Eine *sicherheitspolitische* Analyse zum Nachrichtendienstgesetz des Bundes (NDG)

Einleitung/Dokumentaufbau

Der Leser dieses Dokuments mag sich fragen, was mich als Nichtjuristen dafür qualifiziert, ein Gesetz zu analysieren und meine Gedanken und Sorgen zum geplanten Nachrichtendienstgesetz des Bundes (NDG) hier niederzuschreiben und weiterzuleiten. Ganz einfach, ich bin Stimmbürger und darf zu Gesetzesvorlagen abstimmen und Unterschriften zu Referenden und Initiativen sammeln, wie es mein Herz begehrt. Der Umstand, dass sich auch Laien letztlich in unserer Demokratie in Sachen Grundrechte und Staatsform wegweisend ausdrücken können, geht beim Schutz unserer Grundrechte und unseres Staates vielfach vergessen.

Unsere Werte nachhaltig zu schützen, heisst unter anderem, in die Ausbildung unserer Jugend in Recht und Demokratie zu investieren. Zudem wird dabei die Integration in unsere Gesellschaft gefördert. Ich z.B. konnte ein Reifezeugnis erlangen und ein Studium technischer Richtung absolvieren, ohne dabei je eine Stunde Recht besucht haben zu „müssen“. Wie können Grundrechte geschützt werden, wenn dabei eine Vielzahl der hier wohnhaften Menschen sich davon keine Vorstellung machen kann?

Das Vertrauen oder der Glaube der grossen Mehrheit der hier wohnhaften, meist aber rechtsunkundigen Bevölkerung an unsere Staatsform und an unser Rechtssystem verleiht Stabilität und somit Sicherheit. Dieser Aspekt bleibt in unserer durch grosse Veränderungen geprägten Zeit vielfach unbeachtet. Im Moment wird das Heil gegen den Terrorismus in den nachrichtendienstlichen Aktivitäten gesucht. Dies ohne damit wirklich zu beginnen, die Sicherheit, damit notwendigerweise auch unsere Haltung und Ausbildung, zu verbessern, bevor die Privatsphäre und weitere Grundrechte verletzt werden. Im Gegenteil! Z.B. mit Internet der Dinge (engl. Internet of Things) machen wir uns zurzeit und in naher Zukunft noch verwundbarer.

Folgende sicherheitspolitische Themen zum NDG werden hier kurz abgehandelt:

- Diplomatische Beziehungen
- Neutralität
- Glaube an die Rechtsordnung
- Wirtschaftliche Sicherheit

Jedem der genannten Themenpunkte wird ein Unterkapitel eingeräumt, und dazu einige sicherheitsrelevante Aspekte dargelegt.

Diplomatische Beziehungen

Gute diplomatische Beziehungen sind für die Sicherheit eines kleinen Landes mit beschränkten militärischen Mitteln wie der Schweiz eminent wichtig. Etwelche Interventionen in anderen Ländern sollten deshalb mit äusserster Zurückhaltung durchgeführt werden. Gute diplomatische Beziehungen sind auch eine Voraussetzung, den Terror auf internationaler Ebene zu bekämpfen. Ohne internationale Zusammenarbeit kann meines Erachtens dem Terrorismus und den Angriffen übers Internet vom Ausland aus nicht wirksam entgegengetreten werden. Deswegen sind wir auf gute Kooperation mit der Polizei und der Strafverfolgungsbehörde im Ausland angewiesen.

Der Nachrichtendienst des Bundes (NDB) kann zur Abwehr von Angriffen auf kritische Infrastrukturen in Computersysteme und Computernetzwerke eindringen, welche sich im Ausland befinden. Dies um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen.[1] Unklar ist in der Informationstechnologie (IT) jedoch meist, ob der Angriff wirklich von diesem Computer aus stattfindet oder der Computer nur vorgeschoben ist und die Strippen von einem Computer von ganz anderswo gezogen werden.

Angenommen, ein Computer im Ausland wird zum Betrieb einer kritischen Infrastruktur eingesetzt und wird für einen Hackerangriff in der Schweiz vorgeschoben verwendet. D.h. die Betreiber der Infrastruktur im Ausland haben keine Kenntnisse von diesem Angriff. Kommt es nun durch die Intervention des NDB zum Absturz der Infrastruktur im Ausland, so kann dies einen diplomatischen Vorfall erster Güte hervorrufen und dadurch die diplomatischen Beziehungen mit diesem Land oder eventuell sogar mit anderen Ländern beeinträchtigen. Bevor der Bundesrat über eine solche Massnahme entscheidet, sollte der NDB dazu verpflichtet werden, falls irgendwie noch möglich, zuerst die Polizei oder eine andere Ermittlungsbehörde des entsprechenden Landes zu benachrichtigen und um Unterstützung anzufragen.

Anmerkung: *Um die Sicherheit einer von einem Hacker-Angriff betroffenen kritischen Infrastruktur in der Schweiz ist es sehr schlecht bestellt, wenn die Sicherheitsfachleute dieser Infrastruktur nicht schneller die Netzwerkadresse desjenigen Computers zu sperren vermögen, wovon der Hackerangriff vermeintlich initiiert wurde. Dies, bevor der Bundesrat eine mögliche Intervention genehmigt hat.*

[1] Art. 37 Abs. 1 NDG

Der NDB kann weiter in Computersysteme und Computernetzwerke im Ausland eindringen, um dort vorhandene oder von dort aus übermittelte Informationen über Vorgänge im Ausland zu beschaffen[2]. Eine solch präventive Massnahme, einhergehend mit der territorialen Verletzung eines anderen Staates, ist mit einer international anerkannten Politik kaum in Einklang zu bringen und der internationalen Gemeinschaft kaum verständlich und nachvollziehbar zu erklären, was den guten diplomatischen Beziehungen mit dem Ausland erheblich schaden könnte. Zudem stellt sich die Frage, ob eine solche präventive Aktion das Völkerrecht verletzt.

