dieser Neuausrichtung

3.1 Das Fehlen einer verfassungsrechtlichen Grundlage

Ein Staatsschutz- und Nachrichtendienstgesetz braucht primär eine verfassungsrechtliche Grundlage. Eine solche *fehlt heute*, wie der Bundesrat im Bericht zum Postulat *Malama* vom März 2012 festgehalten hat.[47] Der Bericht zum Vernehmlassungsentwurf verschweigt das Problem. Der Bundesrat kommt nicht darum herum, einen Verfassungsartikel vorzulegen, der dem Nachrichtendienst die *unerlässliche Legitimation* gibt.[48] Auf Verfassungsstufe müssen Volk und Stände entscheiden, ob der ND wie bisher mit geheimen präventiven Informationstätigkeiten die Verfassungsordnung der Schweiz und die Freiheiten und Grundrechte der Bevölkerung in klaren Grenzen und unter besonderen Kontrollen bewahren helfen soll, oder ob wir einen präventiv und geheim tätigen Nachrichtendienst einrichten wollen, der mit sehr weit gehenden, teilweise exekutivpolizeilichen Befugnissen der Informationsbeschaffung und -verbreitung generell die Handlungsfähigkeit der Schweiz und wesentliche Landesinteressen wahren soll. Auf Stufe der BV sind zudem in Grundzügen auch die Kooperation des NDB mit den kantonalen Polizeidiensten und die bisher immer wieder strittigen Aufsichtsbefugnisse der Kantone zu klären.[49]

3.2 Die Entwicklung des übrigen Sicherheitsrechts des Bundes

Eine Totalrevision des Staatsschutzgesetzes mit der vom NDB seit 2007 gewünschten ausserordentlichen Ausweitung der Aufgaben und Eingriffsmittel muss die

[38] Art. 13 Entwurf NDG; Näheres zu HUMINT bei Rothenbühler (FN 15), 129 ff.

[39] Soweit es um elektronische Kommunikation geht, soll technisch der Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF) im Eidg. Justiz- und Polizeidepartement (EJPD) eingesetzt werden.

[40] Art. 22 ff. Entwurf NDG.

[41] Art. 25–27 Entwurf NDG.

[42] Art. 29 und Art. 71 Entwurf NDG.

[43] Art. 3 Abs. 5 Entwurf NDG.

[44] Art. 5*a* ZNDG, neu Art. 33 Entwurf NDG. Die Funkaufklärung wird durch das Organ Führungsunterstützungsbasis (FUB) – Zentrum elektronische Operationen (ZEO) innerhalb der Armee betrieben. Näheres zu COMINT bei Rothenbühler (FN 15), 146 ff. Zu verfassungs- und völkerrechtlichen Fragen der Funkaufklärung: Bundesamt für Justiz (BJ), Rechtliche Grundlagen der elektronischen Aufklärung, (nicht publiziertes) Gutachten vom 24. April 2003; Bundesamt für Justiz (BJ),Vereinbarkeit der Kommunikationserfassung im Ausland mit der Europäischen Menschenrechtskonvention (EMRK), (nicht publiziertes) Gutachten vom 31. August 2004; sowie Geschäftsprüfungsdelegation der Eidgenössischen Räte, Rechtmässigkeit und Wirksamkeit des Funkaufklärungssystem «ONYX», Bericht vom 9. November 2007 (BBl 2008, 2545 ff.); insbesondere zur Blankettdelegation der Regelung der Funkaufklärung an den Bundesrat vgl. Stéphane Bondallaz, La protection des personnes et de leurs données, Diss. Fribourg, Zurich/Bâle/Genève 2007, 526; sowie bes. Biaggini (FN 25), VPB 4/2009 Nr. 14, 296 ff.

[45] Siehe Art. 34–38 Entwurf NDG.

[46] Vgl. Art. 32 sowie für die Informationsweitergabe ins Ausland Art. 56 Entwurf NDG.

[47] Bericht des Bundesrates in Erfüllung des Postulats *Malama* 10.3045 vom 3.März 2010 Innere Sicherheit. Klärung der Kompetenzen, BBl 2012 4455 ff., 4499.

[48] Ich habe bei den Vorbereitungen zum BWIS die Meinung vertreten, eine strikt auf zentrale Vorkehren für die Sicherung der bundesverfassungsrechtlichen Ordnung konzentrierte Präventivpolizei könnte auf stillschweigende, inhärente Kompetenzen des Bundes abgestützt werden. Doch die zahlreichen Ausweitungen der Tätigkeiten der Staatsschutzdienste in Bund und Kantonen haben gezeigt, dass diese Annahme irrig war. Vgl. Rainer J. Schweizer, Notwendigkeit und Grenzen einer gesetzlichen Regelung des Staatsschutzes, ZBl 1991, 285–309. Markus H.F. Mohler, Vernetzung von Sicherheit, in: Rainer J. Schweizer (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, (SBVR Bd, III/1), Basel 2008, 521 ff., Rz. 60. Ebenso wäre es falsch, das Staatsschutzgesetz auf Art. 57 BV abstützen zu wollen, der nach einhelliger Rechtsauffassung keine Bundespolizeikompetenzen begründet (vgl. oben FN 21).

[49] Vgl. Markus H.F. Mohler, Staatsschutz braucht klare Regeln, digma 2009.2, 60 ff.; Markus Schefer/Reto Müller, Schutz der inneren Sicherheit – historische Entwicklung und aktuelle Fragestellungen, Sicherheit & Recht 2010 2, 57–71; Markus Müller/Christoph Jenni, Kantonale Aufsicht über die Staatsschutztätigkeit, ZBl 113/2012, 2–20.

Veränderungen des sicherheitsrechtlichen Umfeldes im Blick haben. Hier sollen *nur Stichworte* genannt werden: Die Staatsanwaltschaften und Kriminalpolizeidienste sind erst daran, ihre Erfahrungen mit dem neuen Prozessrecht zu evaluieren; eine Revision der StPO in wichtigen Punkten zeichnet sich aber schon ab. Zudem ist in den vergangenen Jahren die Strafbarkeit von Vorbereitungshandlungen weiter ausgebaut worden,[50] und es werden zu Gunsten der Strafverfolgungsbehörden neue besondere Eingriffsbefugnisse, wie der Einsatz von Trojanern, normiert.[51] Eine *Verschiebung von Strafverfolgungsaufgaben* auf den NDB ist m.E. weder angezeigt noch wäre sie wegen der fehlenden Verteidigungsrechte verfassungs- und völkerrechtlich haltbar. Seit 2008 wird zudem ein wesentlicher Teil jedenfalls der grenzüberschreitenden kriminal- und sicherheitspolizeilichen Aufgaben der Kantone und des Bundes *im Rahmen und nach den Regeln des Schengenrechts*[52] *einschliesslich des europäischen Datenschutzrechts*[53] und unter Nutzung weiterer Instrumente der EU wie Europol[54] abgewickelt. Gerade in den Bereichen des Kampfes gegen organisierte Kriminalität, gewalttätigen Extremismus und Terrorismus, aber auch im Kampf gegen Cyber-Crime arbeiten die Kriminalpolizeidienste von Bund und Kantonen intensiv im europäischen Verbund[55]. Wie weit kann und darf hier eine nationale Sondereinheit wie der NDB nach Schweizer Sonderrecht weitgehend geheim tätig werden? Sodann wurden auch neue Instrumente des «Staats-Schutzes» beschlossen.[56] Nicht zuletzt muss auch aktiv auf andere sachliche Bedürfnisse geachtet werden, etwa bezüglich der Stärkung der Massnahmen zum Schutz vor Cyber-Risiken, z.B. mittels die Melde- und Analysestelle für Informationssicherung (Melani) des Bundes.[57]

Zu bedenken ist immer auch der *laufende Wertewandel*: Ein Beispiel: Auf den für den Staatsschutz zentralen Zwölften Titel des StGB über Verbrechen und Vergehen gegen den öffentlichen Frieden folgen jetzt seit 2010 der Zwölfte Titel^{bis} über Völkermord und Verbrechen gegen die Menschlichkeit, der Zwölfte Titel^{ter} über Kriegsverbrechen, zu denen noch gemeinsame Bestimmungen im Zwölften Titel^{quater} kommen (Art. 264–264m StGB).[58] Für deren Durchsetzung wären z.B. auch mehr polizeiliche und staatsanwaltschaftliche Mittel notwendig; dass sich der NDB dieser Bedrohungen auch annimmt, ist nicht bekannt.

