

Soziologisches Seminar zu "Öfflichkeitstheorien"

Seminararbeit bei Prof. Dr. Patrik Ettinger und Eveline Zwahlen (Tutorin)

Soziologisches Institut, Universität Zürich, HS2015

Geheimdienste im Kontext von Öffentlichkeitstheorien

Eine Auseinandersetzung am Beispiel des Schweizer Geheimdienstes

Nachrichtendienst des Bundes NDB auf Basis geltender und normativer

Grundlagen entsprechend dem Nachrichtendienstgesetz NDG

Hernani Marques

Abgabedatum: 30. Januar 2016 [überarbeitete Fassung]

Inhaltsverzeichnis

1	Einleitung	2
1.1	Motivation und Erkenntnisinteresse	2
1.2	Grundannahmen und Hypothesen	4
2	Theorien, Konzepte und Grundbegriffe	6
2.1	Bedingungen für (demokratische) Öffentlichkeit	6
2.2	Sphärentheorie im Bereich der Persönlichkeitsrechte	7
2.3	Widerspruch Staatsraison und Öffentlichkeitsprinzip	11
3	Normen Schweizer Geheimdienstarbeit	13
3.1	Offizielle (beschränkt öffentliche) Kontrollmechanismen	13
3.2	Eingriffe Privatsphäre und Öffentlichkeit: gestern, heute und morgen	15
4	Schlussbetrachtungen	25
5	Nachtrag: Überarbeitung und Reflexion	27
5.1	Veränderte Stellen	27
5.2	Reflexionen / Begründung unveränderter Stellen	29
5.2.1	Definition der Lebenssphären und Abgrenzung über Daten . .	29
5.2.2	Ausbildung von Geheimbereichen auch in westlichen Demokratien	30
5.2.3	Zusammenhang demokratische Öffentlichkeit und Grenzziehungsproblematik öffentlich/privat	31
5.2.4	Geheimdienstkontrolle nach dem liberalen Paradigma	31
5.2.5	Zu Sinn und Unsinn staatlicher Informationskontrolle	32
	Quellenverzeichnis	33

1 Einleitung

Sobald sich Geheimdienste finanziell und gesellschaftlich etabliert haben, denken sie, sie sind das Gesetz. Das ist das Problem.

– William Binney¹ am 4. Dezember 2015²

1.1 Motivation und Erkenntnisinteresse

Obwohl die Missbrauchsgefahren von Geheimdiensten mit der Befugnis in die *Intim- und Privatsphäre*³ der (mithin: globalen) Bevölkerung einzudringen, spätestens mit den durch Edward Snowden enthüllten *NSA-Komplex* (vgl. [Rosenbach und Stark](#) 2014) weithin bekannt geworden sein dürften, werden auch in der Schweiz die Geheimdienstbefugnisse weiter ausgebaut – dies in Anbetracht der historischen Altlasten der Schweiz mit der 1989 aufgefliegenen *Fichenaffäre* und in Licht der Tatsache, dass schon heute die Schweiz über erhebliche Überwachungskapazitäten verfügt – gerade in Zusammenarbeit mit ausländischen Geheimdiensten, mit denen der Schweizer Geheimdienst *NDB* kooperiert und Daten austauscht; dass mit der *NSA* Daten ausgetauscht würden, wird zudem nicht explizit verneint, sondern mit der Floskel umgangen, dass dies nicht “direkt” erfolge. (Vgl. [Zeller und Häfliger](#) 2014)

Die Arbeit soll im Wesentlichen der Frage nach der Vereinbarkeit von Geheimdiensten und *demokratischer Öffentlichkeit* (vgl. [Fraser](#) 1996: 169) nachgehen. Dies wird am Beispiel der Schweiz und bestehender sowie neu zu schaffender gesetzlicher Grundlagen für den Geheimdienst (konkret: dem Nachrichtendienstgesetz *NDG*) thematisiert.

Um diese Aufgabe zu erfüllen, werden in Kapitel 2 demokratie- und öffentlichkeitstheoretische, doch auch rechtliche Begriffe und Konzepte als Grundlage gelegt;

¹Von 1970–2001 (zunächst Analyst und zuletzt Technical Director der *NSA* und (nebst Edward Snowden) bekannt als scharfer Kritiker von Praxen der *Massenüberwachung*.

²[Schön](#) 2015

³Nach [Habermas](#) (2009: 89ff.) gehört diese zum “Verfassungsdesign” von Rechtsstaaten; hinzu kommen auch “gleiches Kommunikationsrecht” für alle und Informationsfreiheit. Dabei dient der Verfassungsstaat dem Schutz der “höchst persönlichen Lebenspläne”.

wo erforderlich, werden auch technische Tatsachen oder Beispiele konkreter (geheimdienstlicher oder informatischer) Praxen aufgezeigt, um die zugrundeliegenden sowohl soziologischen als auch rechtlichen Normen in ihrem Wirklichkeitsgehalt zu beleuchten.

Es ist Erkenntnis nicht zuträglich, wenn in *Öfflichkeitstheorien* davon ausgegangen wird, dass der Zugang zu Informationen allen frei steht, im Internet allerdings sowohl tatsächlich als auch normativ Inhalte (sanft oder hart) zensiert sind – im Sinne davon, dass diese für gewöhnliche Internet-Akteure nicht abrufbar sind oder als irrelevant sortiert werden. Gleichzeitig ist eine rechtliche Norm über die Kontrolle von Geheimdienstpraxen von geringem Nutzen, wenn die bisherige Empirie (auch in Anbetracht anderer Gesellschaften mit ähnlichen Wertesystemen und Erfahrungen) darauf hindeutet, dass Norm und Wirklichkeit auseinanderdriften. Zudem sind viele juristische Regelungen der Kontrolle, wie sie in gesetzlichen Normen gefunden werden können, nicht mit der technischen Wirklichkeit in Einklang zu bringen.

Mit Kapitel 3 werden die aufgeworfenen Hypothesen auf Grund der normativen Grundlagen aus Kapitel 2 im Zusammenhang mit Geheimdiensten – am Beispiel des Schweizer Geheimdienstes *NDB* – betrachtet.

Es wird hierbei auf zwei Aspekte theoretisch fokussiert:

1. Den offiziellen (beschränkt öffentlichen) Kontrollmechanismen von Geheimdiensten allgemein, mit besonderem Augenmerk auf die Schweizer Situation der Vergangenheit und Gegenwart im Geheimdienstbereich
2. Den Eingriffen, welche dem Geheimdienst bisher und zukünftig möglich sind und zwar hinsichtlich der überwachten *Privatsphäre* der Akteure und Gruppen und der dadurch (theoretisch) möglichen Auswirkungen auf die (Entstehung von) *Öffentlichkeit*

Kapitel 4 stellt das Fazit der Arbeit dar und fasst die Erkenntnisse noch einmal zusammen.

1.2 Grundannahmen und Hypothesen

Folgende Grundannahmen werden getroffen:

- Nicht nur Diktaturen, sondern auch westliche Demokratien verfügen – legitimiert durch die Staatsraison – über Geheimbereiche (und bilden diese weiter aus), welche im Widerspruch zum Gebot des Öffentlichkeitsprinzips beziehungsweise der Transparenz staatlichen Handelns stehen.⁴ (Vgl. [Fraser 1996: 154](#))
- Es findet eine zunehmende Vermengung von Öffentlichkeits- und Privatinteressen, insbesondere privaten Wirtschaftsinteressen, statt. (Vgl. [Martinsen 2010: 51ff.](#))
- Lebensbereiche von (individuellen) Akteuren lassen sich in verschiedene Sphären der Intimität, respektive Öffentlichkeit, betrachten. Ein Staat selber besitzt keine eigentliche *Intimität* oder *Privatsphäre*, sehr wohl aber kann ein solcher *Geheimnisse* besitzen.⁵

Folgende Hypothesen werden bei dieser Arbeit aufgeworfen; diese gilt es am Beispiel bestehender (in dem Fall: Schweizer) Normen gesetzlicher Art oder empirischer Befunde zu plausibilisieren:

- Der Schweizer Geheimdienst *NDB* entwickelt sich mittels neu zu schaffender gesetzlicher Normen in Form des Nachrichtendienstgesetzes NDG vom “blossen” Sicherheits- zum Macht- und Wirtschaftsinstrument.
- Geheimdienste verfügen bereits in ihren Normen – abgesehen ihrer daraus entwickelten (weitergehenden) Praxen –, je nach Einflussphären (und Eingriff in die Persönlichkeitsrechte) über Kompetenzen, die geeignet sind, die *demokratische Öffentlichkeit* zu unterwandern und die rechtsstaatliche Ordnung *faktisch* ausser Kraft zu setzen, auch wenn dies *normativ* ausgeschlossen

⁴Darin eingeschlossen ist Intransparenz über verwendete Methoden und Ausmass von Überwachung, d. h. mit welchen Mitteln und Wegen genau Eingriffe in die Privatsphäre der Bürger erfolgen und ob diese bei Formen der Massenüberwachung (wie in der Schweiz bei der “Funkaufklärung”) sich überhaupt noch Gewahr darüber sein können, dass eine Überwachung erfolgt; damit wird Bürgern auch die Möglichkeit genommen, sich “adäquat” auf den Zustand der (Massen-)Überwachung einzustellen und angepasst zu handeln: vgl. [GPDel \(2003: 1513; 1523\)](#).

⁵Vgl. Redebeitrag von Constanze Kurz, Sprecherin des Chaos Computer Club CCC, im Rahmen einer Podiumsdiskussion: [Scharloth et al. 2015](#).

wird, weil davon ausgegangen wird, dass die in demokratischen Staaten eingerichteten (parlamentarischen) Gremien der Geheimdienstkontrolle wirksam funktionieren. (Vgl. [Wyss 2011: 7](#))

2 Theorien, Konzepte und Grundbegriffe

2.1 Bedingungen für (demokratische) Öffentlichkeit

Öffentlichkeit ist Spiegel der Gesellschaft und zeigt wie sie sich selbst referenziert. Ferner ist Gesellschaft ohne *Öffentlichkeit* schwierig zu denken, denn erst durch die Sichtbarkeit von *öffentlichen* Verlautbarungen oder durch die Möglichkeiten für Akteure, sich an Orten der *Öffentlichkeit* einzubringen, entsteht das *Kollektivsubjekt* der Gesellschaft. Akteure können sich als Teil von etwas Grösserem verstehen, das *öffentlich* – potenziell für alle – sichtbar ist. (Vgl. Imhof 1996: 3ff.)

Nach Martinsen (2010: 46ff.; 60) lassen sich je nach theoretischem *Paradigma*, (1) *liberale*, (2) *deliberative* und (3) *partizipatorische* (oder: *republikanische*) Elemente ausmachen, abhängig vom zugrundeliegenden Verständnis von *Demokratie* oder dem angenommenen Modell von *Öffentlichkeit*.

