

**Datenschutz in Deutschland –
Informationelle Selbstbestimmung im
Konflikt zwischen Marktinteressen und
Bürgerrecht**

Masterarbeit im Masterstudiengang
Politikwissenschaft: *Demokratisches Regieren und
Zivilgesellschaft* der Universität Osnabrück

vorgelegt am 30.10.2014

von Kristina Pfaff

Inhaltsverzeichnis

I Einleitung	1
1) Fragestellung und Hypothese	2
2) Forschungsstand	3
3) Aufbau.....	7
4) Inklusive Sprache und Textgestaltung	7
II Relevanz und Entwicklungstendenzen.....	9
1) Politischer Kontext	10
2) Technologischer Kontext.....	13
3) Spezifische Einflussfaktoren.....	16
a) Politikfeld im Mehrebenensystem.....	16
b) Enthüllungsplattformen, Whistleblower und ihre Folgen	17
III Methode.....	20
1) Forschungsdesign.....	20
2) Operationalisierung der Grundbegriffe	21
3) Datenmaterial und Auswahl der Akteure	22
IV Theoretischer Rahmen	25
1) Ressourcenmobilisierungsansatz.....	25
a) Klassische Ressourcenmobilisierungstheorie	26
b) Mobilisierung und kollektive Aktion	27
2) Advocacy Coalition Framework.....	31
3) Synthese.....	36
V Datenpolitische Akteure und ihre Aktivitäten	39
1) Zivilgesellschaftliche Datenschutzgruppen.....	40
a) Chaos Computer Club (CCC).....	41
b) Arbeitskreis Vorratsdatenspeicherung	46
c) Deutsche Vereinigung für Datenschutz	50

2) Privatwirtschaftliche Akteure	54
a) BITKOM	54
b) Google.....	58
c) Initiative D21.....	64
3) Blogger_innen und Netjournalismus.....	68
a) Netzpolitik.org.....	68
b) Spackeria	71
c) Sonderfall WikiLeaks	75
4) Parteien und staatsnahe Akteure	76
a) Piratenpartei	77
b) Bündnis 90/ Die Grünen.....	82
c) Landesdatenschutzbeauftragte	86
d) Zwischenfazit	90
VI Advocacy Coalition Frameworks.....	93
VII Fazit.....	99
Literaturverzeichnis	103
Abkürzungsverzeichnis.....	121

I Einleitung

Datenschutz war in den letzten Monaten ein medial dominantes und gesellschaftlich breit diskutiertes Thema. Lange schien es für Internetuser nahezu selbstverständlich, für Dienste und deren leichte Bedienbarkeit mit persönlichen Daten zu zahlen. Diese wurden zu einer Art Ersatzwährung, die in beinahe unbegrenztem Maße vorhanden und verfügbar war. Während Unternehmen nach der Dotcom-Blase neue Geschäftsmodelle im Internet dadurch finanzieren, dass sie personalisierte Werbung schalten, aus dem Nutzungsverhalten Marketingstrategien ableiten und mit den Daten ihrer User handeln, formiert sich in Deutschland nach und nach Widerstand gegen diese Praxis. Spätestens seit den Enthüllungen auf der Plattform WikiLeaks sowie durch den Whistleblower Edward Snowden konnte Entsetzen vieler Menschen über das Ausmaß staatlicher Überwachung durch ausländische Geheimdienste festgestellt werden. Diese konnte umso lückenloser vollzogen werden, da gerade die großen Internetfirmen bereitwillig mit den Geheimdiensten kooperierten und gespeicherte Informationen weitergaben. Was lange als Verschwörungstheorie abgetan wurde, schien plötzlich real und die Vorstellung, dass technische Ausspähmöglichkeiten durch Geheimdienste nicht genutzt würden, entpuppte sich bald als naiver Irrglaube. Auch die deutschen Bundesregierungen (sowohl bestehend aus CDU/CSU und FDP, als auch aus CDU/CSU und SPD) konnten nicht ausreichend aufklären, welche Überwachungsmaßnahmen durch ausländische Geheimdienste ergriffen wurden, was die Resultate dieser Maßnahmen waren und wie weit die Verstrickungen mit den eigenen Geheimdiensten gingen. Vielmehr erweckten sie den Eindruck, die politische Aufklärung verhindern und aus dem öffentlichen Diskurs heraushalten zu wollen. Zu groß schienen die Konsequenzen eines Vertrauensverlustes der eigenen Bevölkerung gegenüber „befreundeten“ Staaten.

Datenschutz wurde vom *Special-Interest*-Thema zu einem Gegenstand von breitem öffentlichen Interesse. Die Unverletzlichkeit des Fernmeldegeheimnisses wurde massiv missachtet (vgl. z.B. Prantl 2014) und private Kommunikation schien plötzlich nicht mehr in vollem Umfang gewährleistet zu sein. Nach und nach wurden auch auf juristischem Wege Weichenstellungen für eine Abkehr bisheriger

Datenpolitik vorgenommen. So wurde nach dem Urteil des Bundesgerichtshofs (BGH) im Jahre 2010 auch seitens des Europäischen Gerichtshofs (EuGH) die umstrittene Vorratsdatenspeicherung für unrechtmäßig erklärt, nachdem sich zuvor breiter Widerstand innerhalb der Netzgemeinde regte.

Anhand der Entwicklungen der letzten Jahre lassen sich zwei diametrale Tendenzen feststellen: Auf der einen Seite die zunehmende Sammlung, Speicherung und Auswertung personenbezogener Daten durch Unternehmen und staatliche Ermittlungsbehörden, auf der anderen Seite eine wachsende Gruppe, die dem Prozess kritisch gegenübersteht und einen stärkeren Datenschutz fordert. Natürlich lassen sich nicht nur diese beiden Pole auf einem Kontinuum identifizieren, vielmehr gibt es diverse Abstufungen zwischen Datenschutz und Datenfreiheit, die in dieser Arbeit aufgezeigt werden. Die zentralen Diskursstränge und die wichtigsten Akteursgruppen sollen den Kern dieser Arbeit bilden.

1) Fragestellung und Hypothese

Diese Masterarbeit wird die datenschutzrelevanten Entwicklungen der letzten Jahre herausstellen und darlegen, welche nichtstaatlichen Akteure den Diskurs rund um Datenschutz und das Recht auf informationelle Selbstbestimmung prägten. Der Fokus wird zum einen auf den *netzpolitischen* Veränderungen liegen, also jenen Veränderungen, die die Informations- und Kommunikationstechnologien (im Folgenden IKT) betreffen. Dabei wird der Zeitraum der Untersuchung auf die Jahre zwischen 2001 und 2014 beschränkt bleiben, da das Internet in diesem Zeitraum tiefgreifenden Wandlungsprozessen unterworfen war, auf die im zweiten Kapitel genauer eingegangen wird. Auch beschränkt sich die Untersuchung nicht allein auf zivilgesellschaftliche Akteure, sie bezieht darüber hinaus auch führende journalistische Onlinemedien, staatsnahe Organisationen sowie privatwirtschaftliche Akteure ein, um das Spektrum des Forschungsgegenstandes „Datenschutzpolitik“ zu erweitern und ein möglichst umfassendes Bild diverser Aktionsformen und Beeinflussungsmöglichkeiten von nationalen *policies* zeichnen zu können. Durch die Aussparung staatlicher Institutionen kann ein Fokus auf *Bottom-Up*-Prozesse gelegt

werden, die dieses Politikfeld maßgeblich beeinflussen und formen. Auch wird erforscht, welche Koalitionen die einzelnen Akteure eingehen, um ihre politischen Ziele zu erreichen. Unter Einbeziehung dieser Prämissen lautet die Fragestellung dieser Arbeit: „Wie nehmen nichtstaatliche Akteure Einfluss auf digitale Datenschutzpolitik und welche Koalitionen gehen sie dazu ein?“

Aus dieser Fragestellung leite ich folgende Hypothesen ab: (1) Es gibt einen Unterschied zwischen den Akteursformen bezüglich ihrer Koalitionsbildung: Zivilgesellschaftliche Gruppen sind aufgrund ihrer geringeren Ressourcen stärker geneigt, Kooperationen mit anderen Gruppen einzugehen, um synergetische Effekte nutzen zu können, während privatwirtschaftliche und journalistisch agierende Akteure relativ autonom handeln können und nicht von Kooperationen und Netzwerkbildungen abhängig sind. (2) Netzpolitik wird vornehmlich als Wirtschaftspolitik betrachtet: Privatwirtschaftliche Unternehmen genießen einen privilegierten Zugang zu relevanten politischen Entscheidungsträger_innen zur Unterstützung ihrer Interessenpolitik, während zivilgesellschaftliche Akteure aufgrund ihrer begrenzten finanziellen Ressourcen Methoden nutzen, die darauf ausgelegt sind, ihrem Anliegen öffentlich Gehör zu verleihen und ihre Positionen in dem Diskurs in breite Gesellschaftsschichten zu tragen.

2) Forschungsstand

Eine Entwicklungslinie bisheriger politikwissenschaftlicher Forschung im Bereich der Netzpolitik bezieht sich auf den Einfluss der *Infrastruktur* Internet auf soziale Bewegungen und Zivilgesellschaften. Wie verändern neue IKT zivilgesellschaftliches Engagement, soziale Bewegungen oder Partizipation im Allgemeinen? Wodurch zeichnen sich die neuen Formen digitaler Vernetzung und Kommunikation aus? Welche Vorteile bieten neue Mobilisierungs- und Verbreitungsstrukturen? Wong und Brown fassen die Haupttendenz der Forschung wie folgt zusammen: „To date, many have considered the role of technology as a way to retool existing ways of participating in citizen movements“ (Wong, Brown 2013: 1016). Das Internet und Soziale Netzwerke wurden dementsprechend häufig nicht als Ausdruck tiefgreifenden Wandels ver-

standen, sondern lediglich als neue Werkzeuge, die zivilgesellschaftliche Gruppen für die Durchsetzung ihrer Interessen nutzen.

Vor dem Hintergrund des arabischen Frühlings wurde der Einfluss von sozialen Netzwerken für Proteste gegen autoritäre Regime untersucht und sehr kontrovers bewertet. Während einige Forscher_innen und Journalist_innen behaupteten, die Revolutionen von heute würden über Facebook und Twitter organisiert und koordiniert, bezweifeln andere diese These und betonen die Bedeutung physischer Anwesenheit von Menschen sowie deren „analoge“ Mobilisierung bei Protesten (vgl. z. B. Morozov 2011). Doch auch in westlichen Demokratien wird die Entwicklung der Zivilgesellschaft unter der Fragestellung betrachtet, wie sich Partizipation in Zeiten der zunehmenden Vernetzung ändert und welche Auswirkungen dies auf Gesellschaften und staatliche Institutionen hat. Die Proteste rund um ACTA (Anti-Counterfeiting Trade Agreement) oder die *Occupy*-Bewegung wurden durch die Möglichkeiten neuer Medien sowie sozialer Netzwerke maßgeblich geprägt und vielleicht erst möglich gemacht. Die Chancen und Risiken der zunehmenden Digitalisierung werden unter dieser Perspektive diskutiert: Sinken die Hürden für gesellschaftliche Partizipation und kann daraus eine stärkere Einbindung der Bevölkerung folgen oder sind die neuen unverbindlichen Formen der politischen Aktivität zu flüchtig, um langfristige und fundierte Veränderungen herbeizuführen? Auch hier lassen sich bisher keine eindeutigen Antworten finden, der Forschungsprozess steht hier noch am Anfang. Darüber hinaus müssen auch erst Instrumente entwickelt werden, um diese Formen der Partizipation wirklich messen und erforschen zu können. Auch die Frage nach dem Institutionalierungsgrad politischen Aktivismus stellt sich oft: Sind die digitalen Partizipationsmöglichkeiten überhaupt geeignet, sich in klassische institutionalisierte Organisationen zu transformieren?

Darüber hinaus nimmt in der soziologischen Perspektive die Untersuchung der digitalen Netzgemeinde eine herausgehobene Stellung ein. Um welche Personengruppen handelt es sich dabei? In welchen Milieus sind die Aktiven verankert? Welchen Einfluss hat das auf ihre Identitätsbildung? So stellt z. B. Vowe fest: „hier bildet sich ein *neues Elitensegment* heraus“ (Vowe 2014: 42, Hervorhebung im Original), während andere bereits eine „Nerdokratie“ (Passig/ Lobo 2012: 175) am Horizont

wählen. An diese Ausgangslage anknüpfend befasst sich ein Forschungsstrang vor allem mit dem sog. *digital divide*, also der Frage danach, welche Auswirkungen es hat, dass einige Menschen das Internet kaum oder gar nicht nutzen (können) und welche Gefahren daraus für die Gesellschaft entstehen. Zudem werden in diesem Kontext Möglichkeiten diskutiert, wie diese digitale Spaltung überwunden oder zumindest verringert werden kann, sodass die Vorteile der Digitalisierung auch Gruppen zugutekommen, die bisher keinen Zugang zum Internet und digitalen Medien hatten.

Ein weiterer Untersuchungsstrang behandelt Datenschutzpolitik vor allem auf einer rein institutionellen Ebene. So stellen sich z. B. Fragen im Zusammenhang mit der Harmonisierung der Datenschutzgesetze auf europäischer Ebene durch die EU-Datenschutzrichtlinie. Auch entstand mit zunehmender Überwachung in den letzten Jahren eine Art „Überwachungsforschung“ die zum einen die staatlichen oder unternehmerischen Maßnahmen untersucht, die mit einer verstärkten sicherheitspolitischen Orientierung in Staaten des globalen Nordens einhergehen, auf der anderen Seite aus einer soziologischen Perspektive versucht herauszuarbeiten, welche Resultate sich aus diesen Maßnahmen auf Gesellschaften, die sich als freiheitlich verstehen, ergeben. Aus deutscher Perspektive kann Nils Zurawski als führender Forscher auf dem Gebiet gelten, da seine wissenschaftlichen Veröffentlichungen sowie das von ihm als Teil eines Forschungsnetzwerkes geführte Blog surveillance-studies.org international Anerkennung fanden und einen wichtigen Beitrag zum Überwachungsdiskurs innerhalb der *scientific community* leisten.

Kaum wurde jedoch bisher zu den netzpolitischen Akteuren in Deutschland geforscht. Wendelin und Löblich untersuchten zwar den Netzpolitik-Aktivismus in Deutschland, ihre Untersuchungsreichweite ist jedoch in zweierlei Hinsicht eine andere als in dieser Arbeit: Zum einen untersuchen sie allein zivilgesellschaftliche Gruppen oder besonders aktive Personen, andere netzpolitische Akteure werden nicht in ihre Untersuchung einbezogen. Darüber hinaus spezialisieren sie sich weniger auf Datenschutz, sondern klassifizieren ihn nur als einen Teilaspekt netzpolitischen Aktivismus, der gleichberechtigt neben Informationsfreiheit, Fragen des Urheberrechts und der Einbeziehung einer Genderperspektive in der Netzpolitik steht (vgl. Wendelin/ Löblich 2013). Der Politikwissenschaftler Johannes Fritz ver-

glich netzpolitische Entscheidungsprozesse in den Bereichen Datenschutz, Urheberrecht und Internetsperren zwischen Deutschland und Großbritannien, doch auch hier wurden die Akteure nicht tiefergehend und systematisch untersucht (vgl. Fritz 2012). Eine Gemeinsamkeit zwischen dieser Arbeit und dem Werk von Fritz liegt in der Verwendung des *advocacy coalition framework* als theoretisches Rahmenkonstrukt.

Daraus resultierend stellt diese Arbeit einen neuen Beitrag zur wissenschaftlichen Forschung dar, in dem viele der oben genannten Aspekte miteinander verwoben und zueinander in Beziehung gesetzt werden. Zum einen wird die Datenschutzpolitik aus einer neuen Perspektive betrachtet, die nicht die staatlich-institutionalisierte ist. Der Akteursbezug wird hier vor allem durch die Fokussierung des nicht-staatlichen Sektors hergestellt, womit die Arbeit in ein sozialwissenschaftliches Vakuum vordringen kann, da eine dezidierte Analyse netz- und datenschutzpolitischer Akteure und Organisationen bisher für die BRD ausgeblieben ist. Dementsprechend kritisieren Betz und Kübler: „Leider ist das Schrifttum zu den Zielen, zur Struktur und zum Einfluss dieser Organisationen äußerst dürftig“ (Betz/ Kübler 2013: 92). Diese Masterarbeit könnte ein erster Schritt sein, diese Lücke zu füllen. Sie stößt damit auch in den Bereich der Zivilgesellschaftsforschung vor, der Schwerpunkt der Untersuchung soll deshalb auf den diversen Interaktionsmustern und Kooperationsformen liegen. Dazu werden Praktiken und Aktionsrepertoires der Interessengruppen ebenso herausgearbeitet, wie ihre inhaltlichen Positionen. Gleichzeitig werden auch die Ressourcen der einzelnen Akteure beleuchtet und zueinander in Beziehung gesetzt. Diese Masterarbeit kann insofern neue Erkenntnisse beitragen, als dass bisher eine strukturelle Analyse der Akteursebene in Verbindung mit der Prozessebene für den Bereich der Datenschutzpolitik in Deutschland noch nicht erarbeitet worden ist. Besonders ist hierbei, dass nicht allein rein zivilgesellschaftliche Gruppierungen in den Fokus genommen werden, sondern durch das *advocacy coalition framework* eine Kontrastierung verschiedener Gruppen und *stakeholder* vorgenommen werden kann.

3) Aufbau

Diese Arbeit gliedert sich in insgesamt sieben Kapitel. Im Anschluss an diese Einleitung folgt eine Einordnung der Thematik aus politischer und technologischer Perspektive. Dabei sollen die wichtigsten Entwicklungstendenzen skizziert und aktuelle Ereignisse der letzten Jahre thematisiert werden. Das dritte Kapitel widmet sich der Beschreibung und Rechtfertigung des Forschungsdesigns und der wissenschaftlichen Methode. Darüber hinaus werden die wichtigsten Begriffe definiert und damit für die wissenschaftliche Auseinandersetzung operationalisiert.

Den Kern dieser Arbeit bildet die Untersuchung zentraler Akteure und Akteursgruppen der Datenschutzpolitik. Abgeleitet aus der Verbindung zweier theoretischer Modelle, dem Ressourcenmobilisierungsansatz und dem *advocacy coalition framework*, werden im vierten Kapitel Kategorien entwickelt, anhand derer die Untersuchung durchgeführt werden soll. Das nächste Kapitel dringt in den Kern der Fragestellung vor und beinhaltet eine tiefergehende Analyse von zivilgesellschaftlichen, privatwirtschaftlichen, journalistischen und staatsnahen Akteuren der Daten(schutz)politik. Das sechste Kapitel schließlich gibt Antworten auf die Forschungsfrage und *clustert* die Akteure, um das Netzwerk herauszustellen, in dem sie sich in ihrer täglichen Arbeit bewegen. Ziel der Arbeit ist eine möglichst vollständige *Policy*-Analyse des nichtstaatlichen Sektors im Politikfeld der Datenschutzpolitik. Ein abschließendes Fazit fasst die Ergebnisse zusammen und zeigt Anknüpfungspunkte für die weitere wissenschaftliche Auseinandersetzung mit der Thematik auf.

4) Inklusive Sprache und Textgestaltung

Gerade in einem derart männlich dominierten Bereich wie Netzpolitik wird es unerlässlich sein, die Einbeziehung der Kategorie „Geschlecht“ auch sprachlich zu markieren und damit ausdrücklich andere als die zwei hegemonialen gender-Formen einbeziehen. Deshalb werde ich in dieser Masterarbeit nicht das generische Maskulinum nutzen, sondern - wo nötig - einen Unterstrich, die sog. Gender-gap, setzen, auf die die weibliche Endung –in als Suffix folgt. Konsequenterweise wird

diese Schreibung auch in Komposita verwendet, obwohl mir bewusst ist, dass es die Lesbarkeit des Textes ungünstig beeinflusst. Leider lässt die deutsche Schriftsprache jedoch keine eleganteren Lösungen zur Gewährleistung gender-inklusive Ausdrucksmöglichkeiten zu. Bei englischen Bezeichnungen jedoch werde ich konsequent die einzige Form nutzen, auch wenn sie in der deutschen Sprache mit dem weiblichen Suffix verknüpft werden, so z. B. bei User, (nicht User_in).

Der vorliegende Text steht vor der Herausforderung, englische Begriffe und den Verzicht von Großbuchstaben derart in den Lesefluss zu integrieren, als dass dieser nicht empfindlich gestört wird. Dies soll durch eine Kursiv- und Kleinschreibung dieser Begriffe gewährleistet werden, sofern diese allein stehen. Treten sie als Begriffspaar zusammen mit einem deutschen Substantiv auf, werden sie kursiv- und großgeschrieben, ein Bindestrich macht an dieser Stelle die Wortgrenzen deutlich.

Auch ist an dieser Stelle darauf hinzuweisen, dass die Zitation nach dem Autor-Jahr-Prinzip die Schwierigkeit birgt, Internetquellen korrekt in den Fließtext zu integrieren, da häufig die Schlüsselinformationen Autor_in und Jahr der Quelle nicht zu entnehmen waren. In diesen Fällen fehlt die entsprechende Information im Beleg, trotzdem ist darauf geachtet worden, die Quelle innerhalb des Textes derart zu chiffrieren, dass sie eindeutig und vollständig im Literaturverzeichnis identifizierbar ist.

II Relevanz und Entwicklungstendenzen

„Schutz vor Datenmacht – dahinter steckt die Überzeugung, dass informationelle Verhältnisse auch Machtbeziehungen sind und der Einzelne vor asymmetrischen Informationsbeziehungen geschützt werden muss“ (von Lewinski 2012: 23). Anhand dieses Zitates wird die Bedeutung des Politikfelds Datenschutz deutlich, denn im Zuge der Transformation von der Industrie- zur Informationsgesellschaft, wie sie zum Beispiel Castells, aber auch viele andere beschreiben, manifestieren sich Daten zu einem Machtmittel, das in der Lage ist, menschliche Beziehungen zu strukturieren und Hierarchien darüber auszubilden. Damit dies nicht willkürlich oder illegitim geschehen kann, gibt es eine Reihe von Mechanismen, welche die Mitglieder einer Gesellschaft vor übermäßiger Datenmacht schützen sollen. Diese Mechanismen sind jedoch über die Jahre hinweg Gegenstand politischer und gesellschaftlicher Diskurse und Veränderungsprozesse, darüber hinaus werden sie ebenfalls von technologischen Entwicklungen beeinflusst und geprägt. Im Folgenden werden die wichtigsten Entwicklungstendenzen der Daten(schutz)debatte skizziert, um deutlich zu machen, wie sich Konzeptionen, Vorstellungen, Werte und Möglichkeiten wandeln und daraus ein zutiefst dynamisches Politikfeld entsteht. Dafür werden zunächst die politischen und historischen Rahmenbedingungen erläutert, indem die wichtigsten Diskurse und Entscheidungsprozesse um den Datenschutz dargestellt werden. In einem zweiten Schritt sollen die technischen, in erster Linie netzbezogenen Aspekte betrachtet werden, die den Umgang mit Daten immer wieder verändern und damit den gesellschaftlichen Diskurs über Datenschutz oder auch Datenbefreiung qualitativ beeinflussen. In einem dritten Punkt werden schließlich die aktuellen Tendenzen des letzten Jahres skizziert, um die Relevanz und Bedeutung des Themas zu betonen und aufzuzeigen, dass der Umgang mit personenbezogenen Daten zunehmend gesellschaftlich relevant wird, er sich von einem Experten- zu einem Massendiskurs entwickelt hat und es auch immer noch tut.

1) Politischer Kontext

Die Bundesrepublik Deutschland hat bei der Datenschutzgesetzgebung eine weltweite Vorreiterrolle inne. Bereits 1977 wurde das erste Bundesdatenschutzgesetz verabschiedet. Als Pionier kann das Bundesland Hessen gelten, in dem das erste Datenschutzgesetz weltweit 1970 in Kraft trat und dessen Parlament 1971 bereits einen Datenschutzbeauftragten ernannte. Diese frühen Entwicklungen entstanden losgelöst von einem vorangegangenen gesellschaftlichen Diskurs und bezogen sich stärker auf Datensicherheit als auf den Schutz des Individuums vor Datenmacht (vgl. von Lewinski 2012: 29). Dies änderte sich jedoch in den 1970er Jahren: Mit der zunehmenden Computerisierung strebten Behörden verstärkt eine „Verwaltungsautomation“ (Berlinghoff 2013: 15) an, die zwar eine effiziente und arbeitserleichternde Bürokratie zum Ziel hatte, bei weiten Teilen der Bevölkerung jedoch die Angst vor dem Verlust der Privatsphäre und vor allgegenwärtiger Überwachung durch staatliche Institutionen schürte. Befeuert wurde diese Angst zusätzlich durch die immense Expansion der computergestützten Kriminalitätsbekämpfung, aber auch –prävention durch das BKA und die Einführung der Rasterfahndung. Bereits 1978 wurden die ersten illegalen Überwachungsaktionen öffentlich, die den Rücktritt des damaligen Bundesinnenministers Werner Maihofer (FDP) und des Bundesverteidigungsministers Georg Leber (SPD) zur Konsequenz hatten (vgl. ebd.: 18). Die von der Bundesregierung für 1984 geplante Volkszählung erregte bei vielen Menschen zusätzliches Misstrauen: Es formierte sich großer Protest, der nicht selten auf Analogien zu der in George Orwells Roman „1984“ beschriebenen Dystopie der totalen Überwachung zurückgriff (vgl. Berlinghoff 2013: 16-18) und schließlich in einer Vielzahl von Verfassungsbeschwerden mündete.

In diesem historischen Kontext entstand das sog. Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983, das unter Rückgriff auf das Persönlichkeitsrecht (Art. 2 Abs. 1 GG) in Verbindung mit dem Schutz der Menschenwürde (Art. 1 Abs. 1 GG) das Recht auf informationelle Selbstbestimmung formulierte und damit auf einen breiten Protest der Bevölkerung gegen eine allgemeine Volkszählung reagierte (vgl. von Lewinski 2012: 29). Das vom Verfassungsgericht entwickelte Grundrecht auf informationelle Selbstbestimmung sollte es Bürger_innen

ermöglichen, ihre Privatsphäre vor unrechtmäßigem Eingriff insofern zu schützen, als dass ihnen das Recht garantiert wird, selbst zu entscheiden, wem sie private Informationen anvertrauen und wem nicht. Darüber hinaus müssen verarbeitende Stellen sicherstellen, dass die Daten nur zu dem Zweck ausgewertet werden dürfen, zu dem sie auch erfasst worden sind. Ziel dieser Regelungen war es, eine Souveränität der Bürger_innen über ihre persönlichen Daten juristisch zu verankern, da davon auszugehen ist, dass Menschen in dem Bewusstsein von Überwachung ihr Verhalten verändern und dies das gesamte gesellschaftliche Zusammenleben beeinflusst. Diese „Anpassungs- und Veränderungsprozesse“ (vgl. Weidemann 2014: 6) schränken Individuen in ihrer autonomen Lebensführung ein und beschneiden damit elementare Freiheitsrechte. Die daraus resultierende, diskursive Veränderung des Konzeptes der Privatsphäre fasst Berlinghoff wie folgt zusammen:

„Die freie Kombinierbarkeit der Informationen führte zu einer Abkehr vom Modell der Privatsphäre hin zu einem breiteren Verständnis von Privatheit, das nicht eine bestimmte Information als privat und damit besonders schützenswert kennzeichnete, sondern grundsätzlich dem Prozess von Erhebung, Sammlung und Auswertung von Daten mit Misstrauen begegnet“ (Berlinghoff 2013: 19).

Auch die Europäische Union erkannte die Bedeutung des Datenschutzes für den Binnenmarkt, sodass 1995 eine europäische Datenschutzrichtlinie (Richtlinie 95/46/EG) verabschiedet worden ist, die zu einer Harmonisierung nationaler Gesetzgebungen führen und damit Rechtssicherheit für Unternehmen und Internetuser herstellen sollte (vgl. Roßnagel 2012: 331). Im Jahre 2000 fanden schließlich das Recht auf Privatsphäre (Art. 7) und der Schutz personenbezogener Daten (Art. 8) Eingang in die EU-Grundrechtecharta (vgl. Hustinx 2012: 324).

Den wohl gravierendsten Paradigmenwechsel innerhalb des Datenschutzdiskurses stellen die Terroranschläge vom 11. September 2001 dar, da sie die Sicherheitsarchitektur vieler Staaten grundsätzlich ins Wanken brachten. Eine Vielzahl neuer, staatlicher Überwachungsmethoden und -technologien konnten durch dieses *window of opportunity* implementiert werden. Gesetzliche Verschärfungen und neue Kompetenzen der Strafverfolgungsbehörden folgten bald, zunächst ohne dass sich Protest formierte oder die Frage nach der Legitimität dieser Maßnahmen in

weiten Bevölkerungsteilen gestellt wurde. Sofern es dem Kampf gegen den Terrorismus diene, wurde das Durchdringen des täglichen Lebens mittels Kontroll- und Überwachungsmaßnahmen toleriert. Zwar gingen die europäischen Länder bei der Ausweitung staatlicher Überwachung nicht so weit wie die USA mit ihrem PATRIOT Act von 2001 (vgl. Levi/ Wall 2004: 196), da die europäischen und nationalen Datenschutzgesetze dies nicht ohne weiteres ermöglichten, trotzdem waren die Folgen für nahezu alle Bürger_innen deutlich spürbar, da der Zugriff der US-amerikanischen Behörden auf persönliche Daten auch durch Unternehmen ermöglicht wurde, die Dependancen in anderen Staaten unterhalten (vgl. Betz/ Kübler 2013: 169). Levi und Wall nennen in diesem Zusammenhang zum einen Maßnahmen der „hard security“ wie z. B. den Schutz vor illegaler Nutzung staatlicher Strukturen für terroristische und kriminelle Zwecke. Auf der anderen Seite wird durch staatliche Überwachung eine „soft security“ angestrebt, also eine präventive Methode, die Sicherheitsgefährdungen erkennen soll, noch bevor sie ausgeübt werden (vgl. Levi, Wall 2004: 198-200). Diesem Ansatz liegt jedoch eine fundamentale Neuinterpretation der Vorstellung von einer Bevölkerung zugrunde: Wurde bisher immer die generelle Unschuldsvermutung als zentrales Prinzip der Rechtsstaatlichkeit verstanden, werden nun durch staatliche Überwachung nahezu alle Individuen einer Gesellschaft einem Generalverdacht ausgesetzt, den sie ihrerseits allein durch normkonformes Handeln beseitigen können, wobei selbst dann Nachteile zu befürchten sind, wenn den Überwachungsstellen Fehler unterlaufen oder falsche Interpretationen bestimmten Handelns zu falschen Ergebnissen führen. Zugunsten der Sicherheit, womit in dem Diskurs faktisch die Ausweitung der Methoden von Strafermittler_innen gemeint ist, wurden nach und nach bürgerliche Freiheitsrechte beschnitten und eingeschränkt. Levi und Wall stellen fest: „Of concern is that the combined effect has tipped the security/privacy balance in favour of security interests and away from considerations of individual privacy and existing privacy protections“ (ebd.: 203). Weitere Bedenken beziehen sich auf die Gewöhnung an Überwachung, das bedeutet auf die Einbindung in alltägliche Lebenspraktiken, sodass von „ideological normalization of surveillance“ (Fuchs, Boersma et. al. 2011: 11) nach 9/11 gesprochen werden kann.

2) Technologischer Kontext

Nicht allein politische Rahmenbedingungen prägen Diskurse und Debatten, auch neue technologische Entwicklungen und die daraus resultierenden Möglichkeiten können einen Handlungsdruck erzeugen, Regulierungen notwendig machen oder neue Aspekte beleuchten. Dies lässt sich am Beispiel des Internet mit der Verknüpfung der Datenschutzdebatte nahezu exemplarisch ablesen. Häufig wird für die Beschreibung der digitalen Datenverarbeitung ein 3-Phasen-Modell angelegt, welches ich auch im Folgenden nutzen möchte, um die daraus entstehenden Datenschutz Tendenzen aufzuzeigen. Dabei sei jedoch angemerkt, dass aufgrund des begrenzten Umfangs dieser Arbeit nicht die ganze Geschichte der Digitalisierung und des Internets beschrieben werden kann. Nichtsdestotrotz werden die wichtigsten Entwicklungslinien skizziert und unter dem Aspekt der Relevanz für Datenschutzfragen analysiert.

In seiner ersten frühen Phase, auch „Web 1.0“ genannt, diente das Internet den meisten Usern lediglich als Informations-, Einkaufs- oder Dienstleistungsquelle. Diese Phase zeichnet sich dadurch aus, dass der Konsum von Dienstleistungen und Produkten sowie die Suche nach bestimmten Informationen im Vordergrund stehen und diese Tätigkeiten eher individuell als kooperativ ausgestaltet sind. Die wenigsten Privatpersonen nutzten die Möglichkeiten, eigene Seiten zu betreiben oder sich interaktiv an Diskussionen zu beteiligen. Die Dotcom-Blase wird häufig als Wendepunkt ausgemacht, der zu vielen Innovationen und neuen Geschäftsideen im Netz führte, da offensichtlich wurde, dass die bisherigen Finanzierungskonzepte der Internetbranche nicht erfolgreich waren (vgl. z. B. O’Reilly 2005). Die neuen Dienste und Plattformen wurden zum Kernstück der zweiten Phase: das Web 2.0.

Der Unterschied dieser Phase zum Web 1.0 liegt vor allem in der Interaktivität und Produktivität begründet. User vernetzen sich, produzieren selbst Inhalte, diskutieren mit Anderen und tragen damit zu einer Diffusion der Themen und der Interaktionsformen bei. Dieser Trend wird durch soziale Netzwerke aufgegriffen und verstärkt. Plattformen, Wikis und Foren laden User explizit dazu ein, sich aktiv an der Produktion von Inhalten zu beteiligen, sie zu teilen, zu re-tweeten und zu remixen. In der Literatur wird in diesem Zusammenhang auch von *Producership* (vgl.