3.3 Die Weite des Aufgabenbereichs

Der enorm breite Aufgabenbereich wird (sofern die personellen Ressourcen ausreichen) dazu führen, dass nachrichtendienstliche *Eingriffe für zahlreiche behördliche Anliegen weit über den Staatsschutz hinaus möglich* werden. Zu Recht kritisiert Markus H. F. Mohler, dass das Gesetz eigentlich ein Gesetz über besondere Methoden (bzw. Informationstätigkeiten) sei, aber keine *klare Zweckbindung und Zweckbegrenzung mehr* kenne.[59] Vor einer solchen Ausweitung der Aktionsfelder muss sich der Gesetzgeber fragen, ob denn nicht schon viele andere Instanzen von Bund und Kantonen – von diversen technischen Sicherheitsbehörden über das Eidgenössische Departement für auswärtige Angelegenheiten (EDA), über die Bundeskriminalpolizei und das Grenzwachtkorps bis zu den kantonalen Polizeikorps und zur Militärischen Sicherheit der Armee – solche Gefahren ermitteln und verhüten müssen.

---

[50] Siehe Art. 182, Art. 226ter, Ergänzungen von Art. 260bis oder Art. 271 Ziff. 3 StGB.

[51] Zum Stand der Diskussion siehe: Olivier Jotterand/Jérémie Müller/Jean Treccani, L'utilisation du cheval de Troie comme mesure de suveillance secrète, Jusletter 21. Mai 2012; Sylvain Métille, Mesures techniques de surveillance et respect des droits fondamentaux en particulier dans le cadre de l'instruction pénale et du renseignement, thèse Neuchâtel 2010, Bâle/Neuchâtel 2011, 153.

[52] Siehe z.B. Stephan Breitenmoser, Die Grundlagen der polizeilichen Zusammenarbeit im Rahmen von Schengen, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen in der Praxis, Zürich/St. Gallen/Wien/Baden-Baden 2009, 25 ff.; Adrian Lobsiger, Die Umsetzung der Weiterentwicklungen des Schengen-Besitzstandes im schweizerischen Recht unter besonderer Berücksichtigung der polizeilichen Amtshilfe, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen und Dublin in der Praxis, Weiterentwicklungen der Rechtsgrundlagen, Zürich/St. Gallen/Baden-Baden 2010, 187 ff.; Markus H.F. Mohler, Polizeiliche Zusammenarbeit Schweiz – EU, eine Annäherung, Sicherheit & Recht, 3/2013, 135, sowie Reinhard Mokros, Polizeihandeln auf Ebene der Europäischen Union, in: Hans Lisken/Erhard Denninger, Handbuch des Polizeirechts, 5. Aufl., hrsg. von Erhard Denninger und Frederik Rachor, 1407 ff., zum Schengenrecht: 1430 ff., zum Polizeihandeln in einem anderen EU- bzw. Schengen-Mitgliedstaat: 1445 ff., zum Polizeihandeln für einen anderen Schengen-Mitgliedstaat: 1461 ff.

[53] Dazu etwa Beat Rudin/Sandra Stämpfli, Datenschutzrechtliche Weiterentwicklungen – neue Herausforderungen, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen und Dublin in der Praxis, Zürich/St. Gallen/Baden-Baden 2010, 197 ff.; Caroline Gloor Scheidegger, Datenschutz und Rechtsschutz bei SIS, Eurodac und VIS, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Rechtsschutz bei Schengen und Dublin, Zürich/St. Gallen/Baden-Baden 2013, 119 ff.

[54] Siehe Abkommen zwischen der Schweizerischen Eidgenossenschaft und dem Europäischen Polizeiamt (mit Anhängen) vom 14. September 2004 (SR 0.362.2). Mohler (FN 52); Mokros (FN 52), 1416 ff.

[55] Der NDB hat seit dem 29. Juni 2011 die Befugnis, Europoldatenbanken abzufragen, vgl. Briefwechsel vom 27. April und 29. Juni 2011 zwischen der Schweizerischen Eidgenossenschaft und Europol betreffend Änderung von Anhang II des Abkommens vom 24. September 2004 zwischen der Schweizerischen Eidgenossenschaft und dem Europäischen Polizeiamt, AS 2012 407 ff. (nicht in der SR).

[56] Z.B. das Bundesgesetz über die Wahrung von Demokratie, Rechtsstaat und Handlungsfähigkeit in ausserordentlichen Lagen vom 17. Dezember 2010, eine Paketregelung (AS 2011 1381–1384).

[57] Vgl. Bericht des Bundesrates «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» vom 27. Juni 2012, BBl 2013, 563 ff.; dazu z.B. Alexander Frei, Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken, Sicherheit & Recht 1/2013, 38 ff.

[58] Vgl. Bundesgesetz über die Änderung von Bundesgesetzen zur Umsetzung des Römer Statuts des Internationalen Strafgerichtshofs vom 18. Juni 2010, in Kraft seit 1. Jan. 2011 (AS 2010 4963; BBl 2008 3863).

[59] Mitteilung von Markus H.F. Mohler an den Verfasser vom 1. November 2013. Entsprechend hält er auch den Titel für unzutreffend. Der jetzige Titel BWIS sei von der notwendigen Bestimmtheit her besser. Das geplante NDG ist kein «Nachrichtendienstgesetz» mehr, sondern ein Gesetz über geheime Informationstätigkeiten im Bundesinteresse.

3.4 Die Konkurrenzen mit den Strafverfolgungsorganen

Vor allem dürfte sich mit der Ausweitung des Tätigkeitsfeldes, etwa beim Schutz kritischer Infrastrukturen, sehr *heikle und fragwürdige Konkurrenzen mit den Organen der Strafverfolgung* ergeben, die z.B. heute schon einen Schwerpunkt in der Bekämpfung der organisierten Kriminalität setzen.[60] Die Strafverfolgungsbehörden von Bund und Kantonen haben im Übrigen nach der StPO und nach Europa- und Völkerrecht sehr viel bestimmtere und genauer festgelegte geheime Beschaffungskompetenzen (vgl. namentlich Art. 269–298 StPO), als sie jetzt für den NDB normiert werden sollen.[61] Die Konkurrenzen zur polizeilichen Ermittlung und staatsanwaltlichen Untersuchung, welche durch die bestehenden und die neu erweiterten gesetzlichen Auskunftspflichten der Strafverfolgungsbehörden noch aggraviert werden,[62] führen unweigerlich zu bundesstaatlich-kompetenziellen Schwierigkeiten[63] und vor allem zu Einbussen beim Rechtsschutz der verdächtigten Personen.[64] Zudem wird das bisherige Trenngebot zwischen der nachrichtendienstlichen und der strafprozessual geregelten Informationsbeschaffung übergangen.

3.5 Die Rechtsprobleme der Auslandseinsätze

Seine Instrumente kann der NDB (wie gesagt) grundsätzlich *auch* gegen Personen und Organisationen *im Ausland* nutzen. Indessen sind dafür praktisch keine innerstaatlichen Rechtskontrollen vorgesehen,[65] und die völkerrechtlichen Beschränkungen konzentrieren sich auf vereinzelte Verträge zum Schutz klassifizierter Informationen (wie sie z.B. mit Österreich, Belgien und Australien bestehen) und Absprachen zum Quellenschutz.[66] Auch wenn nachrichtendienstliches Handeln im Ausland international akzeptiert (jedoch in allen Staaten selbstverständlich strafbar, vgl. Art. 272–274, 301 StGB[67]) ist, so ist es doch *keinesfalls rechtsfrei*. Nicht nur das Strafgesetzbuch, sondern vor allem das Völkerrecht macht die Schweiz namentlich für eine Missachtung des Interventionsverbotes durch sicherheitspolizeiliche (extraterritoriale) Zwangsmassnahmen[68] sowie für ein menschenrechtswidriges Handeln im Ausland, z.B. ein illegales Eindringen eines schweizerischen Agenten oder mandatierten Informanten in eine Wohnung[69], *verantwortlich*[70]. Die betroffenen Personen im Ausland müssen von der Schweiz, wenn diese in eine Rechtsverletzung involviert ist, dieselben Garantien erhalten wie die Menschen im Inland.[71] Zudem haben

---

[60] Vgl. für den Bund z.B. die Leistungen der Zentralstelle für die Bekämpfung des organisierten Verbrechens nach Art. 7 *f.* Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes (ZentG) vom 7. Oktober 1994 (SR 360).

