Unkontrollierbare Überwachung die freiheitliche Demokratie

Rainer J. Schweizer
em. Ordinarius für öffentliches Recht, Europarecht und Völkerrecht, St. Gallen; Advokat;
ehemaliger nebenamtlicher Bundesrichter und ehemaliger Präsident der Eidgenössischen Datenschutzkommission

Der im Parlament beratene Gesetzesentwurf will den Nachrichtendienst zu einer «Allzweckwaffe» machen. Das Gesetz hat erhebliche Mängel, eine Verfassungsgrundlage dafür fehlt.

1. Paradigmenwechsel für den Staatsschutz

Der Nationalrat hat im März 2015 den Entwurf eines Nachrichtendienstgesetzes beraten, das ihm der Bundesrat mit Botschaft vom 19. Februar 2014 vorgelegt hat,[1] und der Ständerat will diesen Gesetzesentwurf in der Junisession 2015 behandeln. Das Gesetz führt zu einem fundamentalen Paradigmenwechsel für den Schweizer Staatsschutz.

Das Bundesgesetz über die Wahrung der inneren Sicherheit (BWIS) vom 21. März 1997 zog, wie man sich erinnern mag, die Konsequenzen aus der 1989/1990 vom Parlament untersuchten Fichenaffäre im Schweizer Staatsschutz mit der ungesetzlichen, ungehemmten Datensammlerei, und das Gesetz war auch ein indirekter Gegenvorschlag zur Volksinitiative «S.o.S. Schweiz ohne Schnüffelpolizei».[2] Das Konzept des BWIS war, dass der Auslandnachrichtendienst die für die Schweiz relevanten strategischen sicherheitspolitischen Entwicklungen ermitteln und fortlaufend dem Bundesrat darstellen sollte und dass sich der Inlandnachrichtendienst auf die präventive Aufklärung der sogenannte Staatsschutzdelikte, der Art. 262–278 StGB (Verbrechen und Vergehen gegen den Staat und die Landesverteidigung) sowie der Artikel 258–263 StGB (Verbrechen und Vergehen gegen den öffentlichen Frieden) konzentrieren sollte.

Entsprechend bestimmt dieses noch geltende Staatsschutzgesetz in Art. 2, dass der Bund vorbeugende Massnahmen treffen soll gegen Gefährdungen durch Terrorismus, verbotenen Nachrichtendienst, gewalttätigen Extremismus sowie gegen den verbotenen Handel mit Waffen und radioaktivem Material sowie gegen verbotenen Technologietransfer. Bezüge solcher Straftaten zur organisierten Kriminalität sollten auch erfasst werden, denn namentlich der Terrorismus hat viele Übereinstimmungen mit der organisierten Kriminalität.

Ursprünglich sollte der Nachrichtendienst des Bundes (nachfolgend NDB) seine präventiv polizeilichen Abklärungen nur mit Informationen von amtlichen Stellen oder aus öffentlichen Quellen ausführen. Seit der Teilrevision von 2011 ist der NDB aber auch befugt, zur geheimen Informationsbeschaffung «Informantinnen und Informanten», allenfalls mit einer Tarnidentität, einzusetzen[3] sowie eine Funkaufklärung gegenüber Abstrahlungen von ausländischen Telekommunikationssystemen zu betreiben.[4]

Doch das nun entwickelte «Nachrichtendienstgesetz» (NDG) verfolgt einen grundlegend anderen Ansatz: Der NDB soll künftig keineswegs nur mögliche Staatsschutzdelinquenten erfassen, sondern darüber hinaus (nach Art. 6 Abs. 1 Bst. a Ziff. 4 Entwurf NDG) auch Angriffe auf Informations-, Kommunikations-, Energie-, Transport- und andere unerlässliche Infrastrukturen – also zum Beispiel Hackerangriffe – verhüten helfen, dann zur «Wahrung der Handlungsfähigkeit der Schweiz beitragen» (in welchen Beziehungen?, vgl. Art. 6 Abs. 1 Bst. c E NDG) und gar vom Bundesrat «zur Wahrung weiterer wesentlicher Landesinteressen» wie zum Beispiel «zum Schutz des Werk-, Wirtschafts- und Finanzplatzes Schweiz» (sic!) eingesetzt werden können (Art. 3 E NDG).