Baringhorst 2014: 103) gesprochen, also einem sog. Kofferwort aus Producing und Usage. Aus der Entwicklung neuer Ideen und unkonventioneller Aktivitäten können wiederum andere, neuartige Interaktionsformen und Inhalte entstehen, die ihrerseits dem Prozess der Aneignung und Weiterverarbeitung unterliegen. Dieser Trend wird durch die dezentrale Netzwerkstruktur des Internet ebenso verstärkt wie durch den kooperativen Charakter mit niedrigen Eintrittsschwellen, die eine Partizipation erleichtern und die Bereitschaft dazu erhöhen. Neben der reinen Informationsquelle dient das Internet nun der Selbstdarstellung, der Identitätsbildung, dem Aufbau und der Pflege sozialer Beziehungen und oft auch dem politischen Aktivismus, kurz: Es nimmt einen Dreh- und Angelpunkt im Leben vieler Menschen ein. Ihr Handeln ist nicht länger geprägt von „Eins-zu-n-Beziehungen“, sondern entwickelt sich zu dynamischen, kollaborativen „N-zu-n-Netzwerken“ (Behördenspiegel 2013: 1). Die Folge dieser Entwicklung liegt jedoch auf der Hand: Jede_r einzelne hinterlässt deutlich mehr digitale Spuren im Internet, die darüber hinaus deutlich detailliertere Aussagen über persönliche Vorlieben, Interessen, Beziehungen und Einstellungen zulassen. Gerade diese Informationen sind es, die für private Unternehmen, aber offensichtlich auch für staatliche Stellen relevant werden: Erstere n

utzen sie, um dadurch Gewinne zu erwirtschaften, Letztere um Bürger_innen zu überwachen und dadurch einschätzen bzw. kontrollieren zu können.

Die dritte Phase wird häufig als „Internet der Dinge“ beschrieben, was jedoch den Kern nicht wirklich trifft und eher wie eine irreführende Vereinfachung wirkt. Der Begriff *ubiquitous computing*, also allgegenwärtige Computer, scheint an dieser Stelle angemessener und ist auch im wissenschaftlichen Bereich durchaus verbreiteter. Gemeint ist damit die allgegenwärtige Rechenleistung und Vernetzung von Alltagsgegenständen. Die Entwicklung in Richtung *ubiquitous computing*

„erfasst alle Lebensbereiche und diese potenziell vollständig. In dieser Welt wachsen Körperlichkeit und Virtualität zusammen. Informationen aus der virtuellen Welt werden in der körperlichen Verfügbar, Informationen aus der realen Welt in die virtuelle integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es keinen Ausweg“ (Roßnagel 2006: 10).

So werden bereits in Autos, Heizungsanlagen, Armbanduhren etc. Computer eingebaut, die ihrerseits Nutzungsdaten speichern und gegebenenfalls auch an die Hersteller übermitteln, ohne dass sich die User dessen unbedingt bewusst sind. Das Ergebnis ist die nahezu vollständige Erfassung jeglicher menschlicher Tätigkeit, auch innerhalb privater Schutzräume. Es liegt auf der Hand, dass diese dritte Stufe die größten Herausforderungen an den Datenschutz und das Recht auf informationelle Selbstbestimmung birgt.

In diese Entwicklungstendenz fällt auch die Frage nach dem Umgang mit *Big Data*. Gemeint sind damit Datenvolumina, die so groß sind, dass die Verarbeitung und Auswertung dieser Daten eine technologische Herausforderung darstellt. Wurden vor einigen Jahren „relevante“ Datenmengen noch in Terrabyte gemessen, füllen Big Datasets heute zum Teil schon Petabytes, was eintausend Terrabyte entspricht (vgl. Magoulas, Lorica 2009: 2-3). Diese Datensätze können für wissenschaftliche, administrative oder kommerzielle Zwecke genutzt werden. Welche Auswirkungen dies für Individuen hat, hängt von der Art der Massendatenanalyse ab und kann nicht pauschalisiert werden.

An dieser Stelle ist anzumerken, dass es zwischen den oben dargelegten Stufen der Digitalisierung zwar deutliche Unterschiede gibt und eine Innovation im Laufe der letzten 20 Jahre festzustellen ist, jedoch kann an keiner Stelle von einer wirklichen Zäsur der Technologie gesprochen werden. Vielmehr sind es neue Nutzungsformen, die diese Entwicklung bedingen, ohne die alten vollständig abzulösen. Das Nutzungsrepertoire erweitert sich, während etablierte Methoden beibehalten werden. So nimmt z. B. das Verschicken und Empfangen von Emails seit Jahren einen zentralen Stellenwert in der individuellen Internetnutzung ein (vgl. Fuchs, Boersma et. al. 2011: 5). Auch die grundlegende Struktur des Internet (wie z. B. die Dezentralität, die Protokollformen) ist seit den 1990er Jahren von Kontinuität geprägt. Trotzdem lassen sich Tendenzen identifizieren, die in allen drei Phasen relevant waren und sich durch die gesamte Geschichte des Internets ziehen: So werden Rechenkapazitäten und dadurch auch Datenvolumina immer größer und kostengünstiger. Die digitale und unbegrenzte Speicherung ist für einen Großteil der kommerziellen Betreiber von Diensten insofern interessant, als dass sie wenig Ressourcen bindet und trotzdem sehr ertragreich sein kann, sobald diverse Daten mit-

einander verknüpft werden und sich daraus neue marketingrelevante Erkenntnisse ableiten lassen (vgl. Lüke 2012: 154-155).

3) Spezifische Einflussfaktoren

Im folgenden Unterkapitel werden die Besonderheiten der Datenschutz- und Netzpolitik aufgezeigt, um noch einmal die Dynamik des Feldes zu verdeutlichen und gleichzeitig den aktuellen Entwicklungen der letzten Jahre Rechnung zu tragen, die ihrerseits einen großen Einfluss auf das Politikfeld genommen haben.

a) Politikfeld im Mehrebenensystem

Netzpolitische Fragestellungen können niemals rein national reguliert werden. Gerade aufgrund der dezentralen Struktur des Internets und der grenzüberschreitenden Datenflüsse ist es unerlässlich, internationale Regelungen zu finden, um eine Kohärenz der diversen nationalen Politiken zu erreichen. Dies gilt auch für den Datenschutz und den Umgang von Unternehmen mit personenbezogenen Daten. So stellen Kurz und Rieger fest: „Schon allein die Frage, unter welcher Jurisdiktion welchen Landes die Daten gerade gehortet werden, ist schwer zu beantworten“ (Kurz/Rieger 2012: 83). Dies erschwert es nationalen Behörden natürlich auch, Datenschutzgesetze durchzusetzen, die in einem anderen Land weniger rigide formuliert sind. Da sehr viele der weltweit größten Netzunternehmen aus den USA kommen, wurde zwischen der EU und den USA das sog. Safe-Harbor-Abkommen beschlossen, welches ein Mindestmaß an Datenschutz auch innerhalb der Europäischen Union garantieren sollte. Diesem Abkommen liegt die Vorstellung zugrunde, dass sich die Konzepte von Datenschutz kulturell so stark unterscheiden, dass durch eine Sonderregelung eine „Überbrückung der Systemunterschiede“ (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit 2005) angestrebt werden soll. Diesen Systemunterschied fassen Fuchs et. al. treffend zusammen, indem sie schreiben:

„The US approach in privacy regulation relies on the free market and self-regulation by corporations. It makes some exceptions from the self-regulation

rule such as data held by financial institutions and data relating to children (Children's Online Privacy Protection Act 1998). It conceives privacy primarily as a commodity. The EU approach defines privacy as a fundamental right that needs to be protected by the state" (Fuchs et. al. 2012: 10).

Neben der vertikalen Politikverflechtung zwischen internationaler, europäischer, nationaler und föderaler Ebene unterliegt das Feld Netzpolitik auch horizontalen Fragmentierungen. So sind derzeit mehrere Bundesministerien für Internet und Digitalisierung verantwortlich. Auch Datenschutzthemen lassen sich nicht explizit einem Ressort zuordnen, da es Überschneidungen ebenso wie kollidierende Interessen innerhalb der derzeitigen Bundesregierung gibt. Während z. B. das Bundesinnenministerium nach wie vor an dem Vorhaben festhält, die Vorratsdatenspeicherung zu implementieren, sprach sich der Verbraucherschutz- und Justizminister Heiko Maas dagegen aus, einen neuen Anlauf für das Gesetz anzustreben (vgl. Wilkens 2014). Darüber hinaus fühlen sich sowohl das Bundesministerium für Wirtschaft und Energie, als auch das Bundesministerium für Verkehr und digitale Infrastruktur der netzpolitischen Regulierung verpflichtet, was mitunter zu Kompetenzstreitigkeit der Bundesregierung führte. Netzpolitik im Allgemeinen und Datenschutz im Besonderen können also als Querschnittsthemen betrachtet werden, die sich sowohl auf der horizontalen als auch auf der vertikalen Dimension im Mehrebenensystem auszeichnen.

b) Enthüllungsplattformen, Whistleblower und ihre Folgen

Die Enthüllungsplattform WikiLeaks hat die Welt der Informationen buchstäblich auf den Kopf gestellt. Seit 2006 werden auf der Plattform Dokumente veröffentlicht, die aus Perspektive staatlicher Stellen geheim gehalten werden sollten, jedoch von sog. *whistleblowern* weitergegeben und publiziert werden. Dabei werden geheime oder vertrauliche Dokumente vollständig ins Netz gestellt, sie unterliegen vorher keiner journalistischen Edition oder Interpretation, sodass die Leser_innen selbst die Aufgabe haben, Erkenntnisse aus den Dokumenten zu erlangen. Das Ziel dieser Plattform ist ein höheres Maß staatlicher Transparenz, eine gestärkte Informations-

freiheit der Bürger_innen und der Kampf gegen Korruption bei gleichzeitigem Schutz der Quellen.

Den ersten großen und international beachteten Coup landeten die Aktivist_innen mit der Veröffentlichung des sog. „Collateral murder“-Videos, das einen Kampfhubschrauberangriff auf irakische Zivilisten zeigt und damit in den USA eine Debatte über die Legitimität des Kriegs gegen den Terrorismus im Irak und in Afghanistan anheizte. Als im Sommer 2013 der NSA-Angestellte Edward Snowden viele Tausend als geheim klassifizierte Dokumente über die Überwachung durch die National Security Agency sowie vier weiterer Geheimdienste aus Kanada, Australien, Großbritannien und Neuseeland, der sog. *five eyes*, an Journalist_innen weitergab, führte dies zu einem radikalen Paradigmenwechsel in der Wahrnehmung breiter Bevölkerungsgruppen. Die Netzgemeinde war entsetzt darüber, dass ein großer Teil ihrer Lebenswelt, der gesamte digitale öffentliche Raum, Potenzial bietet für ein bisher unbekanntes Maß an Ausspähung durch Dritte. Neben der Arbeitsweise der Spionagesoftware Prism, Tempora und Xkeyscore konnte den Dokumenten auch die Zusammenarbeit US-amerikanischer Nachrichtendienste mit dem Bundesnachrichtendienst BND entnommen werden, welche als „Operation Eikonal“ bekannt wurde (vgl. z.B. Prantl 2014). Auch gab es laut der veröffentlichten Quellen eine enge Kooperation der Geheimdienste und Ermittlungsbehörden mit großen datenverarbeitenden Firmen und Telekommunikationsanbietern. Bis heute wird die politische Aufklärung durch die Bundesregierungen verzögert. Ob die Informationen, die aus den Geheimdienstunterlagen hervorgehen, umfassend genug sind, um die Mechanismen und Maßnahmen dieser umfassenden Überwachungsmaßnahmen wirklich aufzuklären, ist bis heute nicht absehbar.

Die oben skizzierten Entwicklungen führten schließlich auch dazu, dass nach und nach ein Datenschutzmarkt entstanden ist, auf dem mit Gütern gehandelt wird, die das Bedürfnis nach Sicherheit des privaten Raumes und der persönlichen Kommunikation befriedigen sollen. Auf der Nutzungsebene erschien in den letzten Jahren eine Vielzahl an Literatur über den Umgang mit personenbezogenen Daten und auch im Bereich der Aus- und Weiterbildung lässt sich eine Tendenz erkennen, in der sowohl Angebot als auch Nachfrage steigen. Einige Projekte zur Sensibilisierung für die Gefahren der unkontrollierten Veröffentlichung privater Informationen und

zur medienpädagogischen Auseinandersetzung mit diesem Thema setzen schon früh an und beginnen, auch Einzug in die Schulen zu halten.

Gleichzeitig nutzen immer mehr Menschen Verschlüsselungstechnologien, um ihre Kommunikation vor dem Zugriff durch Dritte zu schützen. Viele dieser sog. Privacy Enhancing Technologies (PET) bestehen als Freie Software (Open Source), die kostenlos heruntergeladen werden kann und deren Quellcode offen ist, sodass alle Menschen kooperativ daran arbeiten können, die Software zu verbessern. Die Nutzungszahlen des Tor-Netzwerkes, eines Programms zur Verschleierung der Datenspuren im Netz, sind seit den Enthüllungen Snowdens rapide angestiegen, bevor sie kurz darauf wieder langsam sanken. Dennoch bleiben sie bis heute konstant auf einem höheren Niveau als vor dem August 2013. Auch die Anzahl der Server, die für das Netzwerk zur Verfügung gestellt werden, steigen kontinuierlich an (vgl. Tor Project 2014). User aus Deutschland bilden mit 8,89% aller Tor-Nutzer_innen die zweitgrößte Gruppe nach den USA. Auch andere Verschlüsselungstechnologien werden verstärkt nachgefragt, die Nutzungszahlen für die E-Mail Verschlüsselung über OpenPGP (Pretty Good Privacy) sind seit Sommer 2013 stärker gestiegen als in den Monaten davor (vgl. SKS Keyserver 2014). In nahezu allen größeren Städten bundesweit finden regelmäßig sog. Kryptoparties statt. Dabei handelt es sich um Veranstaltungen, bei denen Verschlüsselungskompetenzen vermittelt und der sichere Umgang mit PET geübt werden sollen, um damit die Hemmschwelle zu senken und die Angst vor einer möglichen technischen Überforderung abzubauen. Für viele Aktivist_innen der Datenschutzpolitik gibt es keine Alternative mehr zur Codierung der digitalen Kommunikation.

III Methode

1) Forschungsdesign

Als Untersuchungsform für diese Masterarbeit wird vornehmlich eine qualitative Methode gewählt, die sich vor allem auf die Interpretation von Veröffentlichungen stützt, da „die Stärke qualitativer Methoden im Verstehen subjektiver Relevanzsysteme und Handlungsstrategien sozialer Akteure liegt“ (Behrens 2003: 227) und damit für die Beantwortung der Forschungsfrage am ehesten geeignet ist. Eine qualitative Methodenauswahl erlaubt eine deskriptive Herangehensweise, bei der die relevantesten Akteure sowie deren Einflussmöglichkeiten im politischen Prozess erkannt und benannt werden, denn es „ist ein zentrales Charakteristikum moderner Politikforschung, dass bei Erklärungen von Politiken heute an konkreten, empirisch identifizierbaren Handlungseinheiten und ihren spezifischen Interaktionsformen angesetzt werden muss“ (Schneider 2003: 107). Dazu eignet es sich am besten, führende Akteure aus den Bereichen Zivilgesellschaft, Privatwirtschaft, staatsnahe Organisationen und Onlinejournalismus auszuwählen, da diese Akteure unmittelbar durch politische Entscheidungen beeinflusst werden und diesbezüglich die größten Anreize haben, sich für ihre Ziele einzusetzen. Gleichzeitig muss an dieser Stelle jedoch darauf hingewiesen werden, dass die Kategorisierung dieser Akteure lediglich operationalen Zwecken dient und diese Unterscheidung nicht immer zweifelsfrei empirisch zutreffen muss. Schon Betz und Kübler merkten in diesem Zusammenhang an: „Vielmehr sind die Grenzen zwischen bürgerschaftlichem Engagement, der Vertretung wirtschaftlicher Interessen im weiteren Sinne und politischer Einflussnahme in diesem Feld äußerst fließend“ (Betz/ Kübler 2013: 91). Analytisch wird ein politischer Teilbereich, Datenschutz und die Verwertung personenbezogener Daten, als Einzelfalluntersuchung betrachtet. Obwohl dieses Politikfeld – wie oben bereits geschildert – als fragmentiert gilt und von einer Politikverflechtung der internationalen, der europäischen und der nationalstaatlichen Ebene geprägt ist, agieren die Akteure in erster Linie auf nationalstaatlicher Ebene, sodass eine Fokussierung auf bundesdeutsche Akteure auch aufgrund des begrenzten Umfangs dieser Arbeit als gerechtfertigt erachtet wird. Obwohl der theo-

retische Rahmen der *advocacy coalition* einem empirisch-analytischem Anspruch folgt, wird dieses Forschungsprojekt eine explizit normative Komponente enthalten, die die Bedeutung der Privatsphäre sowie deren Schutz vor kommerziellen oder staatlichen Bedrohungen betont und zu einer kritischen wissenschaftlichen Auseinandersetzung mit den politischen und soziologischen Dimensionen der massenhaften Verletzungen der digitalen Grundrechte beitragen soll.

Eine Schwäche des qualitativ ausgerichteten Forschungsdesigns ist womöglich, dass es auf die Interpretation und Auslegung der Ergebnisse sowie deren subjektiver Einordnung angewiesen ist. Somit widerspricht es auf den ersten Blick den postulierten wissenschaftlichen Grundsätze der Objektivität und Reliabilität, jedoch bin ich der Auffassung, dass es zum einen DIE absolute Objektivität nicht geben kann und zum anderen zwischenmenschliches Handeln, welches Grundlage der Politikfeldanalyse ist, stets sozial konstruiert ist und auf subjektive Kommunikation beruht. Unter dem Postulat der Transparenz und Nachvollziehbarkeit wird eine individuelle Interpretation in diesem Zusammenhang eher als Chance begriffen denn als unwissenschaftlicher Makel.

2) Operationalisierung der Grundbegriffe

Im Folgenden werden zentrale Begriffe im Hinblick auf die ihnen zugrunde gelegten Konzepte erläutert, wodurch Ambiguitäten vermieden und eine Operationalisierung dieser Begriffe angestrebt werden sollen.

Zunächst sollte geklärt werden, welche Entitäten unter die Bezeichnung „personenbezogene Daten“ fallen und warum diese Unterscheidung im Gegensatz zu öffentlichen Daten wichtig ist. So verstehen Betz und Kübler unter personenbezogenen Daten „praktisch jede Information, die mit einer natürlichen Person in Verbindung gebracht werden kann. Als persönliche Merkmale zählen etwa Identifikationsmerkmale, äußere Merkmale, aber auch Meinungen, als sachliche werden Beziehungen zu Dritten und zur Umwelt (z. B. Besitz, Vertragsbeziehungen) erachtet“ (Betz/Kübler 2013: 162). Mit dieser Begriffsbestimmung wird eine weite Definition angelegt, indem sie alle Informationen, die Rückschlüsse auf die Identität eines Men-

schen erlauben, berücksichtigt. Da alle diese Informationen für kommerzielle Zwecke oder für den Zweck der Überwachung durch staatliche Geheimdienste oder Ermittlungsbehörden genutzt werden können, können sie auch potenziell missbraucht werden und genießen deswegen einen besonderen Schutz. Öffentliche Daten hingegen sind Informationen, die keinerlei Rückschlüsse auf individuelle Merkmale von Einzelpersonen zulassen, sodass auf diese Merkmale begründete Selektionsmechanismen nicht greifen können.

Bei der Auswahl der Akteure wird in dieser Arbeit der Fokus auf nichtstaatliche Gruppen gelegt. Durch diese Verengung des Akteurskreises kann Datenschutzpolitik als Form von Partizipation aus einer *Bottom-Up*-Perspektive untersucht werden. Darunter werden all jene Beteiligungsformen verstanden, „die Bürger freiwillig, individuell und/oder kollektiv im Verbund mit anderen unternehmen, um polit. Entscheidungen direkt oder indirekt zu ihren Gunsten zu beeinflussen“ (Schultze 2008: 398). Es wird davon ausgegangen, dass Menschen ihre Interessen gegenüber einem Staat vertreten und diese an staatliche Akteure und andere Bürger_innen herantragen. Aufgrund der Neukonfiguration bestehender Machtverhältnisse (vgl. Voss 2014: 18), die einer Partizipation ständig inhärent ist, verdient dieser Prozess besonderes wissenschaftliches Interesse. Da aggregierte Akteursformen im Zentrum dieser Arbeit stehen, wird weniger auf individuelle und persönliche Partizipation von Menschen eingegangen werden. Darüber hinaus wird das Spektrum der Untersuchungsgegenstände erweitert, indem nicht nur zivilgesellschaftliche, sondern auch andere nichtstaatliche Akteure in ihren Aktions- und Interaktionsformen untersucht werden, um damit ein vollständiges Bild politischer Prozesse zu generieren und Interdependenzen aufzuzeigen.

3) Datenmaterial und Auswahl der Akteure

Neben wissenschaftlichen Arbeiten über relevante Organisationen oder das Politikfeld Internet und Datenschutz dienen vor allem die Veröffentlichungen der jeweiligen Akteure als Materialgrundlage dieser Forschungsarbeit. Vor allem Protokolle, Aufzeichnungen und Publikationen über Tagungen, Plenarsitzungen sowie Treffen

mit Parteigremien oder Ministeriumsangehörigen können Aufschluss darüber geben, inwieweit die Akteursgruppe in den Meinungsbildungsprozess eingebunden wird. Diese Informationen sind in erster Linie online verfügbar. Gleichzeitig ist die netzpolitische Aktivist_innenszene geprägt von einer Multimedialität, sodass eine Einschränkung allein auf Textmaterial unzureichend ist. Stattdessen werden ebenso Podcasts, Mitschnitte von Vorträgen, Vlogs (Videoblogs) und Reportagen in die Untersuchung einbezogen werden, um ein möglichst vollständiges Bild der Akteure zu zeichnen. Neben Eigenveröffentlichungen und journalistischen Texten können Informationen auch in unkonventionellen Bereichen wie sozialen Netzwerken, Blogs oder Wiki-Einträgen zu finden sein, dementsprechend werden auch diese Kanäle einbezogen, um Informationen und Stellungnahmen der Gruppierung zu erhalten. Vor allem wird es von Bedeutung sein, herauszufinden, wie groß die Überschneidungen in den *belief systems* der jeweiligen Akteure sein müssen, um eine Kooperation zu ermöglichen. Die Untersuchung dieser Kooperationen mit anderen Organisationen erlaubt es, nicht nur die Selbstwahrnehmung der Akteure wiederzugeben, sondern ebenfalls zu untersuchen, wie sie sich bei Interaktionen mit Dritten positionieren, welche Themen besondere Priorität genießen, wie die *belief systems* strukturiert sind und mit welchen Mitteln die Ziele verfolgt werden. Diese Daten werden schließlich zusammengefasst und dann für die jeweiligen Organisationen zueinander in Beziehung gesetzt. Dabei soll das Augenmerk auf wiederkehrende Positionierungen, Narrative und Symboliken gelegt werden. Keller begründet ein derartiges Vorgehen wie folgt:

„In modernen Gesellschaften sind soziale Akteure in vielfacher Weise in diskursiv strukturierte symbolische Kämpfe über Realitätsdefinitionen eingebunden [...]. Dabei geht es um Bestimmungen dessen, was faktisch der Fall ist, und um politische, moralische, ästhetische Maßstäbe der Bewertung. Die beteiligten Akteure nutzen symbolisch-kulturelle Mittel, um ihren Erzählungen Gehör zu verschaffen“ (Keller 2011: 66).

Für die Auswahl der jeweiligen Akteure wurde eine Verbindung zwischen dem *Most-Different-Ansatz* und dem *Most-Similar-Ansatz* genutzt (vgl. Behrens 2003: 213). Konkret bedeutet das, dass innerhalb der Akteursgruppen diejenigen Akteure ausgesucht wurden, die sich in ihren inhaltlichen Positionen kontrovers gegenüber-

stehen oder ergänzen, nicht jedoch zu stark überschneiden. Auch wurde eine organisatorische Diversität angestrebt. Diese Methode hat den Vorteil, dass ein breites Spektrum an Akteuren abgebildet werden kann. Darüber hinaus soll gewährleistet werden, dass diametrale Interessen akzentuiert und gegeneinander gelesen werden können. Um jedoch eine Vergleichbarkeit und valide Aussagen über bestimmte Akteurstypen treffen zu können, ist es auch wichtig, die Relevanz der Akteure als Kriterium für die Auswahl heranzuziehen. Deswegen sind vor allem Organisationen untersucht worden, die einen faktischen Einfluss auf die Datenschutzpolitik haben, weil sie entweder den Diskurs maßgeblich mitprägen, viele Mitglieder bzw. Aktivist_innen mobilisieren können, starke mediale Aufmerksamkeit genießen oder einen privilegierten Zugang zu den politischen Entscheidungsprozessen für sich beanspruchen können. Diese Verschränkung der beiden Ansätze macht jedoch eines deutlich: Die Liste der Akteure muss zwangsläufig unvollständig und lückenhaft sein, gleichzeitig ist es jedoch nicht der Anspruch dieses Forschungsbeitrages, ein umfassendes Bild der organisierten netzpolitischen Bewegung zu zeichnen.

.

IV Theoretischer Rahmen

Den theoretischen Rahmen dieser Arbeit bildet die Verbindung von zwei durchaus relevanten Konzepten der Policyanalyse und der *Social-Movement*-Forschung, die eine tiefgreifende und substantielle Untersuchung der relevanten, organisierten und nichtstaatlichen Akteure ermöglicht und dadurch das Gerüst für die zu analysierenden Kategorien bildet. Dafür werden die wichtigsten Begriffe sowie deren Zusammenhänge in diesem Kapitel dargestellt und eine schlüssige Synthese dieser Ansätze angestrebt.

1) Ressourcenmobilisierungsansatz

Die Ressourcenmobilisierungstheorie (im Folgenden RMT) wurde in den 1970er Jahren entwickelt und als Ablehnung bestehender soziologischer Erklärungsansätze zu sozialen Bewegungen formuliert. Während die meisten Sozialwissenschaftler_innen bis dato davon ausgingen, soziale Bewegungen entstünden aus irrationalen und emotionalen Beweggründen und allein aus Protest gegen bestehende Verhältnisse, wurde diese *Collective-Behaviour*-Perspektive von den Entwicklern des RMT abgelehnt. Anstatt von Anomalien innerhalb des politischen Systems auszugehen, die an lose ideologische Konzepte gebunden waren (vgl. McCarthy, Zald 1977: 1214), versuchten sie, die strategischen und taktischen Aktionsmuster herauszuarbeiten, die für eine Analyse sozialer Bewegungen unerlässlich schienen. Als Begründer dieses Ansatzes gelten John McCarthy und Mayer N. Zald, die die Bedeutung von Rationalität für Soziale Bewegungen und deren inhärente Organisationen anhand der Sozialen Bewegungen der USA in den 1960er und 1970er Jahren herausarbeiteten. Aufgrund der starken ökonomischen Ausrichtung und der Unterwerfung der handelnden Akteure unter ein rigoroses *Rational-Choice*-Paradigma sind sie häufig kritisiert worden. Dass Akteure zwar tendenziell rational und strategisch handeln, bedeutet nicht, dass sie ihre Aktionen einer permanenten Abwägung von Kosten und Nutzen unterziehen, zumal in den wenigsten Fällen wirklich alle Konsequenzen des eigenen Handelns überblickt werden können. Aus diesem Grund wird in dieser Arbeit ein alternativer Zugang zur

RMT bevorzugt, der eine politische und somit auch soziale Dimension einbezieht und dadurch der Problematik aus dem Weg geht, aktivistisches Handeln aus allein marktlogischer Perspektive zu betrachten. Dieser alternative Zugang wird dadurch gewährleistet, dass McCarthy und Zald zwar den Ausgangspunkt für den theoretischen Rahmen bilden, der Blickwinkel jedoch durch die Schriften Charles Tillys erweitert und dadurch an die Fragestellung dieser Masterarbeit angepasst wird.

a) Klassische Ressourcenmobilisierungstheorie

McCarthy und Zald definieren soziale Bewegungen als „a set of opinions and beliefs in a population which represents preferences for changing some elements of the social structure and/or reward distribution of a society“ (McCarthy, Zald 1977: 1217f.). Demnach liegen ihr lediglich “preference structures directed toward social change” (ebd.: 1218) zugrunde, sodass in diesem Zusammenhang von einer Interessenaggregation gesprochen werden kann. Um soziale Veränderungen in ihrem Sinne herbeiführen zu können, brauchen Akteure demnach Ressourcen, die mobilisiert werden müssen. Strategische und taktische Handlungen innerhalb der sozialen Bewegungen hängen dabei im großen Maße von den Gegebenheiten der Bewegungsumwelt ab. McCarthy und Zald treffen dazu folgende Klassifizierungen: Ein Teil der sozialen Bewegung ist in *social movement organizations* (SMO) organisiert, während der andere Teil keiner institutionalisierten Struktur angehört. Alle SMO innerhalb einer Bewegung bilden die *social movement industry* (SMI), die ihrerseits in dem *social movement sector* (SMS) aufgeht, der jedoch auch die Industrien anderer Bewegungen umfasst. Je nachdem, wie die Konfigurationen innerhalb dieser jeweiligen Strukturen ausgestaltet sind, reagieren SMOs rational und taktisch auf diese und koordinieren ihre Strategien zur Ressourcenmobilisierung anhand ihrer Position im *Social-Movement-Gefüge*. Dieser Vorstellung liegt zugrunde, dass es in Gesellschaften eine Nachfrage nach Interessenvertretung gibt und SMIs ein Angebot dafür liefern (ebd.: 1216). Politisches Handeln wird dadurch zu einem Produkt (ebd.: 1229), das von Anhänger_innen einer sozialen Bewegung konsumiert werden

kann. Darüber hinaus werden Bewegungsorganisationen gleichgesetzt mit Unternehmen, die gewinnmaximierend agieren.

Wie oben bereits angedeutet, gehen McCarthy und Zald davon aus, dass unterschiedliche Konfigurationen, Organisationsformen, Ressourcenverteilungen und Positionen innerhalb des SMS Einfluss darauf haben, wie sich SMOs verhalten und welche Strategien sie anwenden, um ihren Ressourcenpool zu erhöhen. Diese Grundannahmen sind für die Untersuchung der SMI Datenschutzpolitik nicht besonders aufschlussreich, da daraus keine Kategorien entwickelt werden können, einzelne Akteure zu untersuchen, ohne die vollständige Soziale Bewegung samt all ihrer darin eingebundenen Organisationen zu untersuchen. Alternativ sollte deshalb ein vollständigeres Konzept herangezogen werden, das Ressourcenmobilisierung als eine wichtige Aufgabe von Akteuren versteht, jedoch eine differenziertere Sicht auf die Ableitung strategischer Handlungsmuster vorschlägt. Ein solches Konzept wurde von Charles Tilly formuliert, der Mobilisierung als eine Komponente unter vielen versteht, die Einfluss auf die Aktion, Reaktion und Interaktion von Akteuren hat. Im Folgenden wird Tillys Konzept herangezogen, um einen Teil des theoretischen Rahmens dieser Arbeit zu bilden.

b) Mobilisierung und kollektive Aktion

Tilly entwickelt seinen Ansatz deutlich politischer als McCarthy und Zald. Er geht einen Schritt weiter und verwendet den Begriff der *Gruppe*, wodurch eine Personalisierung der Akteure möglich wird, wobei sich dieser Begriff gleichzeitig von dem anonymen Verständnis von „Interessenaggregation“ abgrenzt. Darüber hinaus betont er die Bedeutung von Überzeugungen gegenüber bloßen Präferenzen: „By a social movement we often mean a group of people identified by their attachment to some particular set of beliefs“ (Tilly 1978: 9). Er bezieht sich weniger auf die strukturelle Ebene von sozialen Bewegungen als vielmehr auf die Handlungsebene, indem er die kollektiven Handlungen von Gruppen untersucht und dabei konstatiert: „Collective action is about power and politics; it inevitably raises questions of right or wrong, justice and injustice, hope and hopelessness“ (ebd.: 5). Damit stellt Tilly fest: Aktivistische Handlungen sind nicht lediglich an der

Mobilisierung von Ressourcen ausgerichtet, sie sind in ihrem Kern zutiefst politisch und verändern oder bezweifeln Machtkonstellationen, sie fordern bestehende Verhältnisse heraus und finden sich in ein Netz aus Interaktionen ein.

Als Komponenten kollektiver Aktionen nennt Tilly (1) *interests*, (2) *organization*, (3) *mobilization*, (4) *opportunity* und (5) schließlich die *collective action* selbst (ebd.: 56). Erst das Zusammenspiel dieser fünf Komponenten macht es möglich, das Handeln von Akteuren nachzuvollziehen und rational zu erklären. Hier wird bereits deutlich, dass die Mobilisierung von Ressourcen als ein Baustein von vielen zum wissenschaftlichen Verständnis von sozialen Bewegungen beiträgt. Folgt man Tilly, müssten diese fünf Bestandteile einer sozialen Bewegung untersucht werden, damit diese substantiell erforscht werden kann. Für die Forschungsfrage wird es nicht notwendig sein, jede einzelne Komponente und ihre Ausprägungen sowie die daraus folgenden Schlussfolgerungen in der gleichen Intensität nachzuzeichnen, wie sie bei Tilly entwickelt werden. Zwar werden die Komponenten erläutert, ihr kompliziertes und ausgereiftes Zusammenspiel, auf das Tilly hinweist, kann an dieser Stelle jedoch nicht lückenlos und in seiner Gänze dargestellt werden.