[61] Näheres z.B. bei Alberto Fabri, Geheime Beweiserhebung in der Schweiz im Rahmen der internationalen Strafrechtskompetenzen, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Rechtsschutz bei Schengen und Dublin, Zürich/St. Gallen/Baden-Baden 2013, 39–66.

[62] Siehe Art. 13*a* BWIS sowie Art. 17–19 Entwurf NDG.

[63] Wie das heute z.B. auf so bestürzende Art und Weise beim ausgeweiteten polizeilichen Einsatz des Grenzwachtkorps (GWK) sichtbar wird: Siehe Rainer J. Schweizer/Markus H.F. Mohler, Die polizeilichen Ausgleichsmassnahmen des Bundes und der Kantone nach dem Wegfall der Personenkontrollen an der Landesgrenze in verfassungsrechtlicher Sicht, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen in der Praxis, Erfahrungen und Ausblicke, Zürich/St. Gallen/Wien/Baden-Baden 2009, 111 ff.; sowie zur geplanten Ausdehnung der polizeilichen Befugnisse des GWK durch die 2013 geplante Zollgesetznovelle (Vernehmlassungsvorlage vom 13. Juli 2013): Markus H.F. Mohler, Ungenügende Polizeibestände. Lösungsansätze unter Respektierung der verfassungsrechtlichen Kompetenzordnung, Sicherheit & Recht 2/2013, 62, 68 ff. und bes. 75 ff.

[64] Vgl. die kritischen Feststellungen von Biaggini (FN 25), VPB 4/2009 Nr. 14, 291 ff. Allfällige Verletzungen völkerrechtlicher Vertragspflichten sind fallweise zu beurteilen.

[65] Wie oben gesagt, sind keine gerichtliche Genehmigung, keine Pflicht zur nachträglichen Mitteilung und kein Rechtsschutz vorgesehen.

[66] Vgl. Bundesamt für Justiz und Direktion für Völkerrecht, Rechtliche Einschränkungen im Austausch von Informationen ausländischer Nachrichtendienste zwischen dem DAP und dem SND, Gutachten vom 22. Dezember 2006, VPB 2007.3.1, 76–97.

[67] Siehe Günther Stratenwerth/Felix Bommer, Schweizerisches Strafrecht, Besonderer Teil II, Straftaten gegen Gemeininteressen, 6. Aufl., Bern 2008, 282 ff., 332 ff.; Gutachten des Bundesamtes für Justiz und der Direktion für Völkerrecht vom 10. März 2009, Rechtsgrundlage für Computernetzwerkoperationen durch Dienststellen des VBS, VBP 2009, 10a, 141 ff. bes. 160 ff.

[68] Siehe Horst Fischer, Friedenssicherung und friedliche Streitbeilegung, in: Knut Ipsen (Hrsg.), Völkerrecht, 5. Aufl., München 2004, § 59 Gewaltverbot, Selbstverteidigungsrecht und Intervention im gegenwärtigen Völkerrecht, Rz. 50 ff.; Andreas R. Ziegler, Einführung in das Völkerrecht, 2. Aufl., Bern 2011 Rz. 617 ff.; Matthias Herdegen, Völkerrecht, 12. Aufl., München 2013, § 35, 265 ff.; Christoph Gusy, Spionage im Völkerrecht, in: Neue Zeitschrift für Wehrrecht, 26/1984, 187 ff., bes. 192 ff.; Salish Sule, Völkerrechtliche, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtschaftsspionage, Diss. Saarbrücken, Baden-Baden 2006, 72 ff.; Rothenbühler (FN 15), 172 ff. m.w.H.

[69] Oder der Mitwirkung eines Agenten oder mandatierten Informanten an einer illegalen Beweisbeschaffung, Festnahme, Befragung oder einer der Folter ähnlichen, erniedrigenden Behandlung; vgl. EGMR-Urteile in FN 71.

[70] Namentlich zur extraterritorialen Verantwortlichkeit bei Menschenrechtsverletzungen vgl. Franz Matscher, Bemerkungen zur extraterritorialen oder indirekten Wirkung der EMRK, in: FS für *Stefan Trechsel*, Zürich 2002, 25 ff.; N. Karagiannis, Le territoire d'application de la Convention européenne des droits de l'homme, RTDH 2005, 33 ff.; Rothenbühler (FN 15),184 ff.; Christoph Grabenwarter/Katharina Papel, Europäische Menschenrechtskonvention, 5. Aufl., München/Basel/Wien, 2012, § 17 Rz. 13 ff.; in diesem Zusammenhang vgl. Andreas Felder, Die Beihilfe im Recht der völkerrechtlichen Staatenverantwortlichkeit, Zürich/Basel/Genf 2007, Rz. 127 ff. Eine Verpflichtung nach EMRK besteht für einen Staat auch dann, wenn Personen und Personengruppen unter dessen Gewalt und Kontrolle («authority and control») stehen: s. EGMR *Al-Saadoon u. Mufdhi gegen UK*, Nr. 61498/08 (2010); EGMR *Al-Skeini u.a. gegen UK*, Nr. 55721/07 (2011), Ziff. 135 (Grosse Kammer); EGMR *Medvedyev u.a.gegen France*, Nr. 3394/03 (2009).

[71] Leitentscheide sind die Urteile des EGMR in der *Soering*-Rechtsprechung: EGMR *Soering gegen Vereinigtes Königreich*, Nr. 14038/88 (1989) und Folgeentscheide, z.B. EGMR *Chahal gegen Vereinigtes Königreich*, Nr. 22414/93 (1996), Ziff. 73 f., 79 ff. u.a.m. Weitere Hinweise zur Rechtsprechung und Literatur z.B. bei Stephan Breitenmoser/Robert Weyeneth, Rechtsschutz bei der Polizeizusammenarbeit, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen und Dublin in der Praxis – Weiterentwicklung der Rechtsgrundlage, Zürich/St. Gallen/Baden-Baden 2010, 155, 176 ff.; Rainer J. Schweizer, Anforderungen der EGMR-Rechtsprechung an die in-

schweizerische Vertretungen im Ausland die besonderen völkerrechtlichen Pflichten des diplomatischen und konsularischen Personals zu beachten, weshalb z.B. ein Abhören von einer Botschaft aus völkerrechtswidrig ist.[72]