Neutralität

Die Schweiz hat sich dazu entschlossen, sich in internationalen Konflikten neutral zu verhalten. Die Abkehr von einer Neutralitätspolitik bei gleichzeitiger Wahrung der Sicherheit kann für ein kleines Land mit beschränkten militärischen Ressourcen nur mit dem Beitreten eines militärischen Bündnisses einhergehen. Eine Neutralitätspolitik zu verfolgen und dabei von der internationalen Gemeinschaft nicht als neutraler Staat anerkannt zu werden, ist für die Sicherheit wenig zielführend. Folglich stellt die internationale Anerkennung der Neutralität ein wesentlicher Sicherheitsfaktor für die Schweiz dar. In diesem Sinne sollte die Schweiz möglichst keine Selektion bei Konflikten vornehmen.

Der NDB kann, *d.h. muss aber nicht*, Personendaten ans Ausland weitergeben, falls die rechtlichen Voraussetzungen erfüllt sind[3]. Die Weitergabe der Daten ist selektiv, weil nicht alle Länder in den Genuss des Informationstransfers gelangen werden. Innerhalb der Selektion ist sie zudem ohne Nennung von Gründen und somit nicht nachvollziehbar optional. Z.B. ist die Weitergabe der Information selbst dann optional und zugleich selektiv, wenn sie zum Schutz von Leib und Leben notwendig ist[4].

Die optionale und selektive Weitergabe sind der internationalen Gemeinschaft im Kontext zur Neutralität vermutlich schwer verständlich zu machen. Insbesondere dann, wenn publik würde, dass mit der Weitergabe der Informationen vermutlich ein Bombenanschlag verhindert und Menschen vor Tod oder Invalidität bewahrt hätten werden können.

Anmerkung: Die Neutralitätspolitik ist ein Mittel der Aussen- und Sicherheitspolitik und ein Handlungsziel der vereinigten Bundesversammlung (Art. 173 Abs. 1 lit. a), wie auch des Bundesrats (Art. 185 Abs. 1 BV). Sie enthält jedoch keine übergeordneten Grundsätze (Rhinow/Schefer, Schweizerisches Verfassungsrecht, 2.A., Rz. 3533). Folglich sind die hier vorgebrachten Argumente politischer und nicht rechtlicher Natur. Doch hier steht die „sinnvolle“ Sicherheitspolitik im Vordergrund.

[2] Art. 37 Abs. 2 NDG

[3] Art. 61 Abs. 1 NDG

[4] Art. 61 Abs. 2 Bst. e NDG

Glaube an die Rechtsordnung

Einleitung

Der Glaube an den Sinn, an die Zweckmässig- und mehrheitlich an die Richtigkeit der bestehenden Rechtsnormen, kurz der Glaube an die Rechtsordnung, ist für die Stabilität und somit für die Sicherheit eines Landes wichtig. Dies besonders in Zeiten mit grossen gesellschaftlichen Umwälzungen, nicht zuletzt auch durch die Informationstechnologie (IT) hervorgerufen. Es ist sogar mit einer Zunahme der gesellschaftlichen Veränderungen infolge der geplanten, weltweiten Ausbreitung von „Internet der Dinge“ zu rechnen. (Zu Internet der Dinge, s. z.B. Weber)

Verhältnismässigkeit, Rechtsgleichheit, Berufsgeheimnis

Für die Rechtsgleichheit ist das Anwaltsgeheimnis eine notwendige, aber nicht ausreichende Bedingung. Denn ein Otto-Normalbürger sollte vor dem Strafrichter mit gleichem Wissen und Fähigkeiten wie ein wegen des gleichen Delikts angeklagter Jurist ausgestattet sein. Dies um sich ähnlich geschickt verteidigen und seine Sicht der Dinge in für ihn vorteilhafter Weise präsentieren zu können. In diesem Sinne hat das Gespräch zwischen dem Anwalt und seinem Mandanten grundsätzlich vertraulich zu bleiben und sollte nicht für die Strafverfolgung verwendet werden.

Der Nachrichtendienst des Bundes (NDB) darf Vorgänge an öffentlichen und allgemein zugänglichen Orten in Bild und Ton ohne vorherige Genehmigung, d.h. uneingeschränkt und systematisch, aufnehmen.[5] Er kann dabei auch Fluggeräte (z.B. lautlose Drohnen) und Satelliten einsetzen. Das heisst also, dass das Gespräch, welches in der Öffentlichkeit z.B. bei einem Spaziergang oder an einem abgelegenen oder menschenleeren Ort oder in einem allgemein zugänglichen Gebäude dem Arzt, dem Rechtsanwalt, dem Geistlichen, dem Journalisten oder dem Vermögensverwalter anvertraut wurde, aufgezeichnet werden darf.

> Wenn man sich bei der Definition von „allgemein oder öffentlich zugänglich“ auf das Bundesgesetz zum Schutz von Passivrauchen[6], auf die Bundesverordnung BehiV[7] oder auf Art. 179^{quater} Strafgesetzbuch abstützt, ist Folgendes zulässig: Das Abhören eines Gesprächs zwischen einem Arzt oder Krankenschwester und den Patienten in einem Spitalpark oder im allgemein zugänglichen Bereich eines Spitals. Kirchen gelten m.E. ebenfalls als allgemein zugänglich, da ihr Zutritt nicht eingeschränkt ist.

[5] Art. 14 Abs. 1 NDG

[6] Art. 1 Abs. 2 Bst. a

[7] Art. 2 lit. c BehiV

Zwar sind die Bild- und Tonaufnahmen, welche dem privaten Bereich zuzurechnen sind, nicht zulässig[8]. Doch dieser nicht zulässige Bereich bezieht sich meines Erachtens auf die privaten Räumlichkeiten und nicht auf den Inhalt des aufgezeichneten Gesprächs (so auch die Botschaft zum NDG S. 47, Abs. 3). Die im NDG aufgeführte Respektierung des Berufsgeheimnisses nach Art. 21 NDG bezieht sich nur auf die Auskunftspflicht gemäss Art. 19 und 20 NDG und somit nicht auf die Beschaffung von Informationen an öffentlichen oder allgemein zugänglichen Orten[9].