Die erste Komponente sind **Interessen**. Sie werden von Tilly definiert als „the gains and losses resulting from a group’s interaction with other groups“ (ebd.: 7). Es wird deutlich, dass die Untersuchung von Interessen Forscher_innen vor große Herausforderungen stellt. Tilly zeigt in diesem Kontext die folgenden zwei Dilemmata auf: 1. Reicht es aus, allein die Äußerungen der Gruppe selbst zu analysieren oder muss ihre Position innerhalb des sozialen Systems (nach Marx innerhalb des Produktionssystems) ebenfalls Teil einer Untersuchung sein (vgl. ebd.: 60f.)? 2. Wie wird mit Aussagen von Individuen umgegangen, um Aufschluss darüber zu erlangen, ob diese Position eine persönliche Meinungsäußerung oder den Standpunkt der ganzen Gruppe darstellt? Was, wenn Standpunkte divergieren (vgl. ebd.: 61f.)? Als Lösung bietet Tilly eine Unterscheidung zwischen kurzfristiger und langfristiger Betrachtung an: Die Position innerhalb des sozialen Systems gibt Aufschluss über langfristige Interessen, während direkte Äußerungen kurzfristige Positionsbestimmungen darstellen können (vgl. ebd.: 61). Gibt es divergierende Positionen zwischen einzelnen Mitgliedern einer Gruppe und der Gruppe als Ganzes, soll dies einfach als Variable betrachtet werden, die auf Dauer die Kosten für kollektive Aktionen erhöht oder

einer kollektiven Anpassung vorangeht (vgl. ebd.: 62). Im folgenden Unterkapitel wird ein alternativer Zugang zu dieser Kategorie vorgeschlagen, der diese Dilemmata umgeht.

Organisation wird wie folgt definiert: „The organization which concerns us most is that aspect of a group’s structure which most directly affects it’s capacity to act on its interests” (ebd.: 7). Die Organisation hat also unmittelbare Auswirkungen auf die *Fähigkeiten* einer Gruppe, sie begrenzt oder erweitert ihre Einflussmöglichkeiten. Zwar lässt sich der Organisationsgrad nicht quantitativ messen, jedoch formuliert Tilly Variablen, die diesbezüglich untersucht werden können: Identität und Netzwerke. „The more extensive its common identity and internal networks, the more organized the group“ (ebd.: 63). Es wird deutlich, dass hier die Organisation einer Gruppe maßgeblich davon abhängt, inwieweit Individuen darin involviert sind. Die zentralen Fragestellungen sind an dieser Stelle: Wie stark können sich die Mitglieder einer Gruppe mit ihr identifizieren und wie ausgeprägt sind persönliche Netzwerke? Bemerkenswerterweise macht Tilly keine Angaben zur Formalität von Gruppen und deren Auswirkungen auf die oben genannten Variablen Identität und Netzwerke. Die Art und Weise, die Form, in der sich eine Gruppe nach außen als solche präsentiert, kann nicht nachrangig sein und wird im fünften Kapitel mit einem besonderen Augenmerk untersucht.

Für diese Arbeit ist die Kategorie der **Mobilisierung** eine besonders wichtige: Wie schaffen es Gruppen, im politischen Raum ihre Interessen durchzusetzen? Welche Ressourcen müssen sie dafür akquirieren? Wie gelingt ihnen das? Wovon ist die Mobilisierung abhängig? Aufschlussreich ist in diesem Zusammenhang Tillys Definition von Mobilisierung: „The word ‘mobilization’ conveniently identifies the process by which a group goes from being a passive collection of individuals to an active participant in public life” (ebd.: 69). Anders als McCarthy und Zald und in Anlehnung an die klassischen Produktionsfaktoren aus den Wirtschaftswissenschaften nennt er vier Formen von Ressourcen, die gebraucht werden, um mobilisieren zu können: Arbeit, Kapital, Land und technische Expertise, jeweils gemessen an deren Marktwert. Ob es schließlich jedoch wirklich zur Mobilisierung, also zur Akkumulation dieser Ressourcen kommt, hängt davon ab, inwiefern Mitglieder einer Gruppe bereit sind, diese auch wirklich zur Verfügung zu stellen,

wenn sie gebraucht werden. Hier wird die starke Interdependenz zwischen den jeweiligen Kategorien deutlich, denn um beurteilen zu können, wie hoch die Bereitschaft ist, der Organisation Ressourcen zur Verfügung zu stellen, hängt vom Identifikationsgrad, oder nach Tilly, von der Loyalität und Solidarität innerhalb der Gruppe ab (ebd.: 69f.). Diese Faktoren sind von außen schwer zu beobachten, eine quantitative oder qualitative Messung ist schier unmöglich.

Darüber hinaus lassen sich drei Arten von Mobilisierung unterscheiden: Defensive, offensive und vorbereitende. Defensive Mobilisierung dient dazu, Ressourcen unter die Kontrolle der Gruppe zu bekommen, um Gefahren durch einen Feind abzuwehren und dadurch die Gruppe und deren Möglichkeiten der Interessendurchsetzung vor Schaden zu bewahren. Dem gegenüber steht die offensive Mobilisierung, in dessen Zentrum sich Ressourcenakkumulation für die Nutzung von Handlungspotenzialen und –möglichkeiten befindet. Hier tun sich Gelegenheiten auf, die im Sinne der Gruppe gestaltet werden sollen und dadurch deren Einfluss erhöhen könnten. Die dritte Form der Mobilisierung, die vorbereitende Mobilisierung lässt sich zwischen den oben genannten positionieren, allerdings an einer anderen Position auf der Zeitachse: In Erwartung einer neuen Situation versucht die Gruppe, an Ressourcen zu gelangen um entweder neue Gelegenheiten nutzen zu können oder aber erwartete Gefahren abzuwehren. Zukunftsprognosen sind in diesem Fall ein wichtiger Bestandteil der Bemühungen um die Kontrolle über Ressourcen und dementsprechend ein riskanter Bestandteil dessen (ebd.: 73ff.).

Durch den Begriff der *collective action* begibt Tilly sich auf die Handlungsebene. Demnach handeln Gruppen zusammen, um ihre Interessen zu verfolgen und gemeinsame Ziele („*collective goods*“) zu erreichen. Die Bewertung dieser Ziele hängt natürlich von der Gruppe und ihren Interessen ab (ebd.: 86), es handelt sich hier also nicht um messbare Werte oder reale Güter, sondern um relationale *outcomes*, deren Wert sowohl innerhalb als auch außerhalb der Gruppe individuell variieren kann. Dementsprechend ist eine Untersuchung der Handlungen lediglich gemessen an dem Ergebnis unzureichend. Tilly schlägt vielmehr vor, drei Variablen einzubeziehen, um die Aktionen zu analysieren: Die Dauer der Aktion, ihre Größe (im Sinne einer Reichweite) und ihre Häufigkeit. Alle drei Variablen weisen analytische Fallstricke auf, da auch sie nicht ohne weiteres quantifizierbar sind: Ab wann gehören

mehrere kleine Aktionen verteilt über einen längeren Zeitraum zusammen? Können Dauer und Größe einfach addiert werden? Es bietet sich an dieser Stelle an, eine qualitative Komponente einzubeziehen, die Aktionssequenzen und –Zusammenhänge offenlegt und dadurch die Handlungen in einen breiteren Kontext einordnet. Das Konzept der *opportunities*, also der Möglichkeiten, nimmt die Gesamtheit der handelnden Akteure in den Fokus. Die erste Dimension nennt er *repression/facilitation* und meint damit grundsätzlich die Akzeptanz des Staatsapparates gegenüber einer Gruppe. Demnach sind all jene Interaktionsformen, die die Kosten der Mobilisierung und dadurch des kollektiven Handelns senken, förderlich für die Gruppe. Als Repression hingegen gelten Interaktionen, die das Handeln der Gruppe erschweren oder gar unmöglich machen (vgl. ebd.: 100). Während diese erste Dimension von staatlicher Seite ausgeht, wird in der zweiten Dimension, *power*, die Interaktion zwischen Staat, Gruppe und anderen Gruppen (vgl. ebd.: 115) betont: Welche Position hat eine Gruppe innerhalb eines Gefüges? Wie viel Einfluss kann sie darin nehmen? Diese beiden Dimensionen beziehen sich vor allem auf die Gegenwart. Die dritte Dimension schließlich erweitert die Perspektive auf zukünftige Entwicklungen (vgl. ebd.: 133). Welche Veränderungen innerhalb der oben genannten Gefüge sind zu erwarten, mit welcher Wahrscheinlichkeit treten sie ein und was wären die Folgen? Die Beantwortung dieser Frage hängt schließlich mit der Mobilisierungsstrategie und nicht zuletzt mit der Ausgestaltung möglicher kollektiver Handlungen zusammen.

Tillys Ansatz, der die Ressourcenmobilisierung als eine Komponente von vielen versteht, ermöglicht es, Untersuchungskategorien zu entwickeln und auf bestimmte Variablen zu untersuchen. Und doch gibt es eine Reihe von Perspektiven, die davon nicht betroffen werden. Diese betreffen vor allem die Interaktionen mit anderen Gruppen. Dafür wird ein anderer wichtiger Ansatz der *Policy*-Analyse eingeführt.

2) Advocacy Coalition Framework

Paul A. Sabatier veröffentlichte 1988 zum ersten Mal einen konzeptionellen Rahmen, der multikausale Erklärungsansätze für langfristige Veränderungen von *policies* geben konnte: Das *advocacy coalition framework* (AFC). Dieses Konzept ist

aus mehreren Gründen besonders geeignet für diese Untersuchung, da es Voraussetzungen definiert, nach denen politisches Handeln der Akteure untersucht werden kann. Darüber hinaus erlaubt es eine Einbeziehung politischer Überzeugungen und liefert Begründungen, warum politische Akteure sich entsprechend ihrer Position innerhalb einer (potenziellen) Koalition verhalten. Um eine Operationalisierung der von Sabatier genutzten Begriffe gewährleisten zu können, werden sie in diesem Kapitel nachgezeichnet und erklärt.

Als Untersuchungsfeld bestimmt Sabatier *policy subsystems* anstelle klassischer Politikfelder, da die Reichweite kleiner ist und die beteiligten Akteure besser in *advocacy coalitions* klassifiziert werden können, wenn der Kreis auf eine politische Fragestellung oder Problematik verengt wird und die Anzahl der Akteure aggregiert werden kann, ohne an analytischer Schärfe zu verlieren. Sabatier unterscheidet zwei Möglichkeiten, warum sich diese *subsystems* entwickeln können: Entweder entstehen sie aus einer Professionalisierung und Differenzierung bestehender Politikfelder heraus oder aber aus der Unzufriedenheit einer Gruppe über ein bisher programmatisch nicht behandeltes Problem (vgl. Sabatier 1988: 24). Unter **Akteuren** innerhalb eines *policy subsystems* wird in erster Linie die politische Elite verstanden (ebd.: 16), was Sabatier als „those actors from a variety of public and private organizations who are actively concerned with a policy problem or issue [...]“ (ebd.: 17) konkretisiert. Eine solche Vorgehensweise hat für diese Arbeit mehrere Vorteile: Zum einen begünstigt sie eine Präzision der Fragestellung durch eine thematische Verengung auf Datenschutzpolitik bei gleichzeitiger expliziter Einbeziehung aller relevanten Akteure: Sowohl der Zivilgesellschaft, dem Journalismus, der Wissenschaft und der Privatwirtschaft wird eine Rolle im *policy process* zugeordnet. Die Eingrenzung des Forschungsfeldes auf die Entwicklungen der Datenschutzpolitik ist insofern sinnvoll, als dass sie eine Begrenzung der Anzahl aller relevanten Akteure in diesem Feld erleichtert und ebenfalls eine ausführlichere Untersuchung dadurch erst möglich und im Rahmen dieser Arbeit umsetzbar gemacht wird. Gleichzeitig wird betont, dass eine eindimensionale Untersuchung vermieden werden soll, vielmehr sollen die Akteure auch auf der subnationalen Ebene (vgl. ebd.: 17) betrachtet werden, was unter Berücksichtigung des oben beschriebenen Mehrebenen-Charakters der Datenschutzpolitik unerlässlich ist.

Nach Sabatier lassen sich die Akteure am sinnvollsten anhand ihrer politischen Grundsätze, Werte und Weltbilder und nicht anhand ihrer institutionellen Stellung innerhalb des Subsystems aggregieren. Solange die unterschiedlichen Akteure unabhängig von der Organisation, der sie angehören, thematisch in den wichtigsten Punkten übereinstimmen und ihr politisches Handeln miteinander koordinieren, bilden sie relativ stabile und langfristige *advocacy coalitions* (ebd.: 25), da eine Zusammenarbeit die gemeinsamen Positionen im öffentlichen Raum betont und Ressourcen bündelt (ebd.: 26).

Der **Zeitraum**, in dem eine Untersuchung über politisches Handeln sinnvoll ist, bezieht sich nach Sabatier auf mindestens eine Dekade, denn erst nachdem ein *policy cycle* durchlaufen sei, können die Ergebnisse in einem angemessenen Kontext retrospektiv evaluiert werden. Diese Evaluation, die sowohl von politischen Eliten als auch von Journalist_innen und Wissenschaftler_innen geleistet wird, kann ausschlaggebend für einen *policy change* sein. So stellt Sabatier fest:

„The literature on policy implementation also points to the need for utilizing time frames of a decade or more, both in order to complete at least one cycle of formulation, implementation, and reformulation and to obtain a reasonably accurate portrait of program success and failure“ (Sabatier, 1988: 16).

Diese Feststellung liegt insofern nahe, als dass Veränderungen der politischen Agenda häufig aus Korrekturen der bisherigen *policies* resultieren und unerwünschte Konsequenzen eliminieren sollen. Wie bereits oben dargestellt, wird das Handeln der politischen Akteure deshalb über einen längeren Zeitraum betrachtet, anstatt lediglich schlaglichtartig aktuelle Positionen wiederzugeben.

Ein Geflecht aus unterschiedlich bewerteten und priorisierten Kernüberzeugungen, die Sabatier *belief systems* nennt (vgl. ebd.: 31), verbindet unterschiedliche Gruppen. Die Struktur dieser *belief systems* lässt sich in einem dreistufigen Modell darstellen: Zu dem *deep core* zählen „fundamental normative and ontological axioms“ (ebd.), die für alle Politikfelder gleichermaßen gültig sind und grundlegende Menschen- und Weltbilder verkörpern. Sie sind relativ stabil und ändern sich, wenn überhaupt, nur über einen langen Zeitraum, da sie häufig das Resultat bestimmter Sozialisationsprozesse und Erfahrungen sind und tief im subjektiven Bewusstsein

verankert liegen. Zu ihnen gehören Konzepte von Werten wie Freiheit, Sicherheit und Gerechtigkeit ebenso wie eine Positionsbestimmung des Selbst innerhalb der Gesellschaft. Der *near policy core* hingegen umfasst konkretere politische Vorstellungen sowie strategische Einstellungen, wie politische Ziele zu erreichen sind und bezieht sich auf das jeweilige Politikfeld. In diesen Bereich fallen z. B. Beurteilungen der Relation zwischen Staat, Markt und Gesellschaft, oder die Bewertung von Umweltfragen. Der *near policy core* ist ebenfalls relativ stabil, eine Änderung der Einstellungen in diesem Bereich geschieht nur, wenn starke externe Einflüsse eine Neukonfiguration dieser Einstellungen erfordern. Die *secondary aspects* hingegen können, wie der Name schon suggeriert, schnell zur Disposition gestellt werden, da es sich hierbei lediglich um die Mittel und Wege handelt, wie der *near policy core* erreicht und umgesetzt werden soll. Sie beziehen sich in erster Linie auf das Subsystem und sind so dynamisch, dass sie sich dem politischen Geschehen anpassen können, wenn es z. B. um Ressourcenallokation oder Verfahrensregelungen geht, ohne dass dies zu gravierenden Veränderungen persönlicher Einstellungen führen müsste (vgl. ebd.: 28-31).

Advocacy coalitions formieren sich entlang dieses *belief systems*, wenn Gruppen in weiten Teilen des *near policy core* übereinstimmen und ihr Handeln miteinander koordinieren. Zwar müssen die Vorstellungen in diesem Bereich des *belief systems* nicht vollkommen übereinstimmen, es sollten jedoch große Überschneidungen bestehen, um von einer stabilen Koalition auszugehen. Um diese Stabilität zu erreichen, sind die Akteure auch bereit, Teile der *secondary aspects* aufzugeben und durch geeignetere Verfahren zu ersetzen, um ihre Ziele in Regierungsprogrammen umgesetzt zu sehen (vgl. ebd.: 34).

Auch Sabatier bezieht die zur Verfügung stehenden Ressourcen der Akteure in seine Überlegungen ein und bewertet sie als einen kritischen Faktor, der das strategische Handeln beeinflusst. So stellt er fest, dass die Ressourcen der Möglichkeit dienen, Regierungsprogramme zu beeinflussen, Mitglieder zu gewinnen und ihre Interessen durchzusetzen (vgl. ebd.: 29). Vor diesem Hintergrund stehen die Akteure innerhalb einer *advocacy coalition* vor einem wissenschaftlich interessanten Dilemma: Auf der einen Seite müssen sie versuchen, ihre Ressourcen so einzusetzen, dass sie der Stabilität und der Arbeitsfähigkeit der Koalition zuträglich sind, auf der anderen

Seite stehen sie dadurch jedoch auch im Wettbewerb zu den anderen Akteuren der Koalition, indem sie um Mitglieder konkurrieren. Aufgrund der Überschneidungen der *near policy cores*, die – wie oben erwähnt –, möglichst umfangreich sein sollten, ähneln sich auch die politischen Vorstellungen, Werte und Positionen der Anhängerschaft und könnten dadurch ein Klima des Wunsches nach inhaltlicher Abgrenzung schaffen. Dieser Aspekt wird bei Sabatier lediglich angedeutet, eine Beurteilung der Chancen und Risiken, die mit der Bildung einer *advocacy coalition* für die betreffenden Akteure und ihre Ressourcen einhergehen, fehlt in dieser Theorie leider. Ebenfalls wird nicht darauf eingegangen, dass allein die Koordination und Kooperation in einer *advocacy coalition* Ressourcen bündelt, da Arbeitskraft und auch monetäre Mittel für z. B. Reisekosten aufgebracht werden können. Die Vorstellung, dass *advocacy coalitions* lediglich Vorteile bringen, ohne mit Kosten verbunden zu sein, erscheint hier doch befremdlich. Eine genauere Untersuchung der Zusammenhänge zwischen Kooperationsaufwand und -nutzen hätte eine wichtige Erkenntnislücke schließen können.

Doch warum ist Sabatiers ACF nun relevant für diese Masterarbeit und die Erforschung der datenschutzpolitischen Akteure? Sabatiers Konzept grenzt sich deutlich vom *Rational-Choice-Ansatz* ab, da offensichtlich wird, dass Akteure nicht allein nutzenmaximierend handeln. Dies ist allein deswegen nicht möglich, weil sie die Möglichkeiten und Konsequenzen ihres Handelns in ihrer Gesamtheit nicht überblicken und bewerten können: „Rationality is limited rather than perfect“ (ebd.: 30). Darüber hinaus werden abstrakten „Interessen“, einer bei Tilly grundlegenden Kategorie sozialer Bewegungen, durch die Betonung der Werte- und Weltvorstellungen weitere Aspekte beigelegt: „While belief system models can thus incorporate self/organizational interests, they also allow actors to establish goals in quite different ways (e.g. as a result of socialization) and are therefore more inclusive“ (ebd.: 28). Dadurch wird auch das oben formulierte Dilemma umgangen, wie mit widersprüchlichen Positionen innerhalb einer Gruppe umgegangen werden soll: Individuelle Meinungen werden erst problematisch für eine Gruppe, wenn die *near policy cores* zu stark divergieren und dadurch die Stabilität gefährden. Auch lassen sich Werte und Überzeugungen leichter aus Veröffentlichungen der Gruppen herauslesen als Interessen. Darüber hinaus bietet dieser Ansatz den Vorteil, simplifi-

zierende Fallstricke wie eine zu starke Staats- oder Akteurszentriertheit zu vermeiden und die Beweggründe zu betonen, warum einige Akteure verschiedene Kooperationen eingehen, während andere vollkommen darauf verzichten.

3) Synthese

Mit einem Umweg über die klassische Ressourcenmobilisierungstheorie und durch Einbeziehung des Advocacy-Coalition-Ansatzes kann schließlich an dieser Stelle ein Gerüst entwickelt werden, welches die systematische Untersuchung der relevanten, nichtstaatlichen Akteure im Bereich Datenschutz in weitem Umfang erlaubt. Eine Kombination dieser beiden konzeptionellen Ansätze hat in den Vorteil, dass die Schwachstelle des einen Konzeptes durch die Stärke des jeweils anderen ausgeglichen werden kann: Während der Ressourcenmobilisierungsansatz sozio-psychologische Erklärungen auf der Mikroebene lediglich benennt, nicht jedoch tiefergehend untersucht (vgl. Jenkins 1983: 530), können diese mit den *belief systems* nach Sabatier erklärt werden. Darüber hinaus krankt der Ressourcenmobilisierungsansatz daran, dass ihm eine Zeitdimension und damit eine dynamische Komponente fehlt, die jedoch im Advocacy-Coalition-Ansatz eine wichtige Bedeutung einnimmt. Weiterhin erlaubt es der Advocacy-Coalition-Ansatz, die Netzwerkstruktur dieses Politikfeldes offenzulegen und mögliche Kooperationspotenziale aufzuzeigen. Unter Einbeziehung dieser beiden theoretischen Rahmen werden folgende Kategorien gebildet, anhand derer die Akteure untersucht werden:

1) **Organisation:** Hat die untersuchte Gruppe eine institutionalisierte Form? Wenn ja, welche? Gibt es so etwas wie eine gemeinsame Identität oder ein starkes Netzwerk, in dem sich die Individuen der Gruppe bewegen? Wie stark ist die Bindung an die Gruppe? All diese Fragen sind nicht leicht zu beantworten, zumal dies keine qualitativ-empirische Längsschnittstudie ist, die die Einstellungen vieler Menschen, die sich der Gruppe zugehörig fühlen, erfassen könnte. Nichtsdestotrotz wird eine Gruppe, die eine gemeinsame Identität bilden konnte, diese auch nach außen artikulieren, was die Beantwortung der Frage nach der Organisation einer Gruppe ermöglicht.

2) **Zeit:** Seit wann gibt es diese Gruppe? Aus welchem Kontext ist sie entstanden? Gab es besonders aktive/inaktive Phasen? Lassen sich starke Schwankungen des Interaktionsverhaltens feststellen? Hierzu wird eine chronologische Betrachtung notwendig sein, die davon abhängig ist, ob Informationen und Dokumente über einen längeren Zeitraum aufbewahrt, archiviert und öffentlich zugänglich gemacht werden.

3) **Ressourcenmobilisierung:** Welche Ressourcen stehen der Gruppe zur Verfügung? Woher stammen monetäre Einnahmen? Wofür werden sie eingesetzt? Wie werden die Einnahmen generiert? Wie stabil sind sie? Wie ist die Relation zwischen ehrenamtlichen und hauptamtlichen Mitarbeiter_innen? Wie stark engagieren sich ehrenamtliche Helfer_innen? Wie entwickeln sich die mobilisierten Ressourcen über einen längeren Zeitraum?

4) **Belief Systems:** Anstelle von Interessen wird analysiert, welche Werte, Weltanschauungen und Überzeugungen die Mitglieder einer Gruppen haben und welchen Stellenwert diese in der politischen Arbeit einnehmen. Welche Themen werden prioritär behandelt oder im Laufe der Zeit aufgegeben? Lässt sich eine Unterscheidung zwischen *deep cores*, *near policy cores* und *secondary aspects* vornehmen? Verläuft die Trennlinie zwischen diesen Begriffen stets analytisch eindeutig? Anknüpfungspunkte könnten die Erkenntnisse der ersten Kategorie liefern, da die zugrundeliegenden Werte ein wichtiger Bestandteil der Identität des Menschen sind.

5) **Collective Action:** Mit welchen Mitteln versuchen die Gruppen, ihre Interessen umzusetzen? Welchen Einfluss nehmen sie auf die Bevölkerung, auf Regierungsorgane, auf andere Interessengruppen? Wie generieren sie Öffentlichkeit für ihr Anliegen? Wie regelmäßig finden diese kollektiven Aktionen statt und wie viele Menschen beteiligen sich daran?

6) **Advocacy Coalitions:** Welche Bündnisse gehen Akteure der Datenschutzpolitik ein, und wie stabil sind diese Bündnisse? Lassen sich starke Übereinstimmungen der *belief systems* feststellen? Gibt es womöglich Kooperationspotenziale, die nicht genutzt werden?

7) **Opportunities:** In welcher Beziehung stehen die Akteure zum Staatsapparat? Sind sie von Repressionen betroffen oder haben sie privilegierte Zugänge zu politischen Entscheidungsträgern? Lassen sich Kanäle identifizieren, über die Einfluss auf Re-

gierungen genommen werden kann? Wie werden diese Kanäle genutzt? Eine Schwierigkeit dieser Kategorie liegt darin begründet, dass nur formelle Zugänge und Interaktionen untersucht werden können, während informelle Einflussnahmen, Zusammentreffen und nicht öffentliches Lobbying nicht bearbeitet werden kann.

Der aus den Kriterien abgeleitete Fragenkatalog wird nicht umfassend für jeden Akteur beantwortet werden können. Die Herausforderung besteht darin, ein möglichst umfassendes Bild der in dieser Arbeit behandelten Akteure zu zeichnen und ihre Position innerhalb des Subsystems herauszuarbeiten. Gleichzeitig reicht es nicht aus, die Gruppen isoliert zu betrachten, auch die Zusammenhänge und Netzwerke bieten Aufschluss darüber, welchen Dynamiken dieses Politikfeld unterliegt und welche Entwicklungen sich vollzogen haben. Trotzdem bilden diese Kategorien mit den daraus resultierenden Fragestellungen das Herzstück der vorliegenden Masterarbeit und werden im folgenden Kapitel so umfangreich wie nur möglich behandelt.

V Datenpolitische Akteure und ihre Aktivitäten

Ziel dieser Arbeit ist es, die Netzwerkstruktur des Politikfeldes Datenschutz zu untersuchen und wirkliche oder potenzielle Koalitionen zwischen den einzelnen Akteuren aufzuzeigen. Entlang der Definitionen von McCarthy und Zald wird also die *Social Movement Industry* SMI um den Themenkomplex Datenschutz untersucht. Analytisch bietet sich eine Unterscheidung in Subindustrien an, um das Untersuchungsfeld einzugrenzen und dadurch eine Operationalisierung dessen vorzunehmen. Folgende Unterscheidung erscheint in diesem Kontext sinnvoll: Zunächst werden zivilgesellschaftliche Gruppen analysiert. Sie lassen sich als „Social Movement Organisations“ im klassischen Sinne verstehen und streben eine einflussreiche Position im öffentlichen Diskurs an, um ihre Ziele durchzusetzen. Zur zweiten Gruppe, die auf ihre Positionen und Handlungen untersucht wird, zählen privatwirtschaftliche Akteure. Sie haben in diesem Zusammenhang eine Doppelrolle inne: Einerseits sind sie Anbieter von digitalen Dienstleistungen und Produkten, die ein kommerzielles Interesse an den Daten ihrer Kund_innen haben und die Erhebung und Auswertung personenbezogener Informationen als wichtigen Teil ihres Geschäftsmodells sehen, welches explizit Auswirkungen auf ihre Gewinnerwartungen hat. Andererseits sind sie selbst auch von negativen Auswirkungen von zu großer Datenmacht und -unsicherheit betroffen und haben deswegen ein potenzielles Interesse an staatlicher Regulierung, um ihre Position auf dem Markt zu sichern. Die dritte Gruppe beinhaltet Akteure, die sich journalistisch engagieren und damit die Willens- und Meinungsbildung ihrer Leser_innen sowie die medialen Diskurse beeinflussen. In der vierten Gruppe sind staatsnahe Akteure zusammengefasst. Zwar beschränkt sich diese Arbeit explizit auf nichtstaatliche Akteure, es ist jedoch der Vollständigkeit geschuldet, auch Parteien und Datenschutzbeauftragte in eine Untersuchung zu integrieren, da diese eine wichtige diskursprägende Rolle innerhalb des Politikfeldes einnehmen und einen privilegierten Zugang zum politischen Institutionengefüge genießen.

Die Akteure sind aufgrund bestimmter Kriterien ausgewählt worden. Zum einen sollten sie seit mehreren Jahren existieren. Dieses Kriterium ist nicht so banal, wie es zunächst erscheint, denn die neue Daten(schutz)bewegung ist in Teilen noch sehr

jung. Dementsprechend ist es nicht verwunderlich, dass diese Szene von Umbrüchen, Neustrukturierungen und tagesaktuellen Dynamiken geprägt ist. Um aber eine Konstanz über etwa eine Dekade herstellen zu können, besitzt zeitliche Kontinuität für die *Policy*-Analyse einen besonderen Stellenwert. Darüber hinaus werden die Gruppen anhand ihrer Relevanz ausgewählt: Es werden also Akteure beleuchtet, die bereits Medien- und Öffentlichkeitswirksamkeit generieren konnten und darüber hinaus eine breite Basis an Mitgliedern aufweisen können, die sie in ihrer Arbeit legitimiert. Auch wurden Gruppen ausgewählt, die möglichst kontroverse Ansichten zum Thema Datenschutz vertreten und damit diametrale Positionen innerhalb des Diskurses einnehmen. Es lässt sich also feststellen, dass sowohl der *most-similar* als auch der *most-different*-Ansatz verbunden werden: Ähnlich sind sich die Akteure insofern, als dass sie bereits über einen längeren Zeitraum bestehen, also in der Szene etabliert, und im öffentlichen Diskurs in ihrer Akteursqualität anerkannt sein dürften. Gleichzeitig wird versucht, die Unterschiedlichkeit herauszuarbeiten und dadurch ein breites Spektrum an Positionen, Organisationsformen und Aktionen abzudecken.

1) Zivilgesellschaftliche Datenschutzgruppen

Unter zivilgesellschaftlichen Datenschutzgruppen werden Akteure verstanden, die nicht profitorientiert arbeiten und ein politisches Interesse an Datenschutzpolitik haben. Konkret werden all jene Gruppen in diesem Bereich zusammengefasst, die in einer Sphäre zwischen dem Privaten und dem Staat agieren, eine organisatorische Autonomie besitzen und „ihre materiellen wie immateriellen Interessen artikulieren“ (vgl. Thiery 2008: 655). Diese Interessen werden nicht dadurch verfolgt, dass politische Ämter oder politisch institutionalisierte Macht angestrebt wird, stattdessen soll vielmehr über die Formung des öffentlichen Diskurses politischer Einfluss erlangt werden (vgl. ebd.: 655).

a) Chaos Computer Club (CCC)

Der Chaos Computer Club versteht sich als eine Hackervereinigung, die sich neben technischen Aspekten auch mit der sozialen und gesellschaftlichen Dimension von Digitalisierung und Computernutzung auseinandersetzt.

Organisation: Der CCC hat nach eigenen Angaben c.a. 4500 zahlende Mitglieder (vgl. CCCde Videos, 2013) und keine hauptamtlichen Mitarbeiter_innen, d.h. alle Aktiven arbeiten in dem Club ehrenamtlich und erhalten dafür kein Gehalt. Neben der Zentrale in Hamburg gibt es bundesweit in 24 Städten sog. Erfahrungsaustauschkreise „Erfas“, sie bilden ein Netz aus lokalen Hackertreffs, die jedoch nicht auf Landesebene organisiert sind, sondern relativ autonom arbeiten. Eine Vernetzung dieser Erfas erfolgt über den sog. Erfa-Beirat, der viermal im Jahr tagt und der Koordination lokaler Arbeit dient. Formal ist der CCC ein eingetragener Verein und arbeitet gemeinnützig. Das höchste Organ des Vereins bildet die Mitgliederversammlung, diese wählt den aus fünf Personen bestehenden Vorstand (vgl. CCC e.V. 2014). Eine Reihe von lose organisierten, sog. Chaostreffs sympathisiert zwar mit dem Club, findet allerdings keine Entsprechung in der Entscheidungsstruktur der bundesdeutschen Zentrale, vielmehr sind die Chaostreffs lose organisiert und haben auch keinerlei festgeschriebene Verpflichtungen dem Club gegenüber.

Eine zentrale Referenz für die Identität vieler Hacker bilden die Richtlinien der ursprünglich 1984 von Steven Levy verfassten Hackerethik, die zentrale Verhaltensregeln vorschreibt und damit ein Repertoire an erwünschtem und unerwünschtem Handeln der Individuen umreißt. Auf die Hackerethik wird in vielerlei Hinsicht verwiesen, sie bildet einen elementaren Kodex und gleichzeitig eine Richtlinie, die es erlaubt, sich von jenen abzugrenzen, die gegen diese Ethik verstoßen. Trotzdem sind die innerhalb der Hackerethik formulierten Grundsätze nicht unumstößlich: Immer wieder werden sie von Aktivist_innen diskutiert und zur Disposition gestellt (vgl. Schrutzki 2002: 38f.). Außerdem erfuhr der Kodex eine Ergänzung um zwei Punkte, die den Datenschutz betreffen. Dazu zählt zum einen das Verbot, fremde Daten zu missbrauchen und zum anderen der Schutz privater Daten bei gleichzeitiger Nutzbarmachung öffentlicher Daten (vgl. CCC e.V. a). Darüber hinaus veröffentlichte der CCC zwei sogenannte Hackerbibeln, in denen grundlegende Werte

des Clubs und der Hacker im Allgemeinen formuliert und die aufsehenerregendsten Hacks dokumentiert wurden.

Belief Systems: Aufgrund der sehr persönlichen und subjektiven Charakteristika der *deep cores* lassen diese sich nicht für einen ganzen Verein wie den CCC festlegen. In erster Linie werden deshalb die *near policy cores* untersucht und herausgearbeitet. In der Präambel der Satzung wird die grundsätzliche Ausrichtung des Vereins deutlich, darin steht:

„Die Einsatzmöglichkeiten der automatisierten Datenverarbeitung und Datenübermittlung bergen Chancen, aber auch Gefahren für den Einzelnen und für die Gesellschaft. Informations- und Kommunikationstechnologien verändern das Verhältnis Mensch-Maschine und der Menschen untereinander“ (vgl. CCC e.V. 2014).