So orientiert sich (1) das *liberale Paradigma* in demokratietheoretischer Hinsicht am Bewährten und hat systemisch betrachtet den Fokus, Stabilität zu wahren – als Ort der *Öffentlichkeit* und Einflussnahme gelten die Parlamente und als *öffentliche Meinung* gilt die *Mehrheitsmeinung*; (2) *deliberative Ansätze* sind darauf bedacht, Entscheidungen herbeizuführen, die an der *Vernunft* (des besseren Arguments) orientiert sind – als Ort der *Öffentlichkeit* gelten (geordnete) “gesellschaftliche und politische Kommunikationsprozesse”, die dann als *öffentlichen Meinung* gelten, wenn der entsprechende Diskurs zum *Konsens* führt; und (3) ist das *partizipatorische Paradigma* vor allem auf *Inklusion* bedacht: wichtiges Anliegen ist, dass alle partizipieren können. Als *öffentliche Meinung* gilt die Summe der Einzelmeinungen, so dass sich das *Kollektivsubjekt* von *partizipatorischer Öffentlichkeit* beispielsweise als *soziale Bewegung* manifestieren kann, so dass eine Funktion von *Öffentlichkeit* erfüllt wird, die als (zivilgesellschaftliche) *Kontrolle* gilt.

Zwei wichtige Bedingungen für eine (allgemein) *demokratische Öffentlichkeit* sind nach Martinsen (2010: 51ff.) normative Umstände, die mit dem Ideal des *deliberati-*

ven Modells von *Öffentlichkeit* zusammenhängen und die

1. sowohl der *liberalen* als auch *partizipatorischen (republikanischen)* – synthetisiert zur *deliberativen* – Tradition entnommen sind: wo sowohl der im *Liberalismus* wichtige *Pluralismus* (im Sinne von einem “Verständnis von Politik als Austragung von Konflikten”, wo auch klare (parteiliche) Standpunkte (jeweils) möglich sind) als auch die *republikanische* Forderung nach einem *Gemeinschaftsbezug* (mit objektiver Darstellung von Sachverhalten auf Basis einer *Wertegemeinschaft*) erlaubt sind. Praktisch müssen *Teilöffentlichkeiten* möglich sein, die sich auf der einen Seite (der *liberalen* Tradition folgend) eher konfliktiv (pluralistisch) zeigen, als auf der andere Seite solche, die sich “eintönig” (ausgewogen) und konsensorientiert artikulieren.
2. *staatliche Eingriffe* ermöglichen, um das “freie Spiel der Marktkräfte” dahingehend zu korrigieren, dass sich alle medialen *Diskurstypen* entfalten können: “investigative, inklusive und parteiische”. Damit würde verhindert, dass auf Grund der “Unvollkommenheiten des Marktes” Gruppen “disprivilegiert” würden, die klein oder marginalisiert sind.

2.2 Sphärentheorie im Bereich der Persönlichkeitsrechte

Privatheit kann nach [Fraser](#) (1996: 168) den Privatbesitz in der Marktwirtschaft betreffen, doch auch das intime oder persönliche Leben.

Im Bereich des Persönlichkeitsrechts kann nach [Schrödter](#) (2009) zwischen mindestens drei Lebenssphären unterschieden werden, die sich von innersten Privatbereichen des menschlichen Daseins bis hin zu Bereichen erstrecken, wo der einzelne Akteur bewusst an die Öffentlichkeit tritt:

- Intimsphäre
- Privatsphäre
- Sozialsphäre

Intimsphäre

Es handelt sich hierbei um Kenntnisse oder Daten über eine Person, die dieser eigen (mithin: nur ihr selber bekannt) und besonders persönlichen (intimen) Charakters sind. Sie geben beispielsweise über “Sexualität, Krankheiten, Gefühle und Gedankenwelt” Auskunft.

Die *Intimsphäre* betrifft – in Abgrenzung – zur (allgemeinen) *Privatsphäre* Lebensbereiche, deren (ungewollte) Einsicht oder Bekanntgabe sich nicht durch ein Interesse der *Öffentlichkeit* rechtfertigen lässt. Es wird vorausgesetzt, dass Informationen aus der *Intimsphäre* keine (wichtige, bedeutende) Funktion dabei erfüllen, *Öffentlichkeit* (von Belang) zu erzeugen (vgl. Imhof 1996: 6). Ihr Schutz vor (unerwünschter Kenntnisnahme) sollte in westlichen Demokratien entsprechend “absolut” gelten.

Privatsphäre

Daten über Akteure, welche die *Privatsphäre* betreffen, sind nur (ausgewählten) privaten oder staatlichen Personen(kreisen) und (in aller Regel) zur Erfüllung einer bestimmten Funktion bestehende Daten, welche sogenannten “personenbezogen” oder “personenbeziehbar” sind und welche die (konkrete) Bestimmung einer Person ermöglichen.

Nach Schweizer Datenschutzgesetz *DSG*⁶ wird bei der *Privatsphäre* auch ein qualitativer Unterschied gemacht, wenn von “*besonders schützenswerten Personendaten*” die Rede ist, welche gemäss Art. 3 Bst. c DSG über

1. *die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,*
2. *die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,*
3. *Massnahmen der sozialen Hilfe [und]*

⁶Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand: 1. Januar 2014)

4. administrative oder strafrechtliche Verfolgungen und Sanktionen [...]

einer Person Auskunft geben, wobei diese Definition sowohl dem Wort nach (Abs. 2 der Regelung) als *Intimsphäre* zuzüglich (inneren) Bereichen der *Privatsphäre* verstanden werden muss. Es handelt sich entsprechend um eine Sphäre zwischen der *Intimsphäre* in Überschneidung mit der allgemeinen *Privatsphäre* – insofern eine strikte Trennung überhaupt möglich ist.

Im einfachsten Fall gehören zu Daten, die der *Privatsphäre* im Allgemeinen unterliegen auch Daten wie Geburtsdatum und -ort, Vor-, Nachnamen, Familienbeziehungen, Wohnadressen, Telefon-Nummern oder andere sogenannte Telekommunikationsmerkmale – geheimdienstlich auch als (harte) *Selektoren* bekannt (vgl. [Biermann und Beuth](#) 2014). In Zeiten der Digitalisierung werden laufend personenbezogene Daten erzeugt, mit denen Akteure *profiliert* werden können: dies ist etwa dann schon der Fall, wenn das eigene *Smartphone* ständig den Standort speichert und an *Social-Media*-Plattformen weitergibt. Bereits der Fakt, dass netzfähige Mobilgeräte ständig mit funkbasierten Zugriffspunkten⁷ oder Antennenmasten (bei der Mobilfunktelefonie) in Verbindung stehen, erlaubt die ständige Standortbestimmung von Personen – als wären diese verwandt. Kommt es zu Straftaten an bestimmten Orten, kann der repressive oder präventive Staatsapparat auf Grund solcher Standortdaten und (vorliegender weitergehender) Bewegungsprofile (einer weiter zurückliegenden Vergangenheit) Verdachtsmomente schöpfen.

Nach dem *liberalen* Demokratieverständnis gehört der Schutz der *Privatsphäre* zu den Kernwerten. Das Wahren (gewisser) privater Informationen an *Öffentlichkeit* beteiligter Akteure ist zudem wichtig, nur schon um die Norm der *bürgerlichen Öffentlichkeit* zu erfüllen, wo davon ausgegangen wird, dass Gesprächspartner sich ohne Etikette, auf gleicher Ebene, begegnen können – dies ist auch im Sinne der *Inklusionsfunktion* von *Öffentlichkeit*, die beim *partizipatorischen* Demokratieverständnis konstituierendes Element ist. (Vgl. [Martinsen](#) 2010: 46; [Fraser](#): 160)

Andernfalls ist nicht ausgeschlossen, dass Personen auf Grund bestimmter *in-*

⁷Wireless Access Points WLAN-APs

timer Attribute⁸ diskriminiert würden, womit die *Partizipation* an der *Öffentlichkeit* be- oder gar verhindert würde.

Es muss empirisch festgehalten werden, dass auch in Fällen, wo die Daten “bloss” *privat*⁹ kursieren, sie in “falschen Händen”¹⁰ Einfluss auf die private Lebensführung oder den Werdegang von Personen haben können: als bekannte Beispiele in der Schweiz gelten solche der *Fichenaffäre*, wo nicht bloss von wesentlichen Teilen der Bevölkerung *intime* oder *private* Personendaten gesammelt wurden, sondern (darauf aufbauend) auch (behördliche) Einflussnahme erfolgte.¹¹

Sozialsphäre

Die *Sozialsphäre* betrifft den Lebensbereich von Akteuren, wo diese bewusst an die *Öffentlichkeit* treten und entsprechend im *Licht* eines breiten Publikums stehen. (Vgl. Imhof 1996: 6)

Grundsätzlich können Akteure als in der *Sozialsphäre* befindlich gesehen werden, wenn sie sich bereits räumlich im *öffentlichen Raum* aufhalten: somit ist es nicht ohne Weiteres möglich, sich bei der Videoüberwachung des *öffentlichen Raumes* auf Rechte der *Privatsphäre* zu berufen. Öffentliche Verlautbarungen auf *Social-Media*-Plattformen gelten ferner genauso als in der *Öffentlichkeit* befindlich, wie Äusserungen, die in Presseartikeln oder im Rahmen von *Versammlungsöffentlichkeiten* (vgl. Imhof 1996: 10) erfolgen.

⁸Diese können – wie im Falle von Krankheiten – auch fester, unveränderlicher Form sein.

⁹*Privat* ist hier im Sinne einer eingeschränkten Publizität gemeint: die Datensammlungen können aber sowohl staatlich (etwa in Gemeinderegistern oder bei Geheimdiensten) als auch privatwirtschaftlich (etwa bei Unternehmen oder Vereinen) vorliegen.

¹⁰Im Sinne davon, dass die Daten Personen(kreisen) zugänglich sind, welche konträre Interessen zu der Person verfolgen, über welche diese vorliegen.

¹¹Es existieren dokumentierte Fälle, wo Personen der Zugang zu konkreten Arbeitsstellen (strukturell) erschwert oder verunmöglicht wurde. (Vgl. Frischknecht 1990)

2.3 Widerspruch Staatsraison und Öffentlichkeitsprinzip

Im Rahmen der Überprüfung von 40'000 Suchbegriffen¹² für den deutschen NSA-Untersuchungsausschuss, welcher (zur Zeit dieser Arbeit) Praxen der *Massenüberwachung* der NSA in Deutschland (im Zusammenhang mit dem deutschen Geheimdienst *BND*) untersucht, beruft sich Berichterstatter [Graulich](#) (2015: 2) auf ein Zitat Habermas' seines für die *Öffentlichkeitstheorie* wichtigen Werkes "*Strukturwandel der Öffentlichkeit*" (vgl. [Habermas](#) 2009):

Nicht durch öffentliche Kommunikation, sondern durch die Kommunikation der öffentlich-manifestierten Meinungen wird das Publikum der nicht-organisierten Privatleute im Sog demonstrativ oder manipulativ entfalteter Publizität beansprucht. Eine im strengen Sinne öffentliche Meinung kann sich hingegen nur in dem Maße herstellen, in dem die beiden Kommunikationsbereiche durch jene andere, die kritische Publizität, vermittelt werden.