Falls dies rechtlich unklar sein sollte, ein Grund mehr skeptisch zu werden, weil dagegen kein Rechtsmittel aus Unkenntnis der Sachlage und wegen des eingeschränkten Auskunftsrechts ergriffen werden kann. Zum restriktiven Auskunftsrecht im NDG siehe auch Plädoyer Artikel 4/ 2015 von Prof. Dr. Rainer Schweizer.

Die nicht zulässigen Aufnahmen sind zwar umgehend zu löschen[10]. Doch hier stellen sich weitere Probleme ein. Z.B. derjenige im NDB, welcher auswertet und darüber entscheidet, was gelöscht werden soll, hat Kenntnis über den Inhalt des Gesprächs. Somit ist der Geheimniskreis des z.B. mit dem Arzt im Freien oder an einem allgemein zugänglichen Ort geführten Gesprächs erweitert worden. Wer kontrolliert zudem, dass die nicht rechtmässig erlangten Informationen auch wirklich gelöscht werden?

Dass die Kontrolle der nachrichtendienstlichen Überwachung und die Rechtsmittel dagegen ungenügend sind, siehe dazu neben dem erwähnten Artikel aus dem Plädoyer 4/2015 auch Art. 63 Abs. 2 Bst. c NDG. Dies berechtigt den NDB, die Auskunft an eine Person über ihre Daten aufzuschieben, selbst dann, wenn gar keine Informationen über diese Person bearbeitet worden sind.

Der NDB darf unaufgefordert seine genehmigungsfreien Erkenntnisse unter Wahrung des Quellenschutzes zur Strafverfolgung an andere Behörden weiterleiten[11]. Für welche Delikte der NDB seine Erkenntnisse an die Strafverfolgungsbehörde weiterleiten darf, ist nicht definiert und ist vermutlich nicht beschränkt worden, wie beispielsweise in Art. 269 Abs. 2 Bst. a der Strafprozessordnung (StPO). Durch den Quellenschutz kann unter Umständen von aussen gar nicht festgestellt werden, ob die Erkenntnisse des NDB für die Strafverfolgung auf einer unrechtmässigen Beschaffung von Informationen beruhen.

Es kann entgegnet werden: „Nur diejenige Delikte, gegen welche das Gesetz zu schützen bezweckt, dürfen zur Strafverfolgung an die Strafverfolgungsbehörde weitergeleitet werden. Alles andere ist unrechtmässig und unterliegt dem Beweismittelverbot.“ Artikel 60 Abs. 3 NDG umfasst jedoch meines Erachtens noch weitere Delikte, zu welchen Informa-

[8] Art. 14 Abs. 2 NDG

[9] Art. 14 NDG

[10] Art. 14 Abs. 2 NDG

[11] Art. 60 Abs. 2 NDG

tionen weitergegeben werden dürfen, welche aber nicht mit dem Zweck des Gesetzes übereinstimmen.

Im NDG besteht bei der genehmigungsfreien Überwachung keine Pflicht, analog zu Art. 271 Strafprozessordnung (StPO) Informationen, welche dem Berufsgeheimnis zugeordnet werden, auszusondern und der Strafverfolgungsbehörde vorzuenthalten. Die genehmigungsfreie Überwachung aus dem NDG ist der Observation (Art. 282, 283 StPO) bei der Strafprozessordnung ähnlich. Jedoch unterscheiden sie sich in folgenden, wesentlichen Punkten:

- Beim NDG besteht keine Mitteilungspflicht an den Observierten; im Unterschied zu Art. 283 Abs. 1 StPO.
- Beim NDG besteht keine zeitliche Beschränkung von einem Monat wie bei der polizeilichen Observation nach Art. 282 Abs. 2 StPO.
- Die Observation nach NDG beschränkt sich nicht auf eine bestimmte tatverdächtige Person
- Es wird beim NDG kein Tatverdacht für die Überwachung benötigt.
- Zudem attestiert das NDG ein Recht auf systematische und für viele betroffene Personen unerkennbare[12] Überwachung[13].
- Aus der Art der genehmigungsfreien Überwachung nach NDG erübrigt sich meines Erachtens eine Diskussion über die Verwertung von Zufallsfunden, u.a. da die genehmigungsfreie Überwachung nicht zielgerichtet und personenbezogen sein muss und folglich die Erkenntnisse aus den Observationen auf Zufall basieren.
- Uneinig ist sich die Lehre darüber, ob im Fall einer Observation bei Einsatz hochtechnischer Geräte es einer Genehmigung bedarf (s. dazu Donatsch, Kommentar zu Art. 282, Rz. 9). Bei der genehmigungsfreien Überwachung nach NDG ist anzunehmen, dass hier in puncto Technik keine Schranken gesetzt sind.

  Anmerkung zur Observation nach Art. 282-283 StPO: Die Respektierung des Berufsgeheimnisses wird im 1. und 2. Abschnitt des Kapitels 8 der StPO attestiert, nicht aber im 3. Abschnitt (Observation), auch nicht im 4. Abschnitt zum Bankgeheimnis. Somit kann in Analogie dazu vermutet werden, dass die aus der genehmigungsfreien Überwachung gewonnen Erkenntnisse gemäss dem NDG selbst bei Verletzung des Berufsgeheimnisses strafrechtlich verwertet werden dürfen. In den drei einschlägigen Werken Riedo, Schmid und Donatsch ist zur Observation nach StPO betreffend die Verwertung von Berufsgeheimnissen nichts erwähnt worden. In WOSTA ebenfalls nicht.