Welcher Natur die Chancen und Gefahren sind, wird in der Präambel nicht erläutert. Spezifischer wird Datenschutz in dem letzten Grundsatz der Hackerethik formuliert: „Öffentliche Daten nützen, private Daten schützen“ (CCC e.V. a). Zum einen wird also eine umfassende Informationsfreiheit gefordert, gleichzeitig wird dem Schutz der Privatsphäre ein wichtiger Stellenwert eingeräumt. Dabei werden sowohl staatliche als auch kommerzielle Versuche, private Daten zu erfassen und zu verarbeiten, in diesen Grundsatz einbezogen und problematisiert. In erster Linie werden diese Aktivitäten als illegitime Eingriffe in die Privatsphäre bewertet, die der Verein in Pressemitteilungen, Stellungnahmen und Veröffentlichungen immer wieder ablehnt. Ein besonderer Arbeitsschwerpunkt der letzten Jahre lag in der Beanstandung biometrischer Datenerfassung, vor allem der Fingerabdrücke im e-Pass, da durch diese Methoden eine eindeutige Zuordnung von Merkmalen zu einem Menschen nicht vollkommen gegeben und mit Risiken verbunden sei und ein Fingerabdruck sehr leicht gefälscht und missbraucht werden könne. Darüber öffne diese Form der Datenerfassung einer staatlichen Überwachung Tür und Tor und dringe tief in die Privatsphäre der Bürger_innen ein (vgl. Erdgeist 2008).

Es wird schnell deutlich, dass Datenschutz, der Schutz der Privatsphäre und gleichzeitig die absolute Informationsfreiheit für öffentliche Daten zu den *near policy cores* des CCC gehören. Zum einen wurde die Hackerethik um zwei den Datenschutz betreffende Grundsätze ergänzt und dadurch an die Wertvorstellungen des Clubs

angepasst, zum anderen bildet das Thema Datenschutz einen essentiellen Baustein der vom CCC initiierten Aktionen, was unten näher erläutert wird. Zu den *secondary aspects* zählen laut Sabatier in erster Linie die Mittel und Wege, die eine Gruppe nutzt, um ihre *policies* durchzusetzen. Für den CCC kann festgestellt werden, dass die Maßnahmen von Kontinuität geprägt sind, wie in einem Geleitwort der *Datenschleuder* (dem Vereinsmagazin) zu lesen ist: „Der CCC wollte, will und wird sein: Ein Hackerclub, der zuerst seinem eigenen Anspruch gerecht werden muss. Und der besteht darin, Spaß zu haben, die Welt zu verstehen und sie ein kleines bißchen [sic] besser zu machen. Wir müssen nichts, wir wollen nur manchmal“ (Redaktion der *Datenschleuder* 2011: 2). Es wird eine relativ unverbindliche Grundhaltung zu den *secondary aspects* deutlich, diese werden bereitwillig uminterpretiert, um dem „eigenen Anspruch gerecht“ zu werden, welcher stets im Fokus des Handelns stehen müsse. Gleichzeitig ist die Themenauswahl des Clubs häufig von dem individuellen Handeln der Mitglieder geprägt: „Ob sie [die Aktivistenvereinigungen] zu einer politischen Frage Stellung beziehen, hängt davon ab, ob ihre Mitglieder dies für notwendig erachten und sich entsprechend engagieren wollen“ (Fritz 2012: 89).

Zeit: Der CCC wurde 1984 gegründet und veranstaltete seitdem jedes Jahr auch einen Kongress, den Chaos Communication Congress. Bereits seit 1981 fanden regelmäßig Treffen von computeraffinen Menschen in den Räumlichkeiten der Tageszeitung taz statt, aus denen der Club hervorging. Einer der bekanntesten Gründungsväter ist der taz-Redakteur Wau Holland, der die inhaltliche und programmatische Entwicklung des Clubs maßgeblich prägte (vgl. Röhr 2012: 58-73). Eine wichtige Zäsur stellt der sog. NASA-Hack dar, bei dem Hacker aus Deutschland in amerikanische Rechensysteme eindringen und Informationen über das US-amerikanische Raumfahrtprogramm an den KGB weitergaben (vgl. Anonymus 1988: 109-111). Obwohl eine eindeutige Verbindung der Hacker zum CCC nicht festgestellt werden konnte, geriet der Club trotzdem ins Visier der Ermittler_innen und wurde öffentlich als Vereinigung wahrgenommen, die illegale Handlungen deckt. Erst nach Jahren konnte der CCC interne Streitigkeiten beseitigen, das verlorene Vertrauen zurückgewinnen und das Image der „ehrlichen“ Hacker wiederherstellen (vgl. Glasstetter/ Meyer: 2012). Von diesem Zeitpunkt an konnte der Club kontinuierlich wachsen, seit 1997 stieg die Anzahl der Neueintritte sprunghaft an (vgl. CCCde

Videos 2012). Eine Stagnation oder gar ein Negativtrend der Mitgliedszahlen lässt sich nach 1997 nicht mehr feststellen.

Ressourcenmobilisierung: Den größten Teil der monetären Einnahmen bestreitet der CCC aus den Beiträgen seiner Mitglieder. Interessanterweise verzichtet der CCC auf aktive Mitgliederwerbung, d.h. es wird nicht versucht, aktiv auf Menschen zuzugehen, um sie zum Beitritt zum Club zu bewegen. Stattdessen sprechen die Mitglieder eine Einladung an alle aus, die sich für die Ziele und Belange CCC interessieren und sich darin engagieren möchten. Auch die Einnahmen aus dem Ticketverkauf für den Chaos Communication Congress oder anderen Veranstaltungen sowie Spenden von Einzelpersonen gehören zu den wichtigsten Einnahmequellen.

Sponsoring findet beim CCC vor allem in Form von Sachspenden oder dem Zugang zu Infrastruktur statt: Es werden Server (z. B. zum Betreiben des Tor-Netzwerkes) zur Verfügung gestellt und ihre Unterbringung sichergestellt (vgl. CCC e.V. b). Auch für den jährlichen Chaos Communication Congress wird Sponsoring betrieben, indem technisches Equipment und Hardware von Unternehmen gestellt wird (vgl. Events CCC).

Collective Action: Wie oben bereits erwähnt, ist Datenschutz ein zentrales Anliegen des CCC und kann als eines der wichtigsten Interessen gelten. In der Satzung wird unter dem Paragraphen „Zweck und Gemeinnützigkeit“ festgehalten: „Der Club fördert und unterstützt Vorhaben der Bildung und Volksbildung in Hinsicht neuer technischer Entwicklungen, sowie Kunst und Kultur im Sinne der Präambel oder führt diese durch“ (vgl. CCC e.V. a). Dementsprechend haben Aktive des Clubs in den letzten Jahren eine Reihe von Aktivitäten unternommen, um dieses Anliegen umzusetzen. Die wohl wichtigste und weitreichendste Aktion des CCC ist die jährliche Ausrichtung des Chaos Communication Congress, an dem im letzten Jahr 6600 Besucher_innen teilgenommen haben (vgl. Krempel 2013). Darüber hinaus halten einige Mitglieder Vorträge und veranstalten Workshops, die sich mit den Konsequenzen von Digitalisierung, *big data*, Web 2.0 und *ubiquitous computing* auseinandersetzen. Auch lässt sich beim CCC ein Trend feststellen, Privacy Enhancing Technologies (PET) stärker einzusetzen und damit möglicher Überwachung und Erfassung zu entgehen. Ziel ist es, durch die Verschlüsselung privater Kommunikation und Internetverhalten eine Überwachung durch staatliche Behörden, aber

auch große datenverwertende Unternehmen zu verhindern, Autonomie im Netz zurückzuerlangen und die eigene Privatsphäre zu schützen, ohne dass die eigenen Spuren zurückverfolgt und/oder ausgewertet werden können. Dementsprechend organisieren viele Erfas bundesweit Kryptoparties und geben Tipps, wie die Anonymität des Surfens erhöht werden kann.

In der Zeitung des Clubs, der Datenschleuder, werden regelmäßig Verstöße gegen das Recht auf informationelle Selbstbestimmung veröffentlicht oder Auswirkungen der Überwachung auf die Gesellschaft diskutiert. Mit ca. 4000 Auflagen (vgl. Reus 2011) hat das „Fachblatt für Datenreisende“ jedoch eine geringe Reichweite, ein Großteil der Bezieher_innen ist Mitglied des Clubs.

Ebenfalls ist der CCC Mitveranstalter und Bündnispartner der seit 2006 in regelmäßigen Abständen stattfindenden Demonstration „Freiheit statt Angst“ und vergibt zusammen mit Digitalcourage und der Deutschen Vereinigung für Datenschutz den Negativpreis „Big Brother Award“ (Big Brother Awards 2014).

Advocacy Coalitions: Die engste und kontinuierlichste Koalition lässt sich mit der Bürger_innenrechtsvereinigung Digitalcourage e.V. feststellen. So führt der CCC Digitalcourage ausdrücklich als Teil der *Chaos family* auf, ein Attribut, welches ansonsten nur auf Gruppen zutrifft, die enger mit dem CCC assoziiert sind und sich als Teil dessen verstehen. Bis 2010 wurde die ideelle Verbindung zu Digitalcourage (damals noch FoeBuD e.V.) auch in der Datenschleuder betont, seit dem Heft #95 fehlt jedoch ein Hinweis auf die Chaosfamilie in der Zeitschrift. Eine weitere Vernetzung findet auch auf supranationaler Ebene statt, hier ist der CCC Mitglied von EDRi (European Digital Rights) das seinerseits finanziell von der Europäischen Kommission für Justiz unterstützt wird.

Interessant sind die finanziellen Aktivitäten des CCC: Nach Angaben der Süddeutschen Zeitung hat die Wau-Holland-Stiftung, die dem Club sehr nahe steht, der Enthüllungsplattform WikiLeaks 2010 1,3 Mio. EUR gespendet, damit diese ihre Arbeit fortsetzen kann (vgl. SZ-Redaktion 2011). Auch die europäischen Anwälte von Edward Snowden sowie der Blog Netzpolitik.org erhielten Spenden vom Club im fünfstelligen Bereich (vgl. z. B. heise online 2014).

Opportunities: Im Laufe der letzten Jahre konnten einzelne Mitglieder des CCC sich als Expert_innen für die Schnittstelle zwischen Technik und Gesellschaft etablieren

und dadurch auch Zugang zur Legislative und zur öffentlichen Verwaltung gewinnen. So saß die Sprecherin des Clubs, Constanze Kurz, in der Enquete-Kommission „Internet und Digitale Gesellschaft“, wo sie sich in den Projektgruppen „Medienkompetenz“, „Netzneutralität“ sowie „Zugang, Struktur und Sicherheit im Netz“ engagierte (vgl. Deutscher Bundestag 2013). Darüber hinaus wurden Aktivist_innen des CCC als Sachverständige vom Bundesverfassungsgericht wiederholt um Stellungnahmen zu Verfahren gebeten (vgl. z. B. Bundesverfassungsgericht 2012). Auch die Medien scheinen dem Club positiv gesonnen: So werden Mitglieder des CCC immer wieder als Expert_innen für Internet und Datenschutzpolitik zitiert, stellen eine wichtige Informationsinstanz für Journalist_innen dar und haben sich lange in der Medienlandschaft etabliert. Ein Beispiel dafür ist die monatliche Sendung „Chaosradio“ des CCC Berlin, die bei einem öffentlich-rechtlichen Sender, dem RBB ausgestrahlt wird.

Zusammenfassend lässt sich feststellen, dass der CCC europaweit eine der wichtigsten Anlaufstationen für Hacker darstellt und Datenschutz eines der zentralen Anliegen und damit auch Teil der Identität des Clubs ist. Gleichzeitig weist die Organisation einen erstaunlich niedrigen Professionalisierungsgrad auf, da es bundesweit keine hauptamtlichen Angestellten gibt, die das Alltagsgeschäft erledigen und an der Konzeption von Kampagnen mitwirken. Auch wird keine Mitgliederwerbung betrieben, um den Ressourcenpool der Organisation zu erhöhen.

b) Arbeitskreis Vorratsdatenspeicherung

Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) ist ein Aktionsbündnis und damit ein informeller Zusammenschluss von Aktivist_innen und Gruppen, die sich für mehr Privatsphäre im Internet einsetzen und deren Ziel es ist, die Ausspähung privater Kommunikation durch Dritte zurückzudrängen und zu verhindern.

Organisation: Für die Organisation des AK Vorrat ist es charakteristisch, dass es keine institutionalisierte Organisationsform gibt. Dadurch soll vermieden werden, dass es innerhalb des Arbeitskreises zur Herausbildung einer unerwünschten Hierarchie kommt. Freies Arbeiten unter Gleichen soll für alle Aktiven gelten und ist

gelebter Grundsatz. Der Arbeitskreis versteht sich als Bündnis, in dem unterschiedliche Personen aus diversen Kontexten, Gruppen und Organisationen gleichberechtigt mitarbeiten.

Der Arbeitskreis ist auch in der Fläche organisiert, nämlich in Gruppen, die lokal vor Ort arbeiten und sich neben bundesweiten auch mit regionalen Themen befassen und entsprechende Aktionen planen und durchführen. Die Homepage des AK Vorrat listet insgesamt 107 dieser Ortsgruppen auf. Bei genauerer Betrachtung stellt man jedoch schnell fest, dass viele der Gruppen seit mehreren Jahren inaktiv sind und keine inhaltliche Arbeit mehr leisten. Lediglich in den Großstädten Berlin, Hamburg, Bremen und Köln-Bonn treffen sich noch regelmäßig Aktive, um sich für ihre Vorstellungen von Freiheitsrechten einzusetzen. In Bremen ist die Gruppe eng verbunden mit dem Chaos Computer Club, in Bielefeld gibt es starke Verknüpfungen mit Digitalcourage e.V. (vgl. AK Vorrat 2013 a).

Belief System: Gegründet wurde der AK Vorrat mit dem Ziel, die Einführung der in der EU-Richtlinie 2006/24/EG vorgesehenen, anlasslosen Vorratsdatenspeicherung zu verhindern und Widerstand gegen diese Überwachungspraxis zu mobilisieren. Dementsprechend kann diese Position als *near policy core* bezeichnet werden: Der Schutz des Rechts auf informationelle Selbstbestimmung, auf Privatsphäre und unbeobachtete Kommunikation sind zentrale Werte, die alle im Arbeitskreis Aktiven teilen (vgl. AK Vorrat). Zu den *secondary aspects* gehört vor allem die Mobilisierung und Koordination von Protest gegen Überwachung sowie die Bereitstellung einer Plattform, auf der politische Arbeit geleistet und mit vielen Organisationen vernetzt werden kann.

Zeit: Das Bündnis wurde am Rande des Chaos Communication Congress 2005 gegründet, als erste Anstrengungen für ein Gesetz zur Vorratsdatenspeicherung (VDS) seitens der EU unternommen wurden. In Deutschland gelang es dem Bündnis, 34.000 Unterstützer_innen für die Verfassungsbeschwerde gegen die VDS zu gewinnen (vgl. bpb 2009). Nach einer Welle des starken Engagements und der Bildung vieler regionaler Ortsgruppen, ebnete das Interesse der Aktivist_innen an dem Bündnis schnell wieder ab. Seit 2010/2011 lässt sich nicht mehr von einer Struktur mit hoher, in der Region verankerter Reichweite sprechen, vielmehr existieren nur noch

wenige Ortsgruppen in Großstädten, die allerdings noch sehr aktiv sind und Aktionen planen.

Ressourcenmobilisierung: Das Bündnis finanziert sich allein aus Spenden und bezieht sonst keine regelmäßigen Einnahmen. Ebenso wenig gibt es eine feste Mitgliedschaft, die mit der Entrichtung von Beiträgen verbunden wäre.

Collective Action: Die für den Arbeitskreis wohl wichtigsten Aktionen des Bündnisses stellen die in regelmäßigen Abständen von ca. einem Jahr stattfindenden „Freiheit statt Angst“ – Demonstrationen dar, die sich gegen die Überwachungspraktiken von Staat und Wirtschaft richten. Im August 2014 haben nach eigenen Angaben 6500 Menschen an der Demonstration in Berlin teilgenommen (vgl. Freiheit statt Angst 2014).

Neben der Demonstration findet seit 2011 jährlich der sog. AKtiVCongrEZ statt, an dem auch der AK Vorrat federführend beteiligt ist. Ziel ist es, die Vernetzung zwischen den einzelnen Gruppen zu stärken, eine Bewegungsstruktur aufzubauen und inhaltliche Arbeit zu leisten oder zu koordinieren. Datenschutz und entsprechende, auf dieses Thema bezogene Gesetzesvorhaben bilden einen wesentlichen Themenschwerpunkt bei diesem Kongress und werden mit hoher Priorität behandelt (vgl. Wiki Vorratsdatenspeicherung).

Darüber hinaus werden in dem Blog auf der Homepage regelmäßig Informationen zu aktuellen und geplanten Überwachungsmaßnahmen veröffentlicht und bereitgestellt, die den Diskurs in eine der Überwachung kritisch gegenüberstehende Richtung lenken sollen. Gleichzeitig dient der Blog der Dokumentation aller bisherigen Aktivitäten und soll allen Interessierten und Aktiven die Möglichkeit bieten, sich Wissen zu den für sie relevanten Themenbereichen anzueignen (vgl. Blog Vorratsdatenspeicherung 2014).

Auch hat der Arbeitskreis für die Bundestagswahl 2013 Wahlprüfsteine aufgestellt und entsprechende Fragen von den Parteien beantworten lassen. Die Auswertung wurde im Anschluss auf der Homepage veröffentlicht (vgl. AK Vorrat 2013 b).

Advocacy Coalition: Für den AK Vorrat ist es insofern nicht ganz leicht, *advocacy coalitions* aufzuzeigen, da der Arbeitskreis selbst die Struktur einer *advocacy coalition* aufweist. An dieser Stelle soll deshalb nicht nur beschrieben werden, welche Koalitionen von diesem Akteur eingegangen werden, sondern welche Koalitionen

ihm bereits inhärent sind. Diese Vorgehensweise hat den Vorteil, dass dadurch ebenfalls ein sinnvoller Beitrag zur Identifikation der Netzwerkstruktur dieses Politikfeldes geleistet werden kann.

Zu den wichtigsten Akteuren innerhalb des Arbeitskreises lassen sich Digitalcourage e.V. (ehemals FoeBuD) und der CCC zählen. Hier gibt es starke personelle und strukturelle Überschneidungen, aber auch die Piratenpartei arbeitet in vielen Punkten eng mit dem AK Vorrat zusammen, sodass viele Aktionen gemeinsam durchgeführt oder füreinander beworben werden können (vgl. z. B. Manigk 2011). Ein Mitglied des Arbeitskreises hat einen Beobachter_innenstatus bei EDRi inne (vgl. European Digital Rights 2014). Der Netzwerkcharakter des AK Vorrat wird darüber hinaus an einer Stelle besonders augenscheinlich: Die Überschneidungen bei der Arbeit in verschiedenen Gruppen sind im zivilgesellschaftlichen Bereich relativ hoch, der AK Vorrat fungiert dabei als wichtige Koordinationsplattform.

Opportunities: Viele Aktive des Arbeitskreises haben sich im Laufe der Jahre Reputationen erarbeitet, welche sie als Sachverständige im Bereich der staatlichen Überwachung auszeichnen. So wurde z. B. Christiana Mauro 2011 als Sprecherin zum Krakauer Forum der Europäischen Kommission eingeladen (vgl. Europäische Kommission), welches sich mit Fragen des gemeinsamen Europäischen Binnenmarktes beschäftigt.

Die Ausrichtung des AktiVCongrEZ findet in Kooperation mit der Bundeszentrale für politische Bildung statt (vgl. wiki Vorratsdatenspeicherung 2014), einer nachgeordneten Behörde des Bundesministeriums des Innern (vgl. Bundeszentrale für politische Bildung 2011: 73). Auch der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, lobte das Engagement des Arbeitskreises und dessen „unermüdlichen Einsatz für die Freiheitsrechte und als Sprachrohr für den Datenschutz“ (vgl. Netzpolitik.org 2010), woraus sich die wohlwollende Haltung dieses staatsnahen Akteurs gegenüber dem AK Vorrat erkennen lässt. Insgesamt lässt sich feststellen, dass der Arbeitskreis von staatlicher Stelle durchaus akzeptiert und zum Teil auch gefördert wird, obwohl er sich in Opposition zu geplanten Gesetzesvorhaben der Bundesregierungen positioniert. Außerdem zeigt der Streit über die Vorratsdatenspeicherung sowie dessen Ablehnung durch

den Bundesgerichtshof, dass diese Opposition auch von juristischer Seite Gehör finden konnte.

Zusammenfassend lässt sich sagen, dass der AK Vorrat mit seiner Bündnisstruktur zwar eine Plattform für die Koordination von Aktionen zwischen bereits bestehenden Gruppierungen bietet, faktisch bleiben die Handlungskompetenzen des Arbeitskreises jedoch beschränkt: Weder lässt sich eine kontinuierliche Arbeit in den einzelnen Ortsgruppen umsetzen, noch die Schaffung einer stabilen Ressourcenbasis realisieren.

c) Deutsche Vereinigung für Datenschutz

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) hat ihren Sitz in Bonn und ist einer der wichtigsten deutschen Verbände, die sich ausschließlich mit Datenschutz und der Rolle von Privatsphäre in der Gesellschaft beschäftigen.

Organisation: Anders als die bisherigen Akteure ist die DVD nicht bundesweit regional verankert und besitzt keinerlei föderale Struktur. Vielmehr handelt es sich um eine zentralisierte Struktur, bei der keine untergeordneten Ebenen definiert sind und die Mitglieder sich nicht regional vor Ort in die Arbeit des Verbandes einbringen. Auch gibt es keine Rechte und Pflichten für die Mitglieder, die aus einer institutionalisierten regionalen Struktur erwachsen könnten.

Dem Vorstand besteht aus drei Vereinsmitgliedern sowie bis zu sechs Beisitzer_innen. Alle Organe werden ausschließlich ehrenamtlich besetzt, hauptamtliche Mitarbeiter_innen sind laut der Satzung nicht vorgesehen (vgl. DVD e.V. 2006: 5-7). Zwar kann der Verein Arbeitskreise bilden, ein Großteil der Verbandsarbeit wird jedoch allein vom Vorstand geleistet, was mitunter der stark zentralisierten Struktur des Verbandes geschuldet ist. Innerhalb des Vorstandes haben die Mitglieder bestimmte Schwerpunktsetzungen vorgenommen, die die inhaltliche Vereinsarbeit personell verteilt. Laut der Lobbyliste des Bundestags hat die DVD 300 Mitglieder (vgl. Deutscher Bundestag 2014: 241), wobei daraus nicht hervorgeht, ob diese Zahl lediglich natürliche oder auch juristische Personen beinhaltet.

Belief Systems: Der Verband versteht sich selbst als „Graswurzelnitiative“ (vgl. Alenfelder/ Weichert 1999), also als eine *bottom-up*-orientierte Organisation, die sich in einer breiten gesellschaftlichen Basis verankert sieht. Gleichzeitig wurde sie auch als „bürgerrechtlich, staatskritisch und linksliberal“ (ebd.) gelabelt. Ähnlich wie auch bei den oben genannten Akteuren besteht das Hauptanliegen im „Schutz der Bürgerinnen und Bürger, auch betroffener Einzelner vor mißbräuchlicher [sic] Datenmacht“ (DVD e.V. 2006). Dieses Ziel lässt sich als *near policy core* beschreiben, denn es legt die grundlegende politische Sichtweise vieler Datenschützer_innen offen: Zu große Datenmacht birgt ein Missbrauchspotenzial, welches vielen Menschen schaden kann. Das Grundrecht auf informationelle Selbstbestimmung ist für die DVD ein sehr hoch geschätztes, schützenswertes Gut, welches gegen Dritte verteidigt werden muss.

Als *secondary aspect* schlägt die DVD z. B. vor, die deutschen Geheimdienste abzuschaffen, da diese demokratisch nicht kontrollierbar seien und sowohl volkswirtschaftlichen als auch immateriellen Schaden in Bezug auf das Vertrauen der Bürger_innen in den Rechtsstaat verursachen (vgl. DVD e.V. 2014).

Interessant ist die starke Dienstleistungsorientierung dieses Akteurs. Während die anderen zivilgesellschaftlichen Gruppen sich zunächst als aktivistischen Teil einer sozialen Bewegung verstehen, politische Entscheidungen beeinflussen möchten oder ihren Mitgliedern einen Raum zur politischen Entfaltung bieten, betont die DVD, welche Dienstleistungen sie für andere erbringen: „Beratung in Fragen des Datenschutzes“ (DVD Satzung 2006), die Erstellung von Gutachten, Informationsveranstaltungen für Organisationen und Parteien werden als wichtiger Teil der Vereinsarbeit betrachtet. Wie die meisten anderen Organisationen in diesem Bereich ruft auch die DVD dazu auf, die Privatsphäre im Netz durch die Verschleierung der eigenen digitalen Spuren zu schützen, damit Daten nicht mehr ohne weiteres automatisiert abgefangen werden können. Die Nutzung von Kryptografie-Software und das Surfen über Proxy-Server soll „Selbstdatenschutz“ (Schuler 2014: 34) ermöglichen und darüber hinaus die Monopolstellung vieler datenhungriger Onlinedienste schwächen. Die als sehr hoch eingeschätzte Bedeutung der *privacy enhancing technologies* kann als *secondary aspect* betrachtet werden und ist den meisten Datenschutzorganisationen inhärent.

Zeit: Die Deutsche Vereinigung für Datenschutz ist der älteste der bisher analysierten Akteure. Gegründet wurde der Verband 1977, zu einem Zeitpunkt, als Begriffe wie Datenmacht oder Datenschutz noch nicht die gesellschaftliche Relevanz aufwiesen, die sie zu Beginn der 1980er Jahre und in den Jahren darauf bekamen. Seit dieser Zeit arbeitet der Verein kontinuierlich an der Thematik und prägte damit in der Vergangenheit den öffentlichen Datenschutzdiskurs mit (vgl. Alenfelder/ Weichert 1999).

Ressourcenmobilisierung: Mitgliedsbeiträge, Spenden und Überschüsse aus Seminaren und Veranstaltungen sind die Einnahmequellen des Verbandes. Eine genaue Bezifferung der Einnahmen ist den öffentlich zugänglichen Quellen der DVD nicht zu entnehmen.

Collective action: Eines der wichtigsten Anliegen des Vereines ist die regelmäßige Veröffentlichung der Zeitschrift „Datenschutznachrichten – DANA“. Diese Zeitschrift erscheint viermal jährlich und hat einen explizit politischen und kritischen Anspruch, was sie von vielen rein juristischen oder technischen Publikationen über Datenschutz unterscheidet.

Ein zentrales Ziel des Vereins ist die kritische Begleitung der Datenschutzpolitik in Deutschland. Unmittelbar gelingt dies immer wieder durch Anhörungen und Stellungnahmen in Parlamentsausschüssen oder im Bundesrat. Für die Sachverständigen des Verbandes besteht in diesem Zusammenhang die Chance, ihre Vorstellungen, aber auch Kritik an Gesetzesvorhaben zu äußern und sich damit unmittelbar in den Gesetzgebungsprozess einzubringen (vgl. DVD e.V. 2011).

Zusammen mit anderen Organisationen, die sich für Datenschutz in der digitalen Welt stark machen, verleiht die DVD einmal jährlich den sog. „Big Brother Award“, einen Negativpreis, mit dem die größten „Datenkraken“ ausgezeichnet werden.

Advocacy Coalitions: In den 1970er und 1980er Jahren arbeitete der Verband bei vielen Themen eng mit den Gewerkschaften zusammen, diese Kooperation hat sich jedoch nach und nach gelöst und ist heute nur noch vereinzelt und sporadisch wahrnehmbar (vgl. Alenfelder/ Weichert 1999). Gleichzeitig legt der Verband Wert auf eine breite Vernetzung und listet eine Reihe von Partnerorganisationen auf, mit denen regelmäßige Kooperationen und Unterstützungen realisiert werden. Zu den wichtigsten gehören z. B. Digitalcourage, Campact sowie der Bundesverband der

Datenschutzbeauftragten Deutschlands. Ähnlich wie der AK Vorrat hat auch die DVD einen Beobachter_innenstatus bei EDRI, sodass auch von einer europäischen Vernetzung gesprochen werden kann (vgl. European Digital Rights 2014).

Kritische Distanz ist vor allem in Bezug auf Parteien und die Datenschutzbehörden charakteristisch für die DVD. Dies liegt zum einen an dem eigenen Anspruch, unabhängig zu bleiben und sich nicht von Regierungsparteien einnehmen zu lassen (vgl. DVD e.V. 2006: 2), zum anderen aber auch in der Absicht, allen staatsnahen Akteuren kritisch gegenüber zu stehen und ihre Arbeit zu kontrollieren, da auch der Staat ein Interesse daran hat, personenbezogene Daten zu sammeln und auszuwerten.

Opportunities: Zwischen der Selbst- und der Fremdwahrnehmung der DVD besteht ein interessantes Paradoxon: Auf der einen Seite versteht sich die Organisation als wichtige oppositionelle Kraft und steht der „hilflos bis devot agierenden politischen Klasse“ (Schuler 2014: 34) eher skeptisch gegenüber, gleichzeitig bildet die Lobbyarbeit bei eben dieser politischen Klasse einen zentralen Baustein der Verbandsarbeit. So ist die Vorsitzende des Vereins Karin Schuler Sachverständige für IT-Produkte beim Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (Schuler 2014: 36) und damit durchaus involviert in die Arbeit dieser als staatsnah einzustufenden Behörde. Auch sind Parteien und Ministerien immer wieder Auftraggeber der DVD, indem sie Stellungnahmen und Gutachten anfordern. Eine durchgehend kritische Distanz zu den staatsnahen oder staatlichen Institutionen könnte sich daher nachteilig darauf auswirken, welche Aufträge an den Verband herangetragen werden. Auch könnte ein Interessenkonflikt zwischen den Zielen der Organisationen und der Erwartung an die Zusammenarbeit mit Behörden oder Parteien ergeben. Ob und wie sich in diesem Kontext die immer wieder betonte Unabhängigkeit und das durchweg kritische Image glaubwürdig aufrechterhalten lässt, scheint zumindest fragwürdig. Nichtsdestotrotz kann in diesem Kontext festgehalten werden, dass die DVD zum einen aufgrund ihres langjährigen Bestehens, zum anderen aber auch aufgrund der hohen Expertise als etablierter Akteur der Datenschutzpolitik gelten kann und von staatlicher Seite durchaus anerkannt wird.

Die Deutsche Vereinigung für Datenschutz ist eine relativ kleine Organisation, die jedoch Kontinuität beweisen konnte und zu einem festen Bestandteil der deutschen

Datenschutz-Landschaft geworden ist. Vor allem die Professionalität der Aktivist_innen führte zur Anerkennung der qualitativ hochwertigen Arbeit des Verbandes, was sich z. B. in der Sachverständigenposition bei Anhörungen wieder spiegelt.

2) Privatwirtschaftliche Akteure

In diesem Unterkapitel werden die wichtigsten privatwirtschaftlichen Akteure der Datenschutzpolitik betrachtet. Zum einen wird mit Google ein ebenso erfolgreicher wie umstrittener *global player* untersucht, zum anderen werden auch jeweils eine Netzwerkorganisation und ein Branchenverband behandelt, um eine organisatorische Bandbreite abzudecken.

a) BITKOM

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) ist der größte deutsche Dachverband der IT-Branche und vertritt nach eigenen Angaben 90% der am Markt agierenden Unternehmen. Aus diesem Grund versteht sich BITKOM als „Sprachrohr der IT-, Kommunikations- und Neue-Medien-Branche“ (vgl. BITKOM e.V.) und kann als zentraler Akteur für den Diskurs um Datenschutz, Datensicherheit und Datenverwertung gelten.

Organisation: Der Branchenverband hat nach eigenen Angaben derzeit etwa 1400 Mitgliedsunternehmen, deren Interessen der Verband gegenüber Dritten vertritt. Natürlichen Personen kann durch das Präsidium eine Mitgliedschaft im BITKOM verliehen werden, die jedoch das Wahl- und Stimmrecht ausschließt. Dieses Privileg bleibt allein Mitgliedsunternehmen vorbehalten. Eines der wichtigsten Organe ist der Hauptvorstand: Er wird von der Mitgliederversammlung auf zwei Jahre gewählt und übt seine Tätigkeiten ehrenamtlich aus. Derzeit haben 19 Vertreter_innen des Verbandes dieses Amt inne. Das Präsidium besteht aus 15 Personen, wird durch den Hauptvorstand gewählt und ist für die Ausgestaltung der inhaltlichen Ausrichtung des Verbandes zuständig. Die Geschäftsführung schließlich ist für die Ausführung des Tagesgeschäftes zuständig und arbeitet hauptamtlich auf Weisung des Präsidiums (vgl. BITKOM e.V. 2013a: 6-11).

Neben der zentralen Organisationsstruktur gibt es eine regionale Vernetzung in sechs Bundesländern, die sich schlicht Netzwerke nennen und jeweils eigene Landessprecher wählen. Die inhaltliche Arbeit und Positionierungen des Verbandes gegenüber Dritten werden vor allem in den vielen Arbeitskreisen geleistet, in denen sich die Vertreter_innen der Mitgliedsunternehmen engagieren und mit Nicht-Mitgliedern austauschen können (vgl. ebd.: 11f.).

Belief Systems: BITKOM versteht sich als Dienstleister für privatwirtschaftliche Unternehmen, die in der IT-Branche tätig sind. Datenschutz spielt insofern eine maßgebliche Rolle, als dass dieser als volkswirtschaftlich relevant eingestuft wird und Einfluss auf das Vertrauen von Konsument_innen in IK-Technologien nimmt. Ein Verlust dieses Vertrauens wird als problematisch eingestuft, weil er Wachstum bremst, Innovation hemmt oder dazu führt, dass „die Potentiale neuer Technologien nicht umfassend erschlossen werden“ (BITKOM e.V. 2013b : 1). In seinem Positionspapier kritisiert der Verband außerdem die Ausspähung durch ausländische Geheimdienste sowie all jene Maßnahmen, die „die informationelle Selbstbestimmung verletzen oder der Wirtschaftsspionage dienen, die Vertrauen in neue Technologien beschädigen, die unverhältnismäßig sind oder gar gegen geltendes Recht verstoßen“ (ebd.).