Damit protestiert¹³ der Berichterstatter gegen angebliche *massenmedial* transportierte "Schablonen" wie "anlasslose, globale Massenüberwachung" und sieht seinen Bericht (hingegen) als (konzisen) kritischen Beitrag zur Debatte.¹⁴

Einerseits besteht in westlichen Demokratien Konsens darüber, dass staatliches Handeln rechenschaftspflichtig ist, was sich nicht zuletzt damit erklärt, dass der Staat das Gewaltmonopol besitzt. Die dafür nötige Transparenz wird unter anderem durch das in vielen Ländern existierende Öffentlichkeitsprinzip der Verwaltung¹⁵ sichergestellt, das von Journalisten oder einer *kritischen Öffentlichkeit* genutzt werden kann, um die Transparenz im Staat zu erhöhen. Andererseits bestehen

¹²Im Geheimdienst-Kontext auch *Selektoren*: vgl. [Biermann und Beuth](#) 2014

¹³Gemäss Aussagen von Berichterstatter Kurt Graulich im NSA-Untersuchungsausschuss vom 5. November 2015. (Vgl. [Biselli 2015b](#))

¹⁴Sein Bericht wird schliesslich sowohl von der technikaffinen *netzpolitischen* Gemeinde als auch von den *Massenmedien* rasch für technisch fehler- und lückenhaft und – auf Grund der sowohl personalen als auch räumlichen Nähe der Zusammenarbeit mit dem deutschen Geheimdienst *BND*, bei der Abfassung des Berichts – von *Massenmedien* als nicht unabhängig betrachtet und somit in seiner angepriesenen kritischen Natur (ironischerweise) in Frage gestellt. (Vgl. [Biselli 2015a](#); [Biermann](#) 2015)

¹⁵In der Schweiz besteht das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) vom 17. Dezember 2004 (Stand: 19. August 2014).

im Staat Geheimbereiche, wie solche der Geheimdienste, die dieser Sphäre der Öffentlichkeit normativ ausgeschlossen sind.¹⁶

Offiziell werden Geheimdienste (vgl. [Zeller und Häfliger 2014](#)) im Sinne von *Staatsraison* und *vernunftgeleitet* nach Möglichkeit *deliberativer Auffassung* (im Konsens) als Instrumente der Sicherheit verkauft, haben aber auch politisch und wirtschaftlich eine hohe Bedeutung und sind somit nachweislich (zumindest) genauso Werkzeuge für diplomatische oder Wirtschaftsspionage und damit Macht- und Wirtschaftsinstrument. (Vgl. [Schmid 2011: 70ff.,108ff.](#); [Wendekamm 2014: 87ff.](#))

Denn: von Habermas festgestellte Prozesse der *Privatisierung* und “*Refeudalisierung*” der *Öffentlichkeit* (vgl. [Martinsen \(2010: 51ff.\)](#)), die sich dadurch zeigen, dass *privaten Wirtschaftsinteressen* Vorrang zukommt, lassen sich auch im Zusammenhang mit der schwindenden Bedeutung, den *öffentlichen* Verfassungsauftrag ernst zu nehmen, die durch Verfassungsrecht und internationale Konventionen zugesicherten Persönlichkeitsrechte der *Intim-* und *Privatsphäre* zu wahren. Der regelrechte Handel mit Informationen aus der *Intim-* und *Privatsphäre* ist belegt: er erlaubt es staatlichen Akteuren einerseits (politisch) Wissensvorsprünge gegenüber anderen Staaten oder individuellen Akteuren zu erlangen, als auch einen Handel zu begründen, wo entweder Geld oder Daten (im Tauschhandel) angenommen werden. (Vgl. [Hanimann 2015](#); [Wendekamm 2014: 88ff.](#))

In dem Kontext ist es wichtig, die Zweckartikel normativer Grundlagen für die Geheimdienste – wie beispielhaft beim Schweizer Nachrichtendienstgesetz *NDG* –, wonach der Geheimdienst dafür da sei, die “innere oder äussere Sicherheit” zu sichern, die “Handlungsfähigkeit der Schweiz zu unterstützen”, zur “Wahrung internationaler Sicherheitsinteressen beizutragen” oder in “besonderen Lagen” zur “Wahrung weiterer wesentlicher Landesinteressen” eingesetzt zu werden, *kritisch* hinsichtlich solcher (in- und ausländischer) Praxis – und entsprechend der (geheimdienstlichen) Wirklichkeit – zu betrachten.

¹⁶Vgl. Art. 7 Abs. 1 Bst. c BGÖ

3 Normen Schweizer Geheimdienstarbeit

Theoretisch wird der Verfassungsschutz schon jetzt durch das Parlamentarische Kontrollgremium des Bundestages überwacht. Geholfen hat dies anscheinend auch nicht viel. Geheimdienste lassen sich nicht wirklich kontrollieren. Zudem triebe aus meiner Sicht die "Überwachung von Überwachern" das ganze System noch weiter ins Absurde. Wer überwacht denn dann die Überwacher der Überwacher?

– Jens Petermann¹⁷ am 6. August 2012¹⁸

3.1 Offizielle (beschränkt öffentliche) Kontrollmechanismen

Geheimdienste entwickeln ein Eigenleben¹⁹ und sind durch parlamentarische Gremien grundsätzlich nicht kontrollierbar. Beispiele eklatant fehlgeschlagener *parlamentarischer Kontrollen* finden sich bei den deutschen Geheimdiensten Bundesamt für Verfassungsschutz *BfV* und Bundesnachrichtendienst *BND*,²⁰ dem (vereinigten²¹) Inlands- und Auslandsgeheimdienst *NDB* (Schweiz)²² bis hin zu den US-amerikanischen Geheimdiensten, allen voran dem Auslandsgeheimdienst *NSA* (USA).²³

Die Willkür während der sogenannten (Schweizer) *Fichenaffäre* ist amtlich belegt – gemäss dem entsprechenden parlamentarischen Untersuchungsbericht²⁴ über die Vorkommnisse im Eidgenössischen Justiz- und Polizeidepartement *EJPD* hatte die Datensammlung in der Schweiz über Jahrzehnte willkürlichen und uneinheitlichen Charakter:

Die von der PUK [Parlamentarische Untersuchungskommission] durch-

¹⁷Rechtspolitischer Sprecher der (deutschen) Partei *Die Linke*

¹⁸Vgl. [Jamal](#) 2012

¹⁹Vgl. [Marcinkowski](#) (2002: 111ff.) zur Tendenz, dass Teilsysteme unabhängig ihrer Umwelt werden und nur noch eigener Gesetzmässigkeiten horchen.

²⁰Vgl. [Jamal](#) 2012; [Jelpke](#) 2015

²¹Bis 2009 existierte in der Schweiz ein Inlandsgeheimdienst als Dienst für Analyse und Prävention *DAP* und getrennt davon der Auslandsgeheimdienst Strategischer Nachrichtendienst *SND*.

²²Vgl. [Häfliger](#) 2013

²³Vgl. [Rosenbach und Stark](#) 2014

²⁴[Leuenberger und Meier](#) 1989: 810

geführten Abklärungen haben weiter ergeben, dass das Sammeln von Informationen zum Teil äusserst unsystematisch und zufällig erfolgt. Da einheitliche Kriterien fehlen, hängt es weitgehend vom jeweiligen Sachbearbeiter ab, welche Informationen er als relevant erachtet. Ebenso hat es sich gezeigt, dass die einzelnen kantonalen Nachrichtendienste unterschiedliche Schwerpunkte setzen, so dass die bei der Bundespolizei zusammenlaufenden Informationen lückenhaft sind.

Die Geheimdienstkontrolle in der Schweiz heute wird im Wesentlichen nur (mehrfach) indirekt und offiziell durch zwei Instanzen sichergestellt, die nach dem *liberalen Paradigma* funktionieren, wonach die Kontrolle parlamentarischer Art ist; verantwortlich sind im Wesentlichen zwei (selber geheim) operierende Personen(kreise) mit beschränkter *Öffentlichkeit*, die keine Funktion der *Inklusion* von *Öffentlichkeit* erfüllen:²⁵

- Geschäftsprüfungsdelegation *GPDel*: sie überwacht allgemein den Schweizer Geheimdienst *NDB* und wird durch indirekte Wahlen vom Schweizer Parlament zusammengesetzt.
- Unabhängige Kontrollinstanz *UKI*: diese überwacht Aufträge, die an die sogenannte *Funkaufklärung* erteilt werden, was eine Form der *Massenüberwachung* auf Basis von Suchbegriffen oder anderen Kommunikationsmerkmalen satellitenbasierten Kommunikationsverkehrs darstellt. Überwachungsaufträge gehen sowohl vom *NDB* als auch dem Schweizer Militär aus. Die Arbeit der *UKI* entzieht sich der *Öffentlichkeit* gewissermassen doppelt, indem diese ihre Erkenntnisse ausschliesslich mit der *GPDel* oder dem *Bundesrat* teilt, die der *UKI* glauben müssen und die ihrerseits Informationen an die *Öffentlichkeit* nur gefiltert weiter geben. Die *UKI* wird durch Ernennung vom Schweizer *Bundesrat* zusammengestellt.

Diesen Instanzen muss *vertraut* werden, dass diese ihre Aufgabe *vernünftig* (entsprechend der *deliberativen* Kernforderung) und in einer Art, dass es dem *Gemeinwohl* dient, wie dies vom *partizipatorischen* Ansatz gefordert würde, erfüllen.

²⁵Bestenfalls können Akteure ausserhalb der Kontrollgremien – gelegentlich – Zuschauer sein.

Entsprechend der Konzeption der Geheimdienstkontrolle nach den *liberalen Paradigma* kann zumindest in der Schweiz²⁶ nicht die Rede davon sein, dass eine (öffentliche oder zumindest kritische) *Öffentlichkeit* die Vorgänge der Schweizer Geheimdienstarbeit kontrollieren könnte. Dieser Umstand wird auch im neuen Nachrichtendienstgesetz *NDG*, seinem Wesen nach, nicht verändert.

3.2 Eingriffe Privatsphäre und Öffentlichkeit: gestern, heute und morgen

Bevor es zu gesetzlichen Grundlagen für einen Schweizer Staatsschutz kam, wurde bis mindestens 1990 in einem (undurchsichtigen) Zusammenhang unter Führung von Bundespolizei und -staatsanwaltschaft sowie der Zulieferung seitens kantonalen Stellen und Privatleuten – auf jeden Fall: ohne gesetzliche Grundlagen – in der Schweiz präventiv überwacht; “fichierte” oder (auf Einzelbasis) registriert und *profiliert* wurden über 900'000 Einzelakteure und Gruppen: betroffen waren insbesondere *Gegenöffentlichkeiten*, aber auch *Teilöffentlichkeiten* im Allgemeinen (vgl. [Martinsen](#) 2010: 52ff.; 58ff.): grundsätzlich schien im Kontext des *Kalten Krieges* alles, was von der *öffentlichen Meinung* – im Sinne der *liberal-paradigmatischen Mehrheitsmeinung* – abwich und *anders* oder *innovativ* war, gefährdend zu sein und wurde überwacht.

Was die *Intim-* und *Privatsphäre* betrifft, so ist bekannt, dass Telefone abgehört oder Wohnungen verwantzt wurden; in der *Sozialsphäre* der *Öffentlichkeit* wurde gemäss einem Beschrieb der *Ficheneinträge* minutiös jede Form der *öffentlichen* Äusserung, Verlautbarung oder Erwähnung erfasst (vgl. [Leuenberger und Meier](#) 1989: 811):

Die erfasste Person war Verfasser oder Betroffener eines unter einem bestimmten Gesichtspunkt interessierenden Presseartikels oder einer andern öffentlichen Verlautbarung.