Bei der genehmigungspflichtigen Überwachung wird ebenfalls der Schutz des Berufsgeheimnisses nur insofern attestiert, dass die Erweiterung der genehmigungspflichtigen Überwachung auf Berufsgeheimnisträger untersagt ist[14]. Die Erkenntnisse dürfen der Strafverfolgungsbehörde weitergeleitet werden, wenn die Strafverfolgungsbehörde eine

[12] Art. 5 Abs. 4 NDG

[13] Art. 14 Abs. 1 NDG

[14] Art. 28 Abs. 2 NDG

ähnliche strafprozessuale Massnahme ergriffen hätte[15]. D.h. eine richterliche (unabhängige) Genehmigung fürs Weiterleiten der Informationen ist nicht erforderlich. Im Fall der Überwachung des Post- und Fernmeldeverkehrs wird in der StPO jedoch verlangt, dass Berufsgeheimnisse auszusondern sind und der Strafverfolgungsbehörde nicht zur Kenntnis gelangen dürfen[16].

> *Weiter ist mit der Einführung des NDG nicht eine Gesetzesänderung in der StPO angedacht, wie mit den Informationen, welche vom NDB geliefert werden, umzugehen ist.*

Falls bei der Verletzung des Berufsgeheimnisses doch ein Beweisverwertungsverbot bestünde, dann hätte dies folgenden Nachteil: Wenn ein Staatsanwalt nicht weiss, wer die Straftat begangen hat, dann kann er sich in den Untersuchungen verzetteln, weil er nicht weiss, ob sich der Aufwand für eine Ermittlung in eine bestimmte Richtung lohnt. In Anbetracht dessen, dass die Staatsanwaltschaft heutzutage meistens überlastet ist, ist ein Hinweis durch den NDB „willkommen", in welche Richtung die Suche erfolgversprechend ist.

Ebenfalls kann der NDB oder kantonale Organe, welche mit dem Vollzug des Gesetzes betraut sind, Informationen von den Sozialversicherungsinstitutionen beziehen[17], sofern kein überwiegendes privates Interesse entgegensteht. Über die Auskunft ist meines Erachtens Stillschweigen zu wahren[18]. Somit hat der Betroffene kein Rechtsmittel dagegen.

Es besteht auch die Gefahr, dass mit Hilfe dieses Wissens oder mit den Erkenntnissen aus den Überwachungen an öffentlichen oder allgemein zugänglichen Plätzen die Berufsgeheimnisträger selber gegenüber der Nachrichtendienstbehörde gefügig gemacht werden können. Die Überwachung kann nämlich auch für Berufsgeheimnisträger belastendes Material hervorbringen.

[15] Art. 60 Abs. 3 NDG

[16] Art. 271 Abs. 1 und 3 StPO

[17] 2015 BBL 7260 ff

[18] Art. 19 Abs. 3 NDG

Folgende Frage stellt sich betreffend die Verhältnismässigkeit der Überwachung:

- Warum kann im Sinne der Rechtssicherheit nicht analog zu Art. 269 StPO die Informationsweitergabe des NDB an die Strafverfolgung eingeschränkt werden? Dies auch im Sinne der Verhältnismässigkeit und einer Rechtsgüterabwägung u.a. zwischen der Verletzung der Privatsphäre und dem Interesse an Strafverfolgung.
- Warum kann nicht eine Genehmigungspflicht bei der Überwachung an allgemein zugänglichen Orten gefordert werden, wenn die allgemein zugänglichen Orte normalerweise Tätigkeitsgebiete sind, an denen Berufsgeheimnisträger arbeiten? Wie z.B. Kirchen, Spitäler, Gerichte, Gebäude von Behörden.
- Ist es für unseren Schutz notwendig, dass das Stimm- und Petitionsgeheimnis im neuen Nachrichtendienstgesetz nicht mehr so absolut garantiert wird, wie dies bisher noch im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS Art. 3 Abs. 3) getan wird? Zwar wird der Schutz der politischen Rechte im NDG (Art. 5 Abs. 5) attestiert, doch besteht eine Ausnahmeklausel (Art. 5 Abs. 6), insbesondere für verbotenen Nachrichtendienst. Dies ist aber lediglich ein Vergehen.

Exkurs Patientendossier

Unter anderem Behörden, welche für den Betrieb von Informatiksystemen zuständig sind, haben dem NDB Auskunft zu erteilen[19]. Dabei definiert der Bundesrat im digitalen Zeitalter seinen Kompetenzumfang bei der Informationsbeschaffung durch den NDB selber und darf diesen Umfang unseren Bürgern verschweigen[20]. Ob nun das Bundesamt für Gesundheit (BAG) im Rahmen des Patientendossiers informationspflichtig ist, ist unbedingt abzuklären. Wenn dem so ist ja, dann weiss niemand ausserhalb, in welchem Umfang das BAG im Rahmen seiner Möglichkeiten dem NDB auskunftspflichtig ist.

Man mag nun einwenden, dass das Berufsgeheimnis wegen Art. 21 NDG geschützt und somit nicht gefährdet ist. Doch ein Recht zu besitzen, ohne dabei zu wissen, wann es verletzt wurde und folglich dagegen keine Rechtsmittel ergreifen zu können, ist mehr oder weniger bedeutungslos. Das BAG hat nämlich bei der Auskunftserteilung an den NDB Stillschweigen gegenüber den Betroffenen zu wahren[21]. Falls sich das BAG weigerte, Informationen wegen möglicher Verletzung des Berufsgeheimnisses zu senden, dann entscheidet die gemeinsame Aufsichtsbehörde, d.h. in diesem Fall der Bundesrat, endgültig[22].

[19] Art. 20 Abs. 1 Bst. i

[20] Art. 20 Abs. 4 NDG

[21] Art. 20 Abs. 2

[22] Art. 22 Abs. 1 NDG

Somit wird nie ein unabhängiges Gericht darüber befinden, und die Betroffenen werden nie davon erfahren.