Man wird argumentieren, die Bedrohungen des modernen Staates seien viel komplexer geworden, weshalb der Auftrag des NDB viel weiter gefasst werden müsse. Deshalb soll er, vor allem angesichts der technologischen Fähigkeiten der möglichen «Gefährder», nach Antrag des Bundesrates für diesen erweiterten Auftrag unbedingt neue weitreichende Kompetenzen zu geheimen Informationsbeschaffungen bekommen (siehe Art. 25–32 sowie Art. 36–42 E NDG) – vor und ausserhalb von einem Verdacht auf eine Straftat.

Mit dieser fundamental neuen Zwecksetzung und den neuen Zugriffsbefugnissen kann der NDB quasi als «Allzweckwaffe» zum Beispiel bei drohenden schweren Wirtschafts- und Sozialkonflikten oder Spannungen mit ausländischen Partnerstaaten eingesetzt werden (wobei die dafür nötige Fachkompetenz doch fraglich sein dürfte). Durch den breiten Wirkungsbereich und die weitreichenden Eingriffskompetenzen, welche die Mittel jeder Strafverfolgungsbehörde übertreffen, wird das NDG vom Staatsschutzgesetz zu einem «Massnahmengesetz» (wie Markus Mohler treffend sagt)[5] für präventive Staats-, Gesellschafts- und Wirtschaftskontrollen.

2. Keine ausreichende Verfassungsgrundlage

Der Gesetzesentwurf gibt als Verfassungsgrundlage die Zuständigkeiten des Bundes in der Aussen-

ruiniert den Rechtsstaat und

politik nach Art. 54 Abs. 1 sowie die Generalklausel von Art. 173 Abs. 2 BV an, welcher die Letztzuständigkeit der Bundesversammlung ausdrückt. Jedenfalls für den Nachrichtendienst im Inland kann für das Gesetz offensichtlich keine Sachzuständigkeit des Bundes genannt werden. Nun kann man argumentieren, dass die Kernaufgabe eines Nachrichtendienstes, nämlich der Landesregierung fortlaufend verlässliche Informationen zur Sicherheitslage des Landes bereitzustellen, auf einer ungeschriebenen, inhärenten Verfassungskompetenz des Bundes beruhe.

Doch damit fehlt aber für all die schweren Eingriffskompetenzen gegenüber den Bewohnerinnen und Bewohnern des Landes sowie für die starken Beschränkungen der kantonalen Polizeizuständigkeiten in der Sicherheits-, Ordnungs- und Kriminalpolizei klar die nötige BV-Grundlage. Der Bundesrat hat selber im Bericht vom 12. März 2012 zum Postulat Malama festgehalten, dass in der BV eine ausdrückliche Grundlage geschaffen werden müsse, in der die Befugnisse des Bundes im Staatsschutzbereich klar umrissen werden.[6] Jetzt soll dies nicht mehr gelten, geschweige denn nötig sein.

3. Wieweit braucht es eine präventiv ermittelnde Polizei?

Die Grundsatzfrage, wieweit eine präventiv ermittelnde Polizei nötig ist, wird im Rahmen dieser Gesetzgebung gar nicht diskutiert. Rechtsverletzungen sollen grundsätzlich nachträglich repressiv, allenfalls disziplinarisch verfolgt und sanktioniert werden. Die konstitutive und limitierende Voraussetzung dafür ist ein begründbarer Straftatverdacht. Darauf gestützt klären die sanktionsbefugten Behörden die allfällig begangenen Straftaten auf. Dass unter Umständen frühzeitige Abwehrmassnahmen nötig sein können, ist unbestritten.