Auf Grund der heutigen normativen Grundlagen und der zukünftigen Grundla-

²⁶Dies gilt generell aber auch andernorts: vgl. [Wyss](#) 2011.

gen für den Schweizer Geheimdienst *NDB* kann diskutiert werden, inwiefern die *Möglichkeit* besteht, verstärkt in die verschiedenen Lebenssphären der Menschen einzugreifen und was das für die individuelle Handlungsfähigkeit und für die in Demokratien fundamentale Güter wie Meinungs-/äusserungs- oder Versammlungsfreiheit bedeutet bzw. inwiefern diese Rechte in ihrem ganzen Ausmass (noch) wahrgenommen oder (umgekehrt) verfälscht werden können. Schliesslich sind diese Rechte erforderlich, damit sich *demokratische Öffentlichkeit* überhaupt bilden kann.

Zur Zeit geltende gesetzliche Normen nach den Gesetzen BWIS²⁷ und ZNDG²⁸ sowie den (bundesrätlichen) Verordnungen V-NDB²⁹ und VEKF³⁰ geben dem Geheimdienst *NDB* folgende (nicht abschliessende) Kompetenzen:

- Bewaffnung³¹
- Verbot von Tätigkeiten (via Bundesrat)³²
- Speicherung von (besonders schützenswerten) Personendaten, welche die *innere Sicherheit* betreffen³³
- Löschpflicht *unrichtiger* oder *unerheblicher* Daten in eigenen Datenbanken³⁴
- Austausch von Daten mit Polizei, Strafverfolgungsbehörden oder dem Ausland³⁵
- Führen *geheimer* Liste zu überwachender Vorgänge³⁶
- Führen teils *öffentlicher* (internationaler), teils *geheimer* (nationaler) Liste zu überwachender Organisationen oder Gruppen³⁷

²⁷Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vom 21. März 1997 (Stand: 16. Juli 2012)

²⁸Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) vom 3. Oktober 2008 (Stand: 1. November 2014)

²⁹Verordnung über den Nachrichtendienst des Bundes (V-NDB) vom 4. Dezember 2009 (Stand: 1. November 2014)

³⁰Verordnung über die elektronische Kriegführung und die Funkaufklärung (VEKF) vom 17. Oktober 2012 (Stand: 1. November 2012)

³¹Art. 5a Abs. 1 BWIS, allerdings nur bei *Notwehr* (Art. 5a Abs. 2 Bst. a BWIS) und *Notstand* (Art. 5a Abs. 2 Bst. b BWIS)

³²Art. 9 BWIS

³³Art. 10a Abs. 1 BWIS

³⁴Art. 10a Abs. 3 BWIS

³⁵Art. 10a Abs. 4 und Art. 17 BWIS

³⁶Art. 11 Abs. 2 BWIS

³⁷Art. 11 Abs. 3, 5, 6 und 7 BWIS

- Informationspflicht für Kantone, den NDB *unaufgefordert* über “*konkrete Gefährdungen der inneren oder äusseren Sicherheit*” zu orientieren³⁸
- Informationspflicht für *abschliessende* und *nicht abschliessende* Stellen von Bund, Kantone, Organisationen, die *öffentliche* Aufgaben erfüllen oder gewerbliche (*private*) Transporte durchführen, den NDB *aufgefordert* Auskünfte zu erteilen³⁹
- Auskunftsrecht, die Identität und Adressen von Telefon- oder Internetanschlüssen festzustellen (via Dienst ÜPF⁴⁰)⁴¹
- Löschung oder Zensur von Webinhalten bei “*Propagandamaterial*” (via fedpol⁴²)⁴³
- Überwachung und Auswertung *öffentlicher* Quellen, (technische) Überwachung *allgemein zugänglicher* Orte sowie Einsicht in *geheime* Amtsregister, sofern das *Inland* betroffen ist⁴⁴
- Einsatz *verdeckter* Methoden der Informationsbeschaffung ohne besondere (technische, räumliche) Einschränkungen, sofern das *Ausland* betroffen ist⁴⁵
- Anhalten von Personen und Überprüfen von Identitäten (via Polizeibehörden von Bund und Kantonen)⁴⁶
- Einsatz inoffizieller Mitarbeiter (mit Schwarzgeldzahlungen)⁴⁷
- Fabrikation und Veränderung von (falschen) Identitäten, Ausweisen, Urkun-

³⁸Art. 12 BWIS

³⁹Art. 13 und Art. 13c BWIS

⁴⁰Der Dienst ÜPF führt Überwachungen für den Strafverfolgungsbereich gemäss Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000 (Stand: 16. Juli 2012) durch. Dieses Gesetz wird parlamentarisch zur Zeit totalrevidiert und mag 2016 zur Schlussabstimmung gelangen: viele (neuerer) invasiver Überwachungsmittel, die der NDB via NDG *neu* erhalten soll, sind auch im neuen BÜPF vorgesehen. Einige der Mittel, die tief in die Privatsphäre von Personen oder Gruppen eingreifen können – wie beispielsweise *IMSI-Catcher* oder *Staatstrojaner* – wurden aber auch ohne explizite, normative (gesetzliche) Grundlage bereits von Staatsanwaltschaften von Bund und Kantonen eingesetzt.

⁴¹Art. 13 Abs. 1^{bis} BWIS

⁴²Bei fedpol handelt es sich um das Bundesamt für Polizei, einer polizeilichen Fachbehörde vom Bund mit “präventiver, repressiver und flankierender” Funktion. Vgl. URL https://www.fedpol.admin.ch/fedpol/de/home/ueberuns/recht_grundlagen.html (Abruf: 3. Januar 2016).

⁴³Art. 13e Abs. 5 Bst. a und b BWIS

⁴⁴Art. 14 Abs. 2 BWIS

⁴⁵Art. 16 V-NDB

⁴⁶Art. 17 V-NDB

⁴⁷Art. 14a BWIS

den oder weiterer Unterlagen (zur *Tarnung*)⁴⁸

- *Massenüberwachung* satellitenbasierten Kommunikation, wobei das soziale Kommunikationsnetzwerk fünf Jahre und die Inhalte der Kommunikation 18 Monate lang gespeichert werden können⁴⁹

Schon mit den heutigen normativen Kompetenzen, die der *NDB* besitzt, können die diversen Forderungen und Funktionen, welche für *liberale*, *deliberative* oder *partizipatorische* Formen von *Öffentlichkeit* vorausgesetzt werden, (empfindlich) gestört werden – nachfolgend jeweils anhand von zwei Beispielen:

- Beim **liberalen Paradigma** fällt beispielsweise ins Gewicht, dass Normen dafür bestehen, gewissen Akteure Sonderrechte einzuräumen oder Legalitätsprinzipien umzudrehen, wenn etwa (1) die Normen betrachtet werden, die dem *NDB* erlauben, Dokumenten- und Identitätsfälschungen zu betreiben oder (2) Schwarzgeldzahlungen zu tätigen, während von allen anderen Bürgern verlangt wird, dass sie sich gesetzestreu verhalten und ihre Einkommen dem Staat gegenüber präzise angeben.
- Das **deliberative Paradigma** wird zumindest dadurch negativ beeinträchtigt, dass (1) sogenanntes “Propagandamaterial” gelöscht oder zensiert werden kann, was Akteure zweiteilt in solche, die Zugang haben oder sich diesen (an der Löschung⁵⁰ oder Zensur vorbei) verschaffen können und solchen, die von Informationsquellen abgeschnitten sind,⁵¹ (2) kann das Bewusstsein darüber, dass die verschiedenen Lebenssphären vom Staat überwacht werden, dazu führen, dass sich Akteure in ihrer Kommunikationsbereitschaft zurückhalten – *Chilling-Effects* können sich einstellen. (Vgl. [Steinschaden](#) 2015)
- Was das **partizipatorische Paradigma** betrifft, so fällt (1) das Verbot von Tätigkeiten negativ auf, was – je nach politischer Führung oder amtlicher Besetzung – normativ die Möglichkeit eröffnet, Manifestationsformen von *Öffentlichkeit* als beispielsweise *soziale Bewegungen* zu unterdrücken; (2) kann

⁴⁸Art. 14c BWIS

⁴⁹Art. 4a ZNDG; Art. 4 Abs. 2 und 3 VEKF

⁵⁰Inhalte im Internet können schwerlich dauerhaft gelöscht werden. Zumindest muss immer damit gerechnet werden, dass Kopien (fort)bestehen.

⁵¹Hier können auch Effekte des *Digital-Divide* eine Rolle spielen. (Vgl. [Martinsen](#) 2010: 59)

der Einsatz inoffizieller Mitarbeiter oder “Spitzel” gerade bei Bürgergruppen, die sich zusammenschliessen, um Missstände *öffentlich* zu machen und damit ihrer *Kontrollfunktion* von Gesellschaft nachzukommen, dazu führen, Misstrauen zwischen den Akteuren zu säen und mögliche Aktivitäten im Keim zu ersticken und damit *Öffentlichkeit* zu unterbinden.

Zudem sind die *Intim-, Privat- und Sozialsphäre* betreffend, folgende Eingriffe – zumindest und beispielhaft – gegenwärtig möglich:

- **Intimsphäre:** Intime Daten kann der *NDB* insbesondere im Datenaustausch mit dem Ausland erhalten, beim Einsatz von *Tarnidentitäten* in sozialen Zusammenhängen – in Interaktion mit anderen Akteuren – in Erfahrung bringen oder *massenweise* unter Einsatz seiner Communications-Intelligence *COMINT-Fähigkeiten*⁵², die er dadurch hat, funkgestützte Kommunikation abzuhören,⁵³ beschaffen.
- **Privatsphäre:** Wird der *COMINT*-Bereich betrachtet, sind Daten, welche die *Intimsphäre* betreffen, häufig begleitet von Daten im Sinne der (allgemeinen) *Privatsphäre* wie Namen, Telekommunikationsmerkmalen (wie Telefonnummern, E-Mail-Adressen usw.) oder auch Standortdaten (von Empfänger und/oder Absender), die nicht allen Personenkreisen ohne Weiteres zugänglich sind und entsprechend das Kriterium der *Öffentlichkeit* nicht erfüllen, (potenziell) allen Personen zugänglich zu sein.⁵⁴

⁵²Vgl. [Kelion 2014](#)

⁵³Normativ darf der Geheimdienst die *COMINT*-Kommunikation unter Inländern, sofern beide im Inland stationiert sind, nicht abhören – dies gilt gemäss Art. 5 Abs. 1 allerdings nur, sofern dies auch erkannt wird und es sind Ausnahmeregelungen vorhanden, für Fälle, wo diese Informationen dem Schutz der “inneren Sicherheit” dienlich sind (vgl. Art. 5 ZNDG). Zudem ist die Tauschfähigkeit des *NDB* nicht zu unterschätzen: dadurch, dass er den gesamten “ausländischen” Verkehr abhören kann, erhält dieser Tauschmaterial für inländische Daten von ausländischen Geheimdiensten, die diese wiederum von Inländern (normativ legal) beschafft haben. So fängt auch der deutsche Auslandsgeheimdienst *BND* Daten auf funk- oder kabelbasierten Wegen massenweise ab – unter anderem auch von Schweizer Akteuren. (Vgl. [Hanimann 2015](#))

⁵⁴Dies verhält sich abrupt anders, wenn es zu *Hacks* mit anschliessender Datenveröffentlichung kommt, im Zuge deren die Daten einem breiten (globalen) Publikum zugänglich gemacht werden; so geschehen kürzlich mit E-Mails von *CIA*-Direktor John Brennan: vgl. [Graw 2015](#). Unabhängig der Legalität, kann die Legitimität dieses Vorgangs entweder unter dem Gesichtspunkt demokratischer Kontrolle betrachtet werden, weshalb die entsprechenden E-Mails auch vom Enthüllungsportal *WikiLeaks* veröffentlicht wurden oder aber als illegitim erkannt werden, weil es einen Eingriff in die Privatsphäre eines Bürgers darstellt oder staatlich betrachtet (gegeben die Funktion des *CIA*-Direktors), Staatsgeheimnisse betrifft und damit die Staatsraison tangiert; d. h. legitim ist die Aktion, wenn das Interesse der *Öffentlichkeit* überwiegt, illegitim hingegen, wenn das Interesse der *Privatsphäre* bzw. (staatlicher) Geheimhaltung stärker gewichtet wird.