Glaube an die Richtigkeit der Normen

Es ist auch für den in der Schweiz wohnhaften Otto-Normal-Bürger schwer nachvollziehbar, wenn der NDB dessen Daten wegen eines Vergehens wie verbotener Nachrichtendienst, eventuell sogar wegen eines Bagatelldelikts, an eine Strafverfolgungsbehörde weiterleiten darf[23], aber sich das Recht vorbehalten kann, Personendaten zum möglichen Schutz von Leib und Leben ans Ausland weiterzuleiten. Über die Weiterleitung von Erkenntnissen an die Strafverfolgungsbehörde kann man geteilter Meinung sein. Doch in diesem Kontext ist folgende Kompetenzerteilung durch das Parlament an den NDB für mich als Otto-Normalbürger nicht nachvollziehbar:

> Im Ausland wohnhafte Personen, welche Informationen für den NDB beschaffen, oder Mitarbeiter ausländischer Nachrichtendienstbehörden, muss der NDB gemäss dem geplanten Nachrichtendienstgesetz nur preisgeben, wenn diese Personen wegen schwerer Verbrechen gegen die Menschlichkeit oder wegen eines Kriegsverbrechens beschuldigt werden[24].

Die Identität der in der Schweiz wohnhaften Menschen, welche den NDB mit Informationen versorgen, wird aber bereits bekannt gegeben, wenn sie wegen einer von Amtes wegen verfolgten Straftat beschuldigt werden oder die Bekanntgabe unerlässlich ist, um eine schwere Straftat aufzuklären[25]. Eine Offenlegung der Identität kann jedoch eine gesellschaftliche Ächtung dieser Person und somit auch eine Vermögenseinbusse zur Folge haben.

„Princes in this case do hate the traitor,
though they love the treason“
Samuel Daniel

Zur Ungleichbehandlung der Informationszuträger im In- oder aus dem Ausland sei angemerkt: „Loyalität definiert sich anders.“ *Loyalität ist aber ein wichtiger zwischenmenschlicher Faktor bei den Behörden, welche für die Aufrechterhaltung der Ordnung verantwortlich sind.*

[23] Art. 60 Abs. 2 NDG

[24] Art. 35 Abs. 1 NDG

[25] Art. 35 Abs. 2 NDG

Die folgende Konstellation birgt meines Erachtens etwas Menschenverachtendes und Abstossendes:

- das Schützen von Schwerverbrechern im Ausland durch eine Behörde in der Schweiz. Damit ist gemeint, dass der NDB das Recht hat, die Identität eines möglichen Schwerverbrechers nicht preisgeben zu müssen, ausser wenn er wegen eines Kriegsverbrechens oder eines Verbrechens gegen die Menschlichkeit angeklagt ist.
- die Kompetenz derselben Behörde, Erkenntnisse über eine hier wohnhafte Person zwecks Strafverfolgung eines Vergehens weiterleiten zu dürfen; wobei möglicherweise dieses Wissen unter Verletzung des Berufsgeheimnisses erlangt wurde. Im Moment noch unklar, ob dies auch für ein beliebiges Delikt erfolgen kann oder nur für Delikte, welche das NDG bezweckt, zu verhindern oder zu verfolgen.
- keine Pflicht zu besitzen, Personendaten ans Ausland zum Schutz von Leib und Leben unbeteiligter Dritter weiterzuleiten.
- Personendaten ohne vorherige Kontrolle Dritter an ein Land zu senden, was für die betroffenen Personen beim Besuch dieses Landes je nach veränderter politischer Situation eventuell schädliche bis existenzielle Konsequenzen haben kann.
- die rechtsungleiche Behandlung betreffend Schutz der Informationszuträger im In- und aus dem Ausland, wobei die Informationszuträger, welche durchs NDG geschützt werden, Schwerbrecher sein dürfen.
- dies alles u.a. zum Schutz gegen ein Vergehen wie den verbotenen Nachrichtendienst (Art. 272 - 274 StGB)[26].

Nicht nachvollziehbare und gegen das elementare Gerechtigkeitsempfinden zuwiderlaufende Bestimmungen sind der Unterstützung der Rechtsnormen durch die Allgemeinheit abträglich und fördern die Nichtbeachtung oder die Renitenz gegen bestehende Gesetze und Normen.

Rechtsdurchsetzung

Wenn Gesetze nicht konsequent durchgesetzt werden, besonders wenn dies mit Einschränkung der Grundrechte verbunden ist, so kann dies auch bewirken, dass das Vertrauen oder der Glaube in die bestehende Rechtsordnung schwindet.

[26] Art. 6 Abs. 1 Bst. a Ziff. 2 NDG

Als Beispiel dazu sei hier der verbotene wirtschaftliche Nachrichtendienst (Art. 273 StGB) erwähnt. Mit dem Outsourcing von Informatikdienstleistungen an ausländische Unternehmen oder mit der Einführung von Cloud Diensten von ausländischen Unternehmen lässt sich in den meisten Fällen nicht verhindern, dass Geschäftsgeheimnisse den Outsourcing- oder Cloud-Unternehmen zugänglich gemacht werden. Somit müsste generell ein Cloud oder Outsourcing Verbot mit ausländischen Unternehmen an diejenigen Schweizer Unternehmen ausgesprochen werden, welche durch diesen Strafgesetzartikel geschützt werden. Dies wurde bisher nicht konsequent durchgesetzt, und wird es kaum je werden.

Anmerkung: „Geschützt werden die wirtschaftlichen Gesamtinteressen des Staates". Trechsel, Kommentar zu Art. 273 Rz 2, unter Verweis auf BGE 101 IV 313 „Art. 273 ahndet ein Delikt gegen den Staat… Der Staat hat ein Interesse daran, dass die…usw." Als Rechtsfertigungsgrund genügt auch nicht die Einwilligung des verletzten privaten Wirtschaftssubjekts, Trechsel, Rz 14 zu Art. 273.