BITKOM hat zum Datenschutz ebenfalls in Bezug auf das geplante und sehr umstrittene Freihandelsabkommen mit dem Namen Transatlantic Trade and Investment Partnership (TTIP) Stellung bezogen und spricht sich an den Stellen für eine Selbstregulierung aus, wo die Differenzen in den unterschiedlichen Datenschutz-traditionen unüberbrückbar erscheinen: „Dort, wo die Datenschutz-Regimes als Ganzes nicht so weit angepasst werden können, dass der Datenschutz-Standard generell gegenseitig als angemessen anerkannt werden kann, können Selbstregulierungsmechanismen das erforderliche Niveau schaffen, soweit hiermit vergleichbare Schutzstandards etabliert werden“ (ebd.: 8). Selbstregulierung kann hier also als *secondary aspect* verstanden werden, wie Datenschutz aus der Sicht des Verbandes am effektivsten erreicht werden könnte.

Zu den Mitgliedern des Verbandes zählen auch Unternehmen wie die deutschen Dependancen von Facebook, Microsoft und Google. Diese Schwergewichte des Internetmarktes sind in den letzten Jahren von Datenschützer_innen regelmäßig

kritisiert worden, weil sie ihre Datenschutzrichtlinien immer weiter aufgeweicht haben und sich durch unzuverlässige Datenschutzpraktiken sowie den Verkauf personenbezogener Daten hervortaten. Vor diesem Hintergrund ist die Selbsteinschätzung von BITKOM interessant, die Mitglieder seien stets an seriöser Datennutzung interessiert:

„Die Unternehmen der Netzwirtschaft haben keinerlei Interesse daran, sich an der Ausspähung ihrer Kunden oder anderer Internetnutzer zu beteiligen. Die Unternehmen haben das alleinige Interesse, ihren Kunden sichere und hoch vertrauenswürdige Dienste anbieten zu können. Dabei sind sie bestrebt, den Schutz von Daten und Kommunikation und die Unversehrtheit der Privatsphäre jederzeit sicherzustellen und Angriffe und Zugriffe von außen zu verhindern“ (ebd.: 2).

An dieser Stelle wird deutlich, dass BITKOM staatliche Überwachung als Bedrohung erkennt, der es entgegenzuwirken gilt. Die subjektiven Auswirkungen auf das Individuum durch wirtschaftliche Datenerhebung und –auswertung sowie Speicherung auf unbestimmte Zeit erscheinen nach dieser Konzeption als unbedenklich und der „Unversehrtheit der Privatsphäre“ (ebd.) nicht entgegenzustehen; zumindest äußert sich der Verband zu diesen Fragen in seinem Positionspapier nicht.

Zeit: Gegründet wurde BITKOM 1999 in Berlin (vgl. Betz/ Kübler 2013: 94) und arbeitet seitdem kontinuierlich daran, die politischen, wirtschaftlichen und gesetzlichen Rahmenbedingungen für die Internetbranche zu verbessern und ein günstiges Marktumfeld zu schaffen.

Ressourcenmobilisierung: BITKOM kann anders als die zivilgesellschaftlichen Verbände auf deutlich höhere finanzielle Ressourcen zurückgreifen: Da der Verband für sich in Anspruch nimmt, eine breite Palette an Dienstleistungen für die Mitglieder anzubieten und diese Mitglieder in erster Linie Unternehmen und nicht natürliche Personen sind, liegen deren Beiträge deutlich höher als bei anderen Akteuren. Die genaue Höhe ist auch gestaffelt nach Unternehmensdaten, sodass größere Firmen einen höheren Betrag zahlen als kleinere oder sehr junge Unternehmen. Als größter Branchenverband ist BITKOM e.V. ein hochprofessionell agierender Akteur, der ein hohes Maß an wirtschaftlicher und technischer Expertise aufweisen kann, die sich aus den Mitgliedsunternehmen speist. Diese Professionalität wird durch die haupt-

amtliche Mitarbeiter_innenstruktur weiter ausgebaut und unterstützt, da erworbene Kompetenzen der Mitarbeiter_innen über einen längeren Zeitraum in dem Verband bleiben und die Expertise kontinuierlich erhöhen.

Collective Action: Den Begriff der *collective action* auf einen Wirtschaftsverband anzuwenden, gestaltet sich nicht ganz einfach. Vielmehr ist in diesem Fall davon auszugehen, dass BITKOM seinen Mitgliedern Lobbying als Dienstleistung anbietet und darüber mit ihnen interagiert. Kollektive und aggregierte Handlungen größerer Entitäten innerhalb der Gruppe finden in diesem Kontext nicht statt, weshalb in diesem Unterkapitel auf die Leistungen eingegangen wird, die der Branchenverband in Bezug auf die Datenschutzpolitik erbringt.

Zu den wohl wichtigsten Instrumenten des Verbandes gehören die Stellungnahmen und Positionspapiere, die den Zweck erfüllen sollen, politische Entscheidungsprozesse zugunsten von BITKOM zu beeinflussen und dadurch bessere Rahmenbedingungen für die Mitgliedsfirmen zu schaffen. Auch hat das Unternehmen ein Instrument entwickelt, um via E-Learning Grundkenntnisse zum Datenschutz zu vermitteln. Dieses Angebot richtet sich sowohl an Privatpersonen als auch an Angestellte in Unternehmen, die zum Thema Datenschutz sensibilisiert werden sollen. Dabei werden die Vorteile von Datenprofilen für User hervorgehoben, kritische Statements und Fürsprache für mehr Anonymität beim Einkauf finden sich darin aber kaum (vgl. BITKOM e.V. a).

Einmal jährlich veranstaltet der Verband den sogenannten Trendkongress, auf dem die wichtigsten Entwicklungen und Innovationen sowie marktrelevante Themenkomplexe dargestellt und diskutiert werden. Auf der Liste der Speaker finden sich auch Politiker_innen wie z. B. die Bundesministerin für Bildung und Forschung Johanna Wanka (vgl. BITKOM Trend Kongress 2014).

Advocacy Coalition: Ähnlich wie beim AK Vorrat ist es auch bei BITKOM nicht unproblematisch, von *advocacy coalitions* zu sprechen, da der Branchenverband naturgemäß selbst als *advocacy coalition* fungiert. Trotzdem lassen sich auch Koalitionen finden, die der Verband eingeht, um seinen Einfluss zu erhöhen. Dazu gehört zum einen der Bundesverband der Deutschen Industrie e.V. (BDI), der wohl einflussreichste Wirtschafts- und Arbeitgeberverband der Bundesrepublik (vgl. BDI e.V.). Besonders relevant für die Datenschutzpolitik ist die Vernetzung von BITKOM

mit SRIW (Selbstregulierung Informationswirtschaft e.V.), einem Verband, der Daten- und Verbraucher_innenschutz dadurch anstrebt, dass freiwillige Selbstverpflichtungen der Internetwirtschaft formuliert und umgesetzt werden können. Dadurch ließen „sich viele Herausforderungen der Onlinewelt schnell und pragmatisch angehen. Schneller als es zum Beispiel der Gesetzgeber realisieren könnte“ (vgl. SRIW e.V. 2014a).

Opportunities: „Politik gehört zum Kerngeschäft von BITKOM. Dabei setzt BITKOM auf eine sachorientierte, vertrauensvolle Zusammenarbeit mit der Bundesregierung, Ministerien, Parlament und Parteien“ (vgl. BITKOM e.V. b). Aus dieser Aussage wird deutlich, dass der Branchenverband gute Kontakte zu politischen Entscheidungsträger_innen pflegt und aktiv in die Ausgestaltung von gesetzlichen Regulierungen involviert ist. Dieter Kempf, der Präsident von BITKOM steht zusammen mit Bundeswirtschaftsminister Sigmar Gabriel der Arbeitsgruppe 1 „Digitale Wirtschaft in Deutschland“ des sog. „Nationalen IT-Gipfels“ vor und pflegt somit Kontakte in höchste Regierungskreise. An dieser Schnittstelle zwischen Industrie und Politik sollen „Ziele und Maßnahmen der neuen Digitalen Agenda 2014-2017 der Bundesregierung“ (BMWi, 2014a) diskutiert und beraten werden. Fragen des Datenschutzes hingegen fallen nicht in diese Arbeitsgruppe, und werden in einer anderen Arbeitsgruppe adressiert, an der BITKOM nicht direkt beteiligt ist. Der Vizepräsident von BITKOM, Ulrich Dietz, ist darüber hinaus Mitglied im Beirat „Junge Digitale Wirtschaft“, welcher Bundesminister Gabriel in „Fragen der Informations- und Kommunikationswirtschaft, insbesondere zur Entwicklung und zu den Potenzialen der jungen digitalen Wirtschaft und neuer digitaler Technologien“ (BMWi 2014b) berät.

b) Google

Mit der Bearbeitung von über 90% aller Suchanfragen bei Internetsuchmaschinen in Deutschland ist Google der meistgenutzte Internetdienst und ein netzpolitisch äußerst wichtiger Akteur, da das Unternehmen versucht, die wirtschaftlichen und politischen Rahmenbedingungen zugunsten der eigenen Chancen auf dem IKT-Markt zu beeinflussen.

Organisation: Mit weltweit fast 50.000 Mitarbeiter_innen und 750 Mitarbeiter_innen in Deutschland ist Google einer der einflussreichsten Internetdiensteanbieter der Welt. Der Firmensitz der Google Deutschland GmbH befindet sich in Hamburg. Die Organisationsstruktur ist geprägt von schlanken Hierarchien und einer hohen Durchlässigkeit. Finkle stellt fest: „Ideas were critiqued by your peers not just your managers. At Google, position and hierarchy seldom won an argument“ (Finkle 2011: 880). Ein wichtiger Teil der Unternehmensphilosophie ist demnach, Autoritäten nicht ohne weiteres anzuerkennen, ihnen Widerstand zu leisten und unkonventionelle Wege zu beschreiten. Trotzdem lässt sich auch bei Google ein Mindestmaß an hierarchischen Strukturen feststellen: So hat z. B. Philipp Justus als Managing Director Sales & Operations seit 2013 die Unternehmensleitung inne (vgl. Pimpl 2013). Die vier Geschäftsführer heißen John Herlihy, Graham Law, Lloyd Martin und Kent Walker (vgl. Staufenbiel 2014).

Belief System: Google hat eine sehr ausgeprägte und klar definierte Unternehmensphilosophie, die häufig als durchgehend philanthropisch interpretiert wird: „Google’s mission was not based on money alone; rather it was to improve the world. The heart and soul of Google was based on entrepreneurship and innovation“ (Finkle 2011: 879) Zusammengefasst lautet das Credo: „Geld verdienen, ohne jemandem damit zu schaden“ (google). Bezogen auf Datenschutzpolitik wird schnell deutlich, dass Privatsphäre und der Schutz personenbezogener Daten keinen hohen Wert für Google darstellen. Eric Schmidt, Googles CEO, hat diesen Standpunkt in einem Interview mit folgendem Satz sehr deutlich gemacht: „If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place“ (CNBC on youtube 2009). Hinter dieser Einstellung lässt sich die *Post-Privacy*-Einstellung erkennen, nach der alle Informationen frei und für jede_n zugänglich sein sollten

Zeit: Google wurde am 04.11.1998 von Larry Page und Sergei Brin – dem Klischee des kalifornischen Garagen-Start-Ups entsprechend – in einer Garage in Menlo Park, Kalifornien gegründet (vgl. Finkle 2011: 864-866). Dem Geschäftsmodell liegt der sog. *PageRank*-Algorithmus zugrunde, der eine Priorisierung relevanter Inhalte auf Webseiten erlaubt und kontinuierlich weiterentwickelt wurde (vgl. Manne/ Wright 2011: 193). Seit 2004 ist das Unternehmen als Aktiengesellschaft an der Technik-

börse NASDAQ in den USA notiert und konnte seit der Unternehmensgründung kontinuierlich wachsen sowie jährlich steigende Umsätze und Gewinne verzeichnen. Eine weitere Kontinuität besteht in der permanenten Innovation der Produktpalette, die weit über den reinen Anzeigenverkauf bei Suchanfragen hinausgeht: Google hat im Bereich der Hardware-Produktion investiert und ist zu einem der größten Hardware-Hersteller geworden. Dabei werden die Produkte jedoch nicht auf dem Markt gehandelt, sie werden lediglich hergestellt, um die eigenen Rechenzentren zu betreiben (vgl. McMillan 2012). Wie hoch das Produktionsvolumen für Google wirklich ist, legt der Konzern jedoch nicht offen.

Ressourcenmobilisierung: Die wohl entscheidendste Ressource für Google ist der Umsatz und daraus resultierend auch der Unternehmensgewinn. Der Umsatz lag 2013 weltweit bei knapp 60 Mrd. US-Dollar (statista 2014a) und der Gewinn bei 12,92 Mrd. US-Dollar, (statista 2014b) was etwa 21,5% des Umsatzes entspricht. Für Deutschland liegen lediglich die Daten des Geschäftsjahres 2012 vor. Demnach erwirtschaftete Google Germany einen Umsatz von 202,8 Mio. EUR und einen Nettogewinn von 10,6 Mio. EUR. Dies sind lediglich 5,2% des Umsatzes (vgl. Bundesanzeiger 2013). Laut Süddeutscher Zeitung hat das Unternehmen Google Inc. (der Konzern, zu dem auch die Google Deutschland GmbH gehört) Finanzreserven von 34,5 Milliarden Dollar in Steueroasen angelegt (Brinkmann 2014). Die Monopolstellung des Unternehmens scheint sich zunehmend zu stabilisieren: In Deutschland entfallen 90% aller Suchanfragen auf diese Suchmaschine (Martin-Jung 2014). Aus diesem Grund gibt es seitens der EU-Wettbewerbskommission Bestrebungen, dem Konzern Beschränkungen aufzuerlegen, die seine derzeitige marktdominierende Stellung begrenzen sollen (Busse 2014). Anderen Unternehmen, die bei Google werben möchten, stellt das Unternehmen eine Reihe von Analysetools zur Verfügung, um die bestmöglichen Einstellungen für das Schalten der Werbung zu wählen. Diese Unternehmen zahlen schließlich nicht pauschal an Google, sondern erst ab dem Moment, wo User auf den Link klicken.

Neben dem monetären Gewinn setzt das Unternehmen vor allem auf Innovation und Expertise. Deshalb ist es unerlässlich, hochprofessionelle Entwickler_innen einzustellen und zu beschäftigen, die diese Innovation vorantreiben und neue Projekte realisieren. Um dies zu gewährleisten, arbeiten die Mitarbeiter_innen zu 80% ihrer

Zeit an der Produktentwicklung, in der Regel in Dreier-Teams mit klar verteilten Rollen. Die restlichen 20% der Arbeitszeit sollen dafür aufgewendet werden, eigene, individuelle Projekte zu entwickeln und auszuarbeiten (vgl. Finkle 2011: 882). Diese Arbeitsatmosphäre soll Kreativität und Leistungsbereitschaft fördern. David A. Vise hat dies wie folgt formuliert: „It's a graduate school campus on steroids that aims to stimulate creativity and teamwork by eliminating the distinction between work and play“ (Vise 2006: 23).

Collective Action: Ähnlich wie auch bei BITKOM stellt sich für den Akteur Google die Frage, ob der Begriff der *collective action*, der von Tilly stark auf Soziale Bewegungen bezogen worden ist, auf ein Wirtschaftsunternehmen angewendet werden kann. Fest steht jedoch: Google agiert schon lange nicht mehr allein in seiner Rolle als Wirtschaftsunternehmen, sondern versucht mit politischen Mitteln, seine hervorgehobene Stellung auf dem Markt beizubehalten und auszubauen (vgl. z. B. Betz/ Kübler 2013: 53). Längst beschränkt sich das Unternehmen nicht mehr auf den Betrieb einer Suchmaschine, sondern hat seine Produktpalette ausgeweitet und sehr heterogen und vielfältig aufgestellt. E-Mail-Dienste, das Android-Betriebssystem für Handys und Tablets sowie die größte Videoplattform YouTube gehören mittlerweile zum Kerngeschäft und werden konsequent weiterentwickelt. Das soziale Netzwerk Google+ stellt die größte Alternative zu Facebook dar (vgl. statista 2014c). Wie genau personenbezogene Daten aggregiert und nach welchen Algorithmen sie ausgewertet werden, wem sie zur Verfügung gestellt werden, all das gibt Google nicht preis. Das Geschäftsmodell von Google besteht aus personalisierter Werbung, sie ist das Rückgrat des Unternehmens. Dementsprechend speichert Google alle durch die Nutzung der Dienste anfallenden und damit automatisch zur Verfügung gestellten Daten der User, auch Metadaten wie Ort und Uhrzeit, um aus diesen Personenprofile zu erstellen und dazu passende Werbeeinblendungen zu schalten.

Gleichzeitig erregt Google schon seit einigen Monaten Aufsehen und Unbehagen aufgrund seiner stetig wachsenden Marktmacht und kann als Paradebeispiel für undurchsichtige Datenverarbeitung gelten. Dabei folgt das Unternehmen einer einfachen Verwertungslogik, die wie folgt zusammengefasst werden kann:

„Die Nutzung von Plattformen und Internetdiensten ist die Leistung, die Google anbietet. Die Daten, die der Nutzer bei Google hinterlässt, sind die Gegenleistung. Über die Auswertung der Daten und personalisierte Werbung erwirtschaftet Google die Umsätze, die für den erfolg- (und gewinn)reichen Betrieb der Dienste benötigt werden“ (vgl. Härting/ Schneider 2011: 233).

Kritisiert wird an Googles Geschäftspraxis, dass durch die Ausgabe der mit Algorithmen gefundenen Antworten auf Suchanfragen *filter bubbles* entstehen, innerhalb derer nur kleine Ausschnitte der Informationen präsentiert werden. Die richtige Information ist demnach diejenige, die andere Nutzer_innen mit einem ähnlichen Profil interessierte. Durch das Ranking entsteht eine Priorisierung, die für die User nicht nachvollziehbar ist, ihnen aber als Abstufung einer objektiv richtigen Antwort suggeriert wird. Das Resultat besteht in den „Vermischungen von Werbung und Information, Marktmacht und Profit“ (Betz/ Kübler 2013: 61).

Nun hat der Europäische Gerichtshof im Mai 2014 beschlossen, dass Ergebnisse von Suchanfragen durch Google gelöscht werden müssen, wenn sie bestimmte Kriterien erfüllen (vgl. EuGH, Große Kammer 2014). Zwar verschwinden diese Seiten nicht aus dem Netz, es wird jedoch um ein vielfaches schwieriger, sie zu finden, wenn sie nicht als Ergebnis einer Suchanfrage verlinkt werden. Damit wird dem Datenschutz auf europäischer Ebene ein erheblich höherer Stellenwert beigemessen, indem das „Recht auf Vergessen“ oder auch das „digitale Radiergummi“ gesetzlich verankert wird.

Advocacy Coalitions: Aufgrund seiner Position innerhalb des Akteursgefüges geht Google kaum tiefgreifende Kooperationen mit anderen Akteuren ein. Die einzige Ebene, auf der dies passiert, ist die Organisation in wichtigen Branchen- und Dachverbänden wie BITKOM e.V. oder „eco – Verband der Internetwirtschaft e.V.“, um auf diesem Wege aggregierte Interessenspolitik zu betreiben. Trotz der durchaus privilegierten Marktposition sind jedoch keine Vertreter_innen des Unternehmens aktiv in die Leitung und Organisation der Verbände eingebunden. Hervorzuheben ist jedoch, dass Google Germany Gründungsmitglied der Selbstregulierung Internetwirtschaft e.V. (SRIW) ist, welche Regulierungen seitens des Gesetzgebers zugunsten einer freiwilligen Selbstbeschränkung ablehnt (vgl. SRIW e.V. 2014b). Auf dem Markt befindet Google sich in Konkurrenz zu seinen Mitbewerbern – Koopera-

tionen werden auf dieser Ebene nicht eingegangen. Vielmehr ist Google bekannt dafür, vielversprechende Unternehmen mit attraktiven Diensten aufzukaufen und damit vollständig in den eigenen Einflussbereich zu bringen (vgl. Finkle 2011: 871). Google sucht die Nähe zu jungen Unternehmer_innen, StartUp-Unternehmen und der technologischen Forschung. Dazu ist Google auf vielen Fachmessen präsent, schreibt Preise aus und finanziert Projekte, die sich in einer frühen Entwicklungsphase befinden. Dies geschieht jedoch in erster Linie, um die Gewinnchancen durch die Anwerbung der besten Entwickler_innen zu erhöhen: „But, at the very least, Google is putting its money where its mouth is“ (Vise 2006: 23). Bei zivilgesellschaftlichen Gruppen, die digitale Grundrechte, das Recht auf informationelle Selbstbestimmung und mehr Privatsphäre fordern, steht das Unternehmen stark in der Kritik, sodass auch hier keine Kooperation oder inhaltliche Verankerung festgestellt werden kann. Zusammenfassend kann festgestellt werden: Die einzigen Koalitionen die Google eingeht, sind nicht auf *Advocacy* begründet, sondern auf Geschäftsbeziehungen.

Opportunities: Auf staatlicher Seite werden immer wieder Stimmen laut, die der Marktstellung von Google und auch deren Geschäftsmethoden kritisch gegenüber stehen und eine größere Kontrolle des Giganten durchaus begrüßen würden. Dazu gehören die Europäische Kommissarin für Justiz, der Bundeswirtschaftsminister Sigmar Gabriel (SPD) sowie etliche Datenschutzbeauftragte in Deutschland und ganz Europa. Auch hier spielen Unterschiede im Wertesystem und in den kulturellen Gepflogenheiten eine wichtige Rolle: Google verfolgt eine „one-size-fits-all strategy“ (Vise 2006: 24) und kann damit nicht ausreichend auf geographisch unterschiedliche Märkte und tradierte Wertekonzeptionen reagieren. Könnten europäische Standards beim Datenschutz verschärft und auch für Google durchgesetzt werden, entfielen dem Konzern das zugrundeliegende Geschäftsmodell, was mindestens einen schweren ökonomischen Schaden bedeuten würde. Dementsprechend ist es nicht verwunderlich, dass zwischen Datenschützern in Europa und der Unternehmensführung in den USA so große Diskrepanzen bestehen.

c) Initiative D21

Die Initiative D21 e.V. ist insofern ein interessanter Akteur, als dass er als durchaus regierungsnah bezeichnet werden kann und viele Kooperationen mit Behörden und Ministerien eingeht. Zwar versteht sich die Initiative D21 selbst als „Netzwerk für die digitale Gesellschaft“, jedoch sind in erster Linie Vertreter_innen aus der Informations- und Kommunikationswirtschaft in diesem Verband organisiert, andere gesellschaftliche Gruppen sind stark unterrepräsentiert und werden in ihre Arbeit kaum einbezogen.

Organisation: Die Organisationsstruktur der in Berlin ansässigen Initiative D21 gestaltet sich wie folgt: Auf der einen Seite steht das Präsidium, welches als „Lenkungsgremium“ (Initiative D21 a) bezeichnet wird und für die Außendarstellung sowie für die Führung des Alltagsgeschäftes des Verbandes zuständig ist. Darüber hinaus bereitet es die Mitgliederversammlung vor und erstellt den Haushaltsplan für das jeweilige Geschäftsjahr (vgl. Initiative D21 2008: 8). Momentan hat der Geschäftsführer der Intel GmbH, Hannes Schwaderer, das Amt des Präsidenten inne; Robert A. Wieland ist Vizepräsident der Initiative und Geschäftsführer des Marktforschungsinstituts TNS Infratest. Legitimiert wird das Präsidium mit der Ernennung durch den Gesamtvorstand, der seinerseits für die Amtszeit von zwei Jahren von der Mitgliederversammlung gewählt wird. Zu den Aufgaben des Gesamtvorstandes zählen „Projektorganisation“, die Ausarbeitung von „Strategiefragen“ sowie die Umsetzung der „Beschlüsse der Mitgliederversammlung“ (Initiative D21 a). Alle Inhaber_innen dieser Ämter sind ehrenamtlich in dem Verein tätig, lediglich die Geschäftsführung besteht aus hauptamtlichen Mitarbeiter_innen, die die Koordinationsarbeit des Vereines leisten. Hervorzuheben ist in diesem Zusammenhang, dass von fünf Personen, die in der Geschäftsführung tätig sind, vier weiblich sind, was gerade für den männlich dominierten IKT-Bereich als Ausnahme gelten kann.

Die in der Initiative organisierten Unternehmen und Institutionen teilen sich auf in reguläre Mitglieder, Förderer sowie „Politische Partner“, also Behörden, Ministerien und Parteien. Dabei gehört beinahe die Hälfte aller Mitglieder (48%) der IKT-Branche an, lediglich 9% lassen sich im zivilgesellschaftlichen Bereich verorten (vgl. Initiative D21 b). Die enge Verbindung zwischen wirtschaftlichen und privaten

Akteuren stellt den wichtigsten Markenkern dieser Organisation dar. Der Verband wird zentral gesteuert, für die Mitglieder gibt es keine nach regionalen Kriterien festgelegten Arbeitsgruppen, die eine direkte Mitarbeit ermöglichen würden.

Belief Systems: Als *near policy core* kann die Vorstellung beschrieben werden, dass eine zunehmende Digitalisierung der Bevölkerung Deutschlands eine der größten und wichtigsten Herausforderungen der nächsten Jahre darstellt. Gleichzeitig werden die Relevanz dieser Entwicklung und die daraus resultierenden Effekte wie wirtschaftliches Wachstum und zukunftsfähige Arbeitsplätze betont. Dementsprechend wird in der Satzung des Vereins festgehalten: „Zweck des Vereins sind die Weckung und Förderung des Interesses und der Bereitschaft für den Wandel zur Informations- und Wissensgesellschaft in Politik, Wirtschaft, öffentlichen Einrichtungen sowie in der Allgemeinheit“ (Initiative D21 2008: 1). Dabei, so wird ganz deutlich betont, spielt auch der Datenschutz eine maßgebliche Rolle. So wird das Ergreifen von „Maßnahmen zur Erhöhung des Verbraucherschutzes hinsichtlich der Datensicherheit im Internet“ (Initiative D21 2008: 2) als eines der wichtigsten Ziele des Vereines formuliert. Gleichzeitig fordert der Verband nicht pauschal strengere Gesetze oder eine konsequentere Verfolgung bei Missachtung der bestehenden Gesetze, sondern setzt auf Selbstregulierung und betont die wirtschaftlichen Vorteile, die sich durch vertrauenswürdige Onlineprodukte ergeben. Auch sollten die User ihren Datenschutz selbst in die Hand nehmen und vorsichtig mit der Veröffentlichung privater Informationen umgehen (vgl. Initiative D21 e.V./ Bayerisches Staatsministerium der Justiz und für Verbraucherschutz).

Demnach kann ein konsequenter Datenschutz zwar als *near policy core* gelten, gleichzeitig werden jedoch auch die *secondary aspects* augenscheinlich, mit denen dieser *near policy core* erreicht werden soll: Nicht durch stärkere staatliche Regulierung, sondern durch den Markt, innerhalb der IKT-Branche, auf freiwilliger Basis und damit weit weniger institutionalisiert. Auch werden durch die Broschüren der Organisation Ratschläge gegeben, wie persönliche Daten besser geschützt werden können. In keinem Satz wird jedoch auf die PET-Methoden hingewiesen, die eine wirkliche Anonymität herstellen. Auch wird mit keinem Wort auf die Gefahren für den Datenschutz seitens staatlicher Geheimdienste und Ermittlungsbehörden hingewiesen.

Zeit: Die Initiative D21 wurde 1999 gegründet, mit dem Ziel „die digitale Spaltung in Deutschland zu verhindern“ (Initiative D21 b). Bereits zwei Jahre später, im Jahr 2001, wurde mit dem (N)ONLINER Atlas die erste Studie zum Internetnutzungsverhalten des Verbandes veröffentlicht. Seitdem wird sie jedes Jahr durchgeführt und in einer aktualisierten Form veröffentlicht. Die Vereinsgeschichte ist von einer Kontinuität geprägt, die schließlich auch zur Folge hat, dass die Initiative als verlässliche Partnerin seitens politischer Entscheidungsträger wahrgenommen wird.

Ressourcenmobilisierung: Finanziell getragen wird die Organisation durch die Beiträge ihrer Mitglieder. Wie hoch die monetären Ressourcen sind, kann öffentlich nicht eingesehen werden, sodass an dieser Stelle darüber keine gesicherten Informationen existieren. Hervorzuheben ist dennoch, dass ähnlich wie bei anderen wirtschaftspolitisch ausgerichteten Organisationen ein hoher Professionalisierungsgrad der Aktiven festgestellt werden kann. Neben der hauptamtlichen Geschäftsführung sind auch das Präsidium und der Gesamtvorstand mit hochrangigen Verantwortlichen der Internetwirtschaft besetzt, sodass die Ressource „Expertise“ als sehr hoch eingeschätzt werden kann.

Advocacy Coalitions: Die Initiative D21 lässt sich als Bündnis sehr verschiedener netzpolitischer Akteure verstehen, dementsprechend kann die Einordnung in ein größeres System als *advocacy coalition* zweiten Grades erfolgen. Ganz offen wirbt der Verband damit, seine Mitglieder direkt mit wichtigen Akteuren aus Politik und Wirtschaft in Kontakt zu bringen und dadurch „Networking“ zu ermöglichen (ebd.). Diese Nähe zu öffentlichen Institutionen wird in nahezu allen Publikationen des Verbandes deutlich. Alle kooperierenden Partner aufzuzählen, wäre weder zielführend noch notwendig. Es sei jedoch darauf hingewiesen, dass bei nahezu allen Veranstaltungen und Publikationen Bundes- und Landesbehörden, Staatssekretär_innen oder Minister_innen involviert sind und in die Arbeit des Verbandes einbezogen werden (vgl. z. B. die gemeinsame Publikation des (N)ONLINER Atlas mit dem Bayerischen Staatsministerium für Justiz und Verbraucherschutz).

Collective Action: Regelmäßig veröffentlicht die Initiative wissenschaftliche Studien über das Internetnutzungsverhalten der deutschen Bevölkerung. Dazu zählen z. B. der (N)ONLINER-Atlas sowie der Digital Index, in denen Kennzahlen ausgearbeitet wurden, die eine Beurteilung des Nutzungsverhaltens aufgrund von qualitativ

durchgeführten, repräsentativen Interviews ermöglichen (vgl. Initiative D21 2013: 28f.). Daraus werden in einem zweiten Schritt Empfehlungen für politische Entscheidungsträger_innen abgeleitet und an diese adressiert. Dem liegt die oben erläuterte Annahme zugrunde, dass eine verstärkte Internetnutzung aller Mitglieder einer Gesellschaft eben jener zuträglich ist und staatlich gefördert werden sollte.

Bildung ist eines der zentralen Betätigungsfelder dieses Akteurs, was dazu führt, dass die Initiative D21 bei bildungspolitischen Veranstaltungen in Erscheinung tritt. Dazu versucht der Verband, mit Lehrer_innen, Pädagog_innen und Vertreter_innen der Wissenschaft in Kontakt zu treten und Impulse für stärkeres digitales Lernen zu geben. Eine Analyse der Veröffentlichungen der bildungspolitischen Veranstaltungen zeigt jedoch, dass viele Themen stark hardware-basiert diskutiert werden. Medienkompetenz als Fähigkeit, mit den eigenen Daten souverän umzugehen, spielt auf den Veranstaltungen der Initiative kaum eine Rolle.

Opportunities: Die sehr starke institutionelle und auch personelle Nähe der Initiative zu staatlichen Akteuren ist bei diesem Akteur besonders augenscheinlich. Dementsprechend wird auf der Homepage der Organisation auch mit den „politischen Partnern“ geworben: Es ist ein essentieller Bestandteil der Verbandsphilosophie und eines der wichtigsten Ziele, Einfluss auf politische Entscheidungsprozesse im Interesse des Verbandes zu nehmen. Konsequenterweise bestehen enge Kooperationen mit Ministerien und staatlichen Institutionen, sodass von einer ausgeprägten *facilitation* von staatlicher Seite gesprochen werden kann, was die Mobilisierungskosten für den Verband deutlich senkt, da sie diese auf staatliche Infrastrukturen zurückgreifen können.

3) Blogger_innen und Netzjournalismus

Hinter der Einbeziehung von Onlineberichterstattung als nichtstaatliche Akteure in der Datenschutzpolitik steckt die Annahme, dass auch journalistische Beiträge zu der Meinungsbildung in der Öffentlichkeit beitragen und damit eine nicht unerhebliche Rolle für die Ausgestaltung der Netzpolitik und die Lenkung des öffentlichen Diskurses einnehmen. Diese technikaffinen Blogs und Netzzeitungen liefern Argumente, Informationen und Zusammenhänge, die Aktivist_innen wiederum für ihre politische Arbeit nutzen können. Die Form der Medien ist geprägt durch eine starke Interaktivität und die Nutzung diverser Verbreitungs Kanäle. In Foren werden Fragestellungen diskutiert und Meinungen ausgetauscht, via *social media* können die Inhalte schnell verbreitet und damit einer breiten, vernetzten Interessensgruppe zur Verfügung gestellt werden.