Es ist *gewiss ein erheblicher rechtsstaatlicher Fortschritt*, wenn jetzt die Auslandstätigkeiten des NDB aus dem Klandestinen ins Gesetz überführt werden. Selbstverständlich kann der NDB einen breiten Informationsaustausch mit verschiedensten Sicherheitsbehörden im Ausland pflegen. Dieser Austausch mit dem Ausland ist in der Regel bloss von der Nützlichkeit bestimmt; vorbehalten bleiben zwischenstaatliche oder multinationale Vereinbarungen (zu deren Abschluss jetzt der Bundesrat eine spezielle Ermächtigung bekommen soll),[73] in denen die Zusammenarbeit unter den Partnerdiensten spezifiziert wird. Doch das Rechtsproblem ist, dass der NDB bei diesem grenzüberschreitenden Informationsaustausch von personenbezogenen Daten über allfällige «Gefährder» sich weder an die Gesetze und Verträge über die Amts- und Rechtshilfe noch an das den Datenschutz (DSG)[74] gebunden sieht, weil nach herrschender Auffassung angeblich die Lex specialis des BWIS bzw. NDG sowie die «Gewohnheiten» der Geheimdienste vorgehen. Das BWIS enthält in Art. 17 Abs. 4 eine gewisse Schranke für die Weitergabe von Personendaten ins Ausland,[75] denn es ist offensichtlich, dass der NDB bei Informationsaustauschen unter Diensten in Kollision geraten kann mit Pflichten aus Menschenrechtspakten (z.B. wegen Verletzung der Unschuldsvermutung durch eine diffamierende Mitteilung[76]). Allerdings wird der Schutz von Personen vor Verfolgung und Bestrafung wegen ihrer politischen Anschauungen oder aus Gründen der Zugehörigkeit zu bestimmten sozialen, religiösen oder ethnischen Gruppen, wie es das Rechtshilferecht verlangt, zu Unrecht *nicht gewährleistet*.[77] Der freie, oft nicht nachkontrollierbare Informationsaustausch mit dem Ausland führt unvermeidlich zu einer Konkurrenz mit den Strafverfolgungs- und Gerichtsbehörden, die an strikte bundesgesetzliche und völkerrechtliche Vorschriften der polizeilichen Amtshilfe und justiziellen Strafrechtshilfe gebunden sind, und er kann so deren richterliche Unabhängigkeit konterkarieren bzw. beeinträchtigen.[78] Eine Beschränkung auf die Kernaufgaben des Staatsschutzes würde diese Konflikte mindestens reduzieren.

III. Der totale Zugriff der IT-Unternehmen und der Staaten auf elektronische Kommunikation

Gleichzeitig mit der Mitteilung des Bundesrates vom 23. Oktober 2013, dass eine Botschaft für ein neues NDG ausgearbeitet werden soll, erfuhr die Öffentlichkeit, was ansatzweise seit dem Juni 2013 vor allem durch die Enthüllungen des US-Bürgers *Snowden* bekannt geworden war, dass die US-amerikanischen Geheimdienste NSA und CIA sowie der britische Geheimdienst GCHQ, mit denen der Nachrichtendienst des Bundes (mindestens was die CIA betrifft) regelmässig zusammenarbeitet, nicht nur systematisch die UN-Behörden und die ausländischen Missionen bei der UN in Genf, sondern auch[79] die Telefongespräche des Bundesrates sowie von unzähligen Bewohner auch unseres Landes abgehört hätten. Die weltweiten massiven Abhör- und Spionagetätigkeiten der USA und den mit dieser verbundenen Staaten Vereinigtes Königreich, Kanada, Australien und Neuseeland erfassen die Mail-, Internet-, Handy- und Telefon-Kommunikation von Behörden der UN und der EU, vieler befreundeter Staaten, zahlreicher wichtiger Wirtschaftsbereiche sowie Millionen von Menschen in der Schweiz und anderswo in Europa, ganz abgesehen von Institutionen, Unternehmen oder Personen von Staaten anderer Kontinente. Die Aktivitäten der Geheimdienste beruhen wesentlich auf der (behaupteten) «Zusammenarbeit» mit den grossen US-amerikanischen IT-Unternehmen wie Microsoft, Google, Yahoo, Apple, AOL oder Facebook im Spähprogramm «Prism» sowie auf illegalen, massiven Eingriffen der Geheimdienste mit dem Programm «Muscular» in den Datenverkehr zwischen den weltweit verteilten Servern dieser und zahlreicher weiterer Unternehmen. Dabei werden aus den Unternehmensservern und -verbindungen Millionenfach Metadaten der Verbindungen der Kunden, aber auch Einzelinformationen namentlich der weltweiten, Internet-gestützten Kommunikation bezogen. Darüber setzt die NSA z.B. auch automatische Hacker-Systeme ein, namentlich das System FoxAcyd, das ihr heimlich mit massgeschneiderten Methoden Zugang zu fremden Rechnern, Routern und Datenbeständen verschafft. Schliesslich lassen sich die Geheimdienste massenhaft geheim gewonnene Kommunikationsdaten von den befreundeten Diensten liefern.

---

ternationale Amts- und Rechtshilfe. Im Kontext eines europäischen Paradigmenwechsels, in: FS für *Ivo Schwander*, Zürich 2012, 998 ff.

[72] Vgl. Art. 41 Wiener Übereinkommen über diplomatische Beziehungen, abgeschlossen am 18. April 1961, SR 0.191.01; Art. 55 Wiener Übereinkommen über die konsularischen Beziehungen vom 24. April 1963, SR 0.191.02.; dazu Avis de droit de la Direction du droit international public du 5 juin 2013, VPB 68.138; Entscheid des Bundesrates vom 14. August 1991, VPB 56.33; Michael Richtsteig, Wiener Übereinkommen über diplomatische und konsularische Beziehungen, Entstehungsgeschichte, Kommentierung, Praxis, 2. Aufl., Baden-Baden 2010, 211 ff.; Niklas Wagner/Holger Rausch/Thomas Pröpstl, Wiener Übereinkommen über konsularische Beziehungen vom 24. April 1963, Kommentar für die Praxis, Berlin 2007, 371 ff., bes. 378 ff.

[73] Siehe Art. 61 Abs. 3 Entwurf NDG.

[74] Vom 19. Juni 1992 (SR 235.1) an.

[75] Ebenso lautet Art. 56 Abs. 3 Entwurf NDG. Die Bestimmung lehnt sich an Art. 2 Bst. a Bundesgesetz über die internationale Rechtshilfe in Strafsachen (IRSG) vom 20. März 1981 (SR 351.1) zu.

[76] Vgl. EGMR *Ismoilov und andere gegen Russland*. Nr. 2947/06 (2008), Ziff. 165 ff.: betr. Verletzung von Art. 6 Abs. 2 EMRK durch einen vorverurteilenden Auslieferungsentscheid.

[77] Vgl. Art. 2 Bst. b und c sowie Art. 3 Abs. 1 und 2 IRSG.

[78] Vgl. zur richterlichen Unabhängigkeit der entscheidenden Staatsanwaltschaft z.B. BGer 1B_69/2013, Urteil vom 27. Juni 2013; Hans Wiprächtiger, Allgemeine Grundsätze, in: Marianne Heer (Hrsg.), Schweizerische Strafprozessordnung und Schweizerische Jugendstrafprozessordnung, Bern 2010, 72 f.

[79] Gemäss Mitteilung des Chefs NDB.

Zu beachten ist aber auch, dass die weltweit tätigen IT-Unternehmen der USA, von Kanada oder China ihrerseits ihre enormen Geschäfte ganz wesentlich auf den informationellen Auswertungen z.B. von heimlich abgeschöpften Nutzerdaten aufgebaut haben, ja dass sie sogar durch ihre Software die Nutzer zur persönlichkeitsmissachtenden Datenbekanntgabe verleiten, um damit sich und den Werbeindustrien Geschäfte zu ermöglichen. Mit Fug und Recht spricht der schleswigholsteinische Datenschutzbeauftragte davon, dass etwa Facebook «Datenschutzverstoss als Geschäftsmodell» pflege,[80] namentlich durch die systematische Auswertung und Weitergabe an beliebige Dritte und Bewerbung der persönlichen Datenbearbeitungen ohne Einwilligung der Benutzerin oder des Benutzers. Die grossen US-Technologieunternehmen, die heute die illegale Datenbeschaffung durch die NSA beklagen, haben auch bedenkenlos massgeblich in Zusammenarbeit mit den US-Militär- und sonstigen US-Sicherheitsbehörden die Verschlüsselungs- und die Spionagesoftware entwickelt. Die Potenz insbesondere der US-Nachrichtendienste entspricht der Präpotenz der US-IT-Firmen, die für ihre eigenen Geschäftsinteressen seit vielen Jahren die Auswertung der digitalen Kommunikation vorangetrieben haben und weiterhin massiv zu Lasten der kommunizierenden Personen, Unternehmen oder staatlichen Stellen ausnutzen.