- **Sozialsphäre:** In der *Öffentlichkeit* ist dem *NDB* sowohl für die in- als auch ausländische Bevölkerung erlaubt, alle Erkenntnisse zu erfassen und auszuwerten. Im Geheimdienstjargon wird dieser Typ der Informationsbeschaffung auch als Open-Source-Intelligence *OSINT*⁵⁵ bezeichnet. Den Kompetenzen, die der *NDB* heute hat entsprechend, kann dieser beispielsweise (manuelle oder computergestützt automatisierte) Inhaltsanalysen von (Online-)Zeitungen, *Social-Media*-Plattformen⁵⁶ oder (klassischen wie auch modernen – (virtuell) webbasierten) *Versammlungsöffentlichkeiten* (vgl. Imhof 1996: 10) vornehmen und diese Daten nach Belieben (re-)kombinieren. Bereits durch solche Prozesse ist die Gefahr gross, dass Personen in (falsche) Zusammenhänge gestellt und damit (pauschal) verdächtigt werden und entsprechend in den Datenbanken des *NDB* landen.⁵⁷

In den neuen (zukünftigen) normativen Grundlagen,⁵⁸ die für den Schweizer Geheimdienst als Nachrichtendienstgesetz *NDG*⁵⁹ geschaffen werden sollen, finden sich alle bisherigen Punkte wieder, allerdings unter teilweise anderen Bezeichnungen oder mit erweiterten Kompetenzen; nicht abschliessend kommt es zu folgenden Erweiterungen von Kompetenzen oder gänzlich neuen Befugnissen, welche Eingriffe in die *Intim-*, *Privat-* als auch *Sozialsphäre* erweitern und vertiefen:

- Der *NDB* kann mittels “Fluggeräten und Satelliten” den *öffentlichen Raum* (neu zusätzlich) beobachten.⁶⁰

⁵⁵Vgl. Kelion 2014

⁵⁶Bei (zentralisierten) *Social-Media*-Plattformen ist es – sowohl rechtlich als auch technisch – schwierig, einem Akteur zu garantieren, dass *Privatheit* überhaupt existiert, denn: (1) die Anbieter von solchen Angeboten wie *Facebook* oder *Google* behalten sich via ihren (entrechtenden) Allgemeinen Geschäftsbedingungen AGBs vor, den gesamten User-Generated-Content *UGC* beliebig kommerziell (oder anderweitig) weiterzugeben und zu verwerten (vgl. Imhof 2015); (2) dem *NDB* ist zudem erlaubt, Daten von fremden Geheimdiensten zu empfangen und auszuwerten. Darunter können sich auch Daten inländischer Akteure befinden, so dass eine (klare) Zuordnung zu einer der Sphären der *Privatheit*, respektive *Öffentlichkeit* gar nimmer möglich ist – aus den Snowden-Enthüllungen ist beispielsweise das *PRISM*-Programm bekannt, das eine Ausleitung von privatwirtschaftlich gehaltenen Daten für (staatliche) Geheimdienst-Zwecke vorsieht (vgl. Rosenbach und Stark 2014: 127); und (3) sind (geheimdienstliche) Angriffe auf IT-Sicherheitstechnik und -verschlüsselungstechnologien belegt, die ein (inoffizielles) Ausspähen der die *Intim-* oder *Privatsphäre* betreffenden Kommunikation ermöglicht. (Vgl. Spiegel 2014)

⁵⁷Beispielweise wurden in jüngerer Zeit – im Zuge einer eigentlichen *Fichenaffäre 2.0* – sowohl die Ehrendoktorin der Uni Basel Anni Lanz als auch der Nationalrat und Grünenpolitiker Balthasar Glättli fichiert und zudem Zusammenhänge von Akteuren zu “gewalttätigem Extremismus” konstruiert. (Vgl. Foppa 2010; Kühnis 2010; Busch 2011)

⁵⁸Diese unterstehen dem *fakultativen Referendum*.

⁵⁹Bundesgesetz über den Nachrichtendienst (NDG) vom 25. September 2015.

⁶⁰Art. 14 Abs. 1 NDG

- (Private) Betreiber von Videoüberwachungsanlagen können verpflichtet werden, dem *NDB* die Überwachungsdaten zur Verfügung zu stellen – für sowohl *private* als auch *öffentliche* Räume.⁶¹
- Der *NDB* kann Überwachungen nach allen normativen (gesetzlichen) Grundlagen der Strafverfolgungsbehörden anordnen.⁶²
- Es können Wanzen an Personen oder Gegenständen angebracht werden, um sie zu orten.⁶³
- (Private) Räume können – wie zu Zeiten der *Fichenaffäre* – wieder verwanzt werden.⁶⁴
- Computersysteme oder -netzwerke können angegriffen, ausgespäht⁶⁵ und gestört werden.⁶⁶
- (Private) Hausdurchsuchen oder Durchsuchungen von “Fahrzeugen oder Behältnissen” können vollzogen werden – auch dies entspricht einer neu zur Norm erhobenen Praxis der *Fichenaffäre*.⁶⁷
- Der *NDB* kann neben der *Funkaufklärung* auch die *Kabelaufklärung* betreiben, was der *Massenüberwachung* von (Schweizer) Glasfaserleitungen entspricht – damit ist praktisch die gesamte Kommunikation der Schweizer Bevölkerung betroffen.⁶⁸ (Vgl. [Marques](#) 2015: 35ff.)
- Es ist dem *NDB* erlaubt – umgekehrt zu bisherigen Regelungen – “Desinformationen” oder “Falschinformation” zu speichern und zu verarbeiten.⁶⁹

Unmittelbar fallen die (neuen) Normen auf, die zusätzlich zu den bisherigen weitestgehende Eingriffe in *Intim-* und *Privatsphäre* als auch *Sozialsphäre* ermöglichen:

- **Intimsphäre:** Bereits die Möglichkeit, Geräte der Kommunikation und entsprechende Netzwerke von Akteuren direkt auszuspähen oder Wohnungen

⁶¹Art. 25 Abs. 1 Bst. b NDG

⁶²Art. 26 Abs. 1 Bst. a NDG

⁶³Art. 25 Abs. 1 Bst. b NDG

⁶⁴Art. 25 Abs. 1 Bst. c NDG

⁶⁵Mittels als “Staatstrojaner” bezeichnbarer Ausspähtsoftware.

⁶⁶Art. 25 Abs. 1 Bst. d NDG

⁶⁷Art. 25 Abs. 1 Bst. e NDG

⁶⁸Art. 39ff. NDG

⁶⁹Art. 44 Abs. 2 NDG

zu durchsuchen und zu verwanzen, machen deutlich, dass mit dem *NDB* ein eigentlicher *Paradigmenwechsel* erfolgt, welcher dem Geheimdienst *NDB* ermöglicht in die Gedankenwelt⁷⁰ – neu: auch explizit der inländischen Bevölkerung – einzudringen. Gerade bei digital gehaltenen Informationen dürfte es den Betroffenen schwer fallen, den Einbruch zu bemerken – anders bei geheimen Hausdurchsuchungen, die auffallen mögen.

- **Privatsphäre:** Durch die Möglichkeit Überwachungen nach Massgabe der Strafverfolgungsbehörden durchzuführen und (neu) die *Kabelaufklärung* als Kompetenz zu haben, ist es möglich, weite Teile der Schweizer Kommunikation zu erfassen und somit umfassende Kommunikations- und Bewegungsprofile anzulegen. Alleine die Umstands- oder Metadaten, die anfallen und die Auskunft darüber geben, wer, mit wem, wie lange und wo kommuniziert, sind Daten, die der *Privatsphäre* zuzurechnen sind.
- **Sozialsphäre:** Neu könnte der *NDB* Daten von beliebigen Videoüberwachungsanlagen beschaffen, gerade auch explizit wenn diese den *öffentlichen Raum* betreffen und er kann zudem mittels Drohnen und Satelliten von der Luft aus Überwachungen vornehmen.⁷¹

Wird nach Funktionen und Forderungen in *demokratie-* und *öffentlichkeitstheoretischer* Hinsicht gefragt, entsprechend den Paradigmen der *liberalen, deliberativen* oder *partizipatorischen Tradition*, so wird – schon normativ, unabhängig jedweder von der Norm abweichenden (weitergehenden) Praxis von Überwachungsexzessen (im Stile des deutschen *BND* oder der US-amerikanischen *NSA*) – deutlich, dass auch der Schweizer Geheimdienst *NDB* inskünftig das Potenzial hat, eine *demokratische Öffentlichkeit*, wenn nicht direkt zu verhindern, so doch erheblich zu stören.

⁷⁰Zu beachten ist, dass Computergeräte mit Trojaner-Software unbemerkt “verwanzt” und Daten ausgeleitet werden können: dabei können Mikrofon, Kamera oder andere Sensoren aktiviert und abgehört werden, auch unabhängig davon, ob der betroffene Akteur zu jeder Zeit in Kommunikationsvorgängen involviert ist. Konkrete Gedanken können offenbart werden, wenn Chat-, Blog- oder andere Beiträge in Entwurfsfassungen mitgelesen werden können, z. B. während Redigierungsphasen, ehe sie abgeschickt oder publiziert werden. (Vgl. [Kurz et al. \(2015: 6ff.\)](#))

⁷¹Die Überwachung mittels Drohnen mag zudem Aufnahmen von Orten liefern, die – rein örtlich – eigentlich den *privaten Räumen* und damit der *Privatsphäre* zuzuordnen wären. Dies ist z. B. dann der Fall, wenn ein privater Pool oder ein Golfplatz, der vom Boden aus einem beliebigen Akteur nicht ohne Weiteres sichtbar ist, von der Luft aus erfasst werden kann.