Das besondere an Blogs und onlinejournalistischen Informationsquellen ist, dass der *Gatekeeping*-Ansatz, nach dem Redakteure entscheiden, welche Themen relevant genug zur Veröffentlichung sind, teilweise umgangen werden kann (vgl. z. B. Orle 2014). Teilweise deshalb, weil vielerorts Algorithmen anstelle von „menschlichen“ Gatekeepern den Ausschlag dafür geben können, was rezipiert wird und was nicht, da die Suche nach Informationen in vielen Fällen den Umweg über eine Suchmaschine geht. Anders verhält es sich bei Blogs, die eine gewisse Kontinuität und Fixierung der Leser_innen auf persönliche Präferenzen aufweisen und weniger gefährdet sind, in der *filter bubble* unterzugehen. Im Folgenden soll ein kleiner Ausschnitt der Blog- und Journalismuslandschaft mit der Perspektive auf Datenschutzthemen untersucht werden.

a) Netzpolitik.org

Netzpolitik.org ist das wohl wichtigste Blog zu netzpolitischen Themen in Deutschland und wird von vielen Aktivist_innen regelmäßig als Informationsquelle und Diskussionsplattform genutzt. So bewertet Steiner: „das Blog hat sich als erste Anlaufstelle für Digitalpolitik in Deutschland etabliert“ (Steiner 2013: 85).

Organisation: Betrieben wird die Seite netzpolitik.org seit ihrer Gründung von der Agentur newthinking communications GmbH. Einen Großteil der Artikel schreibt der Publizist und Lehrbeauftragte Markus Bechedahl, der ebenfalls Mitarbeiter bei Newthinking ist (vgl. Newthinking). Lediglich drei Blogger_innen sind hauptamtlich für die Abfassung der erscheinenden Artikel zuständig, ein Großteil der Autor_innen (nach eigenen Angaben etwa 30) arbeiten ehrenamtlich für den Blog (vgl. Netzpolitik.org a). Darüber hinaus werden häufig auch Gastbeiträge publiziert, die nicht aus dem personellen Umfeld von netzpolitik.org stammen. Diese Arbeitsstruktur macht es möglich, täglich mehrere Artikel zu netzpolitischen Fragestellungen zu veröffentlichen. Nach eigenen Angaben erreicht der Blog täglich bis zu 40.000 Menschen (vgl. netzpolitik.org b), die Zahl der gelegentlichen Leser_innen dürfte jedoch deutlich höher liegen.

Belief Systems: Die Grundidee hinter dem Blog beschreiben die Betreiber wie folgt:

„netzpolitik.org ist eine Plattform für digitale Freiheitsrechte. Wir thematisieren die wichtigen Fragestellungen rund um Internet, Gesellschaft und Politik und zeigen Wege auf, wie man sich auch selbst mithilfe des Netzes für digitale Freiheiten und Offenheit engagieren kann. [...] Wir verstehen uns als journalistisches Angebot, sind jedoch nicht neutral. Unsere Haltung ist: Wir engagieren uns für digitale Freiheitsrechte und ihre politische Umsetzung“ (netzpolitik.org a).

An dieser Stelle wird deutlich, dass die Betreiber_innen der Homepage keinesfalls eine objektive Berichterstattung für sich beanspruchen, vielmehr erklären sie sich solidarisch mit den Netzaktivist_innen und sprechen sich für eine Gestaltung dieses öffentlichen Raumes durch politisches Engagement und einen öffentlichen Diskurs aus. In diesem Zusammenhang kann auch ein *deep policy pore* identifiziert werden: Freiheit im digitalen Raum. Unter dieser Prämisse wird ein sehr breites Spektrum netzpolitischer Themen bearbeitet. Neben Datenschutz und dem Schutz der Privatsphäre (vor staatlicher und nichtstaatlicher Überwachung) stehen auch Fragen der Internetgovernance, des Umgangs mit Urheberrechten im Netz sowie der Medien- und Internetkultur im Zentrum der journalistischen Tätigkeit des Autorenkollektivs.

Zeit: Gegründet wurde das Blog 2004 von Markus Beckedahl, der bis heute als hauptamtlicher Autor für netzpolitik.org schreibt. Im Laufe der letzten Jahre ist es dem Medium gelungen, stetig zu wachsen und den Leser_innenkreis kontinuierlich auszuweiten. Insgesamt sind nach eigenen Angaben bereits 15.000 Artikel auf dem Blog erschienen. Eine Reihe von Auszeichnungen wie z. B. der Grimme Online Award 2014 würdigen die Arbeit des Blogs (vgl. Grimme Online Award 2014).

Ressourcenmobilisierung: Das Blog hat seine Einnahmen und Ausgaben für das Jahr 2012 im Netz veröffentlicht. Daraus geht hervor, dass netzpolitik.org jährliche Ausgaben von etwa 82.800 EUR hat, die Einnahmen liegen bei lediglich 35.400 EUR (vgl. netzpolitik.org 2013). Letztere generieren sich vor allem aus Werbung, die auf der Seite geschaltet werden kann, Einnahmen aus Veranstaltungen, Workshops und Vorträgen der Autor_innen sowie Mikrospenden von Usern der Seite. Der 2012 fehlende Betrag von 47.400 EUR wird durch die newthinking communications GmbH ausgeglichen, sodass das Unternehmen den Blog faktisch querfinanziert (vgl. ebd). Zwar wird auf die inhaltliche Unabhängigkeit des Blogs von dem Unternehmen hingewiesen, ob diese jedoch in allen Fällen faktisch gegeben ist, kann nicht überprüft werden und sollte zumindest infrage gestellt werden. Leider wurden bisher noch keine Zahlen für das Jahr 2013 veröffentlicht.

Collective Action: Die politische Aktivität des Blogs beschränkt sich auf die Publikation netzpolitischer und –kultureller Artikel. Diese werden ausschließlich online veröffentlicht. Ebenfalls nur digital, nämlich als EBook wurden 2012 und 2013 die Jahrbücher Netzpolitik und 2013 ein Sammelband zu der NSA-Totalüberwachung veröffentlicht.

Advocacy Coalitions: Netzpolitik.org ist für viele Netzaktivist_innen das wichtigste Informationsmedium für netz- und datenschutzpolitische Nachrichten. Dementsprechend werden immer wieder Kooperationen eingegangen, um das gemeinsame Ziel eines freien Internets zu erreichen. Besonders augenscheinlich ist die personelle Verflechtung der Autor_innen des Blogs mit zivilgesellschaftlichen Organisationen und Gruppen, die sich netzpolitisch engagieren, wie dem Chaos Computer Club, den AKs Zensur und Vorrat, der Digitalen Gesellschaft e.V. und vielen weiteren. Viele dieser Akteure werden darüber hinaus insofern unterstützt, als dass sie bereits auf

der Startseite des Blogs verlinkt werden, was den Netzwerkcharakter der Szene offenbart.

Seit einer Großspende des Chaos Computer Clubs an netzpolitik.org im August 2014 in Höhe von 12.000 EUR (netzpolitik.org 2014) kann auch von einer verstärkten finanziellen Verflechtung der Netzgemeinde gesprochen werden. Auch die oben bereits erwähnt newthinking GmbH ist Teil der *advocacy coalition*, womöglich geht die Kooperation auch darüber hinaus.

Opportunities: Als Online-Medium ist der Blog unabhängig von staatlichen Akteuren und deren Einflussnahme. Markus Bechedahl, der Betreiber der Seite wurde jedoch als Sachverständiger in der Enquete-Kommission Internet & Digitale Gesellschaft berufen, wo auf Ebene parlamentarischer Ausschussarbeit Empfehlungen für die künftige Netzpolitik ausgearbeitet werden sollte.

b) Spackeria

„So there can be no self-declared counter-movement to the right for citizens to have control over their private space and their private information. There is no ‘anti-privacy’ movement as there is an ‘anti-abortion’ movement, for example” (Bennett 2012: 413). Anders als bisher angenommen, stimmt diese Behauptung nicht uneingeschränkt: In Deutschland formierte sich eine Gruppe von Menschen, die der Idee von Privatsphäre eine Absage erteilt, sich für mehr Offenheit bei privaten Informationen einsetzt und den Kontrollverlust über private Informationen als Befreiung und einen Schritt zur Emanzipation betrachtet. Die „Spackeria“ ist eine lose organisierte Gemeinschaft, die sich als Anhänger der *Post-Privacy*-Idee versteht. Diese Gruppe wird insofern unter den Bereich des Bloggings bzw. Journalismus eingeordnet, als dass es bisher keine Organisation gibt, die auf ihre strukturellen Merkmale untersucht werden könnte. Vielmehr sind es Einzelpersonen, die in Blogs ihre Ideen diskutieren und Utopien entwickeln, wie eine Gesellschaft ohne Privatsphäre aussehen könnte. Obwohl die Gruppe noch sehr jung ist und dem oben formulierten Anspruch der zeitlichen Kontinuität nicht genügt, ist ihre Analyse aufgrund der kontroversen Position von wissenschaftlichem Interesse und insofern

notwendig, als dass ein wirklich vollkommenes Bild der Positionen in der Datenschutzdebatte nur gezeichnet werden kann, wenn auch die Position von Anhänger_innen der Post-Privacy-Utopie darin Eingang findet.

Organisation: Wie bereits erwähnt, handelt es sich bei der Spackeria um einen losen Zusammenschluss von Personen, die Privatsphäre für ein überholtes Konzept halten, das in einer zukünftigen, freieren Gesellschaft nicht länger notwendig sein wird. Dieser Gruppe liegt keine Organisationsstruktur zugrunde, ebenso wenig wie ein Kanon an gemeinsamen Symbolen oder spezifischen Codes. Stattdessen könne man vielmehr „von einer diffusen Wolke von Leuten sprechen, die ähnliche Gedanken zu dem Thema Privatsphäre haben“ (Seemann 2011). Lediglich über diverse Blogs und andere Soziale Netzwerke wie Twitter und Facebook werden Ideen diskutiert und für eine potenziell interessierte Öffentlichkeit zur Disposition gestellt. Zwar werden laut eigenen Angaben auf netzorientierten Veranstaltungen und Tagungen Vorträge zu *post privacy* gehalten, dies scheint jedoch von wenigen individuellen Akteuren umgesetzt zu werden, die nicht besonders stark mit der Gruppe assoziiert werden, sondern aus anderen Kontexten bekannt sind. Es ist nahezu unmöglich festzustellen, wie viele Menschen in der Gruppe aktiv sind, geschweige denn die Anzahl an Sympathisant_innen und Anhänger_innen zu identifizieren.

Die Namensgebung rekurriert auf eine Aussage der CCC-Sprecherin Konstanze Kurz bei dem Chaos Communication Congress 2010, als sie die Bezeichnung „Post-Privacy-Spackos“ gebrauchte, um Anhänger_innen dieser Denkrichtung zu benennen. Die datenschutzkritische Spackeria übernahm die Bezeichnung, deutete sie für die eigenen Namensgebung positiv um und versteht sich seitdem als Vereinigung der „Spackessen und Spackos“ (vgl. Spackeria).

Belief Systems: Anhänger_innen der *Post-Privacy*-Bewegung gehen davon aus, dass es im Informationszeitalter nicht länger möglich sein wird, private Informationen, die Dritten bekannt sind, vor einer Veröffentlichung in z. B. Sozialen Netzwerken zu schützen. Vielmehr sollte ein gesellschaftlicher Umgang angestrebt werden, in dem Toleranz herrscht und niemand aufgrund privater Informationen diskriminiert wird. Frei nach dem Motto „Let personal data flow and punish abusement“ (Schramm 2011a), wird nicht grundsätzlich die Nutzung von personenbezogenen Daten kritisiert, sondern all jene Selektions-, Kategorisierungs- und Diskriminierungsprozesse,

die sich aus der Nutzung und Auswertung dieser Informationen ergeben. Bereits heute sei es nicht länger möglich, den Datenfluss durchgängig zu kontrollieren. Dementsprechend sei der Anspruch, einen konsequenten Datenschutz anzustreben, veraltet und werde der informations- und kommunikationstechnischen Realität nicht länger gerecht. So beschreibt Michael Seemann *post privacy* als „die diffuse Feststellung, dass bestimmte Vorstellungen und Forderungen aus der analogen Welt nicht mehr so recht in die digitale passen und dass eben Redebedarf besteht“ (Seemann 2011a). Darüber hinaus könne Privatsphäre als Schutzraum gegen staatliche und wirtschaftliche Übergriffe verstanden werden. Würden diese nicht länger existieren, wäre damit auch die Notwendigkeit der Privatsphäre obsolet (vgl. Schramm 2011b). Ein wichtiger Teilaspekt des Post-Privacy-Gedankens ist die kritische Bewertung von Datenschutzbestimmungen und –maßnahmen, da diese den freien Datenfluss stören und dadurch die Freiheit der/des Einzelnen gefährden könnten. Die Anhänger_innen dieser Gruppe bevorzugen eine „Datenliebe statt puritanischer Datensparsamkeit“ (vgl. Seemann 2011b). Es lässt sich festhalten, dass die Post-Privacy-Idee den Grundstein für eine Debatte legte, die die Grenzziehung zwischen Öffentlichkeit und Privatheit im digitalen Zeitalter aufweicht, verschiebt und die Bedingungen dieser Unterscheidung neu definiert.

Zeit: Aus einer zeitlichen Perspektive handelt es sich bei der Spackeria um den jüngsten der bisher untersuchten Akteure. Auch ist die Richtung, in die sich die Gruppierung entwickelt, ungewiss, denn bisher lässt sich keine Kontinuität in der Arbeit feststellen. Gegründet hat sich die Gruppe im Februar 2011 mit dem Ziel, einen datenschutzkritischen Blog zu erstellen, in dem die Schwierigkeiten derzeitiger Datenschutzpolitik formuliert und zur Diskussion gestellt werden sollten. Nach einer sehr aktiven Phase, in der viele Blogbeiträge verfasst sowie kommentiert wurden und die Medien sich mit der Gruppe auseinandersetzten und Interviews mit Aktivist_innen führten, lässt sich seit dem Sommer 2013 nach nur zwei Jahren eine Phase der Stagnation feststellen. Sowohl die Medien als auch die Aktiven selbst scheinen das Interesse an dem Blog zu verlieren, nur noch sehr sporadisch werden Postings veröffentlicht. Die Bedeutung der Privatsphäre sowie deren Schutz gegen ausbeuterische oder repressive Praktiken scheinen im letzten Jahr so stark zugenommen zu haben, dass die Post-Privacy-Idee ihre Relevanz in dem Datenschutzdis-

kurs einbüßte und sich vorläufig nicht als dominante Denkrichtung etablieren konnte.

Ressourcenmobilisierung: Bei der Spackeria handelt es sich nicht um eine institutionalisierte Organisation mit einer Mitgliederstruktur oder –beiträgen. Auch sind für deren Zweck, der Diskussion des Konzeptes Privatsphäre sowie der Maßnahmen zum Schutz ebenjener, keine finanziellen Ressourcen erforderlich, sodass davon ausgegangen werden kann, dass keine nennenswerten Geld- oder Vermögenswerte für die Arbeit der Gruppe akkumuliert worden sind.

Collective Action: Die wohl wichtigste Aktion der Gruppe ist die Veröffentlichung von Artikeln zu Post-Privacy und der Befreiung von Daten. Diesem Zweck dient das Blog der Gruppe. Einige der Autor_innen betreiben auch eigene Blogs, in denen diese Thematik auftaucht, oder halten Vorträge auf Messen und Kongressen der netzpolitischen Szene. Auch auf analogem Wege werden Texte zu *post privacy* veröffentlicht, die sich kritisch mit dem Datenschutzparadigma auseinandersetzen (vgl. z. B. Heller 2014).

Advocacy Coalitions: Aufgrund des sehr eingeschränkten Aktivitätsumfangs ist es für die Gruppe nicht erforderlich, *advocacy coalitions* mit anderen Akteuren einzugehen oder in bestimmten Themenfeldern zu kooperieren, zumal bei der derzeitigen Netzgemeinde kaum organisierte Koalitionäre gäbe, die die datenschutzkritischen Positionen der Spackeria teilen würden. Nichtsdestotrotz lässt sich eine Einbindung in die netzpolitische Szene feststellen: So gibt es z. B. personelle Überschneidungen mit der Piratenpartei, welcher die Mitbegründerin der Spackeria, Julia Schramm, bis März 2014 angehörte. Auch halten einige „spackeria-nahe“ und datenschutzkritische Aktivist_innen Vorträge auf dem Chaos Communication Congress, der Bloggermesse re:publica und Informationsveranstaltungen der Piratenpartei (vgl. z. B. re:publica 2014).

Opportunities: Staatliche Stellen sowie Parteien standen der Spackeria bislang eher indifferent gegenüber. Weder wurden die Positionen der Gruppe als relevant wahrgenommen, noch fand eine Auseinandersetzung mit der Idee von Post-Privacy statt. Dies mag zum einen der Kurzlebigkeit und Diskontinuität dieser Gruppe geschuldet sein, vor allem jedoch dem mangelnden politischen Willen, öffentlich eine Diskussion über den Schutz der Privatsphäre anzustoßen.

c) Sonderfall WikiLeaks

Datenschutzpolitik lässt sich im Jahr 2014 nicht ohne WikiLeaks verstehen. Immer wieder hat die Plattform mit spektakulären Veröffentlichungen von als geheim eingestuftes Dokumenten Schlagzeilen gemacht. Dieser Akteur wird anders als die bisherigen jedoch nicht systematisch untersucht, sondern vielmehr kursorisch und der Vollständigkeit halber beschrieben werden. Der Grund für die ausbleibende Untersuchung anhand der oben festgelegten Kriterien liegt darin begründet, dass diese Kriterien auf nichtstaatliche, auf nationaler Ebene agierende Gruppen ausgelegt sind, was aufgrund der internationalen Ausrichtung auf WikiLeaks nicht zutrifft. Ein weiterer Grund, warum im Rahmen dieser Arbeit nicht systematisch auf WikiLeaks eingegangen wird, liegt darin, dass es unmöglich ist, für die Gruppierung eine personelle Struktur zu identifizieren, da die Menschen, die Dokumente auf der Plattform veröffentlichen, naturgemäß anonym bleiben, um einer möglichen Strafverfolgung zu entgehen. Es gibt demnach keinerlei Struktur, die analysiert werden könnte: Vielmehr handelt es sich um eine lose, spontane Zusammenarbeit von Anhänger_innen der Plattform, die eine hohe Fluktuation und damit eine instabile Dynamik aufweist. Die einzige zugrundeliegende Agenda, der WikiLeaks folgt, ist die Herbeiführung von staatlicher Transparenz und die Veröffentlichung von Informationen für Bürger_innen. Dieser Dualismus aus der Forderung nach staatlicher Transparenz und der daraus resultierenden Ermöglichung öffentlicher Kontrolle der politischen und administrativen Elite bei gleichzeitiger Gewährleistung absoluter Anonymität und Schutz der Quellen ist besonders charakteristisch für die Plattform. Wong und Brown bezeichnen Gruppen wie WikiLeaks oder auch Anonymus als e-bandits und meinen damit Akteure „who capitalize on the Internet and other information technologies to lead disembodied, virtual attacks against physical targets in order to encourage political change“ (Wong/ Brown 2013: 1015). Sie zeichnen sich dadurch aus, dass sie nicht nach monetären Gewinnen streben, sondern einer Ethik folgen, die auf absoluter Informationsfreiheit basiert und dadurch die Entmachtung der Mächtigen anstrebt (ebd.: 1018). Diese Ethik beschreibt WikiLeaks wie folgt:

„The broader principles on which our work is based are the defence of freedom of speech and media publishing, the improvement of our common

historical record and the support of the rights of all people to create new history. We derive these principles from the Universal Declaration of Human Rights" (vgl. WikiLeaks 2011).

Die genutzten Mittel sind Verschlüsselungstechniken, die eine Anonymität der Aktiven bewirkt und diese dadurch schützt. Menschen können in vielen Fällen nur dann dazu bewegt werden, Informationen an WikiLeaks weiterzugeben, wenn sie dadurch keine Repressionen oder Sanktionen erfahren müssen. Das Ergebnis ist eine anarchistische Machtverteilung ohne feste Mitgliedschaften oder Organisationsstruktur:

„It is about getting people involved without giving them faces, names, or even necessarily a position to defend. Rather, the politics of no one allows e-bandits to engage politically through cyberspace, and just as quickly disappear into the digital air" (Wong/ Brown 2013.: 1020).

Seit 2011 werden kaum noch Dokumente auf der Plattform hochgeladen. Trotzdem spielt WikiLeaks insofern eine besondere Rolle für die Datenschutzpolitik, als dass die Plattform seit 2013 Nachrichten zum Überwachungsskandal aggregiert und die Quellen verlinkt. Leser_innen und Twitter-followern wird dadurch die Möglichkeit gegeben, sich systematisch über die journalistische Auswertung der Dokumente von z. B. Edward Snowden sowie anderen Enthüllungen zu informieren.

4) Parteien und staatsnahe Akteure

Der Fokus dieser Masterarbeit liegt explizit bei nichtstaatlichen Akteuren, die die Datenschutzpolitik prägen. Jedoch gibt es Gruppen, die als durchaus staatsnah bezeichnet werden können und gerade in dieser Position eine exponierte Stellung im Diskurs einnehmen. Exemplarisch wird in diesem Unterkapitel zum einen auf die Parteienlandschaft eingegangen, ohne jedoch die Regierungsparteien auf Bundesebene einzubeziehen. Das Ziel der Parteien ist anders als bei bisherigen Akteuren nicht die Beeinflussung politischer Entscheidungsträger_innen oder der öffentlichen Meinung, sondern die Schaffung einer Regierungsposition durch das Erlagen von

Mandaten, sodass sie selbst Entscheidungsprozesse anstreben können, die in ihrem Interesse liegen. Ein Einzug in das Parlament ist dabei zwingend notwendig: „Sofern ihnen der Einzug in die Parlamente nicht gelingt, agieren sie wie eine Aktivistenvereinigung“ (Fritz 2012: 91).

Ebenfalls exemplarisch wird die Arbeit einer der sechzehn Landesdatenschutzbehörden in die Analyse einbeziehen. Sie haben insofern eine Sonderstellung, als dass sie einen besonders institutionalisierten Status genießen und ihre Arbeit gesetzlich reglementiert ist.

a) Piratenpartei

Die Piratenpartei konnte in den letzten Jahren eine große mediale Aufmerksamkeit erlangen und ist Gegenstand politikwissenschaftlicher Forschung geworden, sodass – anders als bei den anderen Akteuren – ein Pool an Forschungstexten vorhanden ist, auf den zurückgegriffen werden kann. Durch ihre netzpolitische Fokussierung und die Akzentuierung des digitalen Raumes hat die Piratenpartei hohe Erwartungen an eine stärkere Modernisierung der Netzpolitik und damit auch das Interesse von Parteien- und Wahlforschern geweckt.

Organisation: Die Piratenpartei Deutschland hat nach eigenen Angaben derzeit 26.071 Mitglieder (vgl. Piratenwiki 2014, Stand am 11.10.2014) und ist in 16 Landesverbände unterteilt. Bayern bildet dabei gefolgt von Nordrhein-Westfalen und Berlin den größten Landesverband. Darüber hinaus lässt sich eine „Untergliederung in Orts-, Kreis-, und Bezirksverbände“ (Niedermayer 2013a: 82) feststellen, die eine Verankerung der Partei auf regionaler Ebene ermöglicht, jedoch noch nicht besonders weit fortgeschritten ist. Die lokalen Treffen werden „Stammtische“ genannt, bei einem informellen Zusammenschluss von Piraten zu kleineren Gruppen spricht man in der Partei von „Crews“ (vgl. ebd.).

Das höchste Gremium der Piraten ist der jährlich stattfindende Bundesparteitag, an dem jedes Mitglied teilnehmen kann. Stimmrecht bekommt es, wenn es die Mitgliedsbeiträge entrichtet hat. Bemerkenswert an dieser Organisation ist, dass die Partei hier dem „Vollversammlungs-, nicht dem Delegiertenprinzip“ (vgl. ebd.: 83) folgt, um dadurch eine stärkere Einbindung und Partizipation der Parteibasis zu

erreichen. Eine weitere Besonderheit stellt der Verzicht auf eine Unvereinbarkeitserklärung dar, die bei anderen Parteien üblich ist. Demnach kann ein Piratenmitglied auch in anderen Parteien Mitglied sein, solange diese den Grundsätzen der Piraten nicht widerspricht (vgl. Piratenpartei 2014: §2, Abs. 2).

Die Piratenpartei hat in lediglich 4 Bundesländern politische Mandate erlangen können: Momentan sind im Landtag Schleswig-Holstein 6 Mitglieder der Piratenpartei vertreten, in Berlin sind es 12. In Nordrhein-Westfalen konnten die Piraten 19 Sitze erlangen und im Saarland besteht die Fraktion aus 4 Piraten (vgl. Landtagspiraten 2014).

Auch auf internationaler Ebene haben sich die Piratenparteien vernetzt: Der 2010 gegründeten Pirate Parties International (PPI) gehören mittlerweile Piratenparteien aus 43 Ländern an (vgl. Pirate Parties International, 2014).

Belief Systems: Wahl- oder Grundsatzprogramme sind sehr geeignet, um in ihnen die wichtigsten Ziele einer der Partei zu identifizieren sowie die innerparteilichen Prioritäten zu erkennen. Auch kann von einer hohen Legitimität der formulierten Aussagen ausgegangen werden, da in aller Regel ein Parteitag das Programm verabschiedete. In dem Wahlprogramm der Piratenpartei aus dem Jahre 2013 wird der Wahrung und dem Schutz des Rechts auf informationelle Selbstbestimmung eine exponierte Stellung eingeräumt. Als erster Punkt in dem Grundsatzprogramm wird der hohe Stellenwert dieses Grundrechts betont, staatliche Überwachung abgelehnt und die Erstellung von Konsumprofilen kritisch bewertet: „Die Piratenpartei Deutschland lehnt die verdachtsunabhängige Durchleuchtung der Bürger und den gläsernen Kunden ab“ (Piratenpartei 2013: 11). Dementsprechend lässt sich „die Stärkung der Rechte des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung personenbezogener Daten zu bestimmen“ (ebd.) als *near policy core* definieren. Um dieses Ziel zu erreichen, soll das Datenschutzgesetz verschärft und ggf. auch über die Europäische Datenschutzrichtlinie hinaus ausgeweitet werden. Ziel sei es, Bürger_innen das Recht zu geben, sowohl durch Behörden als auch durch Unternehmen über die von ihnen gesammelten Daten informiert und von einem Datenabfluss umgehend in Kenntnis gesetzt zu werden. Ähnlich wie der CCC schlägt auch die Piratenpartei dafür einen Datenbrief vor, der Bürger_innen einmal jährlich über die gespeicherten personenbezogenen Daten

informiert (vgl. ebd.: 12). Behörden und Meldeämter sollen nach Ansicht der Piratenpartei keinerlei Informationen mehr an Dritte weitergeben dürfen. Bezüglich staatlicher Überwachung fordern die Piraten, jedwede anlasslose Erfassung und Speicherung von elektronischer Kommunikation zu verbieten und das Brief-, Post- und Fernmeldegeheimnis auf ein allgemeines Kommunikationsgeheimnis auszuweiten, welches digitale Kommunikation einbezieht. Grundsätzlich sollen keine Reise- und biometrische Daten anlasslos und unfreiwillig gesammelt und ausgewertet werden dürfen, da dieser Prozess die „Umkehr der Unschuldsvermutung“ (ebd.: 14) darstelle. Auch verdeckte Zugriffe von Ermittlungsbehörden lehnt die Piratenpartei ab: Weder eine Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), noch den großen Lauschangriff oder Staatstrojaner und Überwachungssoftware sehen sie als legitime Ermittlungsinstrumente an, da nicht zweifelsfrei festgestellt werden kann, welche Daten durch einen Eingriff auf Computersysteme manipuliert werden und damit „die Integrität der gespeicherten Daten [...] nicht mehr gewährleistet“ (ebd.: 16) sei.

Als einer der wichtigsten *near policy cores* kann also formuliert werden, dass der Wert der Privatsphäre als besonders hoch und schützenswert eingestuft wird. Auch solle die Datenmacht der Anbieter von Gütern und Dienstleistungen begrenzt werden: „Persönlichkeitsrechte müssen über dem privatwirtschaftlichen Interesse von Unternehmen stehen“ (ebd.: 13).

Zu den Mitteln, die ergriffen werden müssen, um einen besseren Datenschutz zu erreichen, also den *secondary aspects*, fordern die Piraten die Stärkung der Datenschutzbehörden sowie die Umsetzung der Datenschutzrichtlinie 95/46/EG, die die absolute Unabhängigkeit der Behörden von anderen staatlichen Einrichtungen fordert. Darüber hinaus sollen alle Bürger_innen unentgeltlich und umgehend über die erfassten, verarbeiteten und/oder weitergegebenen Daten informiert werden. Dies gilt auch, wenn Ermittlungsbehörden Kommunikation überwachen und damit das Fernmeldegeheimnis einschränken.

Zeit: Die Piratenpartei Deutschlands ist eine sehr junge Partei und wurde nach dem schwedischen Vorbild im Jahr 2006 in Berlin gegründet (Bartels 2013: 25). Eine breite mediale Aufmerksamkeit sowie größere politische Erfolge konnte die Partei 2009 erzielen, als sie gegen die Pläne der Bundesregierung für Internetsperren (das

sog. Zugangserschwerungsgesetz) mobilisieren und öffentlich wirksam Stellung beziehen konnte (vgl. ebd.). Bereits 2007 waren in 8 Bundesländern Landesverbände gegründet worden; in einer zweiten Gründungswelle nach den überraschend hohen Ergebnissen bei der Bundestags- und der Wahl zum Europäischen Parlament 2009 hatten sich in allen Bundesländern Piraten-Landesverbände gebildet (vgl. Niedermayer 2013a: 82).

Nach den ersten Erfolgen der Jahre 2009 und 2010 jedoch gab es immer wieder interne Streitigkeiten zwischen den Funktionären und Vorstandsmitgliedern, die zu einem erheblichen Vertrauensverlust bei der Anhänger_innenschaft führte und auch die Wahlergebnisse negativ beeinflusste. Seit Mitte 2012 sinken auch die Mitgliederzahlen, was schließlich im September diesen Jahres in einer großen Austrittswelle prominenter Mandatsträger_innen mündete und die Partei personell erheblich schwächte (vgl. z. B. Rzepka 2014).

Ressourcenmobilisierung: Die Ressource „Führungsqualität“ spielt im Kontext der Piratenpartei kaum eine Rolle. Vielmehr werden flache hierarchische Strukturen bevorzugt, die stark an die Parteibasis gekoppelt bleiben und innerhalb derer eigene Entscheidungen nach Möglichkeit in der Breite mit den Mitgliedern abstimmt werden (vgl. Niedermayer 2013: 95). Neben der Mobilisierung von Kapital (monetären Ressourcen), Arbeit (Mitglieder) und technischer Expertise, steht die Partei auch vor der Herausforderung, Wähler_innen zu mobilisieren, um das Ziel, politischen Einfluss zu erlangen, zu erreichen. Eine Untersuchung der Wähler_innen der Piraten hat gezeigt, dass es in erster Linie junge Männer sind, die auf die Partei ansprechen. Sie sind gut ausgebildet, netzaffin und in nahezu allen Berufsgruppen vertreten, lediglich unter den Beamten sind sie deutlich unterrepräsentiert. Auch haben viele Menschen die Partei aus Unzufriedenheit mit den Zielen und Programmen der etablierten Parteien gewählt. Neben der Interpretation, dass es sich um „Protestwähler_innen“ handeln könnte, ist es auch möglich, dass die Stimmen für die Piratenpartei auf eine Unzufriedenheit mit dem Politikstil der anderen Parteien und dem Wunsch nach unkonventionelleren Herangehensweisen hindeuten (vgl. Niedermayer 2013a: 73).

Die monetären Ressourcen der Partei erwachsen zum einen aus den Beiträgen, die die Mitglieder der Partei entrichten, zum anderen aber auch aus den staatlichen

Zuwendungen, die die Partei geltend machen kann, um Wahlkampfkosten zu decken. Die aktuellsten Zahlen über die Einnahmen der Partei beziehen sich auf das Jahr 2011: Da betrug die Höhe der Einnahmen ca. 1,4 Mio. EUR, wobei der Anteil der staatlichen Mittel mit 578.219 EUR bei 41,3% lag. Nach Abzug der Ausgaben konnte für das Jahr 2011 ein Überschuss von 354.529 EUR verbucht werden (vgl. ESC Wirtschaftsprüfungsgesellschaft 2013: 17).

Collective Action: Durch den Parteienstatus der Piraten ist der Charakter ihrer Aktionen gewissermaßen vorgezeichnet: Das Ziel ist die Erlangung politischer Verantwortung in Parlamenten. Dementsprechend beschränkt sich ein Großteil der Aktionen auf Wahlkampfaktivitäten bzw. die Vorbereitung dieser. Da es der Partei für konventionellen „Straßenwahlkampf auch an Erfahrung“ (Niedermeyer 2013, 40) fehle, beteilige sich die Partei verstärkt an Demonstrationen, wie der bereits oben erwähnten „Freiheit statt Angst“-Demonstration, den Protesten gegen das ACTA-Abkommen oder anderen publikumswirksamen Auftritten (vgl. ebd.).

Advocacy Coalitions: Die Piratenpartei hat sehr früh begonnen, sich im Arbeitskreis Vorratsdatenspeicherung zu engagieren (vgl. Niedermeyer 2013 a: 32) und ist damit eine ihrer wichtigsten *advocacy coalitions* eingegangen.

Auch ist sie die einzige Partei, die Datenschutz im digitalen Zeitalter als Markenkern für sich in Anspruch nehmen kann. Zwar hat sie dadurch auf der einen Seite ein nicht zu unterschätzendes Alleinstellungsmerkmal, gleichzeitig bringt der Parteienstatus auch Schwierigkeiten in der Netzwerkbildung mit sich. Gerade die zivilgesellschaftlichen Gruppen sind häufig peinlich genau darauf bedacht, eine zu große Nähe zu politischen Parteien zu meiden, um die eigene Unabhängigkeit nicht zu gefährden und eine Einflussnahme zu verhindern. Dementsprechend fällt es den Piraten oft schwerer, *advocacy coalitions* einzugehen und langfristige Netzwerke aufrecht zu erhalten. Trotzdem engagieren sich viele Aktivist_innen der netzpolitischen Szene auch bei den Piraten und prägen damit die inhaltlichen Positionen der Partei. Auf der Homepage der Piratenpartei lässt sich jedoch feststellen, dass vor allem Digitalcourage e.V. sehr aktiv darin ist, Ankündigungen auch im Forum der Piraten zu publizieren und diese damit als Plattform zu nutzen (vgl. Piratenforum 2014).