Das NDG mit den daraus resultierenden, einschneidenden Überwachungsmassnahmen bezweckt unter anderem den Schutz von Geheimnissen (Art. 272 -274 StGB). Deshalb bleibt Folgendes in diesem Kontext unverständlich:

> Der Bundesrat hat eine technische Lösung für die elektronische Zustellung von Rechtsschriften an die Behörde und zwischen den Behörden genehmigt, welche es ermöglicht, dass elektronisch übermittelte Rechtsschriften, z.B. zwischen Staatsanwaltschaft und Gericht, dem privaten Betreiber der Zustellplattform (z.B. PrivaSphere) zugänglich gemacht oder offenbart werden. Der Betreiber kann somit von aussen unerkennbar Einsicht in die Dokumente nehmen. [27] Diese Lösung wurde bereits realisiert und in Betrieb genommen.

Zweckmässigkeit

Damit ein Gesetz anerkannt wird, muss es auch zweckmässig sein. Das Gesetz ist jedoch betreffend den Schutz kritischer Infrastrukturen ungenügend. Zu den meisten kritischen Infrastrukturen bestehen nämlich keine verbindlichen Sicherheitsvorschriften auf Bundesebene.

[27] Kap. 4.3.1 Abs. 2 lit. c und Kap. 6.5 Abs. 2 Kriterienkatalog Zustellplattformen – Version 2.0 vom 16. September 2014, Artikel im Plädoyer, 3/2013, 3/2014.

Rechtssicherheit

Wenn man nun aufgrund rechtsunsicherer Begriffe wie „auf andere Art und Weise fördern“ ein Tätigkeits-[28] oder ein Organisationsverbot[29] verhängen kann, ist dies für die Rechtssicherheit und folglich für das Vertrauen in das rechtsstaatliche Handeln abträglich. Gegen das Verbot kann zwar eine Beschwerde eingereicht werden, doch sie hat keine aufschiebende Wirkung[30]. Bis zu einem rechtskräftigen Gerichtsurteil kann ein vom Verbot betroffenes Unternehmen oder eine davon betroffene Privatperson ruiniert sein.

Haftung bei unrechtmässigen Interventionen durch den Staat

Eine *gute* Reputation ist heutzutage im Zeitalter der neuen Medien ein äusserst fragiles Gut, aber ein guter Ruf je nach Geschäftstätigkeit unverzichtbar.

Verwechslung ist in der IT im Gegensatz z.B. zur Video-Überwachung ein akutes Risiko. Übers Internet lassen sich nämlich grundsätzlich keine Personen identifizieren. Zudem ist der Schaden infolge eines Reputationsverlusts schwierig zu bemessen, wie auch den adäquaten Kausalzusammenhang zwischen der Rufschädigung und der Einkommenseinbusse zu beweisen.

Diesem Umstand wird im NDG nicht Rechnung getragen. Die Haftung des NDB bei zu Unrecht begangenen Schäden, z.B. infolge Verwechslung und daraus entstandenen Reputationsschaden, sollte deshalb im Nachrichtendienstgesetz speziell geregelt werden. Man mag argumentieren, dass das Verantwortlichkeitsgesetz des Bundes die Haftung der Behörde klärt, und dies folglich ausreicht. Jedoch sollte hier eine Beweislastumkehreingeführt werden; nämlich dass der NDB beweisen muss, dass zwischen der Rufschädigung und der Einkommenseinbusse kein Kausalzusammenhang besteht. Dies aus folgenden Gründen:

- Wegen der asymmetrischen Informationslage zwischen Bürger und dem NDB
- Wegen der Schwierigkeit, die für die Beweisführung notwendigen Informationen zu beschaffen
- wegen des Risikos, welches vom NDB hervorgeht.

Es besteht die Gefahr, dass eine durch den NDB zu Unrecht ge-, aber nicht entschädigte Person und eventuell ihr privates Umfeld den Glauben an unsere Rechtsordnung verlieren.

Anmerkung: Die Begriffe „Identifizieren“ und „Identifikator“ werden in verschiedenen Bestimmungen wie im Bundesgesetz über die elektronische Signatur (ZertES) falsch ver-

[28] Art. 73 Abs. 1 NDG

[29] Art. 74 Abs. 1 NDG

[30] Art. 83 Abs. 2 NDG

wendet[31], führen zu falschen Assoziationen und möglicherweise zu einem falschen Verständnis des Sachverhalts[32]. Eine elektronische Signatur vermag eine Person nicht zu identifizieren, denn die Mittel zum Leisten einer elektronischen Signatur lassen sich ohne nennenswerten Aufwand einer anderen Person aushändigen.

Kontrolle, Schutz vor Amtsmissbrauch

Im Namen unserer Sicherheit,
wer schützt uns vor dem Staatsschutz?

Gerade in Zeiten grosser gesellschaftlicher Veränderungen sollte besonders darauf geachtet werden, dass nicht Menschen, welche eine Umwälzung der bestehenden Rechtsordnung zum Schaden vieler anstreben, viel und unkontrollierbare Machtkompetenz erhalten, z.B. mittels der Kontrolle über die angedachte Nachrichtendienstbehörde. Bei der Kontrolle des NDB und somit beim Schutz gegen Amtsmissbrauch stellen sich folgende Fragen:

- Warum ist es nicht möglich, den Chef des Kontrollorgans für den NDB durch die Bundesversammlung wählen zu lassen?
- Warum ist es nicht möglich, den Chef des Kontrollorgans des NDB den Sicherheitskommissionen des Parlaments zu unterstellen und dort rapportieren zu lassen?
- Weil das Missbrauchspotential bei dem NDB doch beträchtlich ist, warum ist kein qualifizierter Straftatbestand für verbotenen Nachrichtendienst oder für Amtsmissbrauch, begangen von Mitarbeitern des NDB, eingeführt worden?
- Warum ist keine richterliche Genehmigung erforderlich, um kritische Personendaten ins Ausland transferieren zu dürfen?
- Warum kann nicht ein Rechtsbeistand beim Transfer kritischer Personendaten hinzugezogen werden, welcher die Interessen und Rechte der davon betroffenen, ihm aber unbekannten Personen vertreten kann?
- Können mögliche Kompetenzerweiterungen wie in Art. 3 NDG nicht nachträglich und schnellst möglich durch das Parlament abgesegnet werden?