Bei verschiedenen schwerwiegenden Delikten sind jedoch in den letzten Jahrzehnten auch (grundsätzlich sonst nicht strafbare) Vorbereitungshandlungen unter Strafe gestellt worden (vgl. zum Beispiel bei den gemeingefährlichen Delikten nach Art. 221 ff. StGB aufgrund von Art. 226ter StGB oder insbesondere bei den Delikten gegen den öffentlichen Frieden aufgrund von Art. 260bis StGB); damit hat sich das kriminalpolizeiliche Wirkungsfeld erheblich verbessert. Im Grunde ergibt eine separate präventive, geheime, durch die Strafgerichtsbarkeit nicht oder nur ausnahmsweise nachträglich überprüfbare Polizeiarbeit höchstens bei bestimmten schweren Bedrohungen der Demokratie, der Verfassungsordnung und bei existenziellen Gefahren für das Funktionieren des Landes einen Sinn; dabei sollen dann aufgrund von bestimmten nachrichtendienstlichen Erkenntnissen nicht nur Strafverfahren eingeleitet und die Zusammenarbeit mit andern Diensten darauf fokussiert, sondern auch geeignete Verwaltungsmassnahmen wie Landesverweisungen angeordnet werden.

In der vorbeugenden Kriminalitätsbekämpfung zeigt sich auch, dass beispielsweise gegen die bisher verhältnismässig wenigen Aktivitäten mit terroristischem Hintergrund in der Schweiz die wesentlichen Erfolge überwiegend den Strafverfolgungsbehörden von Bund und Kantonen zu verdanken sind.[7]

Ein Hauptmangel des vorliegenden Gesetzesentwurfs ist es, dass er die Schnittstellen der präventiven nachrichtendienstlichen Polizeiarbeit zu den Aufgaben der Strafbehörden in keiner Weise klärt. Es ist nicht gewährleistet, dass der Nachrichtendienst bei Erkenntnissen mit strafrechtlichen Bezügen die zuständige Bundesanwaltschaft oder die Staatsanwaltschaften der betroffenen Kantone umgehend informiert – das bleibt seinem Ermessen überlassen; das kann, wie ausländische Erfahrungen (zum Beispiel mit dem NSU in der BRD) zeigen, verheerende Folgen haben. Noch ist ungeklärt, ob die vom NDB mit zum Teil geheimen Mitteln wie Lauschangriffen oder Trojaner erhobenen Daten überhaupt nachträglich verwertbar sind (vgl. 141 StPO), jedenfalls wenn sie ohne einen begründeten Tatverdacht aufs Geratewohl bei vermeintlichen «Gefährdern» beschafft worden sind.[8]

4. Datenbearbeitung unverhältnismässig

Der Gesetzesentwurf kennt Datenbeschaffungen (zum Beispiel von «menschlichen Quellen» nach Art. 15 E NDG) und Datenweitergaben ans Ausland (zum Beispiel nach Art. 12 E NDG) ohne besondere gesetzlich bestimmte Eingriffsschwellen. Es

1 Geschäft Nr. 14.022, BBl 2014 2105.
2 Vgl. Botschaft des Bundesrates zum BWIS vom 7.3.1994, BBl 1994 II 1127 ff.
3 Art. 14a–14c BWIS (SR 120).
4 Vgl. nähere Hinweise bei Rainer J. Schweizer, «Ein neues Staatsschutzgesetz? Die Sicherung der freien Kommunikation der Menschen geht jetzt der Stärkung der Machtmittel der Geheimdienste vor», in: S&R 3/2013, 123 ff., bes. 125/126. Verordnung über die elektronische Kriegführung und die Funkaufklärung (VEKF) vom 17.10.2012 (SR 510.292); dazu z. B. Tatjana Rothenbühler, Völkerrechtliche Aspekte nachrichtendienstlicher Tätigkeit am Beispiel der mit dem Ausland betrauten Dienststellen des Nachrichtendienstes des Bundes (NDB), Diss. Freiburg, Zürich 2012, 146 ff.
5 In: «Nordwestschweiz», 18.5.2015, S. 4.
6 BBl 2012 4597.
7 Vgl. bspw. Bundesamt für Polizei (Fedpol), Jahresberichte 2013, S. 22, 41 ff., 2014, S. 22 f.
8 Vgl. dazu eindrücklich: Jürg-Beat Ackermann und Patrick Vogler, «Der Nachrichtendienst und die Strafprozessordnung. Wenn vom Nachrichtendienst verdachtlos erhobene Informationen von den Strafverfolgungsbehörden verwertet werden dürfen, verliert der Tatverdacht – Ausgangspunkt jeder strafbehördlichen Untersuchung – seine rechtsstaatliche Funktion im Strafprozess», in: NZZ Nr. 65 vom 19.3.2015, S. 23.