IV. Die Grundlagen der internationalen digitalen Kommunikation sind schwer gestört

1. Ein völliger Vertrauensverlust

Die Grundlagen einer freiheitlichen, demokratisch-rechtsstaatlichen Kommunikation unter Privatpersonen, Geschäftspartnern oder von und mit staatlichen Stellen und Behörden sind einerseits die grundsätzliche Vertraulichkeit jeder zwischenmenschlichen Kommunikation[81] sowie andererseits die Achtung der Privatsphäre, der Meinungs- und Informationsfreiheit sowie der Eigentumsgarantie der teilnehmenden Personen oder Institutionen. Heute aber findet die Internet- und Telefon-basierte Kommunikation auf zahlreichen quasi offenen Plätzen statt, auf denen spioniert, abgehört, Menschen fortgesetzt observiert oder gezielt in die Irre geführt und oft noch blossgestellt werden, zudem Daten unterdrückt, verfälscht oder vernichtet und Urheberrechte an geistigen oder künstlerischen Schöpfungen resp. Werken systematisch gestohlen werden. Die seit den 1990er Jahren wachsende allgemeine Hoffnung auf eine weltweit offene Kommunikation, die durch mehr Informationen und mehr Auswahl den Menschen mehr Freiheit und mehr Wirkungsmöglichkeiten bringen sollte,[82] ist daran, *von den digitalen Feinden der freiheitlichen Demokratie zerstört zu werden.* Mindestens im E-Mail- und Internetverkehr sollte heutzutage jegliche vertrauliche oder riskante Kommunikation besser unterlassen werden.[83]

2. Die Grundannahmen des Datenschutzes stimmen nicht mehr

Das Datenschutzrecht, das zum Schutz der Grund- und Freiheitsrechte die Bearbeitung von Personendaten in der Kommunikation sowie im sonstigen Wirken privater und öffentlicher Personen und Organisationen einer *fairen Ordnung* unterstellen will, wird bekanntlich durch eine breite Palette von Vorschriften des Völker-, Europa-, Bundesverfassungs- sowie Gesetzesrechts von Bund und Kantonen bestimmt und gesichert.[84] Was heute über die Datenbeschaffungen der NSA und ihrer vier Partnerdienste, und damit (mittelbar) auch über die Spionage *vieler* anderer Staaten bekannt ist, aber auch was an täglichen Rechtsverstössen durch die international tätigen IT-Unternehmen geschieht sowie was Hacker (zum Teil angeheuert von Staaten) anrichten, das wirft die deprimierende Frage auf, ob eigentlich das internationale und das schweizerische Datenschutzrecht nicht *weitgehend Makulatur* seien.[85] Jedenfalls werden von ausländischen Staaten, internationalen Unternehmen sowie kriminellen Hackern die Grundsätze der Rechtfertigung einer Datenbearbeitung durch Gesetz oder Einwilligung und das Gebot, dass eine Bearbeitung nach Treu und Glauben zu erfolgen hat und verhältnismässig sein muss (Art. 5 Europäisches Überein-

[80] Thilo Weichert, Datenschutzverstoss als Geschäftsmodell – der Fall Facebook, DUD Datenschutz und Datensicherheit, 10/2012, 716 ff. m.w.H.

[81] Ausnahmen bei der Direktwerbung vorbehalten.

[82] Vgl. z.B. Urs Gasser/John Palfrey, The Promise and Perils of Highly Interconnected Systems, 2012.

[83] Fast scheint es, dass wir im Zweifel zum Informationsaustausch über Briefchen und Papierschnitzel («pizzini») zurückkehren müssen, wie es etwa die sizilianische Mafia mit Erfolg praktiziert hat. Vgl. das wunderbare Werk von Andrea Camilleri, M wie Mafia, 2009, übersetzt von Moshe Kahn, Reinbek 2009; orig.: *Voi non sapete – Gli amici, i nemici, la mafia, il mondo nei pizzini di Bernardo Provenzano*, 2007.

[84] Dazu z.B. Philippe Meier, Protection des données, Fondements, principes généraux et droit privé, Berne 2001, 79–153; Astrid Epiney/Yvonne Schleiss, Völker- und europarechtlicher Rahmen, Eva Maria Belser, Verfassungsrechtlicher Rahmen, sowie Eva Maria Belser/Hussein Nouredienne, Datenschutzgesetzgebung im Überblick, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, 53–507. Vgl. namentlich *zur unerlässlichen Horizontalwirkung* des grund- und menschenrechtlichen Persönlichkeitsschutzes gemäss Art. 35 Abs. 3 BV: Wegleitend Paul-Henri Steinauer, Die Verletzung durch private Datenbearbeitung und die allfällige Rechtfertigung einer Verletzung, Einzelheiten der gesetzlichen Regelung, in: Rainer J. Schweizer (Hrsg.), Das neue Datenschutzgesetz des Bundes, Zürich 1993, 43 ff.; im Weiteren BGE 130 III 28 E. 4.2, 32; 120 II 118 E. 3a, 121; Regina Aebi-Müller, Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes – Unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Bern 2005, 169; Rainer J. Schweizer, St. Galler Kommentar zur BV, 2. Aufl., Zürich/St. Gallen 2008, Art. 13 Rz. 43. Zentral ist vor allem, dass eine private Datenbearbeitung *gegen den ausdrücklichen Willen der betroffenen Person* eine Persönlichkeitsverletzung darstellt (Art. 12 Abs. 2 Bst. b DSG), dazu Meier, 518 ff.

[85] Weiterführende Überlegungen besonders bei Meier (FN 84), Introduction § 6 Défis et développement à venir, 154 ff.

kommen zum Schutz der Menschen bei der automatischen Verarbeitung von personenbezogenen Daten[86], Art. 4 Abs. 1 und 2 DSG sowie Art. 8 Abs. 2 Europäische Grundrechtecharta[87])[88] *systematisch missachtet*. Ebenso missachtet werden etwa die Regeln über die Informationspflichten beim Beschaffen von Personendaten (Art. 14 und 18a DSG)[89] sowie die Massstäbe für eine Bekanntgabe von Personendaten ins Ausland (Art. 2 des Zusatzprotokolls zum Europäischen Datenschutzübereinkommen[90], Art. 6 DSG, Art. 5–7 der Verordnung zum Bundesgesetz über den Datenschutz[91])[92]. Dazu kommt, dass mindestens der privatrechtliche Rechtsschutz nach Art. 15 DSG prohibitiv und ineffizient ist, vor allem weil der datenschutzrechtliche Persönlichkeitsschutz bezüglich Kosten und Beweislast wie Forderungsklagen zu führen ist.[93] Die betroffenen Personen können zudem gegenüber Unternehmen ohne Niederlassung oder Geschäftsstelle in der Schweiz (wie Facebook) ihre Ansprüche faktisch kaum durchsetzen.[94] Schliesslich muss man auch eingestehen, dass die technologische Entwicklung die Rechtsanwendung immer wieder vor neue Herausforderungen stellt. So hat sich z.B. die Datenmenge mit Bezug zu einer bestimmbaren Person enorm erhöht bzw. die technische Verfügbarkeit und die Erschliessbarkeit von aufbewahrten personenbezogenen Daten wurde stark ausgeweitet, was das Gefährdungspotential erhöht und gleichzeitig den Rechtsschutz schwieriger macht.[95] Sicherlich: Sowohl das Bundesverwaltungsgericht und das Bundesgericht als auch der EGMR setzen immer wieder (im Diskurs mit der Wissenschaft) klare Wegmarken und Schranken – auch gerade gegenüber der geheimen polizeilichen Datenbearbeitung;[96] deren Wirksamkeit ist allerdings auf Rechtsstreitigkeiten mit inländischen Datenbearbeitern begrenzt. Grenzüberschreitende Garantien bestehen nur sektoriell, z.B. gegenüber Fehlern der Polizei- und Justizarbeit im Schengen-Raum.[97]

Doch *Resignation wäre falsch*, weil es letztlich immer wieder darum geht, die freie Entfaltung der Menschen gerade in ihren Kommunikationsakten sowie die Werte der offenen, demokratischen Gesellschaft zu schützen. Dementsprechend müssen jetzt *weiterführende Konzepte*[98] und vor allem *wirksame neue Instrumente des Datenschutzes* diskutiert und umgesetzt werden. Nur beispielhaft, gerade auch im Blick auf den Grundrechtsschutz gegenüber den Aktivitäten der Nachrichtendienste, seien einige Postulate genannt: Von besonderer Bedeutung ist m.E., dass die Schweiz eng die Rechtsentwicklung in der EU verfolgt: Die geplante Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr *(Datenschutz-Grundverordnung)*[99] wird via den Schengen-Raum auch für die schweizerischen Polizei- und Justizbehörden massgeblich. Sie enthält z.B. ein *Recht auf Vergessenwerden*,[100] und sie soll auch für Unternehmen gelten, die sich von ausserhalb der EU mit Angeboten an die Bürgerinnen und Bürger wenden. Sodann sollte in Entwicklung von Art. 12 Abs. 2 Bst. b DSG ein *Grundrecht auf Widerspruch* (im Sinne eines «opt-out»-Prinzips) als

[86] Vom 28. Januar 1981 (SR 0.235.1).