Entsprechende Plausibilisierungen erfolgen nachfolgend anhand jeweils zweier Beispiele:

- Was das **liberale Paradigma** betrifft, lässt sich summarisch feststellen, dass (1) angesichts des *Paradigmenwechsels* einer Überwachung vornehmlich der *Sozialsphäre* hin zur Möglichkeit regelrechter “staatliche[r] Übergriffe” (vgl. [Martinsen](#) 2010: 46ff.) in die *Intim-* und *Privatsphäre* hinein, eine grundlegende Verletzung des *liberalen Demokratiemodells* vorliegt; dass (2) *wirtschaftliche Privatinteressen*, die bei *liberalen Ansätzen* wichtigen Rang haben, untergraben werden, wenn der Staat auf grundsätzlich alle Firmen- und Fabrikationsgeheimnisse Zugriff erhält und diese (nach eigenem Ermessen und Erforderlichkeit) mit ausländischen Geheimdiensten oder auch Privaten austauschen kann. Damit hat der *NDB*, rein der Norm nach, die Möglichkeit, in- oder ausländische Konkurrenten mit Informationen so zu beliefern, dass die *Wirtschaftsfreiheit* gestört wird. Er kann dies im Namen übergeordneter – im Sinne der *Staatsraison* sinnhafter – Zwecke tun, wie um “die Handlungsfähigkeit der Schweiz zu unterstützen”⁷² oder “zum Schutz des Werk-, Wirtschafts- und Finanzplatzes Schweiz”⁷³ (im Rahmen der “Wahrung weiterer wichtiger Landesinteressen”⁷⁴).
- Im **deliberativen Paradigma** verschärft sich (1) die bereits für heutige Normen mögliche Rolle von *Chilling-Effects* (vgl. [Steinschaden](#) 2015) in bedeutendem Masse, weil Akteure damit rechnen müssen, sowohl in physischen als auch virtuellen *privaten* und *öffentlichen Räumen* in allen Formen (Text, Ton und Bild) überwacht zu werden – entsprechend können sich Akteure oder Gruppen (unbewusst) dafür “entscheiden”, sich in geringerem Masse zu artikulieren; (2) mit den Möglichkeiten, Computer oder Netzwerke anzugreifen und zu stören (oder auch zu verlangsamen) kann der *NDB* zudem Diskurse beeinträchtigen, und damit die Entstehung von *Konsens* als Form *deliberativer Öffentlichkeit* verhindern.
- Dem **partizipatorischen Paradigma** nicht zuträglich sind sicherlich (1),

⁷²Art. 2 Bst. c NDG

⁷³Art. 3 Bst. c NDG

⁷⁴Art. 3 NDG

die Möglichkeiten, die der *NDB* erhält, praktisch den kompletten *öffentlichen Raum* zu überwachen, der im *partizipatorischen Demokratiemodell* wichtiger Ort zur Versammlung der Summe von Meinungen und für die Entstehung von *Öffentlichkeit* ist – mittels Fluggeräten kann er selbst *Versammlungsöffentlichkeiten* feststellen und in ihren Bewegungsabläufen einordnen, die vom Boden aus nicht oder nur unzureichend beobachtbar sind; (2) die elektronischen Möglichkeiten des “*Cyberwar*”, Personen oder Gruppen daran zu hindern, an Kommunikation (überhaupt) noch zu *partizipieren* oder sich *virtueller Protestformen* zu bedienen, um sich zu artikulieren, sind Möglichkeiten, *partizipatorische Öffentlichkeit* zu schwächen. (Vgl. [Marques 2012: 5ff.](#))

4 Schlussbetrachtungen

Ausgehend von *demokratie-* und *öffentlichkeitstheoretischen* Elementen, die *demokratischer Öffentlichkeit* zuträglich sind, wurden drei theoretische Paradigmen als Grundlage genutzt, *Demokratie* und *Öffentlichkeit* zu fassen:

- die (1) an Stabilität und Bewährtem orientierte *liberale Modelle*, wo sich *demokratische Öffentlichkeit* durch Parlamente und entsprechend durch (indirekte) Wahlen ausdrückt;
- (2) *deliberative Modelle*, wo sich *demokratische Öffentlichkeit* durch *Konsens* im Zuge *vernunftorientierter* Diskursprozesse der (ständigen) Kommunikation zeigt, die sich verschränken;
- und (3) *partizipatorische Modelle*, wo *demokratische Öffentlichkeit* durch weitestgehende *Inklusion* von Akteuren erreicht wird, wie sie als *Teil-* oder *Gegenöffentlichkeiten* im Zuge *sozialer Bewegungen* manifest werden können: *partizipatorische Modelle* sind zudem *gemeinwohlorientiert* und können funktional der *Kontrolle* von Gesellschaft “von unten” dienen.

Ferner wurde das Konzept von *Privatsphäre* dahingehend operationalisiert, dass eine Unterscheidung in drei Lebenssphären, in denen sich Akteure bewegen können, möglich ist, mit

- der *Intimsphäre*, welche dadurch gezeichnet ist, dass damit Daten (oder Attribute) von Akteuren gemeint sind, welche Auskunft über Gefühle, Gedanken oder Krankheiten geben;
- der *Privatsphäre*, worüber *personenbezogene* oder *-beziehbare* Daten aller Art verstanden werden, die es erlauben eine Person zu bestimmen: das können beispielsweise Namen oder Telefonnummern sein;
- und der *Sozialsphäre*, die alle Daten von Akteuren, so sie sich in der *Öffentlichkeit* bewegen, umfasst: sichtbar sind beispielsweise Beziehungsnetzwerke von Personen, sofern sie sich publik (physisch oder virtuell) treffen; es können auch Inhalte der Kommunikation erfahrbar werden, sofern sich Akteure *öffentlich* (les-, hör- oder sichtbar) untereinander austauschen.

Auf Basis dieses theoretischen Fundaments konnte – nach einer kritischen Betrachtung der Schwierigkeit oder Unmöglichkeit Geheimdienste mithilfe *liberaler Demokratiemodelle* zu “kontrollieren” – plausibilisiert werden, dass der Schweizer Geheimdienst *NDB* schon heute über die *Macht* verfügt, *demokratische Öffentlichkeit* durch seine Möglichkeiten direkt oder indirekt in die *Intim-, Privat- und Sozialsphäre* von Akteuren oder Gruppen einzugreifen, (empfindlich) stören kann – und das obschon sein aktueller Fokus und seine eigenen Kompetenzen auf die Überwachung der *Sozialsphäre* liegen.

Werden diesem zusätzliche Machtbefugnisse zu Teil, wie sie durch das Nachrichtendienstgesetz *NDG* zur Zeit diskutiert werden, wird grosses Eingriffs- und damit Störpotenzial sichtbar, *demokratische Öffentlichkeit* in allen der Betrachtungsweisen (*liberal, deliberativ* oder *partizipatorisch*) zu erschweren oder zu verunmöglichen. Denn sein Fokus würde sich dahingehend wandeln, die (Massen-)Überwachung der *Intim- und Privatsphäre* zu ermöglichen und zudem Bereiche der *Sozialsphäre* zu erschliessen, die nach den jetzigen Möglichkeiten noch nicht (explizit, normativ) überwacht werden können.

Wird der theoretischen Betrachtung zudem eine historische wie auch empirisch (technische) Dimension hinzugefügt, muss eindringlich davor gewarnt werden, dem Schweizer Geheimdienst *NDB* zusätzliche Kompetenzen zu geben: denn schon normativ ist deutlich, dass er damit vom (propagierten und heutigen) Sicherheits- zum (eigentlichen und morgigen) Machtinstrument wird.

Da sich Geheimdienste – wie postuliert und empirisch belegt – nicht kontrollieren lassen, scheinen die Gefahren real, dass der *NDB* mit einem *Paradigmawechsel*, massiv die *Intim- und Privatsphäre* von Akteuren zu überwachen, den (Fort-)Bestand *demokratischer Öffentlichkeit* ernsthaft zu gefährden vermag. Dies bereits in Anbetracht dessen, dass der *NDB* mit den neuen Möglichkeiten, wesentliche Elemente aller drei Modelle von *Demokratie* und *Öffentlichkeit* (fundamental) in Frage stellen kann.

Eine Garantie, dass er *vernünftig* und dem *Gemeinwohl* entsprechend mit den neuen Kompetenzen umgehen würde, besteht indes nicht. Es erscheint vor allem eines als sicher: dass jede *parlamentarische Kontrolle* (weiterhin) versagen würde.

5 Nachtrag: Überarbeitung und Reflexion

Auseinandersetzung mit Kritikpunkten an der Arbeit

Die Schriftliche Arbeit SA wurde in der ursprünglichen Fassung vom 5. Januar 2016 als unzureichend eingestuft: der Autor wurde aufgefordert, sich mit Mängeln der Arbeit auseinander zu setzen. Es wurde übereingekommen, eine überarbeitete Fassung per 30. Januar 2016 einzureichen, die auf Kritikpunkte eingeht, um eine zumindest genügende Gesamtleistung (Referat und SA im Seminar) zu berechtigen.

In Punkten, in denen der Kritik aus zeitlichen oder inhaltlichen Gründen nicht gefolgt werden kann, wird sie nachfolgend zumindest schriftlich reflektiert.

5.1 Veränderte Stellen

Unter Punkt 1.2 wird die Referenz zur zunehmenden Bedeutung von Wirtschaftsinteressen geändert auf [Martinsen](#) (2010: 51ff.).

Die Referenz [Wyss](#) (2011: 7) wird unter Punkt 1.2 adäquat wiedergegeben.

Bei den Grundannahmen in 1.2 wird mit einer Fussnote die Referenz [GPDel](#) (2003: 1513; 1523) neu hinzugefügt, um zu belegen, dass ebenfalls Mittel, Wege als auch Ausmass von Überwachung dem Geheimbereich zufallen. Zudem wird – wie kritisiert – festgehalten, dass westliche Demokratien im Sinne der Staatsraison ohnehin “als letzte Arkanbereiche”⁷⁵ über Geheimbereiche verfügen. In Klammerbemerkung wird die Formulierung beibehalten, dass westliche Demokratien Geheimbereiche

⁷⁵Formulierung von Prof. Dr. Patrik Ettinger im Rahmen der Kritik dieser Arbeit.

weiter (darauf aufbauend) ausbilden können: vgl. hierzu die Reflexionen im Abschnitt [5.2.2](#).

Die ungenaue Formulierung über “diverse Modelle von *Demokratie* und *Öffentlichkeit*” unter Punkt [2.1](#) wird in Bezugnahme auf [Martinsen](#) (2010: 46) präzisiert.

Der postulierte Anspruch unter Punkt [3.1](#), dass die Geheimdienstkontrolle in der Schweiz öffentlich erfolgen können soll, wurde dahingehend geöffnet, dass diese zumindest einer kritischen (fragenden) *Öffentlichkeit* möglich sein müsste, die über Methoden und Ausmass der stattfindenden Überwachung orientiert sein möchte. Dem wird dadurch entgegengewirkt, dass sowohl in den heutigen gesetzlichen Grundlagen (*BWIS*) als auch in den zu schaffenden Grundlagen (*NDG*) Regelungen bestehen, das *Öffentlichkeitsprinzip* zu schwächen. Doch selbst der Anspruch an eine öffentliche, über die Massenmedien (mit *Gatekeeper*-Funktion) vermittelte Kontrolle ist vertretbar: dies wird im Zuge der Enthüllungen zum *NSA-Komplex* seit Juni 2013 von diversen Medienhäusern praktiziert. Bisher wurde nicht ersichtlich, inwiefern sich daraus strukturelle Nachteile für die Geheimdienstarbeit erwachsen hätten.

Die missverständliche Argumentation bei der Privatheit/Öffentlichkeit von *COMINT*-Überwachungen unter Punkt [3.2](#) wird aufgegriffen und in der zugehörigen Fussnote mit Erwägungen zu Legitimität und Illegitimität der Veröffentlichung solcher Daten zur Diskussion gestellt.

Die “pointierte These” unter Punkt [3.2](#), wonach der *NDB* neu fähig wäre, mittels den Kompetenzen aus dem *NDG* in die Gedankenwelt von Akteuren vorzudringen, wird mittels einer Fussnote und der neuen Referenz [Kurz et al.](#) (2015: 6ff.) belegt.