Die Geschichte hat uns gelehrt, dass mit Kompetenzerweiterungen in Krisenzeiten sparsam und kontrolliert umgegangen werden sollte. Das Leben und die Geschichte haben mich weiter gelehrt, dass unkontrollierbare Macht in den seltensten Fällen das Gute im Menschen weckt. Die Nacht auf unseren Abstimmungssonntag vom 28.2. ist diesbezüglich ein Datum des letzten Jahrhunderts, welches uns fest in Erinnerung bleiben sollte.

[31] Art. 2 Abs. b Ziff. 2

[32] Plädoyer, 3/2014, Daniel Muster

Manche mögen mich nun wegen meiner Vorsicht als Schwarzseher abstempeln. Wir Menschen neigen jedoch dazu, aus den Erfahrungen in der Vergangenheit die Zukunft vorauszusagen und dabei die unwahrscheinlichen Ereignisse auszublenden. Aus dieser Perspektive und in Anbetracht der politischen Stabilität in der Schweiz mag das Urteil gerechtfertigt sein. Doch unwahrscheinliche Ereignisse treten immer wieder auf, wie die Fichenaffäre, der NSU Prozess in Deutschland und die Zerstörung der beiden Gebäude des World Trade Centers in New York.

Rechtstaatlichkeit

Als Behörde genügt es nicht, Recht zu haben,
sie muss auch noch recht(mässig) handeln.

Behörden des Bundes und der Kantone sowie Organisationen, denen der Bund oder die Kantone die Erfüllung öffentlicher Aufgaben übertragen haben, sind dem NDB bei einer konkreten Bedrohung auskunftspflichtig[33]. In Art. 20 NDG wird weiter aufgelistet, welche Behörden zudem *bedingungslos auskunftspflichtig* sind. Z. B. Gerichte und Behörden, welche für den Betrieb von Informatiksystemen zuständig sind und somit über viele sensitive Informationen verfügen können. *Der Umfang der Auskunftspflicht gegenüber dem NDB bleibt unveröffentlicht und bleibt somit uns allen unbekannt*[34].

> *Dass der selbst zurechtgeschusterte Kompetenzumfang einer Behörde, hier beim Umfang, Informationen einzufordern, der Öffentlichkeit in Friedenszeiten unbekannt ist, widerspricht m.E. den liberalen Grundsätzen des rechtsstaatlichen Handelns.*

Auch durch den Rechtsweg bei Uneinigkeit zwischen einer Bundesbehörde und dem NDB wird keine Transparenz und Einsicht von ausserhalb geschaffen, weil die gemeinsame Aufsichtsbehörde endgültig entscheidet[35].

Gegen die Auskunftspflicht der Behörden, Informationen an den NDB zu einer Person zu liefern, kann die betroffene Person aus Unkenntnis kein Rechtsmittel ergreifen. Die Behörden sind nämlich generell dazu verpflichtet, Stillschweigen betreffend das Auskunftsbegehren zu wahren[36].

Anmerkung: Wenn bekannt wird, dass das BAG betreffend Patientendossier auskunftspflichtig ist, aber der Umfang unbekannt bleibt, so kann dies den Erfolg des Projektes infolge Nicht-Akzeptanz durch die Patienten beinträchtigen.

[33] Art. 19 NDG

[34] Art. 20 Abs. 4 NDG

[35] Art. 22 Abs. 1 NDG

[36] Art. 19 Abs. 3 und Art. 20 Abs. 2 NDG

Schein

Der Bundesrat kann im Falle einer schweren und unmittelbaren Bedrohung den NDB für weitere Zwecke einsetzen, als in Art. 2 NDG aufgeführt ist.[37] Erst bei einer schweren und unmittelbaren Bedrohung mit der Prävention (u.a. mit der Überwachung und dem Sammeln von Informationen) zu beginnen, ist aus sicherheitstechnischer Sicht bedingt wirkungsvoll, wenig zielführend, somit töricht und eine Scheinsicherheit vorgaukelnd.

Ein Zweck des NDG ist der Schutz kritischer Infrastrukturen. Dabei stellt sich im Kontext zur Grundrechtsverletzung durch das NDG die Frage, wie viel Geld der Bund zum Schutz kritischer Infrastrukturen bisher ausgegeben und für die kommenden Jahre budgetiert hat. Ohne wirksamen Schutz ist eine Überwachung der Bürger als Begleitmassnahme zur Sicherheit kritischer Infrastrukturen wenig zielführend und somit unverhältnismässig.

Wirtschaftliche Sicherheit

Das wirtschaftliche Wohlergehen der Schweiz basiert unter anderem auf den guten diplomatischen Beziehungen mit dem Ausland, auf der Neutralitätspolitik, auf der Rechtssicherheit, auf der Konkurrenzfähigkeit durch attraktive wirtschaftliche Rahmenbedingungen, wie auf der Wahrung des Berufsgeheimnisses, und auf der Lebensqualität. Wobei letzteres auch darauf beruht, dass die staatlichen Eingriffe rechtmässig und kontrollierbar sind und sich in akzeptablen Grenzen halten.