Opportunities: Die Piratenpartei galt in ihrer Entstehungsphase als große Hoffnung netzaffiner Menschen und als Paradiesvogel der Parteienlandschaft. Den hohen Erwartungen konnte sie jedoch schon bald nicht mehr gerecht werden. Aus diesem Grund haben viele parteipolitische Akteure und Funktionäre der etablierten Parteien das Interesse an den Piraten verloren und diese nicht länger als Konkurrenz oder Bedrohung empfunden. Gleichzeitig führe der Parteistatus dazu, dass die Piraten aufgrund des Parteiengesetzes und die daraus resultierenden staatlichen Zuschüsse ihre finanzielle sowie personelle Ressourcenbasis ausweiten und zur Mobilisierung von Anhänger_innen nutzen konnten. Es kann aus diesem Grund von einer *facilitation*, also der staatlichen Förderung durch das Parteiengesetz gesprochen werden.

b) Bündnis 90/ Die Grünen

Auch die derzeit kleinste im Bundestag vertretene Fraktion Bündnis 90/ Die Grünen sind zu einem wichtigen Impulsgeber für Netzpolitik und Datenschutz gewachsen. Spätestens seit den Enthüllungen geheimdienstlicher Überwachungen durch die Plattform WikiLeaks hat die Partei die Chance genutzt, sich netzpolitisch zu profilieren und damit als Opposition zur großen Koalition gestaltend tätig zu werden. Ähnlich wie bei der Piratenpartei ist es auch schwierig, die Grünen in ein klassisches rechts-links-Schema einzuordnen, denn gerade in den letzten Jahren konnte die Partei stark in das bürgerliche Milieu eindringen und Wähler_innen für sich mobilisieren.

Organisation: Mit knapp 60.000 Mitgliedern (vgl. Niedermayer 2013 b:2) haben die Grünen zwar mehr als doppelt so viele Mitglieder wie die Piratenpartei, trotzdem gehören sie mit dieser Zahl zu den kleineren Parteien Deutschlands, wenngleich sie in den letzten Jahren kontinuierlich und schnell wuchs.

Eine der bundesweit wichtigsten Struktureinheiten im Bereich der Netzpolitik ist der Arbeitskreis 3 der Bundestagsfraktion, für dessen politische Koordination der stellvertretende Fraktionsvorsitzende und netzpolitische Sprecher Konstantin von Notz zuständig ist. Von Notz ist darüber hinaus auch Obmann des Bundestagsausschusses

Digitale Agenda sowie des Untersuchungsausschusses zur NSA-„Affäre“, beides zentrale Ausschüsse bei Fragen des Datenschutzes und der informationellen Selbstbestimmung. Zwar gibt es auf Bundesebene ebenfalls die Bundesarbeitsgemeinschaft (BAG) Medien und Netzpolitik, diese trifft jedoch eher sporadisch zusammen und ist in ihrer Arbeitsweise von Diskontinuität geprägt. Auffällig ist eine organisatorische Diskrepanz zwischen dem starken Engagement der Bundestagsfraktion für netzpolitische Themen auf der einen Seite und die eher zurückhaltende Mobilisierung für dieses Politikfeld durch die Bundespartei und auch große Teile der Landespartei auf der anderen.

Belief Systems: Die Grünen sind anders als die Piraten keine klassische Netzpartei, trotzdem konnten sie sich in den letzten Jahren glaubwürdig als Partei der digitalen Bürger_innenrechte positionieren. Zwar ist in dem Grundsatzprogramm von 2002 noch keine Rede von den neuen Herausforderungen, die der digitale Wandel mit sich bringt. Seit 2009 jedoch sind Datenschutz und Informationsfreiheit zentrale Themen der Partei, die auch Einzug in das Wahlprogramm halten konnten. So stellt die Bundestagsfraktion fest: „Die grüne Bundestagsfraktion hat den Schutz und den Ausbau der ‚Bürgerrechte in der digitalen Welt‘ zu einem ihrer Schwerpunkte für das Jahr 2014 gemacht“ (B90/ Die Grünen Bundestagsfraktion 2014). Daraus resultierend kann das Recht auf informationelle Selbstbestimmung durchaus als *near policy core* der Partei bezeichnet werden, wenn auch andere Themen wie Ökologie und ressourcensparendes Wirtschaften immer noch deutlich höhere Priorität genießen. Nichtsdestotrotz bestehen große Überschneidungen in den Wertesystemen der Grünen und der „Netzgemeinde“, was die Attraktivität der Partei für diese Wählergruppe offensichtlich macht: Angesprochen werden vor allem junge, gut ausgebildete Menschen mit einem relativ hohen Einkommen, die sich mit postmateriellen Werten identifizieren können. Auch sind die Grünen vor allem in urbanen Räumen populär und verkörpern ein pluralistisches und progressives Partizipationsverständnis (vgl. Probst 2007: 179f.), was sich mit dem Politikverständnis netzaffiner Menschen überschneidet, denen digitaler Datenschutz ein wichtiges Anliegen ist.

Zu den *secondary aspects* zählen nach Ansicht der Grünen die Ergänzung des Fernmeldegeheimnisses auf digitale Kommunikation und Mediennutzung. Auch

werden Onlinedurchsuchung und VDS im Wahlprogramm von 2013 abgelehnt und eine ausdrückliche Einwilligung bei jeglicher Art von Datenerfassung gefordert. Unbemerkt Tracking durch Cookies soll verboten werden (vgl. Bündnis 90/ Die Grünen 2013: 194-196).

Zeit: Mit ihrer Gründung 1980 markierte die Partei die Institutionalisierung der Umwelt- und Anti-Atomkraftbewegung und zog schon bald in die Bundes- und Landesparlamente ein. Für diese Arbeit relevant ist vor allem die parteipolitische Entwicklung seit 2005, als der Diskurs um digitale Bürger_innenrechte und Netzpolitik begann sich zu manifestieren und dadurch eine Auseinandersetzung mit der Thematik notwendig machte, welche schließlich deutlichen Einfluss auf die inhaltliche Positionierung der Grünen hatte.

Ressourcenmobilisierung: Auch für die Grünen sind die Einnahmen lediglich bis zum Jahr 2011 veröffentlicht, sodass dies die aktuellsten Auskünfte sind, die gegeben werden können. 2011 verbuchte die Partei Einnahmen in Höhe von ca. 38.401.000 EUR und Ausgaben in Höhe von 30.720.000 EUR, wodurch ein Überschuss von ca. 7.681.000 EUR entstand. Der Anteil an staatlichen Mitteln betrug in diesem Jahr 15.154.545,27 EUR und damit 39,46% der Gesamteinnahmen (vgl. Bündnis 90/ Die Grünen 2014: 1). Diese Zahlen machen bereits deutlich, dass die Partei die wohl größten Mobilisierungskapazitäten hat, zum einen weil sie besser, stringenter und in der Breite organisiert ist, zum anderen, weil sie auf sehr hohe finanzielle Ressourcen zurückgreifen kann. Trotzdem darf nicht unberücksichtigt bleiben, dass Netzpolitik für die Partei ein Politikfeld neben vielen ist und hinter den Kernthemen Umweltschutz und Grüne Energien weit zurückbleibt, sodass vermutlich nur ein Teil der Anhänger_innen für verbraucher_innen- und datenschutzpolitische Fragestellungen zu mobilisieren ist.

Collective Action: Da Datenschutzpolitik zum einen kein Kernelement grüner Politik ist und zum anderen auch erst seit wenigen Jahren als politisches Thema für die Partei relevant geworden ist, liegt das Hauptaugenmerk der kollektiven Aktionen vor allem auf der Parlamentsarbeit: Im NSA-Untersuchungsausschuss und im Ausschuss Digitale Agenda versucht die Partei, die Politik zugunsten eines stärkeren Schutzes vor staatlicher Überwachung zu beeinflussen und eine modernere und verbraucher_innenfreundlichere Datenschutzpolitik umzusetzen. Auch hat die

Fraktion es geschafft, sich in diesem Zusammenhang unter anderem mit der Forderung nach einem Asyl für den Whistleblower Edward Snowden öffentlich besonders zu exponieren.

Die parteinahe Heinrich Böll Stiftung hat ein ganzes Dossier zum Thema „Überwachung, Geheimdienste & Demokratie“ veröffentlicht. Dabei handelt es sich um eine Collage unterschiedlicher Positionierungen gegen die Überwachungsmaßnahmen, für einen konsequenteren Schutz der Verfassung sowie für die Abschaffung der Geheimdienste. Darüber hinaus finden sich auch dort Hinweise und Ratschläge, wie die Privatsphäre im Netz besser geschützt und mit welchen Programmen eine stärkere Anonymisierung des Surfens erreicht werden kann (vgl. Heinrich Böll Stiftung).

Doch auch die Bundesebene der Partei veröffentlichte eine Reihe von Informationsmaterialien und Flyern zu den Positionen der Partei bei Themen wie dem Trennungsgebot zwischen Polizei und Nachrichtendiensten, Verbrauchermacht im Internet und Digitalen Bürger_innenrechten (vgl. Bündnis 90/ Die Grünen Bundestagsfraktion 2014). In dem Blog „Grün digital“ bloggen vier, auf unterschiedlichen Governance-Ebenen aktive Funktionäre der Partei über „netz-, datenschutz- und bürgerrechtspolitischen Aktivitäten“ (Grün-digital.de), was zum einen der Generierung von Inhalten und Positionen und zum anderen der Mobilisierung der Anhänger_innenschaft dienen soll.

Advocacy Coalitions: Wie die meisten anderen Parteien gehen auch die Grünen kaum langfristige Koalitionen mit anderen Organisationen ein. Dies liegt zum einen daran, dass viele der zivilgesellschaftlichen Gruppen ihre Unabhängigkeit und Unparteilichkeit wahren möchten, auf der anderen Seite muss auch die Partei ihrerseits versuchen, Unabhängigkeit gegenüber partikularen Interessengruppen oder Versuchen wirtschaftlicher Einflussnahme zu wahren. Trotzdem lassen sich vereinzelt Kooperationen feststellen: So sind die Grünen Bündnispartner bei Veranstaltungen anderer zivilgesellschaftlicher Akteure wie z. B. bei den „Freiheit statt Angst“ und „Stop watching us!“– Demonstrationen.

Zwar werden selten langfristige, stabile Bündnisse geschmiedet, doch die Partei versucht, mit Datenschützer_innen ins Gespräch zu kommen und ihnen eine Plattform für die Artikulation der eigenen Positionen zu bieten: So nahmen

Mitglieder vom Chaos Computer Club und von Digitalcourage e.V. an den Netzpolitischen Soirée sowie an Workshops des netzpolitischen Kongresses der Bundestagsfraktion teil (vgl. B90/ Die Grünen Bundestagsfraktion 2012).

Opportunities: Die Grünen sind eine staatsnahe Organisation, die jedoch einen festen Platz in der Parteienlandschaft der Bundesrepublik gefunden hat und auch von allen staatlichen Entscheidungsträgern anerkannt ist. Darüber hinaus erlaubt es das Parteiengesetz, staatliche Zuschüsse in nicht unerheblicher Höhe für sich beanspruchen zu können. Diese Förderung erleichtert die Parteiarbeit und darüber hinaus auch die Mobilisierung von Anhänger_innen.

c) Landesdatenschutzbeauftragte

Das deutsche Bundesdatenschutzgesetz sieht die Einstellung von Datenschutzbeauftragten auf Bundes- und auf Landesebene vor. Thilo Weichert hat in Schleswig-Holstein dieses Amt seit 2004 inne. Die Bundes- und Landesdatenschutzbeauftragten unterscheiden sich vor allem in ihrer Zuständigkeit: Während die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Datensammlung und -verarbeitung von Bundesbehörden überwacht, sind die Landesbeauftragten neben den entsprechenden Landesbehörden auch für den privatwirtschaftlichen Bereich zuständig (vgl. z. B. Betz/ Kübler 2013: 165). Im Folgenden soll exemplarisch die Arbeit des Unabhängigen Landeszentrums für Datenschutz in Schleswig Holstein (ULD) skizziert werden. Dabei ist jedoch auch darauf hinzuweisen, dass die Trennung zwischen staatsnah und staatlich durchaus verschwimmt, da die EU-Richtlinie 96/46/EG insofern nicht umgesetzt worden ist, als dass die „zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt [sind] und damit das Erfordernis, dass diese Stellen ihre Aufgaben ‚in völliger Unabhängigkeit‘ wahrnehmen“ (EuGH, Große Kammer 2010) nicht ausreichend sichergestellt sei. Seit 2011 hat das Land Schleswig-Holstein an dieser Stelle nachgebessert, die Gesetzeslücke geschlossen und das Urteil des EuGH umgesetzt. Diesbezüglich stellt das ULD fest:

„Das Gesetz zur Änderungen des Landesdatenschutzgesetzes tritt am 16. September 2011 in Kraft. Es regelt die Wahl und Amtszeit, die Rechtsstellung der oder des Landesbeauftragten für Datenschutz sowie die Aufgaben des Unabhängigen Landeszentrums für Datenschutz; es genügt den Anforderungen eines Urteils des Europäischen Gerichtshofes, wonach die Unabhängigkeit der Landesdatenschutzbehörden festgeschrieben werden musste“ (Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein 2014a).

Auch heißt es im Landesdatenschutzgesetz „Das Unabhängige Landeszentrum für Datenschutz nimmt die ihm zugewiesenen Aufgaben in Unabhängigkeit wahr und ist nur dem Gesetz unterworfen“ (vgl. Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen LDSG §39 Abs. 1). Es bleibt jedoch fraglich, ob eine faktische Unabhängigkeit tatsächlich ausreichend gewährleistet wird, da das Gesetz durchaus Ambiguitäten aufweist: Zum einen wird der oder die Beauftragte von der Ministerpräsidentin bzw. dem Ministerpräsidenten Schleswig-Holsteins ernannt (ebd. §36, Abs. 1), ein deutliches Indiz dafür, dass die tatsächliche Unabhängigkeit nicht in vollem Umfang garantiert werden kann, sofern mehrere Amtszeiten und eine personelle Kontinuität angestrebt werden. Trotzdem sieht das Landesdatenschutzgesetz die Unabhängigkeit explizit vor: „Die Ministerpräsidentin oder der Ministerpräsident ist Dienstvorgesetzte oder Dienstvorgesetzter der oder des Landesbeauftragten für Datenschutz. Die oder der Landesbeauftragte für Datenschutz untersteht der Dienstaufsicht nur, soweit nicht seine Unabhängigkeit bei der Aufgabenwahrnehmung beeinträchtigt wird“ (ebd. §36, Abs. 3).

Organisation: Die Struktur des ULD Schleswig-Holstein ist gesetzlich wie folgt festgeschrieben: Als rechtsfähige Anstalt des öffentlichen Rechts hat das Zentrum seinen Sitz in der Landeshauptstadt Kiel, Dienstvorgesetzter der gesamten Anstalt ist der Landesdatenschutzbeauftragte und gleichzeitiger Vorstand, der auf fünf Jahre mit der Möglichkeit zur Wiederwahl vom schleswig-holsteinischen Landtag gewählt wird (ebd. §32-35). Seit 2004 hat dieses Amt der Jurist und Politologe Thilo Weichert inne, seine Stellvertreterin ist Marit Hansen. Insgesamt sieben Referate widmen sich jeweils spezifischen Aufgabenbereichen und werden von einer Referentin oder einem Referenten geführt. Insgesamt sind derzeit 42 Beschäftigte für die Erfüllung der Aufgaben des ULD zuständig.

Belief Systems: Es ist nicht davon auszugehen, dass in einer so staatsnahen Organisation wie dem ULD tatsächlich kohärente oder gar homogene *belief systems* bestehen. Das Aufgabenspektrum ist gesetzlich verankert und kann nicht ohne weiteres eingeschränkt oder erweitert werden. Trotzdem kann das Zentrum seine Arbeitsschwerpunkte unabhängig setzen und ihre Mittel frei wählen. Dies macht es durchaus möglich, *secondary aspects* zu formulieren, die zu einem besseren Schutz personenbezogener Daten führen sollen. Dies geschieht vor allem durch Hinweise an Parlamentarier_innen, wie ein moderneres Datenschutzrecht, das den aktuellen Herausforderungen entspricht, ausgestaltet sein könnte. Auch ist die Information der Öffentlichkeit über Maßnahmen, die persönliche Daten schützen, wichtiger Bestandteil der Arbeit des Beauftragten. Die genauen Tätigkeiten der Behörde werden unter der Kategorie *collective action* näher erläutert.

Zeit: Das Landeszentrum wurde im Zuge der Einführung eines Landesdatenschutzgesetzes im Jahre 1978 gegründet. Seitdem wurde die Anstalt von den Beauftragten Ernst Eugen Becker, Dr. Helmut Bäumlner und Dr. Thilo Weichert geführt (vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein 2014b). Die gesetzlich gesicherte Existenz sowie die vom Land Schleswig-Holstein zur Verfügung gestellten Ressourcen erlauben eine über Jahrzehnte hinweg kontinuierliche Arbeit des Landeszentrums sowie eine Professionalisierung der Mitarbeiter_innen.

Ressourcen: Diese Kategorie wird bewusst ohne den Zusatz „Mobilisierung“ betrachtet, da die Landesdatenschutzbehörden nicht darauf angewiesen sind, finanzielle Mittel von Anhänger_innen zu mobilisieren, da die EU-Richtlinie 95/46/EG die Einrichtung von Landesdatenschutzstellen vorsieht und die Bundesländer dementsprechend dazu verpflichtet sind, diese einzurichten und auch finanziell zu unterhalten. Aus dem Landeshaushaltsplan Schleswig-Holsteins geht hervor, dass für das Jahr 2013 ca. 1,9 Mio EUR aus dem Landesetat für das ULD veranschlagt worden sind (Schleswig-Holsteinischer Landtag 2013: 27), um die Ausgaben zu decken.

Collective Action: Das Aufgabengebiet der Behörde ist in großen Teilen gesetzlich umrissen worden: Die wohl wichtigste Aufgabe des ULD liegt in der Aufsicht über die öffentlichen, aber auch nichtöffentlichen Stellen sowie darüber, dass die Datenschutzgesetze auch konsequent umgesetzt und eingehalten werden können. Auch

erfüllt sie Beratungsfunktionen gegenüber öffentlichen Stellen, Wirtschaftsunternehmen und Bürger_innen.

Und doch gibt es eine Reihe von zusätzlichen Aktionen, deren Initiative vom Datenschutzzentrum ausgeht: Besonders gegen das soziale Netzwerk Facebook ist das ULD in den letzten Jahren aktiv geworden und hat sich klar gegen eine Nutzung der Plattform ausgesprochen. Darüber hinaus klagte das Landeszentrum immer wieder gegen öffentliche Stellen, die „Fanpages“ auf Facebook veröffentlichten, da dadurch die Nutzung der datenschutzwidrigen Plattform gefördert würde (vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein 2014c).

Auch werden Informations- und Bildungsveranstaltungen organisiert und durchgeführt: So wird einmal jährlich eine Sommerakademie veranstaltet, welche als Forum für die Diskussion aktueller Fragen des Datenschutzes verstanden wird. In der vom ULD betriebenen Datenschutzakademie finden das ganze Jahr über Qualifizierungs- und Weiterbildungskurse für betrieblichen und behördlichen Datenschutz statt. Das Kursangebot „Entscheide DU – sonst tun es andere für dich“ wurde speziell für Jugendliche konzipiert, um sie für Datenschutz zu sensibilisieren und erreichte im Jahr 2012 900 Schüler_innen des Bundeslandes (Unabhängiges Landeszentrum Schleswig-Holstein 2013b: 163).

Für Behörden, Betriebe und andere Institutionen bietet das Landeszentrum darüber hinaus die Möglichkeit an, sich einem europaweit standardisierten Audit-Verfahren zu unterziehen und sich dadurch mit dem EuroPriSe – European Privacy Seal, einer Art Datenschutz-Gütesiegel zertifizieren zu lassen (vgl. ebd.: 135-138).

Advocacy Coalitions: Wie oben bereits deutlich geworden ist, handelt es sich bei dem Landeszentrum um eine sehr engagierte Behörde, die in vielen Fällen auch über die streng zugewiesenen Kompetenzen hinausgeht, um die Bedeutung der Thematik Datenschutz zu betonen und für die Bürger_innen nachvollziehbar aufzubereiten. Dementsprechend gibt es eine Reihe von Kooperationen, die diese Stelle mit anderen Akteuren eingeht. Zunächst einmal sei auf eine personelle Überschneidung hingewiesen: Der Datenschutzbeauftragte Thilo Weichert war lange Jahre Vorsitzender der oben beschriebenen Deutschen Vereinigung für Datenschutz (DVD) und schreibt bis heute regelmäßig Aufsätze für die von dem Verein veröffentlichte Zeitschrift „Datenschutznachrichten – DANA“. Doch auch für

das Blog netzpolitik.org schreibt Weichert Artikel, in denen er seine Positionen deutlich macht und für eine stärkere Dominanz der Thematik im öffentlichen Diskurs wirbt. Auf der „Stop watching us!“- Demonstration im Jahr 2013 hielt er darüber hinaus bei der Auftaktkundgebung in Hamburg eine Rede für die Stärkung digitaler Bürger_innenrechte (vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein 2014).

Opportunities: Dieser Akteur stellt im Rahmen dieser Arbeit eine Besonderheit dar, denn bisher wurden ausschließlich nichtstaatliche Akteure untersucht. Das ULD als nichtstaatlich zu bezeichnen, würde jeder Grundlage entbehren. Formal ist die Stelle zwar unabhängig von anderen Landesbehörden oder -ministerien, trotzdem wird sie stark aus dem Landeshaushalt bezuschusst, ebenso erhält sie Zuweisungen aus dem Bund und Förderungen der Europäischen Union. Darüber hinaus sind die Mitarbeiter_innen Angestellte des Landes Schleswig-Holstein, sodass eine starke Interdependenz angenommen werden muss. Unter diesen Voraussetzungen kann auch nicht mehr von *facilitation* durch staatliche Akteure gesprochen werden, vielmehr ist das ULD Teil des Staatsapparates und bildet einen Grenzfall zwischen staatlichem und nichtstaatlichem Akteur.

d) Zwischenfazit

In diesem Kapitel der Arbeit ist der Interessengegensatz unterschiedlicher Akteure deutlich geworden. Auf der einen Seite des Spektrums stehen Organisationen, die eine absolute Souveränität der Menschen im Umgang mit ihren Daten fordern: Datensparsamkeit soll gesichert, die Speicherung auf ein Minimum reduziert und die Erstellung von personalisierten Kundenprofilen unterlassen werden. Auf der anderen Seite gibt es Gruppen, die der Meinung sind, Privatsphäre gehöre der Vergangenheit an, Daten müssten befreit und allen zugänglich gemacht werden. In diesen Bereich fallen auch große Teile der Internetwirtschaft, die der Nutzung von persönlichen Daten für ökonomische Zwecke durchaus zustimmen.

Auffallend ist, dass dieser Diskurs analytisch unpräzise geführt wird. In nahezu allen untersuchten Veröffentlichungen fehlen Definitionen, Differenzierungskonzepte

oder Spezifizierungen. Fragen danach, was eigentlich personenbezogene Daten sind, ob eine Hierarchisierung der Daten sinnvoll ist oder ob ein Recht auf Anonymität im Internet geeignet ist, den digitalen Raum zu schützen, werden weder aufgeworfen noch beantwortet. Ähnlich verhält es sich mit staatlicher Überwachung: Welche Auswirkungen hat eine massenhafte Überwachung auf das Kommunikations-, Informations- und Konsumverhalten von Bürger_innen? Macht es einen Unterschied, ob ein Inlandsgeheimdienst die Bevölkerung ausspäht oder der Dienst eines anderen Landes? Eine Spezifizierung der Materie Datenschutz findet seitens der interessenpolitischen Akteure nicht statt, vielmehr bleibt dieses Feld der Wissenschaft vorenthalten.

Es ist festzustellen, dass privatwirtschaftliche Akteure wie Wirtschaftsverbände oder Unternehmensvorstände deutlich privilegierteren Zugang zu Ministerien und Behörden erreichen können als zivilgesellschaftlich orientierte Datenschutzorganisationen. So gelingt den Branchenverbänden und Wirtschaftsinitiativen, eine dauerhafte Kooperation mit dem Bundesministerium für Wirtschaft und Energie herzustellen, den andere Gruppierungen nicht für sich verbuchen können. Hier lässt sich ein Paradigmenwechsel in der Netzpolitik feststellen: Während in der Enquete-Kommission Internet und Digitale Gesellschaft noch heterogene Gruppen repräsentiert waren und zu netzpolitischen Themen beitragen, ist die Einbindung und damit auch der Einfluss nicht-wirtschaftsorientierter Gruppen mit der neuen Bundesregierung zurückgegangen. Zwar sollte die Digitale Agenda der Bundesregierung „gemeinsam mit Wirtschaft, Tarifpartnern, Zivilgesellschaft und Wissenschaft umgesetzt werden“ (vgl. BMWi 2014a), die Besetzung der Arbeitsgruppen des nationalen IT-Gipfel zeigt jedoch eine überdeutliche Dominanz von Wirtschaftsverteter_innen und deren Dachverbänden (vgl. BMWi 2014c). Zivilgesellschaftliche Akteure finden sich ebenso wie Gewerkschaften kaum in Arbeitsgruppen wieder, sodass hier von einem Missverhältnis politischer Einflussnahme gesprochen werden kann.

Anhand dieses Kapitels ist folgende Tendenz deutlich geworden: Während auf der einen Seite Datenschützer sich sowohl gegen staatliche als auch gegen privatwirtschaftliche Überwachung wehren, positionieren sich die datenschutzkritischen Akteure vor allem auf der privatwirtschaftlichen Seite. Sie lehnen staatliche Über-

wachung zu einem großen Teil ebenfalls ab, möchten aber die ökonomische Verwertbarkeit der Daten aufrechterhalten und weiter ausbauen.

Den zivilgesellschaftlichen Akteuren sowie den Journalist_innen, die sich mit der Thematik befassen, bleibt lediglich die öffentliche Mobilisierung von Anhänger_innen anstelle des direkten Lobbying bei politischen Entscheidungsträger_innen. Weidemann urteilt: „Doch alles in allem ist die digitale Zivilgesellschaft eher klein und unorganisiert, wenn auch spontan mächtig“ (Weidemann 2013: 86). Es wird abzuwarten bleiben, ob diese Einschätzung zutrifft, denn bisher wurden die Forderungen nach mehr Transparenz und stärkerem Schutz der personenbezogenen Daten durch die Bundesregierung und auch die Europäische Union bestenfalls ignoriert, in vielen Fällen, wie der NSA-Untersuchungsausschuss zeigt, auch konterkariert. Auch bleibt festzuhalten, dass die Themensetzungen der zivilgesellschaftlichen Akteure geprägt sind durch ein eher passives, reaktives *agenda setting*, welches auf die Abmilderung der Folgen bestehender Zustände abzielt. Es sind eher defensive Strategien, die es nicht erlauben, kreative und aktive Verbesserungsstrategien zu formulieren, die eine unmittelbare Wirksamkeit für die Anhänger_innen oder die Öffentlichkeit entfalten könnten. Die Machtlosigkeit der Akteure bei gleichzeitiger Ignoranz der Gesetzgeber macht eine Mobilisierung und eine aktive Strategieentwicklung besonders schwierig.

VI Advocacy Coalition Frameworks

Im fünften Kapitel konnte die Genese des *Policy*-Subsystems Datenschutzpolitik nachvollzogen werden. Es wurde deutlich, dass es sich in diesem Feld um eine Verschränkung der beiden von Sabatier formulierten Begründungen für die Entstehung eines Subsystems handelt: Auf der einen Seite hat es eine Spezialisierung der Datenschutzpolitik in den letzten Jahren gegeben, die aus der zunehmenden Digitalisierung des öffentlichen Raumes resultierte. Die bisherigen Regelungen stammten jedoch aus den 1990er Jahren und konnten auf aktuelle Entwicklung keine angemessenen Antworten geben. Dies führte auch zu dem Bedürfnis seitens der Akteure, Reformprozesse anzustreben, mitzugestalten und in ihrem Sinne zu beeinflussen. Sowohl die intransparenten Geschäftsmodelle kommerzieller Dienstleister und Versandhäuser, als auch die Undurchsichtigkeit staatlicher Überwachungsmaßnahmen wurden von den Akteuren als Bedrohung ihrer Kommunikations- und Handlungsmöglichkeiten wahrgenommen. Darüber hinaus war es auch möglich, Netzwerkstrukturen zwischen den Akteuren zu identifizieren und Kooperationen mit anderen, in dieser Arbeit nicht behandelten Gruppierungen aufzuzeigen.

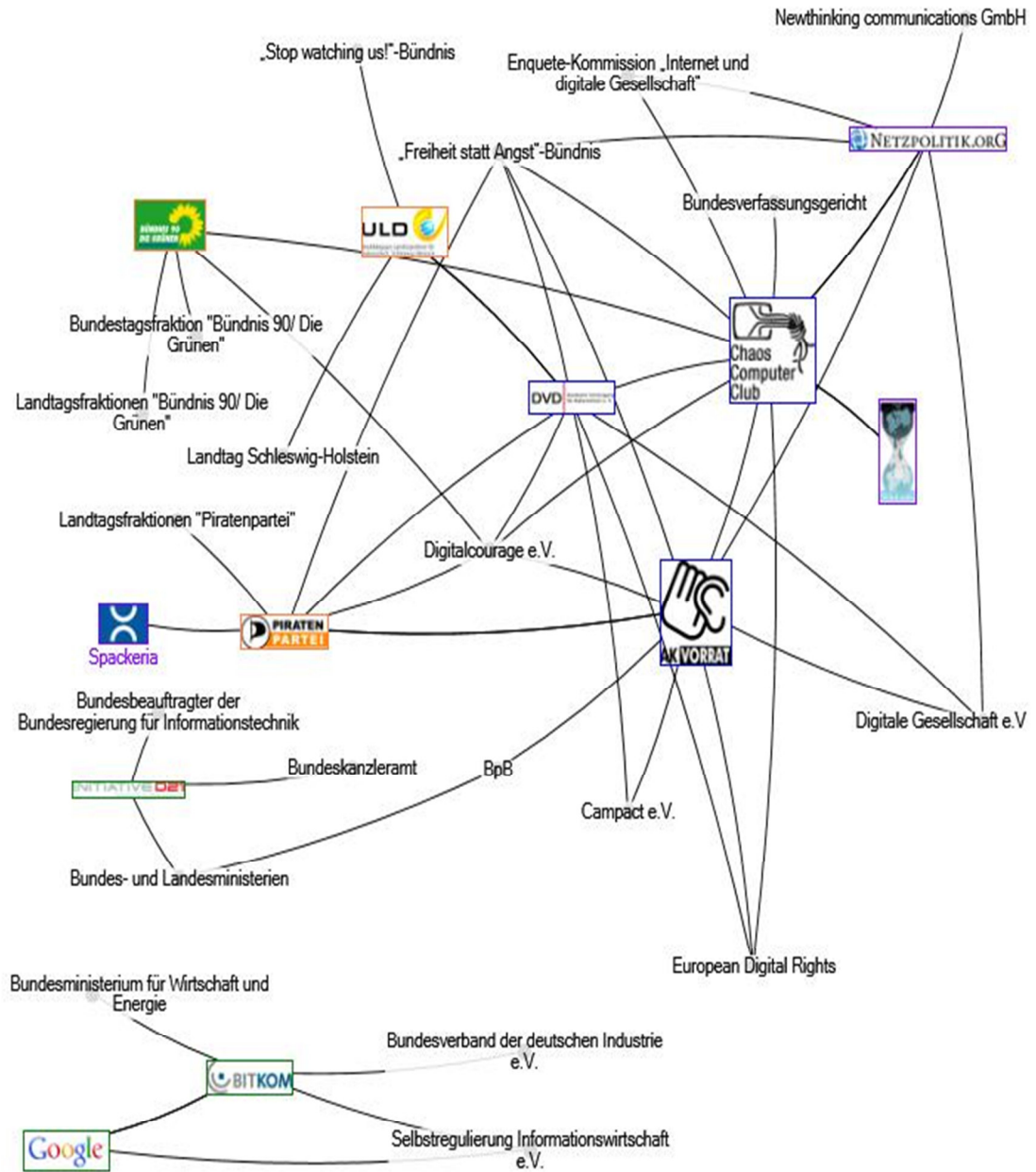
Bevor jedoch eine Aufstellung der Ergebnisse vorgenommen werden kann, müssen zunächst einige Einschränkungen zur Validität der Ergebnisse vorgenommen werden. 1) Obwohl die Komponente Zeit in die Analyse der Akteure einbezogen worden ist, sind viele der Informationen vor allem aktuellerer Natur. Dies führt dazu, dass die festgestellten *advocacy coalitions* eine Momentaufnahme darstellen müssen und keine Aussagen über Entwicklungsprozesse der letzten Dekade zulassen können, obwohl dies von Sabatier gefordert worden ist. Auch ist die Auswahl der Akteure beschränkt und schließt zeitliche Dynamiken nicht ein. Zwar wurde versucht, die wichtigsten Akteure auszuwählen, also jene, die sich als besonders diskursprägend exponieren konnten, jedoch kann diese Einschätzung lediglich subjektiv und damit anfechtbar sein. Trotzdem lassen sich insofern Aussagen über die Struktur und die Beschaffenheit der netzpolitischen Akteure daraus ableiten, als dass diese geclustert und im Gefüge des Subsystems verortet werden können. Im Folgenden werden die *advocacy coalitions* noch einmal aufgelistet:

Akteur	Advocacy Coalition	
	Nichtstaatlich	Staatlich
Chaos Computer Club	Digitalcourage e.V. European Digital Rights Wau-Holland-Stiftung WikiLeaks Netzpolitik.org „Freiheit statt Angst“-Bündnis	Enquete-Kommission „Internet und digitale Gesellschaft“ (bis 2013) Bundesverfassungsgericht (eingeladen als Sachverständige)
Arbeitskreis Vorratsdatenspeicherung	Chaos Computer Club Digitalcourage e.V. Campact e.V. Digitale Gesellschaft e.V. European Digital Rights Piratenpartei	Bundeszentrale für politische Bildung
Deutsche Vereinigung für Datenschutz	„Freiheit statt Angst“-Bündnis Digitalcourage e.V. Campact e.V. Bundesverband der Datenschutzbeauftragten Deutschlands European Digital Rights „Freiheit statt Angst“-Bündnis	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
BITKOM e.V.	Bundesverband der deutschen Industrie e.V. Selbstregulierung Informationswirtschaft e.V. Google Germany GmbH	Bundesministerium für Wirtschaft und Energie
Google Germany GmbH	Selbstregulierung Informationswirtschaft e.V. BITKOM e.V. Eco – Verband der Internetwirtschaft e.V.	
Initiative D21		Bundeskanzleramt

		Kultusministerien, Staatsministerien vieler Länder, Bundesbeauftragter der Bundesregierung für Informationstechnik, u.A.
Netzpolitik.org	Newthinking communications GmbH Chaos Computer Club AK Vorrat Digitale Gesellschaft e.V. „Freiheit statt Angst“-Bündnis	Enquete-Kommission „Internet und Digitale Gesellschaft“ (bis 2013)
Spackeria	Piratenpartei	
WikiLeaks	Chaos Computer Club	
Piratenpartei	AK Vorrat Digitalcourage e.V. „Freiheit statt Angst“-Bündnis	Landtagsfraktionen in Berlin, Schleswig-Holstein, Nordrhein-Westfalen, Saarland
Bündnis 90/ Die Grünen	Chaos Computer Club Digitalcourage e.V. Heinrich-Böll-Stiftung	Fraktionen in allen deutschen Landtagen, Bürgerschaften und Abgeordnetenhäusern; Fraktion im Deutschen Bundestag
Unabhängiges Landeszentrum für Datenschutz Schleswig- Holstein	Deutsche Vereinigung für Datenschutz „Stop watching us!“-Bündnis Netzpolitik.org	Landtag Schleswig-Holstein

Tabelle 1: Akteure und ihre Advocacy Coalitions

Netzwerkstruktur der netzpolitischen Akteure



Anhand der Tabelle 1 können die im Kapitel 1.1 aufgestellten Hypothesen getestet werden. Sie lauteten wie folgt: (1) Es gibt einen Unterschied zwischen den Akteursformen bezüglich ihrer Koalitionsbildung: Zivilgesellschaftliche Gruppen sind aufgrund ihrer geringeren Ressourcen stärker geneigt, Kooperationen mit anderen Gruppen einzugehen, um synergetische Effekte nutzen zu können, während privatwirtschaftliche und journalistisch agierende Akteure relativ autonom handeln

können und nicht von Kooperationen und Netzwerkbildungen abhängig sind. (2) Netzpolitik wird vornehmlich als Wirtschaftspolitik betrachtet: Privatwirtschaftliche Unternehmen genießen einen privilegierten Zugang zu relevanten politischen Entscheidungsträger_innen zur Unterstützung ihrer Interessenpolitik, während zivilgesellschaftliche Akteure aufgrund ihrer begrenzten finanziellen Ressourcen Methoden nutzen, die darauf ausgelegt sind, ihrem Anliegen öffentlich Gehör zu verleihen und ihre Positionen in dem Diskurs in breite Gesellschaftsschichten zu tragen.