gibt aber nach Art. 23 ff. E NDG auch Eingriffskompetenzen wie die geheime Überwachung der Telekommunikation, den Lauschangriff auf Gespräche an nicht öffentlich zugänglichen Orten, das Eindringen in Computersysteme und -netzwerke und das geheime Eindringen und Durchsuchen von Räumlichkeiten, die nur bei einer konkreten Bedrohung der inneren und äusseren Sicherheit zulässig sind und die zudem von einem Abteilungspräsidenten des Bundesverwaltungsgerichts genehmigt und durch den Chef oder die Chefin des VBS «freigegeben» worden sind.

Dieses Bewilligungsverfahren ist voller Probleme: Es ist ein geheimer, nicht öffentlich nachprüfbarer Einzelrichterentscheid in einem nicht-kontradiktorischen Verfahren.[9] Dass zudem ein Mitglied des Bundesrates die Aktion mitverantworten soll, kann für die Glaubwürdigkeit der Landesregierung als Kollegialorgan nur schädlich sein.

Vor allem aber setzt das Gesetz der Nutzung und der Aufbewahrung dieser Personendaten nur ungenügende Grenzen. Grundsätzlich muss die geheime Beschaffung den betroffenen Personen nachträglich mitgeteilt werden, wobei aber mit gerichtlicher Bewilligung auch ein Aufschub oder ein Verzicht auf die Mitteilung zulässig ist (Art. 32 E NDG).

Noch wesentlich problematischer sind die Informationsbeschaffungen im Ausland beziehungsweise die Beschaffung von Daten aus Kommunikationen mit dem oder im Ausland (vgl. Art. 36–42 E NDG). Dazu gehören besonders das Eindringen in Computersysteme und -netzwerke, die Funkaufklärung und die Kabelaufklärung, wobei die völkerrechtlichen Rechtshilfeverträge[10] oder die europäische Computercrime-Konvention[11] nicht beachtet werden müssen! Auch ist nur die Kabelaufklärung gerichtlich genehmigungspflichtig. Hier findet, wie die Funkaufklärung schon heute zeigt, eine massenweise Datenbeschaffung auf Vorrat statt, ohne dass das Gesetz zeitliche Nutzungs- und Aufbewahrungsgrenzen festlegt und ohne irgendeine Mitteilungspflicht an die betroffenen Personen.

Die vorratsweise beschafften riesigen Datenmassen werden mit sogenannten Selektoren durchsucht und ausgewertet, ein Verfahren, das als systematische «fishing expedition» bezeichnet werden muss (was im internationalen Amts- und Rechtshilfezusammenhang verpönt ist). Die sogenannten Restdaten werden schliesslich unabhängig von den Schutzinteressen der betroffenen Personen in einem «Restdatenspeicher» aufbewahrt (Art. 56 E NDG). Zugriffsrechte, Aufbewahrungsdauer und allfällige Datenvernichtung werden ausschliesslich nach den Bedürfnissen des NDB durch die Verordnung bestimmt.

Man muss sich der Tragweite dieses Systems bewusst sein: Die durch die europäischen Höchstgerichte und das Bundesgericht entwickelten Grundsätze für geheime polizeiliche Datenbeschaffung, -auswertung und -aufbewahrung zum Schutz der informationellen Selbstbestimmung der Menschen, von deren Privatsphäre und deren Kommunikationsfreiheiten werden missachtet. Das Bundesgericht hat zum Beispiel schon 2006 die Aufbewahrung von Bild- und Tondaten aus voraussetzungslos funktionierenden öffentlichen Video- und Tonüberwachungen als einen schwerwiegenden Grundrechtseingriff in die Privatsphäre (Art. 13 Abs. 2 BV) bezeichnet, der nicht länger als hundert Tage dauern darf;[12] und der EuGH hat im April 2014 die Vorratsdatenspeicherung allein der Verbindungsdaten von Telefonkommunikationen für sechs Monate wegen der im Blick auf den Schutz des Privatlebens sehr weitreichenden Auswertungsmöglichkeiten und wegen der erheblichen Missbrauchsgefahren, etwa durch private Telekommunikationsdienstleister, selbst zu Zwecken der Bekämpfung schwerer Delikte im Lichte der EU-Grundrechtegarantien als völlig unverhältnismässig und unhaltbar angesehen.[13]