Zum Standortvorteil sei z.B. angemerkt: Viele IT-Dienstleister in der Schweiz, insbesondere Cloud-Anbieter, und der Finanzplatz Schweiz profitieren vermutlich davon, dass sie bis dato einem weniger rigorosen Überwachungsgesetz unterliegen als ihre Mitbewerber in anderen Ländern. Dies verleiht ihnen Marktvorteile gegenüber der Konkurrenz aus dem Ausland, s. dazu auch s. NZZ 14.6.2013. Dieser Wettbewerbsvorteil könnte nach der Einführung des neuen Nachrichtendienstgesetzes nicht mehr vorhanden sein. Ob nun jemand seine Daten an ein schweizerisches oder an ein ausländisches Unternehmen auslagert, spielt dann betreffend Einsichtnahme und die unkontrollierbare Weiterleitung der Informationen ans Ausland keine Rolle mehr.

Fazit

Ein Terroranschlag ist nicht nur ein Angriff auf Leib und Leben, sondern auch ein Anschlag auf unsere Werte und unsere Kultur. Zur Bekämpfung des Terrors unsere Kultur und Werte wie das rechtsstaatliche Handeln oder unsere Grundrechte bedingungslos und ohne öffentliche Diskussion aufzugeben, bedeutet ein Eingeständnis, wenn nicht letztlich eine Kapitulation auf Raten.

Der Terror nimmt uns zudem das Vertrauen in die Politik oder gar in die Rechtsordnung und schafft noch mehr Angst. Dies in einer Zeit, in welcher wegen der grossen gesell-

[37] Art. 3 NDG

schaftlichen Veränderung, wie der anstehenden 4. Industriellen Revolution (Internet of Things), schon bereits grosse existenzielle Ängste bestehen. Angesichts dessen nun eine Institution von unkontrollierbarer Macht zu schaffen, um das „Böse“ zu bekämpfen, kann wie bei der griechischen Tragödie gerade das hervorrufen, wovor man sich eigentlich schützen wollte. Wie z.B. damals die Unterstützung der afghanischen Widerstandskämpfer gegen die russische Besetzung.

Die hier vorgestellten, möglichen negativen Auswirkungen, welche sich infolge des Inkrafttretens des geplanten Nachrichtendienstgesetzes ergeben können, bedürfen noch der weiteren und eingehenden Prüfung, doch sind sie auf den ersten Blick so gravierend, dass offen darüber diskutiert und nachgedacht werden sollte. Im Nachrichtendienstgesetz steckt das Potential, dass mit diesem Gesetz entgegen dessen Zweck die Sicherheit unseres Landes sogar gefährdet wird, wie die Neutralitätspolitik und das Vertrauen oder der Glaube an die Rechtsordnung.

Ein Ausweg aus dem Dilemma zwischen „Schutz von Leib und Leben“ und unseren Grundrechten könnte uns das Urteil des Bundesverfassungsgerichts aus Karlsruhe (D) vom 20. April 2016 zeigen. Es bekennt sich klar zur Überwachung im Kampf gegen den Terrorismus, doch setzt es der Behörde Grenzen. Zugleich lässt es hoffen, dass damit begonnen wird, mit der Historie verantwortungsvoll umzugehen.

Persönliche Anmerkung: Der Autor dieses Textes ist nicht gegen ein Nachrichtendienstgesetz, denn es bedarf eines angesichts der aktuellen und der sich stetig verändernden Bedrohungslage. Aber nicht in dieser Ausprägung, welche Tür und Tor für Missbrauch öffnet und dem elementaren Gerechtigkeitsempfinden zuwiderläuft.

Quellenangabe

	Bundesgesetz zum Schutz vor Passivrauchen vom 3. Oktober 2008, SR 818.31
1 BvR 966/09	Urteil des Deutschen Verfassungsgerichts vom 20. April 2016 betreffend Überwachung
BehiV	Verordnung (des Bundes) über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen vom 19. November 2003, SR 151.31
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, vom 21. März 1997, SR 120
Donatsch	Kommentar zur Schweizerischen Strafprozessordnung (StPO), Herausgeber Andreas Donatsch, Thomas Hansjakob, Viktor Lieber, 2. Auflage, 2014, Schulthess Verlag

NDG	Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG), BBL 7264 ff.
NZZ 14.6.2013	Marie-Astrid Langer, Datengeheimnis wird zum neuen Schweizer Standortvorteil, NZZ vom 14.6.2013
Plädoyer 4/2015	Prof. Dr. Rainer Schweizer, „Unkontrollierbare Überwachung ruiniert den Rechtsstaat und die freiheitliche Demokratie“
Plädoyer, 3/2014	Daniel Muster, Digitaler Austausch gefährdet Rechtsgüter
Rhinow /Schiefer	René Rhinow, Markus Schefer, Schweizerisches Verfassungsrecht, 2. Auflage, Helbling Lichtenhahn Verlag, 2009
Riedo, Folka, Niggli	Christof Riedo, Gerhard Fiolka, Marcel Alexander Niggli, Strafprozess-recht sowie Rechtshilfe in Strafsachen, Helbling, Lichtenhahn Verlag, 2011
Schmid	Niklaus Schmid, Handbuch des Schweizerischen Strafprozessrecht, Dike Verlag, 2009
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0, in Kraft seit 1. Januar 1942
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007, SR 312.0
Trechsel	Stefan Trechsel, Schweizerisches Strafgesetzbuch, Kurzkommentar, Schulthess Verlag, 1992
Urteil, 20. April 2016	Urteil des Bundesverfassungsgerichts in Karlsruhe vom 20. April 2016 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2016/bvg16-019.html
VG	Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Be-hördemitglieder und Beamten vom 14. März 1958, SR 170.32
Weber	Rolf H. Weber, Romana Weber, Internet of Things, legal perspectives, Springer Verlag, 2010
WOSTA	Weisungen der Oberstaatsanwaltschaft für das Vorverfahren des Kanton Zürich, Stand 1. Juni 2013
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur vom 19. Dezember 2003, SR 943.03
Zustellplatt-form	Kriterienkatalog Zustellplattformen – Version 2.0 vom 16. September 2014 (Bundesvorschrift)