5.2 Reflexionen / Begründung unveränderter Stellen

5.2.1 Definition der Lebenssphären und Abgrenzung über Daten

Im Rahmen der Definition der Lebenssphären wird bemängelt, dass diese über Daten (statt Handlungssphären) erfolgt ist: dies wurde beibehalten, um in Bezug auf die gegebenen gesetzlichen Referenzen leichter Vergleiche darüber anstellen zu können, um welches Wissen es sich handelt, das Geheimdienste zuletzt konkret ansammeln. Es ist als illustrative Ergänzung zur zitierten Referenz [Schrödter](#) (2009) gedacht.

Der Feststellung darüber, dass der Schutz, konkret in die *Intimsphäre* einzudringen, “absolut” zu gelten habe, entspringt (so die Bedeutung der Anführungszeichen auch an der betroffenen Stelle) nicht dem Autor selber, sondern der Referenz, die als Grundlage dient und Folgendes festhält:

Die Intimsphäre ist absolut von Eingriffen geschützt. Zu dem höchstpersönlichen und intimen Lebensbereich gehört die Sexualität, Krankheiten, Gefühle und Gedankenwelt (z.B. in Tagebuchaufzeichnungen) und ähnliche die Person betreffenden nicht öffentliche persönliche Dinge wie auch die Intimpflege und der sanitäre Bereich.

Daraus wird die Unschärfe sichtbar, die bei der Abgrenzung zur *Privatsphäre* existiert und sich nicht vollends auflöst: während beispielsweise Krankheiten, Gefühle oder Gedanken Daten sind, die eine Person alleine für sich behalten kann, hängt das bei der Sexualität davon ab, ob es zu Interaktionshandlungen zu anderen Personen kommt. Sexualneigungen oder -sehnsüchte können nur dann strikte zur *Intimsphäre* gezählt werden, wenn damit gemeint ist, dass man sie zu den Gedanken zählt und es zu keinen dementsprechenden Handlungen kommt. Auch bei den Krankheiten lässt sich der strikte Bezug zur *Intimsphäre* mit seinem “absoluten” Schutz wohl auch nur dann halten, wenn damit niemand geschädigt wird: hat ein Akteur z. B. eine (sexuell) übertragbare Krankheit, kann eine Kenntnisnahme durch (staatliche oder betroffene individuelle) Dritte legitim sein.

5.2.2 Ausbildung von Geheimbereichen auch in westlichen Demokratien

Der Autor legt in den Grundannahmen von 1.2 nahe, dass westliche Demokratien Geheimbereiche auch ausbilden können. Beispielhaft für diese Annahme ist die Feststellung, dass gerade westliche Demokratien – im Sinne der Staatsraison – einen Paradigmenwechsel von legitimer zielgerichteter Überwachung von bestimm- baren Personen, hin zu einer Massenüberwachung vollziehen, die anlasslos und verdachtsunabhängig jeden betreffen kann. (Vgl. [Rosenbach und Stark](#) 2014)

In der Schweiz würden dem *NDB* mittels *NDG* zusätzliche Kompetenzen verschafft, die heute – wenn überhaupt – nur den Strafverfolgungsbehörden vorbehalten sind, so dass die Grenzen zwischen der (polizeilichen) Repressions- und (geheimdienstli- chen) Präventionsfunktion verwässert werden: dies ebnet rechtlich den Weg dafür, dass invasive Staatshandlungen mehr im Geheimen stattfinden.

Von Seiten der USA (in Zusammenarbeit mit europäischen Staaten) sind schon heute solche Praxen festzustellen, die in ihrer Intransparenz an Diktaturen grenzen, z. B. durch

- Unterhalt von *CIA*-Geheimgefängnissen in der Guantanamo Bay in Kuba oder in Osteuropa,
- *US-Army*-Drohntötungen auf Grund von Metadaten der Kommunikation, wobei die Daten dafür auch vom deutschen *BND* stammen oder
- *JSOC*-Tötungskommandos mittels geheimer Listen zu eliminierender Akteure.

Wichtig erscheint, die geheime Natur dieser Prozesse hervorzuheben: sowohl die Verschleppungen in inoffizielle Gefängnisse als auch die luft- und bodengestützten Tötungen erfolgen auf Grund unbekannter Auswahlkriterien, die keiner demokrati- schen Kontrolle unterliegen. Sie stehen zudem fairer Gerichtsprozesse fern, wie sie für westliche Demokratien – so auch für die USA – im Rahmen des Justizwesens eingefordert werden. Grundsätze wie die Unschuldsvermutung werden gegen den Generalverdacht und stichhaltige Beweise gegen wage Vermutungen ausgetauscht. Diese eigentliche Paralleljustiz basiert ihr Handeln auf Wissen und “Beweisen” von

militärischen und geheimdienstlichen Akteuren, die wiederum – so wird in der Arbeit argumentiert – keiner wirksamen demokratischen Kontrolle unterliegen. (Vgl. Untersektion 3.1)

5.2.3 Zusammenhang demokratische Öffentlichkeit und Grenzziehungsproblematik öffentlich/privat

Für Abschnitt 2.1 wird gefragt, inwiefern die von [Martinsen](#) (2010: 51ff.) aufgeworfenen zwei wichtigen Bedingungen für das Zustandekommen bzw. Fortbestehen einer *demokratischen Öffentlichkeit* im Zusammenhang mit der doppelten Grenzziehungsproblematik öffentlich/privat von Belang sind.

Um diesen Zusammenhang ging es primär nicht:

Die Ausführungen der zwei wichtigen Bedingungen für *demokratische Öffentlichkeit* wurden dazu bemüht, die Widersprüche zu den (alten und neuen) Normen des *NDB* zu thematisieren: die *demokratische Öffentlichkeit* umschreibt die normativen Umstände, die in einer modernen Demokratie – wie auch der Schweiz – erstrebenswert sind. In Untersektion 3.2 ist es, wo beispielhaft aufgezeigt wird, dass die (geplanten) gesetzlichen Normen *demokratische Öffentlichkeit* gefährden.

Dennoch besteht insofern ein Zusammenhang, als dass im Schutz der *Privatsphäre* eine wichtige Funktion gesehen wird, sich (gegen aussen zuletzt) freiheitlich zu betätigen. Im Zusammenhang mit der Möglichkeit, sich mit verschiedenen Meinungen (Möglichkeit von *Pluralismus*) zu äussern, ist *Öffentlichkeit* überhaupt erst denkbar. (Vgl. [Martinsen](#) 2010: 46ff.)

5.2.4 Geheimdienstkontrolle nach dem liberalen Paradigma

Es wird kritisiert, dass die Darstellung der (Schweizer) Geheimdienstkontrolle in Abschnitt 3.1 als Kontrolle nach dem *liberalen Paradigma* verengt wird, denn auch im *deliberativen Paradigma* spielt das Parlament eine Rolle. Es soll zum Ausdruck gebracht werden, dass die installierte Kontrollart weder auf *Inklusion* setzt – wie beim *partizipatorischen* Ansatz, noch darauf bedacht ist, diejenigen Stimmen zu

Wort kommen zu lassen, die nach rationalen Kriterien die besten Argumente zu bieten hätten und dazu beitragen könnten, den *NDB* effektiver und ohne Partei- oder anderen -Interessen (unabhängig) zu kontrollieren – wie beim *deliberativen* Ansatz typisch. Der Autor will argumentieren, dass es paradigmatisch für den *liberalen* Ansatz ist, dass Vertreter (in dem Fall: gewählte Parlamentarier) die Kontrolle ausüben: sie kann nicht von allen oder zumindest von allen, die willens und fähig sind, ausgeübt werden. Kommt es über massenmedial vermittelte Kanäle oder durch Aktionen im Stile der Snowden-Enthüllungen zu (unintendierter) Geheimdienstkontrolle, die – der Art nach – eher dem *deliberativen*, respektive *partizipatorischen* Ansatz verpflichtet ist, so gilt diese als inoffiziell und gewissermassen ungültig im Sinne des *liberalen Paradigmas*, weil diese ein besonderes Augenmerk darauf hat, dass das *Legalitätsprinzip* eingehalten wird.

5.2.5 Zu Sinn und Unsinn staatlicher Informationskontrolle

In Punkt 3.2 wird in der Arbeit beibehalten, dass die Löschung oder Zensur von “Propagandamaterial” Deliberation nicht zuträglich ist. Kritik daran richtete sich gegenüber der Möglichkeit, dass das betroffene “Propagandamaterial” Regeln der Deliberation, wie Anerkennung, grundlegend verletzen mag, wie dies [Martinsen](#) (2010: 294) als wichtige Regel für Teilnehmer massenmedialer Kommunikation festhält und wofür ein “Gebot der Zensur” als Möglichkeit gesehen wird. Gleichzeitig kann auf das Internet bezogen trotz mangelnder *Gatekeeper*-Funktion (im Vergleich zu den klassischen Massenmedien) auf die “kollektive Qualitätssicherung” gesetzt werden, die sich durch öffentliche Kritik ergibt (ebd.: 295ff.).

Selbst im (klassisch) massenmedialen Bereich hängt die Diskussion davon ab, ob es den Akteuren hinter dem “Propagandamaterial” gelingt, die Botschaft breit (massenmedial) zu streuen oder ob es sich (selber) um marginalisierte Gruppen handelt, die sich (ohnehin) nur schwerlich Gehör verschaffen können. Abgesehen davon müsste auch hier eine Grenzziehungsdebatte geführt werden, wo die Grenzen von Anerkennung und Respekt sind: in der Schweiz werden Diskussionen zu Asyl- und Ausländerfragen (zumindest) grenzwertig ausgetragen, ohne, dass der *NDB*

diese Norm in solchen Fällen bemüht hätte. Damit verbunden ist die einer solchen Regelung innewohnende Gefahr da, dass die Grenzziehung mehr politischen als (vernunftmässigen) deliberativen Regeln gehorchen kann.

Zudem wird im betroffenen Abschnitt bereits erwähnt, dass sich beim Vollzug solcher Regelungen zwangsweise ein Phänomen des *Digital-Divide* einstellt: dadurch, dass weder eine restlose Löschung von Inhalten im Internet möglich ist noch eine vollkommene Zensur funktioniert, trägt eine solche Norm tatsächlich am ehesten dazu bei, dass (breiten) Bevölkerungskreisen Zugangshürden zu Inhalten verschafft werden; Interessierte und technische versierte Kreise von Akteuren können an dieses "Propagandamaterial"-Wissen im Gegenzug aber nach wie vor herankommen und es in Diskussionen verwerten. Insbesondere können gerade Akteure, die nicht an Deliberation interessiert sind, als Multiplikatoren von solchem Wissen fungieren, falls sie fähig sind, die geschaffenen Zugangshürden zu überwinden. Das Bewusstsein dafür und dementsprechende Gegenstrategien bzw. Fähigkeiten, staatliche Massnahmen der Zensur zu unterlaufen, können bei Zusammenhängen, von denen "Propagandamaterial" ausgeht, erwartet werden.

Quellenverzeichnis

Literatur

Kai Biermann. Selektorenbericht. Ein Versuch, den BND freizusprechen. *Zeit Online*, 30. Oktober 2015. URL <http://www.zeit.de/digital/datenschutz/2015-10/selektoren-nsa-bericht-graulich-bnd>. Abruf: 3. Januar 2016.

Kai Biermann und Patrick Beuth. Bundesnachrichtendienst: Was sind eigentlich Selektoren? *Zeit Online*, 24. April 2015. URL <http://www.zeit.de/digital/datenschutz/2015-04/bundesnachrichtendienst-bnd-nsa-selektoren-eikon1>. Abruf: 3. Januar 2016.