Doch offensichtlich sind diese höchstrichterlichen Schranken für schwere Grund- und Menschenrechtseingriffe für den schweizerischen Nachrichtendienst unmassgeblich. Denn «wesentliche Landesinteressen» sollen dem Grundrechtsschutz selbst dann vorgehen, wenn die Grundrechte durch geheime Realhandlungen einer Sicherheitspolizei schwerwiegend verletzt werden. Zu erinnern ist in diesem Zusammenhang daran, dass für das Bundesgericht Bestimmungen in Bundesgesetzen selbst dann massgebend sind, wenn es diese als verfassungswidrig erachtet (Art. 190 BV).

5. Keine Auskunft und in den meisten Fällen kein Rechtsschutz

Es gibt im NDG, wie im BWIS, auch kein datenschutzrechtliches Auskunftsrecht, obwohl dieses ein verfassungs- und völkerrechtlich elementarer Bestandteil des Grund- und Menschenrechts auf informationelle Selbstbestimmung der betroffenen Personen darstellt.[14] Im Gegenteil besteht eine gesetzliche Pflicht zur weitgehenden und dauernden Auskunftsverweigerung bei allen heiklen Datensammlungen, was aber als «Aufschub der Auskunft» bezeichnet wird (vgl. Art. 62–65 E NDG).

Durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und in zweiter

Instanz durch das Bundesverwaltungsgericht wird zwar eine Prüfung der Bearbeitung der Daten, über die eine Person (vergeblich) Auskunft verlangt hat, vorgenommen, doch diese Prüfung dient der verwaltungsinternen und allenfalls verwaltungsgerichtlichen Kontrolle der Rechtsanwendung durch den NDB, nicht dem Grundrechtsschutz der betroffenen Personen (also auch nicht der inhaltlichen Richtigkeit).

Nur: Ohne Auskunft kann auch in den allermeisten Fällen keine Beschwerde erhoben werden! Ein Rechtsschutz ist nur vorgesehen gegenüber bestimmten verfügungsmässigen Anordnungen des NDB, zum Beispiel zuhanden von auskunftspflichtigen Personen oder von zur Mitwirkung angehaltenen Providern, oder in den seltenen Fällen, wo eine nachträglich über einen genehmigungspflichtigen Eingriff informierte Person im Inland die Rechtmässigkeit der Beschaffung bestreitet (vgl. Art. 79 E DSG). Alle Garantien von Art. 6 EMRK resp. Art. 14 UN-Pakt II (aus Verletzungen von Art. 8 EMRK ergeben sich «civil rights»!), von Art. 13 EMRK sowie von Art. 29a BV sind nach diesem Gesetzesentwurf offensichtlich unmassgeblich.

Ich persönlich halte die fast vollständige Verweigerung eines gerichtlichen Rechtsschutzes gegenüber den betroffenen Personen für den wohl schwersten Verstoss eines Gesetzgebers gegen Verfassung und Völkerrecht.