[87] Zum EU-Datenschutzgrundrecht: Hans D. Jarass, Charta der Grundrechte der Europäischen Union, unter Einbezug der vom EuGH entwickelten Grundrechte und der Grundrechtsregelungen der Verträge, Kommentar, München 2010, Art. 8; Heribert Johlen, Art. 8, in: Tettinger Peter J./Stern Klaus (Hrsg.), Kölner Gemeinschaftskommentar zur Europäischen Grundrechte-Charta, München 2006, 301–313.

[88] Zu den allgemeinen Grundsätzen: Meier (FN 84), Première partie § 4 Les grands principes, 257 ff.; Astrid Epiney, Allgemeine Grundsätze, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.) (FN 84), 509 ff.

[89] Zu den Anforderungen an die Erkennbarkeit der Datenbeschaffung: im Privatbereich: Meier (FN 84), Première partie, § 5 Le devoir d'information en matière privée, 345 ff.; im öffentlichen Bereich: Bernhard Waldmann/Jürg Bickel, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.) (FN 84), 691 ff., 827 ff.

[90] Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 8. November 2001 (SR 0.235.11).

[91] Vom 14. Juni 1993 (SR 235.11).

[92] Zu den Grundsätzen und Problemen der grenzüberschreitenden Datenbekanntgabe: Meier (FN 84), Première partie § 8 La communication transfrontière, 436 ff.; Astrid Epiney/Tobias Fasnacht, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.) (FN 84), 559 ff.

[93] Näheres bei Meier (FN 84), 585 ff., 595.

[94] Zu den IPR-Regeln: Meier (FN 84), 596 ff.

[95] Vgl. Thomas Probst, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Person im Datenschutzrecht, AJP 10/2013, 1423 ff.; Rainer J. Schweizer/Severin Bischof, Der Begriff der Personendaten, digma 2011, 152 ff.

[96] Z.B. das Strassburger Gericht mit genauen Vorgaben für geheime staatliche Abhörmassnahmen: EGMR, *Lenev c. Bulgarie*, 41452/07 (2012), Ziff. 146 f.; *Pop Blaga c. Roumanie*, 37379/02 (2012), Ziff. 52 ff.; *Savovi c. Bulgarie*, 7222/05 (2012), Ziff. 55 ff.; *Calmanovici c. Roumanie*, 42250/02 (2008), Ziff. 121; *Liberty et autres c. Royaume-Uni*, 58243/00 (2008), Ziff. 60 ff.; *Association for European Integration and Human Rights et Ekimdzhiev c. Bulgarie*, 62540/00 (2008), Ziff. 76 f.; *Weber et Saravia c. Allemagne*, 54934/00 (2006), Ziff. 95. Diese Grundsätze gelten auch für andere Arten der geheimen Sammlung, Speicherung und Weitergabe von Daten: EGMR, *Rotaru c. Roumanie*, 28341/95 (2000) (Grosse Kammer), Ziff. 59; Grabenwarter/Pabel (FN 70), § 22, Rz. 34 f.; weitere Hinweise: Métille (FN 51), 95 ff.; Lucien Müller, Videoüberwachung in öffentlich zugänglichen Räumen – insbesondere zur Verhütung von Straftaten und Ahndung von Straftaten, Diss., Zürich/St. Gallen 2011, 105 ff.; Rainer J. Schweizer/David Rechsteiner, § 2 Grund- und Menschenrechte, in: Hanspeter Thür et al. (Hrsg.), Datenschutz, Handbücher für die Anwaltspraxis, Basel 2014 (im Druck).

[97] Dazu Hinweise oben FN 53.

[98] Sehr bedenkenswert ist m.E. etwa die These von Alexander Flückiger, dass das Datenschutzgrundrecht von Art. 13 Abs. 2 BV nicht nur der persönlichen Entfaltung (im Sinne von Art. 10 Abs. 2 BV) diene, sondern auch das private Eigentum an den Informationen (vgl. Art. 26 BV) schützen müsse, siehe: L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété? AJP 6/2013, 837 ff.

[99] Vom 25. Januar 2012, KOM (2012) 11; sodann die Fassung des zuständigen Ausschusses des Europ. Parlaments vom Oktober 2013 Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012–2012/0011(COD).

[100] Art. 17 Vorschlag der Kommission; vgl. zu dieser Forderung z.B. Rolf H. Weber, Neue Grundrechtskonzeption zum Schutz der Privatheit, in: Rolf H. Weber/Florent Touvenin (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, 20.

Bestandteil des Rechts auf informationelle Selbstbestimmung anerkannt werden.[101] Der Bedarf nach praktischen Widerspruchsmöglichkeiten wurde z.B. im Urteil betr. Google Street View klar anerkannt.[102] Schliesslich muss in der Schweiz das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* anerkannt werden,[103] wie es vom deutschen Bundesverfassungsgericht in einem Urteil zur Online-Durchsuchung entwickelt worden ist.[104] Last but not least bräuchte es einen Bericht und einen Aktionsplan des Bundesrates zur Stärkung der IT-Sicherheit in der Schweiz, z.B. mit dem Aufbau von unabhängigen Internet-Servern in der Schweiz durch die Swisscom und andere Firmen sowie der Entwicklung und Verteilung von Verschlüsslungscodes für die Eigenrechner.

V. Folgerungen für die Staatsschutzgesetzgebung

Die immensen Entwicklungen in den Informations- und Kommunikationstechnologien, aber vor allem auch die neuen sicherheitspolitischen Herausforderungen wie etwa die seit der Schaffung des BWIS Mitte der 1990er Jahre weiter fortgeschrittene Globalisierung der Wirtschaft, die verstärkte Freizügigkeit der Menschen mindestens im EU-/EWR-Raum, die neuen, schweren bewaffneten Konflikte im Glasis von Europa sowie die weltweit agierende, häufig brutale, organisierte Kriminalität nötigen unstreitig die Bundesbehörden immer wieder zu einer *Evaluierung* des geltenden Sicherheitsrechts (im Sinne von Art. 170 BV[105]) sowie zur ausgemessenen Anpassung der Gesetzgebung. Unzweifelhaft ändern sich in der globalisierten, stark vernetzten Informationswelt die Bedürfnisse nach präventiven Polizeiinformationen, ja sie wachsen in gewissen Bereichen.[106] Und unbestritten ist, dass die Arbeit des NDB der Schweiz heute in grossem Masse rechtlich und tatsächlich klar geordnet und überprüfbar ist.[107] Doch das geplante NDG lässt *zu viele Rechtsprobleme ungeklärt*. Nicht zuletzt auf Grund des erschreckenden, globalen Wandels in der elektronischen Kommunikation sowie des Legitimationsverlustes mindestens der ausländischen unkontrolliert agierenden Geheimdienste sollte die Bundesversammlung ein Eintreten auf die Vorlage des Bundesrates für ein neues Nachrichtendienstgesetz, die ihr in wenigen Monaten zugehen wird, unbedingt *erst beschliessen, wenn bestimmte grundlegende Klärungen erfolgt sind*. Nachfolgend werden einige Postulate im Sinne von *Anregungen* vorgebracht:

1. Allgemeine Klärungsbedürfnisse

- Es sollte, wie verschiedene parlamentarische Vorstösse dies fordern, öffentlich Rechenschaft abgelegt werden, auf Anordnung der Geschäftsprüfungsdelegation (GPDel) als parlamentarisches Aufsichtsorgan über den NDB,[108] über die Informationsaustausche zwischen dem NDB und den (westlichen) Nachrichtendiensten in den vergangenen Jahren.
- Der Bundesrat wäre zu ersuchen, einen genauen Bericht über den Eingang und die Art von Erkenntnissen über Rechtsverstösse von ausländischen Geheimdiensten in der Schweiz vorzulegen sowie über die schweizerische Reaktionen auf diese Verstösse.
- Anzustreben wäre sodann eine Mitwirkung der Schweiz an der Entwicklung von völkerrechtlichen Instrumenten zur rechtlich geordneten Zusammenarbeit der Nachrichtendienste sowie zur Stärkung der Kontrolle derselben, einschliesslich der Gewährung von internationalen Rechtsschutzmitteln.[109]

2. Klärungen betreffend das geplante neue Nachrichtendienstgesetz

Von den verschiedenen oben (Ziff. II.3) erwähnten Rechtsfragen sind m.E. folgende Punkte besonders zentral und vor einer Beratung der Vorlage in den eidgenössischen Räten zu klären:

- Die *Konkurrenzen zwischen den Nachrichtendiensten und den Kriminalpolizeibehörden von Bund und Kantonen* sind bisher nie genauer untersucht worden. Es ist nicht sinnvoll und unter verfassungsrechtlichen Anforderungen an Justizverfahren (Art. 29–32 BV) nicht zu verantworten, dass präventive Informationsbeschaffungen in Staatsschutzdelikten vom Bundeskriminalamt und kantonalen Kriminalpolizeibehörden sowie gleichzeitig vom Nachrichtendienst unternommen werden. Diese Konkurrenzen werden noch erheblich grösser, wenn der NDB die erstrebten weiteren geheimen Informationsbeschaffungsmittel erhal-

[101] Zu diesem vorgerichtlich, unmittelbar gegenüber dem Inhaber der Datensammlung geltend machbaren «droit d'opposition» vgl. etwa Meier (FN 84), 583/4.
[102] BGE 138 II 346 E. 10.6.3.
[103] Als ungeschriebenes Grundrecht (das auch unter der neuen BV möglich ist, siehe Rainer J. Schweizer, St. Galler Kommentar zur BV, Vorbemerkungen zu Art. 7–36, Rz. 13) oder im Rahmen der ohnehin notwendigen Klärung und Ergänzung von Art. 13 Abs. 2 BV.
[104] BVerfGE 120, 274, vom 27. Februar 2008. Vgl. dazu bes. Axel Tschentscher, Das Grundrecht auf Computerschutz, AJP 2008, 383 ff.; Vaios Karavas, Das Computer-Grundrecht, Persönlichkeitsschutz unter informationstechnischen Bedingungen, in: Stefan Keller/Stefan Wiprächtiger (Hrsg.), Recht zwischen Dogmatik und Theorie, FS für *Marc Amstutz*, Zürich/St. Gallen 2012, 99 ff.
[105] Zur Evaluation der Wirksamkeit staatlichen Handelns: z.B. Philippe Mastronardi, St. Galler Kommentar zur BV, 2. Aufl., Zürich/St. Gallen 2008, zu Art. 170 Rz. 3 ff.
[106] Vgl. die wichtigen, differenzierten Ausführungen von Erhard Denninger, Rechtsstaatliche Polizei in Zeiten intensivierter Prävention, in: Sicherheit & Recht 3/2012, 222 ff.
[107] Vgl. bes. Art. 15–28 V-NDB.
[108] Siehe Art. 53 Bundesgesetz über die Bundesversammlung (Parlamentsgesetz, ParlG) vom 13. Dezember 2002 (SR 171.10), sowie zu deren Informationsrechten Art. 154 ff. ParlG. Näheres zur GPDel im Jahresbericht 2012 der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation der eidgenössischen Räte vom 24. Januar 2012 (Geschäft 13.004).
[109] Vgl. den in der UNO von Brasilien und der BRD eingereichten Resolutionsentwurf A/C.3/68/L.45 «The right to privacy in the digital age» (http:www.un.org/en/ga/third/68/propslist.shtml).

ten sollte.[110] Die Zusammenarbeit mit der zuständigen Staatsanwaltschaft im polizeilichen Ermittlungsverfahren (Art. 307 StPO) und die gesetzlichen Verteidigungsrechte nach Strafprozessrecht sprechen dafür, eher die präventiven Fähigkeiten der Kriminalpolizei zu stärken. Auf jeden Fall sollten die respektiven Kompetenzen in der präventiven Polizeiarbeit sowie die Bedingungen der Zusammenarbeit von Staatsschutzorganen und Kriminalpolizei genau festgelegt werden.

- Notwendig erscheinen insbesondere *genauere Spezifizierungen des erweiterten Auftrages des NDB*. Vor allem sollten *für die Eingriffsbefugnisse der NDB genaue gesetzliche Konkretisierungen und Präzisierungen* im Sinne des verfassungsrechtlichen Bestimmtheitsgebotes bezüglich der Voraussetzungen der Anwendung der verschiedenen Zwangsmassnahmen und der Datenlieferungen ins Ausland formuliert werden. Es geht kaum an, dass der NDB bei blosser Annahme einer «Gefährdung» durch irgendwelche Rechtsverstösse schwerwiegende Eingriffe in die Privatsphäre von Personen durchführen kann, während die Polizeiorgane des Bundes und der Kantone sowie das BÜF in der Strafverfolgung konkrete Schwellen der Eingriffe je nach Deliktsart beachten müssen, wenn sie bei einem «erhärteten Verdacht» einer Straftat geheime Datenbeschaffungen durchführen wollen.
- Ganz zentral ist, dass im heutigen Umfeld *die Vorstellung der absoluten Geheimhaltung der Aktivitäten der Nachrichtendienste diskutiert* wird. Warum sollen die Geheimdienste unter technischer Mithilfe von IT-Unternehmen die Bedingungen der für die Demokratie lebensnotwendigen Öffentlichkeit zu Lasten der Ausübung der Bürgerrechte und der Grund- und Menschenrechte bestimmen, statt dass das Öffentlichkeitsprinzip zu Gunsten der demokratischen Kontrollen gestärkt wird?[111] Konkret gesagt stellt sich die *verfassungsrechtliche Grundsatzfrage*, warum die Geheimhaltungsgründe, die es im konkreten Fall der Prävention und Bekämpfung von Rechtsverstössen notwendigerweise braucht (vgl. beispielhaft Art. 6 Abs. 1 EMRK), im Nachrichtendienst ganz andere sein sollen als in der polizeilichen und justiziellen Kriminalitätsbekämpfung. Es ist der GPDel hoch anzurechnen, dass sie heute viel mehr als vor zehn Jahren eine sehr konkrete und auch zum Teil Fall-bezogene Kontrolltätigkeit ausübt und darüber öffentlich Rechenschaft ablegt,[112] doch ihre periodischen Orientierungen reichen in einer rechtsstaatlichen Demokratie nicht aus! Entsprechend müsste das Bundesverwaltungsgericht (wie früher die Rekurskommission) alle seine Entscheidungen über Überprüfungen von Datenbearbeitungen durch den NDB, die sie auf Gesuch einer Person wegen des Ausschlusses des datenschutzrechtlichen Einsichtsrechts nach Art. 18 Abs. 6 BWIS durchführt, auch (selbstverständlich anonymisiert) publizieren;[113] für die Nichtveröffentlichung besteht keine Gesetzesgrundlage. Zusammenfassend sollten also klare Verfassungs- und Gesetzesgrundlagen für die öffentliche Kontrolle und die Transparenz der präventiven Informationstätigkeiten der Organe des Staatsschutzes geschaffen werden.
- Die verheerende Wirkung der Geheimhaltung wird besonders bei der Genehmigung von geheimen Eingriffsmitteln deutlich.[114] Das (geheim arbeitende) Sondergericht zur Bewilligung der Beschaffungsmassnahmen der NSA hat in den letzten Jahren nur in einem Bruchteil von einer Promille Gesuche zurückgewiesen. Das dürfte bei der Genehmigung durch eine Präsidentin oder einen Präsidenten des Bundesverwaltungsgerichts nicht anders sein. Die Erklärung ist vermutlich einfach: Es liegt ein systemischer Fehler in diesen Genehmigungsverfahren, weil es *an einer institutionellen anderen Meinung fehlt*. Zu erwägen wäre, ob nicht z.B. ein institutionalisierter Anwalt der betroffenen Personen ein unabhängiges Zweitgutachten abgeben soll.[115]
- Zu prüfen ist schliesslich, wie *die Fachaufsicht über den NDB gestärkt* werden kann. Diese wirkt jetzt als internes Beratungsorgan der Vorsteherin oder des Vorstehers des VBS.[116] M.E. wäre es das Beste, wenn sie eine institutionelle Unabhängigkeit zwischen Bundesrat und Bundesversammlung erhalten würde, wie sie die Eidgenössische Finanzkontrolle hat.[117]