Anna Biselli. IMSI, IMEI, SIP: Selektoren-Gutachter Graulich verheddert sich im Technik-Dschungel. *Netzpolitik.org*, 4. November 2015a. URL <https://netzpolitik.org/2015/imsi-imei-sip-selektoren-gutachter-graulich-verheddert-sich-im-technik-dschungel/>. Abruf: 30. November 2015.

Anna Biselli. Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: "Selektorenherausgabe wäre Urheberrechtsverletzung". *Netzpolitik.org*, 5. November 2015b. URL <https://netzpolitik.org/2015/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-kurt-graulich-w-a-und-albert-karl/>. Abruf: 3. Januar 2016.

Heinrich Busch. Fichenaffäre 2.0: 28 seiten namen vom kessel in landquart. *WOZ*, 20, 19. Mai 2011. URL <https://www.woz.ch/1120/fichenaffaere-20/28-seiten-namen-vom-kessel-in-landquart>. Abruf: 5. Januar 2016.

Daniel Foppa. Wie der Nachrichtendienst die Fiche von Anni Lanz versteckt. *Tages-Anzeiger*, 10. Dezember 2010. URL <http://www.tagesanzeiger.ch/schweiz/standard/Wie-der-Nachrichtendienst-die-Fiche-von-Anni-Lanz-versteckt-/story/19983203>. Abruf: 5. Januar 2016.

Nancy Fraser. Vermittelte Weiblichkeit. Feministische Wissenschafts- und Gesellschaftstheorie. In: Elvira Scheich, *Öffentlichkeit neu denken. Ein Beitrag zur Kritik real existierender Demokratie*, S. 151–182. Hamburg Edition, Hamburg, 1996.

Jörg Frischknecht. Vorwort. In: Komitee Schluss mit dem Schnüffelstaat [Verein grundrechte.ch], *Schnüffelstaat Schweiz. Hundert Jahre sind genug*. Limmat Verlag [buch & netz]. URL <http://buchundnetz.com/online-buch/schnueffelstaat-schweiz-ob/vorwort/>. Abruf: 3. Januar 2015.

Geschäftsprüfungsdelegation der Eidgenössischen Räte GPDel. Satellitenaufklärungssystem des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (Projekt «Onyx»).

- Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte. 10. November 2003. URL <http://www.parlament.ch/d/dokumentation/berichte/berichte-delegationen/berichte-der-geschaeftspruefungsdelegation/Documents/ed-pa-gpd-onyx-d.pdf>. Abruf: 28. November 2015.
- Kurt Graulich. Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation. Prüfung und Bewertung von NSA-Selektoren nach Massgabe des Beweisbeschlusses BND-26. *Bericht im Rahmen des 1. Untersuchungsausschusses der 18. Wahlperiode des Deutschen Bundestages*, 23. Oktober 2015. URL https://www.bundestag.de/blob/393598/b5d50731152a09ae36b42be50f283898/mat_a_sv-11-2-data.pdf. Abruf: 3. Januar 2016.
- Ansgar Graw. So hackte ein Teenager die E-Mails vom CIA-Chef. 21. Oktober 2015. URL <http://www.welt.de/politik/ausland/article147900244/So-hackte-ein-Teenager-die-E-Mails-vom-CIA-Chef.html>. Abruf: 3. Januar 2016.
- Jürgen Habermas. *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*. Surhkamp, Frankfurt am Main, 2009.
- Carlos Hanimann. «Operation Transit»: Spionagebefehl aus dem Kanzleramt. *Wochenzeitung WOZ (Online)*, 22. Oktober 2015. URL <https://www.woz.ch/1543/operation-transit/spionagebefehl-aus-dem-kanzleramt>. Abruf: 3. Januar 2016.
- Markus Häfliger. Kritik am Nachrichtendienst. Eklatante Führungsmängel im Geheimdienst. *NZZ*, 5. September 2013. URL <http://www.nzz.ch/schweiz/geheimdienst-1.18145217>. Abruf: 3. Januar 2016.
- Kurt Imhof. “Öffentlichkeit” als historische kategorie und als kategorie der historie. *Schweizerische Zeitschrift für Geschichte*, Band 46, 1996. URL <http://retro.seals.ch/openurl?rft.issn=0036-7834&rft.date=1996&lPage=3&PDFRequested=true>. Abruf: 3. Januar 2016.
- Kurt Imhof. *Demokratisierung durch Social Media?*, S. 15–26. 2015. ISBN 978-3-658-10139-8.
- Julius Jamal. Geheimdienste gehören nicht zur Demokratie – Im Gespräch mit Jens Petermann. 6. August 2012. URL <http://diefreiheitsliebe.de/politik/geheimdienste-gehoren-nicht-zur-demokratie/>. Abruf: 3. Januar 2016.
- Ulla Jelpke. Der Terror der Geheimdienste. *Initiative zur Verbesserung der Qualität politischer Meinungsbildung e.V. (IQM)*, *www.NachDenkSeiten.de*, 2015. URL <http://www.nachdenkseiten.de/?p=26060>. Abruf: 3. Januar 2016.
- Leo Kelion. NSA-GCHQ Snowden leaks: A glossary of the key terms. *BBC*, 28. Januar 2014. URL <http://www.bbc.com/news/technology-25085592>. Abruf: 4. Januar 2016.

- Constanze Kurz, Dirk Engling, Frank Rieger, und Thorsten Schröder. Chaos Computer Club. Stellungnahme an das Bundesverfassungsgericht zum BKA-Gesetz und zum Einsatz von Staatstrojanern. *1 BvR 966/09, 1 BvR 1140/09*, 7. Juli 2015. URL http://www.ccc.de/system/uploads/189/original/BKAG_Stellungnahme.pdf. Abruf: 30. Januar 2015.
- Patrick Kühnis. So hilft die Zürcher Stadtpolizei dem Bund beim Schnüffeln. *Tages-Anzeiger*, 22. Juli 2010. URL <http://www.tagesanzeiger.ch/zuerich/stadt/So-hilft-die-Zuercher-Stadtpolizei-dem-Bund-beim-Schnueffeln-/story/10534544>. Abruf: 5. Januar 2016.
- Moritz Leuenberger und Josi Meier. Bericht der Parlamentarischen Untersuchungskommission (PUK). In: *24 Bundesblatt, 142. Jahrgang, Bd. 1*, S. 637–878. 1989. URL <http://www.parlament.ch/d/dokumentation/berichte/berichte-puk/Documents/ed-berichte-puk-ejpd.pdf>. Abruf: 3. Januar 2016.
- Frank Marcinkowski. Massenmedien und die Integration der Gesellschaft aus Sicht der autopoietischen Systemtheorie: Steigern die Medien das Reflexionspotential sozialer Systeme? In: Kurt Imhof, Otfried Jarren, und Roger Blum, *Integration und Medien*, S. 110–121. Westdeutscher Verlag, Wiesbaden, 2002.
- Hernani Marques. Protestformen im Cyberspace. Möglichkeiten und Grenzen aus zivilgesellschaftlicher Sicht. *Sociology in Switzerland. Towards Cybersociety and Vireal Social Relations*, September 2012. URL http://socio.ch/intcom/t_hmarques.pdf. Abruf: 5. Januar 2015.
- Hernani Marques. Massenüberwachung mittels Computerlinguistik und Sprachtechnologie im Lichte der Snowden-Enthüllungen. Recherchen zum Stand der Technik und kritisch-illustratives Datenprojekt zur automatischen Generierung von Selektoren für verdachtsunabhängige Massenüberwachung von Datenströmen mit manueller Evaluation resultierender Treffer. Masterarbeit, Universität Zürich, 2015. URL https://ia801504.us.archive.org/29/items/MA_computerlinguistikmasseneueberwachung/masterarbeit--clmasseneueberwachung_v1.11_web.pdf. Abruf: 5. Januar 2015.
- Renate Martinsen. Öffentlichkeit in der “Mediendemokratie” aus der Perspektive konkurrierender Demokratietheorien. In: Barbara Marcinkowski, Frank und Pfetsch, *Politik in der Mediendemokratie*, S. 37–69. Politische Vierteljahresschrift, Sonderheft 42/2009, VS, Wiesbaden, 2010.
- Marcel Rosenbach und Holger Stark. *Der NSA-Komplex: Edward Snowden und der Weg in die totale Überwachung*. Spiegel-Verlag, Hamburg, 2014.
- Joachim Scharloth, Meyer-Plath Gordian, Anna Biselli, und Constanze Kurz. Die Grenzen des Geheimen. Transparenz und Geheimhaltung im digitalen Zeitalter. Podiumsdiskussion

- (Video-Podcast), Datenspuren 2015, 25. Oktober 2015. URL https://media.ccc.de/v/DS2015-7083-die_grenzen_des_geheimen#video. Abruf: 3. Januar 2016.
- Gerhard Schmid. Bericht über die Existenz eines Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON). 2011/2098 (INI). *Europäisches Parlament. Sitzungsdokument A5-0264/2001 Teil 1*, 11. Juli 2011. URL <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE>. Abruf: 29. November 2015.
- Petja Schrödter. Das Allgemeine Persönlichkeitsrecht. *Jura & Serv. Das juristische Informationsportal der Judikatoren*, 13. Januar 2009. URL <http://www.juraserv.de/medienrecht/das-allgemeine-persoendlichkeitsrecht-apr-01002/all-pages>. Abruf: 3. Januar 2016.
- Raphael Schön. “Kein Staat kann seinen Geheimdiensten vertrauen” – William Binney im Interview. *VICE*, 4. Dezember 2015. URL <http://motherboard.vice.com/de/blog/geheimdienste-sind-teure-datenml-sammler-die-sich-nicht-an-gesetze-halten>. Abruf: 3. Januar 2016.
- Der Spiegel. NSA-Attacken auf SSL, VPN, SSH, Tor etc.: Das sind die Snowden-Dokumente. 29. Dezember 2014. URL <http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-nsa-attacken-auf-ssl-vpn-ssh-tor-a-1010553.html>. Abruf: 3. Januar 2016.
- Jakob Steinschaden. Massenüberwachung zeigt soziale Folgen. 8. Mai 2015. URL <https://www.freitag.de/autoren/netzpiloten/massenueberwachung-zeigt-soziale-folgen>. Abruf: 27. November 2015.
- Michaela Wendekamm. *Die Wahrnehmung von Migration als Bedrohung. Zur Verzahnung der Politikfelder Innere Sicherheit und Migrationspolitik*. VS, Münster, 2014.
- Marco Wyss. Zivile Nachrichtendienstsysteme im europäischen Umfeld der Schweiz. Ausgewählte fusionierte und getrennte zivile In- und Auslandsnachrichtendienste im Vergleich. *Center for Security Studies (CSS), ETH Zürich*, September 2011. URL http://www.vbs.admin.ch/internet/vbs/de/home/documentation/publication/snd_publ.parsysrelated1.91732.DownloadFile.tmp/zivilenachrichtendienste.pdf. Abruf: 3. Januar 2016.
- René Zeller und Markus Häfliger. Interview mit Nachrichtendienst-Chef Markus Seiler. “Wir haben weltrekordverdächtig viele Kontrolleure”. *NZZ*, 19. November 2014. URL <http://www.nzz.ch/schweiz/wir-haben-weltrekordverdaechtig-viele-kontrolleure-1.18427615>. Abruf: 3. Januar 2016.