6. Unzureichende Kontrollen des NDB

Der Gesetzesentwurf führt die bisher bestehenden Kontrollmechanismen weiter: Von praktischer Bedeutung ist einerseits die verwaltungsinterne Kontrolle durch eine kleine Gruppe im Generalsekretariat des VBS, die nach Prüfungsplänen systematische Teil-Überprüfungen vornimmt (Art. 74 E NDG) sowie die parlamentarische Kontrolle durch die Delegation der Geschäftsprüfungskommissionen (GPDel, Art. 77 E NDG; Art. 53 ParlG[15]).[16]

Erfreulicherweise hat die vorberatende Kommission des Ständerates erkannt, dass der Kontrollgruppe des VBS die Unabhängigkeit fehlt (wenn der Chef oder die Chefin des VBS auf die Amtsdirektion hört, statt auf die Kontrolleure, ändert sich nichts) und dass für die parlamentarische Kontrolle sowohl systematische Informationsflüsse, zum Beispiel über die genehmigten Beschaffungen, wie auch die direkten Zugriffsrechte auf die Datenbanken des NDB fehlen.[17] Auch der EDÖB und das Bundesverwaltungsgericht haben für die nicht-öffentlichen Kontrollen aus Anlass eines Auskunftsgesuches keine Zugriffsrechte auf die Datenbanken des NDB, wenn sie zum Beispiel die Löschung anhand von Protokollierungen überprüfen wollen. Nun soll in der Differenzbereinigung nach einem Antrag des Waadtländer Ständerats Luc Recordon eine unabhängige Kontrollbehörde eingesetzt werden.

7. Eine Art extrakonstitutionelle Staatsmacht

Das vom Bundesparlament beratene NDG ist kein modernes, einer offenen freiheitlich-rechtsstaatlichen Demokratie angemessenes Staatsschutzgesetz, sondern es ist ein mit der üblichen Verspätung von kleinen Ländern entworfenes Gesetz im Sinne der US-amerikanischen Gesetzgebung für die NSA, die genau besehen aus dem Kriegsrecht (nach amerikanischem Verständnis: «war on terror») stammt, das unmittelbar nach dem 11. September 2001 beschlossen wurde. Das NDG macht die geheime Überwachung zu einem nicht verfassungskonformen Staatsrechtsprinzip. Sicherlich, eine solche findet in der Internetkommunikation ohnehin schon durch die Wirtschaft statt; doch der Staat hat ganz andere Durchsetzungsmittel als jedes auch globale Unternehmen, und seine Sanktionsmöglichkeiten sind viel weiter entwickelt.

Man könnte also resignieren und denken, dass der Persönlichkeitsschutz heute nicht mehr gewährleistet werden kann. Doch die persönliche Entfaltung und das Bedürfnis nach Meinungsfreiheit und einer freien Kommunikation sind existenziell so elementar, dass sich Menschen nicht dem technologischen und ideologischen Druck beugen.

Dennoch ist das geplante NDG alles andere als ein rechtsstaatlich verantwortbares Staatsschutzgesetz. Mit seinen erheblichen Mängeln ist es nicht akzeptabel, denn es dürfte zu die Gesellschaft vergiftenden Schnüffeleien und zu einem undemokratischen Anpassungsdruck auf kritische Landesbewohner oder abweichend denkende und glaubende Menschen führen, wie wir dies im Kalten Krieg erlebt haben. Das braucht die Schweiz nicht neuerlich.

Die nötigen Verbesserungen gegen die gefährlichsten Bedrohungen des demokratischen Rechtsstaates müssen eben gerade gestützt auf diesen erzielt werden.

9 Was eine «Konkrete Gefahr für die innere und äussere Sicherheit» (nach Art. 19 und 23 E NDG) ist, müsste nachträglich in begründeten, veröffentlichen Entscheiden zur politischen und wissenschaftlichen Diskussion gestellt werden.

10 Vgl. die zahlreichen Verträge in der Systematischen Rechtssammlung des Bundes beginnend mit 0.351.

11 Übereinkommen über die Cyberkriminalität v. 23.11.2001 (SR 0.311.43), in der Schweiz in Kraft seit 1.1.2012.

12 BGE 133 I 77, Erw. 5.3 und 5.4.

13 Urteil des Gerichtshofs (Große Kammer) vom 8.4.2014 (C-293/12).

14 BGE 136 II 508, Erw. 6.1 und 6.3.1.

15 SR 171.10.

16 Für die Funkaufklärung besteht noch eine Unabhängige Kontrollinstanz (Art. 75 E NDG).

17 Zu den Kompetenzen des GPDel siehe Art. 153–155 ParlG.