3. Schlussfolgerung

Das Fazit der vorstehenden Überlegungen ist, dass der demokratische Gesetzgeber in der Schweiz jetzt nicht seine Zeit für das neue umfassende Nachrichtendienstgesetz einsetzen sollte, a) weil das geltende BWIS in der Fassung vom 23. Dezember 2011 sehr wohl erlaubt, die wichtigsten Sicherheitsaufgaben im Staatsschutzbereich wahrzunehmen,[118] b) weil Grundsatzfragen der Tätigkeiten ausländischer Geheimdienste in der Schweiz und der Zusammenarbeit des NDB mit diesen

[110] Das Konzept von BWIS 1997 war, dass der Nachrichtendienst seine Erkenntnisse aus den präventiven Recherchen zu spezifischen Berichten zusammenführt, die er der Bundesanwaltschaft zuleitet.

[111] Weder Art. 2 Abs. 3 Bst. a noch Art. 7 Abs. 1 Bst. c. und d. Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ) vom 17. Dezember 2004 (SR 152.3) rechtfertigen eine pauschale Ausnahme der Anwendung dieses Gesetzes auf die Nachrichtendienste; vgl. Thomas Sägesser, in: Stephan C. Brunner/Luzius Mader (Hrsg.), Stämpflis Handkommentar zum BGÖ, Bern 2008, Art. 2 Rz. 59 ff.; Bertil Cottier, ibidem, Art. 7 Rz. 26 ff.

[112] Vgl. Jahresbericht 2012 der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation der eidgenössischen Räte vom 24. Januar 2012, BBl 2012, 3515, bes. 3572 ff.

[113] Es handelt sich zweifellos um «materielle Entscheide des Bundesverwaltungsgerichts» im Sinne von Art. 6 Abs. 1, Informationsreglement vom 21. Februar 2008 (SR 173.320.4).

[114] Vgl. Art. 25 Entwurf NDG.

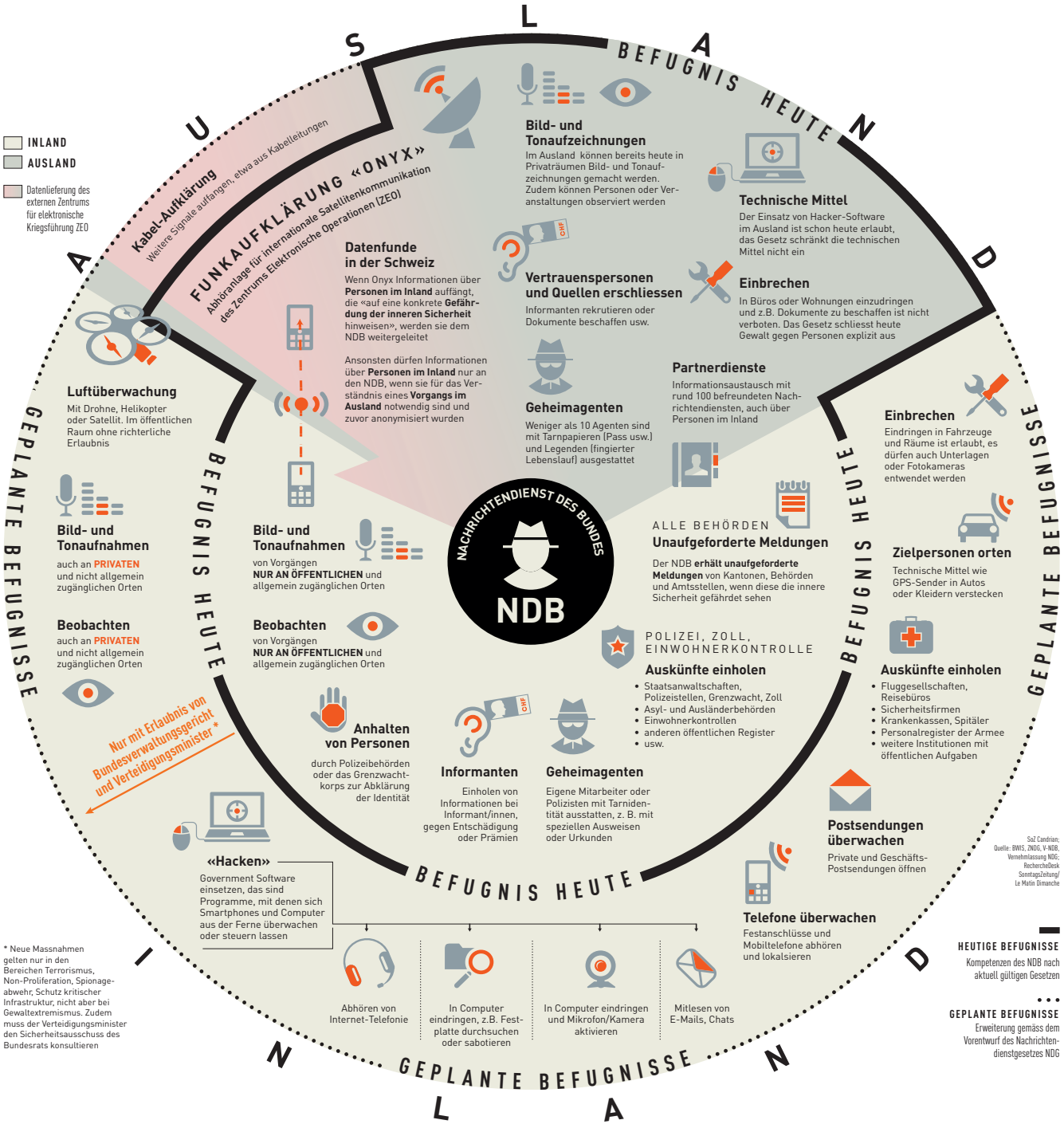
[115] Wobei eigentlich zu diskutieren ist, ob nicht die nachträgliche Mitteilung einer Massnahme auch den gerichtlichen Genehmigungsentscheid und die anwaltliche Stellungnahme in angemessener Form offenlegen sollte, damit ein *wirksamer Rechtsschutz* möglich wird; vgl. EuGH 4. Juni 2013 Rs. C 300/11 (ZZ), Rz. 53–67.

[116] Vgl. Art. 32 ff. V-NDB.

[117] Vgl. Art. 1 Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (SR 614.0).

[118] Vgl. Lagebericht 2013 des NDB (FN 23).

geklärt werden müssen, c) weil es heute in der allseits gefährlichen Telekommunikation unbedingt besondere, neue staatliche und rechtliche Sicherungen der freien Kommunikation und der persönlichen Daten braucht, sowie d) vor allem weil das geplante NDG – jedenfalls nach dem Entwurf vom 8. März 2013 – so erhebliche, grundsätzliche Probleme aufwirft, dass es nicht richtig wäre, dieses Gesetz jetzt als nationales Sonderrecht für geheime präventivpolizeiliche Informationstätigkeiten in genereller Absicht zu beschliessen.



Quellenangabe/Copyright: SonntagsZeitung, Tamedia AG, Zürich