An der obigen Darstellung lässt sich ablesen, dass beide Hypothesen verifiziert werden konnten: Zum einen wird deutlich, dass vor allem die Akteursform der Netzaktivist_innen eine starke Vernetzung innerhalb des Politikfeldes aufweist. Die *advocacy coalition frameworks* bilden ein selbstreferentielles System, bei dem Bündnisse zwischen den Gruppierungen genutzt werden, um Demonstrationen oder große Aktivitäten wie Kongresse zu planen und auszurichten. Auch wurde deutlich, welche Akteure für diesen Bereich der Datenschutzpolitik noch von besonderer Relevanz sind, in dieser Arbeit aber nicht tiefergehend untersucht worden sind. Beispielhaft können Digitalcourage und die Digitale Gesellschaft e.V. genannt werden. Für eine weitergehende Forschung wäre es deshalb wichtig, auch diese Akteure einzubeziehen, um eine wissenschaftlich lückenlose Beschreibung des Politikfeldes zu erreichen. Zwar haben sich Wirtschaftsunternehmen ihrerseits zu Branchenverbänden oder Netzwerkorganisationen zusammengeschlossen, jedoch finden darüber hinaus kaum weitere interne Vernetzungen mit anderen Gruppen oder Organisationen statt.

Des Weiteren geht aus der Tabelle und dem Schaubild hervor, dass besonders die privatwirtschaftlichen Verbände einen privilegierteren Zugang zu staatlichen Institutionen genießen und deshalb davon ausgegangen werden kann, dass der Einfluss auf Gesetzgebungen oder – was für Datenschutz besser zutrifft – die Vermeidung von staatlicher Regulierung, deutlich höher ist als der Einfluss zivilgesellschaftlicher Akteure. Dies wird insofern als problematisch erachtet, als dass sich besonders durch die Enthüllungen staatlicher Überwachungspraktiken durch Whistleblower wie z.B. Edward Snowden die Erkenntnis verstetigt hat, dass eine wirkliche Souveränität über eigene Daten und privates Kommunikationsver-

halten offensichtlich nicht mehr existiert. Weder Staat noch Wirtschaft scheinen ein Interesse an verlässlicher Regulierung zu zeigen. Staatliche Dienste sind auch gerne bereit, gesetzes- oder, wie bei der „Operation Eikonol“ deutlich geworden, sogar grundgesetzwidrig zu handeln (vgl. z. B. Redaktion der Süddeutschen Zeitung 2014). Datenschutzbeauftragten und auch den parlamentarischen Kontrollgremien fehlt dabei jede Handhabe, einen realen Datenschutz der Bürger_innen länger durchzusetzen.

VII Fazit

Diese Arbeit verfolgte drei Ziele, die im Folgenden zusammengefasst werden sollen. Das erste Ziel ist die Darstellung des Kontextes, in dem Datenschutz und Netzpolitik weltweit und auch in Deutschland diskutiert worden sind. Es konnte die enge Verbindung zwischen zunehmender Digitalisierung und der Erfassung und Verwendung personenbezogener Daten seit den späten 1970er Jahren deutlich gemacht werden. Ebenso wurde gezeigt, worin die Befürchtungen eines unregulierten Missbrauchs von persönlichen Daten begründet liegen und welche Herausforderungen die aktuellen Entwicklungen in Bezug auf staatliche Überwachung bergen. Gleichzeitig konnte nachgezeichnet werden, dass der Diskurs einem ständigen Wandel der Konzepte von Öffentlichkeit und Privatheit, aber ebenso einer Veränderung des Verhältnisses zwischen Sicherheit und Freiheit unterliegt und deshalb stets innerhalb des jeweils spezifischen Kontextes betrachtet werden muss. Dass die Argumente der Datenschützer_innen in den 1980er Jahren andere waren als nach den Terroranschlägen vom 11.09.2001, ist ebenso dargelegt worden wie die Sorgen, mit denen sich viele Menschen durch die ausufernde staatliche und kommerzielle Überwachung in den letzten Jahren konfrontiert sehen. Das Herzstück dieser Arbeit war dem Versuch gewidmet, besonders relevante Organisationen oder Gruppierungen nach wissenschaftlichen Kriterien zu analysieren und damit zur Schärfung des Bildes über „die Netzgemeinde“ beizutragen. Natürlich kann dies nur lückenhaft gelingen, zum einen weil nur der aktivistische und privatwirtschaftliche Bereich dieser soziologischen Kategorie betrachtet werden konnte, zum anderen weil selbst diese Betrachtung nur einen Ausschnitt aller relevanten Akteure abdecken konnte. Ein systematisches Vorgehen war für das Verfassen dieser Arbeit unumgänglich, deshalb sind aus der Synthese des Ressourcenmobilisierungsansatzes nach Tilly und des *advocacy coalition framework* nach Sabatier Kriterien entwickelt worden, die die Analyse der Akteure operationalisieren und in ein aussagekräftiges Schema eingliedern sollten. Dabei sind Interessengegensätze zwischen einzelnen Akteursgruppen zutage getreten, die sich vor allem in der Frage nach der Legitimität der Erfassung und Verarbeitung personenbezogener Daten kristallisieren. Während digitalwirtschaftlich orientierte

Gruppen in der Nutzung dieser Daten ein wichtiges Geschäftsfeld verorten, welches makroökonomisch durchaus bedeutend und nicht weiter zu regulieren ist, sehen viele zivilgesellschaftlich agierende Gruppen eine Gefahr in dieser Geschäftspraxis, die es einzuschränken gilt, sodass Informationsbeziehungen sich nicht länger in Machtbeziehungen manifestieren können.

Das dritte Ziel bezog sich auf die Aufdeckung von Kooperationsbeziehungen innerhalb des Politikfeldes. Es sollte herausgearbeitet werden, wie sich die Akteure untereinander vernetzen und in welchen Bereichen sie zusammenarbeiten. Zwei mögliche Szenarien waren vorstellbar: Zum einen hätten die Organisationen in einem Konkurrenzverhältnis zueinander stehen können, bei dem die Abgrenzung gegenüber anderen Gruppen betont und die eigene Bedeutung herausgestellt würde. Auf der anderen Seite wären eine enge Kooperation und eine starke Vernetzung der Akteure denkbar, durch die eine bessere Mobilisierung von Anhänger_innen angestrebt würde. Es zeigte sich im Laufe der Arbeit, dass es einen Unterschied zwischen den Akteursformen in dieser Frage gibt: Während zivilgesellschaftlich Gruppen dazu neigen, ausgiebige Kooperationen zu schließen, Informationen über mehrere Kanäle zu verbreiten und in Bündnissen Proteste vorzubereiten, sind gerade die Dachverbände der Wirtschaftsunternehmen kaum dazu bereit, solche längerfristigen Kooperationen mit anderen nichtstaatlichen Organisationen einzugehen. Sie versuchen stattdessen, Akteure des staatlichen Institutionengefüges zu beeinflussen und für eine Zusammenarbeit zu gewinnen. Es wurde deutlich, dass hier zwei unterschiedliche Strategien für die Interessenpolitik verfolgt werden.

Ebenfalls deutlich geworden ist, dass Datenschutz eines der zentralen Herausforderungen der Zukunft sein wird. Jedoch ist es in diesem Zusammenhang wichtig, die Debatte über gesetzliche Regulierung unaufgeregt und objektiv zu führen. Mit der verschwörungstheoretischen Angst vor der Allmacht und Intelligenz von Computern und der permanenten Heraufbeschwörung des Orwell'schen *Big Brother* ist genauso wenig gewonnen wie mit einer absoluten Freigiebigkeit und Sorglosigkeit im Umgang mit personenbezogenen Daten. Hier ist die Grenzziehung noch Teil der gesamtgesellschaftlichen Auseinandersetzung, jedoch erscheinen beide Extreme auf diesem Kontinuum von falschen Prämissen auszugehen. Fest

steht jedoch, dass diese Auseinandersetzung auch Firmenpolitiken verändern wird. Es ist vorstellbar, dass es eine Ausdifferenzierung verschiedener Onlinedienste geben wird. Denkbar sind etwa zwei unterschiedliche Geschäftsmodelle: Auf der einen Seite monetär bezahlte Leistungen, die einen hohen Wert auf Datenschutz legen, Sicherheit und Anonymität gewährleisten und dabei trotzdem leicht zu bedienen sind. Darüber hinaus könnten aus dem *Do-It-Yourself*-Selbstverständnis vieler Hacker Dienstleistungen hervorgehen, die Gemeinschafts- und *Crowd-sourcing*-Projekte sind und ehrenamtlich von Freiwilligen erstellt und angeboten werden. Zwar werden diese Leistungen unentgeltlich und nicht kommerziell sein, gleichzeitig wird es vermutlich Einschränkungen in der Praktikabilität, Bedienungsqualität oder auch optischem Design geben. Die Grenzen zwischen zivilgesellschaftlichem und wirtschaftlichem Engagement würden in diesem Kontext verschwimmen, die oben getroffene Kategorisierung wird womöglich bald nicht mehr aufrechtzuerhalten sein. Eine weitere Herausforderung wird in den nächsten Jahren an Bedeutung zunehmen und neuen Regulierungsbedarf entstehen lassen: Das *cloud computing*. Sobald Inhalte, zu denen Daten oder auch Big Data, gehören, in externen Rechenzentren gelagert und ausgewertet werden, müssen Schutzmechanismen etabliert werden, die die Sicherheit dieser Inhalte garantiert. Immer wieder erregt der Diebstahl privatester Informationen von Cloud-Diensten öffentliche Aufmerksamkeit, kaum ein größerer Dienst ist nicht durch Hackerangriffe in die Schlagzeilen gekommen. Die Frage nach Datenschutz ist hier aufs Engste verknüpft mit Fragen der Datensicherheit.

In den nächsten Jahren wird das Leben aller Menschen sich noch stärker im digitalen, virtuellen Raum abspielen. Dementsprechend werden immer mehr Personen versuchen, diesen Bereich ihres Lebens mitzugestalten und die darin geltenden Lebensbedingungen in ihrem Sinne zu beeinflussen. Folglich ist anzunehmen, dass sich das Engagement der „Digitalen Gemeinde“ verstärken wird. Die bisherige Forschung hat diese Entwicklung vernachlässigt, denn es gibt kaum umfangreiche Studien zu diversen Akteuren auf den verschiedenen Governance-Ebenen. Diese Masterarbeit konnte lediglich einen kleinen Ausschnitt eines sehr dynamischen und von Interdependenzen geprägten Themenkomplexes beleuchten: Sie beschränkte sich zum einen auf ein klar abgegrenztes Sub-Politikfeld, die

Datenschutzpolitik, zum anderen untersuchte sie nur nichtstaatliche Akteure, deren Interaktionen und Handlungspotenziale mit Entscheidungsträgern nur ein Kriterium von vielen war. Drittens beschränkte sich die Arbeit lediglich auf die nationalstaatliche Ebene der Bundesrepublik, auf andere *Governance*-Ebenen konnte aufgrund des begrenzten Umfangs der Arbeit nicht eingegangen werden. Auch die Rolle von Nationalstaaten sowie die Fähigkeit zur Überwindung von Staatsgrenzen, die dem Web 2.0 häufig zugeschrieben worden ist, konnte nur am Rande thematisiert werden.

Da das Politikfeld der *Internet-Governance* noch sehr jung und teilweise erst im Entstehen begriffen ist, kann die Notwendigkeit, diese Anfänge von vornherein wissenschaftlich zu begleiten und zu untersuchen, nicht hoch genug bewertet werden. Die ersten Untersuchungen sind bereits veröffentlicht oder befinden sich noch im Prozess, und doch gibt es für die *scientific community* noch viel zu tun.

Literaturverzeichnis

Adloff, Frank (2005). *Zivilgesellschaft. Theorie und politische Praxis*, Campus Verlag Frankfurt/Main.

AK Vorrat (2013a). Ortsgruppen, URL: www.vorratsdatenspeicherung.de/component?option=com_mambowiki/Itemid,110/lang,de/. Zugriff am 29.10.2014.

AK Vorrat (2013b). Wahlprüfsteine zur Bundestagswahl 2013, URL: www.vorratsdatenspeicherung.de/content/view/724/1/lang,de/, Zugriff am 29.10.2014.

AK Vorrat. Über uns, URL: www.vorratsdatenspeicherung.de/content/view/13/37/lang,de, Zugriff am 29.10.2014.

Alenfelder, Heinz/ Weichert, Thilo (1999). Meilensteine, URL: www.daten-schutzverein.de/vereinsprofil/meilensteine, Zugriff am 29.10.2014.

Anonymus (1988). In die Falle. In: *Der Spiegel* Nr. 12, 109-111, URL: [magazin.spiegel.de /EpubDelivery/spiegel/pdf/13528129](http://magazin.spiegel.de/EpubDelivery/spiegel/pdf/13528129), Zugriff am 29.10.2014.

Assange, Julian/ Appelbaum, Jacob/ Müller-Maguhn, Andy/ Zimmermann, Jérémie (2013). *Cypherpunkt. Unsere Freiheit und die Zukunft des Internets*, Campus Verlag Frankfurt/Main.

Baringhorst, Sigrid (2014). Internet und Protest. Zum Wandel von Organisationsformen und Handlungsrepertoires - Ein Überblick. In: *Voss, Kathrin* (Hrsg.): *Internet und Partizipation. Bottom-up oder Top-down? Politische Beteiligungsmöglichkeiten im Internet*, Springer Fachmedien Wiesbaden, S. 91-113.

- Bartels, Henning* (2013). Die Vorgeschichte: Die Urheberrechtsdebatte und die schwedische Piratpartei. In: Niedermayer, Oskar (Hrsg.). Die Piratenpartei, Springer Fachmedien, S. 15-28.
- Beckedahl, Markus/ Lüke, Falk* (2012). Die digitale Gesellschaft. Netzpolitik, Bürgerrechte und die Machtfrage, Deutscher Taschenbuch Verlag München.
- Behördenspiegel* (2013). Die Situationslogik von #Neuland. In: Behördenspiegel Nr. 07.
- Behrens, Maria* (2003). Quantitative und qualitative Methoden in der Politikfeldanalyse. In: *Schubert, Klaus/ Bandelow, Nils C.* (Hrsg.). Lehrbuch der Politikfeldanalyse, Oldenbourg München, S. 203-236.
- Bennett, Colin J.* (2012). Privacy advocates, privacy advocacy and the surveillance society. In: *Ball, Kirstie/ Haggerty, Kevin/ Lyon, David* (Hrsg.). Routledge Handbook of Surveillance Studies, Routledge New York, S. 412-419.
- Berlinghoff, Marcel* (2013). Computerisierung und Privatheit - Historische Perspektiven. In: APuZ - Aus Politik und Zeitgeschichte 65, 15-16, S. 14-19.
- Betz, Joachim/ Kübler, Hans-Dieter* (2013). Internet Governance. Wer regiert wie das Internet?, Springer Fachmedien Wiesbaden.
- BDI (Bund der deutschen Industrie) e.V.*: Übersicht aller Mitgliedsverbände, URL: www.bdi.eu/Uebersicht-aller-Mitgliedsverbaende.htm, Zugriff am 29.10.2014.
- Big Brother Award* (2014). URL: www.bigbrotherawards.de, Zugriff am 29.10.2014.
- BITKOM e.V.* (2013a). Satzung, URL: www.bitkom.org/files/documents/BITKOM_Satzung_23.07.2013.pdf, Zugriff am 29.10.2014.
- BITKOM e.V.* (2013b): BITKOM-Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden, Datenschutz und Datensicherheit, URL: www.bitkom.org/files/documents/BITKOM-Positionspapier_Abhoermassnahmen.pdf, Zugriff am 29.10.2014.

- BITKOM e.V.* (a). Datenschutz für alle, URL: www.bitkom-datenschutz.de/43855.aspx, Zugriff am 29.10.2014.
- BITKOM e.V.* (b). Leistungen, URL: www.bitkom.org/de/wir_ueber_uns/38251.aspx, Zugriff am 29.10.2014.
- BITKOM Trend Kongress* (2014). Unsere Sprecher, URL: www.bitkom-trendkongress.de/speaker, Zugriff am 29.10.2014.
- Blog Vorratsdatenspeicherung* (2014). Blog des Arbeitskreises Vorratsdatenspeicherung, URL: blog.vorratsdatenspeicherung.de, Zugriff am 29.10.2014.
- BMWi – Bundesministerium für Wirtschaft und Energie* (2014a). Digitale Agenda, URL: www.bmwi.de/DE/Themen/Digitale-Welt/digitale-agenda.html, Zugriff am 29.10.2014.
- BMWi – Bundesministerium für Wirtschaft und Energie* (2014b). Beiräte beim Bundesministerium für Wirtschaft und Energie, URL: www.bmwi.de/DE/Ministerium/beiraete,did=545858.html, Zugriff am 29.10.2014.
- BMWi – Bundesministerium für Wirtschaft und Energie* (2014c). Nationaler IT-Gipfel, URL: www.it-gipfel.de/IT-Gipfel/Navigation/Gipfel2014/programm.html, Zugriff am 12.10.2014.
- Bpb – Bundeszentrale für politische Bildung* (2009): Hintergrund aktuell, URL: www.bpb.de/politik/hintergrund-aktuell/69237/vorratsdatenspeicherung-14-12-2009, Zugriff am 29.10.2014.
- Brinkmann, Bastian* (2014). Google hortet Milliarden. In: *Süddeutsche Zeitung* vom 22.05.2014, S. 20.
- Bundesanzeiger* (2013). Google Germany GmbH – Jahresabschluss für das Geschäftsjahr vom 1. Januar 2012 bis zum 31. Dezember 2012, URL: www.bundesanzeiger.de/ebanzwww/wexsservlet, Zugriff am 29.10.2014.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2005). Safe Harbor, URL: www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/SafeHarbor.html, Zugriff am 29.10.2014.

Bundesverfassungsgericht (2012). Pressemitteilung Nr. 74/2012 vom 25. Oktober 2012, Informationen und Verhandlungsgliederung zur mündlichen Verhandlung in Sachen „Antiterrordatei“, URL: www.bundesverfassungsgericht.de/pressemitteilungen/bvg12-074.html, Zugriff am 29.10.2014.

Bundeszentrale für politische Bildung (2011): Jahresbericht der Bundeszentrale für politische Bildung 2010/2011, URL: www.bpb.de/system/files/dokument_pdf/bpb_Jahresbericht_web-Reader_0.pdf, Zugriff am 29.10.2014.

Bündnis 90/ Die Grünen (2014). Rechenschaftsbericht für das Jahr 2012 gemäß § 23ff. Parteiengesetz (PartG), URL: www.gruene.de/fileadmin/user_upload/Dokumente/Rechenschaftsbericht_Gesamtpartei_2012.pdf, Zugriff am 29.10.2014.

Bündnis 90/ Die Grünen (2013). Zeit für den grünen Wandel. Bundestagswahlprogramm 2013, URL: www.gruene.de/fileadmin/user_upload/Dokumente/Wahlprogramm/Wahlprogramm-barrierefrei.pdf, Zugriff am 11.10.2014.

Bündnis 90/ Die Grünen Bundestagsfraktion (2012). Netzpolitischer Kongress: Programm, URL: http://www.gruene-bundestag.de/fraktion/netzpolitischerkongress_ID_4385426/programm_ID_4385513.html, Zugriff am 29.10.2014.

Bündnis 90/ Die Grünen Bundestagsfraktion (2014). Newsletter Digitale Bürgerrechte 01/2014, URL: http://www.gruene-bundestag.de/news/newsletter/digitale-buergerrechte/neu-newsletter-digitale-buergerrechte_ID_4392466.html, Zugriff am 29.10.2014.

Bündnis 90/ Die Grünen Bundestagsfraktion (2014). V wie Vorratsdatenspeicherung, URL: http://www.gruene-bundestag.de/themen/digitale-buergerrechte_ID_4390734/v-wie-vorratsdatenspeicherung_ID_4391383.html, Zugriff am 29.10.2014.

- Busse, Caspar* (2014). Alle gegen Google. In: Süddeutsche Zeitung vom 21.05.2014, S. 17.
- Carroll, William K./Hackett, Robert A.* (2005). Democratic media activism through the lens of social movement theory. In: *Media, Culture & Society* 28, S. 83-104.
- CCCde Videos* (2013). Jahresrückblick des CCC 2013 [30C3[preview]]; URL: www.youtube.com/watch?v=a4Mb2BwtliM; Zugriff am 29.10.2014.
- CCC e.V.* (2014). Satzung des CCC e.V.; URL: www.ccc.de/satzung; Zugriff am 29.10.2014.
- CCC e.V. (a).* Hackerethik, URL: www.ccc.de/de/hackerethik, Zugriff am 29.10.2014.
- CCC e.V. (b).* Sponsoren, URL: www.ccc.de/de/sponsors, Zugriff am 29.10.2014.
- Collins, Randall* (2010). The Contentious Social Interactionism of Charles Tilly. In: *Social Psychology Quarterly* 73, 1, S. 5-10.
- CNBC on youtube* (2009). Google CEO Eric Schmidt on privacy, URL: www.youtube.com/watch?v=A6e7wfDHzew, Zugriff am 29.10.2014.
- Deutscher Bundestag* (2013). Mitglieder der Enquete-Kommission Internet und digitale Gesellschaft, URL: webarchiv.bundestag.de/cgi/show.php?fileToLoad=2944&id=1223, Zugriff am 29.10.2014.
- Deutscher Bundestag* (2014). Bekanntmachung der öffentlichen Liste über die Registrierung von Verbänden und deren Vertretern, URL: www.bundestag.de/blob/189456/e00253c016167c41eeb65faf480bb0db/lobby_listeamtlich-data.pdf, Zugriff am 09.10.2014.
- Drezner, Daniel W.* (2010). Weighing the Scales: The Internet's Effect On State-Society Relations. In: *The Brown Journal of World Affairs* XVI, 11, S. 31-44.
- DVD e.V.* (2014). Presseerklärung – Diese Geheimdienste sind nicht reformierbar, URL:

www.datenschutzverein.de/wp-content/uploads/2014/06/2014_06-Geheimdienste.pdf, Zugriff am 29.10.2014.

DVD e.V. (2011). Beschäftigtendatenschutz, URL: www.datenschutzverein.de/themen/arbeitnehmerdatenschutz, Zugriff am 29.10.2014.

DVD e.V. (2006). Satzung der deutschen Vereinigung für Datenschutz, URL: www.datenschutzverein.de/wp-content/uploads/2013/03/satzung_dvd.pdf, Zugriff am 29.10.2014.

Erdgeist (2008). Chaos Computer Club konkretisiert Biometrie-Debatte an Schäubles Fingerabdruck, URL: www.ccc.de/de/updates/2008/schaubles-finger, Zugriff am 29.10.2014.

ESC Wirtschaftsprüfungsgesellschaft (2013). Bericht über die Prüfung des Rechenschaftsberichts der Piratenpartei Deutschland (PIRATEN) für das Kalenderjahr 2011, URL: wiki.piratenpartei.de/Datei:Pr%C3%BCfbericht_Piratenpartei_2011.pdf, Zugriff am 29.10.2014.

EuGH; Große Kammer (2014). Urteil des Gerichtshofes in der Rechtssache C-131/12, URL: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1>, Zugriff am 10.10.2014.

EuGH, Große Kammer (2010). Urteil des Gerichtshofes In der Rechtssache C-518/07, URL: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=528958>, Zugriff am 11.10.2014.

Europäische Kommission (2011). Krakauer Forum 2011 URL: ec.europa.eu/internal_market/forum/krakow-2011/index_de.htm, Zugriff am 29.10.2014.

European Digital Rights (2014). About EDRI, URL: edri.org/about/, Zugriff am 29.10.2014.

- Events CCC*. Supporters, URL: events.ccc.de/congress/2013/wiki/Static:Supporters, Zugriff am 29.10.2014.
- Finkle, Todd A.* (2012). Corporate Entrepreneurship and Innovation in Silicon Valley: The Case of Google, Inc.. In: *Entrepreneurship Theory and Practice* 36, 4, S. 863-884.
- Freiheit statt Angst* (2014). Wir haben viel erreicht. Hilf mit, den Protest weiter zu stärken, URL: freiheitstattangst.de/2014/09/wir-haben-viel-erreicht-hilf-mit-den-protest-weiter-zu-staerken/, Zugriff am 29.10.2014.
- Fritz, Johannes* (2013). Netzpolitische Entscheidungsprozesse. Datenschutz, Urheberrecht und Internetsperren in Deutschland und Großbritannien, Nomos Verlagsgesellschaft Baden-Baden.
- Fuchs, Christian/ Boersma, Kees/ Albrechtslund, Anders/ Sandoval, Marisol* (Hrsg.) (2011). Internet and Surveillance. The Challenges of Web 2.0 and Social Media. In: ebd. Internet and Surveillance. The Challenges of Web 2.0 and Social Media, Routledge New York.
- Gaycken, Sandro* (Hrsg.) (2013). Jenseits von 1984. Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft. Eine Versachlichung, transcript Verlag Bielefeld.
- Geiselberger, Heinrich* (Hrsg.) (2011). WikiLeaks und die Folgen. Die Hintergründe. Die Konsequenzen, edition suhrkamp Sonderdruck Berlin.
- Glasstetter, Gabi/ Meyer, Uta* (2011): Akte CCC - Der Chaos Computer Club (Dokumentarfilm), ZDF/3sat, URL: www.youtube.com/watch?v=lQYAuGBO3Mw, Zugriff am 29.10.2014.
- Google*. Woran wir glauben – Unsere zehn Grundsätze, URL: www.google.com/intl/de_de/about/company/philosophy/, Zugriff am 29.10.2014.
- Grimme Online Award* (2014). Preisträger 2014, URL: www.grimme-institut.de/html/index.php?id=1908, Zugriff am 29.10.2014.

- Gruber, Helmut/ Huemer, Birgit/ Rheindorf, Markus* (2009). *Wissenschaftliches Schreiben. Ein Praxisbuch für Studierende der Geistes- und Sozialwissenschaften*, Böhlau Verlag Wien/ Köln/ Weimar.
- Härting, Niko/ Schneider, Jochen* (2011). Das Dilemma der Netzpolitik. In: *Zeitschrift für Rechtspolitik* 44, 8, S. 233-236.
- Hartmann, Jürgen/Sanders, Luise* (2013). *Literaturkompass Politikwissenschaft. Einführung in die politikwissenschaftliche Literatur*, VS Verlag Wiesbaden.
- Heinrich Böll Stiftung*: Dossier: Überwachung, Geheimdienste & Demokratie, URL: <http://www.boell.de/de/dossier-ueberwachung-geheimdienste-demokratie>, Zugriff am 29.10.2014.
- Heise Online* (2014). Chaos Computer Club unterstützt Edward Snowden mit 36.000 EUR. In: *heise online* vom 10.06.2014, URL: www.heise.de/newsticker/meldung/Chaos-Computer-Club-unterstuetzt-Edward-Snowden-mit-36-000-Euro-2305078.html, Zugriff am 29.10.2014.
- Heller, Christian* (2014). *plomlompom a.k.a. Christian Heller*, URL: www.plomlompom.de/index.de.html#topic_postprivacy, Zugriff am 29.10.2014.
- Hustinx, Peter* (2012). Informationsfreiheit und Datenschutz in der Europäischen Union. In: Schmidt, Jan-Hinrik/ Weichert, Thilo (Hrsg.). *Datenschutz. Grundlagen, Entwicklungen und Kontroversen*, Bundeszentrale für politische Bildung Bonn, S. 322-330.
- Initiative D21* (2013). *D21 - Digital – Index: Auf dem Weg in ein digitales Deutschland?!* URL: www.initiatived21.de/wp-content/uploads/2013/04/digitalindex.pdf, Zugriff am 29.10.2014.
- Initiative D21* (2008). *Satzung*, URL: www.initiatived21.de/wp-content/uploads/2008/11/d21-satzung.pdf, Zugriff am 29.10.2014

- Initiative D21* (a). Struktur und Organisation, URL: www.initiaved21.de/ueber/struktur/, Zugriff am 29.10.2014.
- Initiative D21* (b). Über uns – Vorstellung des Vereins, URL: www.initiaved21.de/ueber/, Zugriff am 29.10.2014.
- Initiative D21 e.V./ Bayerisches Staatsministerium der Justiz und für Verbraucherschutz*. Gut zu wissen! Sicher in sozialen Netzwerken, URL: www.initiaved21.de/wp-content/uploads/2012/08/Soziale-netzwerke_web.pdf, Zugriff am 29.10.2014.
- Jenkins, J. C.* (1983). Ressource Mobilization Theory and the Study of Social Movements. In: *Annual Reviews Sociology* 9, S. 527-553.
- Keller, Reiner* (2011). Diskursforschung. Eine Einführung für SozialwissenschaftlerInnen, 4. Auflage, Springer Fachmedien Wiesbaden.
- Knoepfel, Peter/ Larrue, Corinne/ Varone, Frédéric/ Veit, Sylvia* (2011). Politikanalyse. Verlag Barbara Budrich Opladen & Farmington Hills.
- Krempf, Stefan* (2013). 30c3: Snowden-Effekt beschert Hackertreffen Besucherrekord. In: Heise Online, URL: www.heise.de/newsticker/meldung/30C3-Snowden-Effekt-beschert-Hackertreffen-Besucherrekord-2073128.html, Zugriff am 29.10.2014.
- Kurz, Constanze/ Rieger, Frank* (2012). Die Datenfresser, erweiterte Taschenbuchauflage, S. Fischer Verlag Frankfurt am Main.
- Landtagspiraten* (2014). Die Piratenpartei in deutschen Landtagen, URL: www.landtagspiraten.de, Zugriff am 29.10.2014.
- Levi, Michael/ Wall, David S.* (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society. In: *Journal of Law and Society* 31, 2, S. 194-220.

- Lewis, James A.* (2010). Sovereignty and the Role of Government in Cyberspace. In: The Brown Journal of World Affairs XVI, 11, S. 55-65.
- Lüke, Falk* (2012): Datenschutz aus Verbrauchersicht. In: Schmidt, Jan-Hinrik/ Weichert, Thilo (Hrsg.). Datenschutz. Grundlagen, Entwicklungen und Kontroversen, Bundeszentrale für politische Bildung Bonn, S. 154-164.
- Magoulas, Roger/ Lorica, Ben* (2009). Big Data. In: Release 2.0, O'Reilly Radar 11, S. 1-39.
- Manigk, Robert* (2011). ePetition: Bürgerrechtler sammeln 50.000 Unterschriften für Verbot der Vorratsdatenspeicherung, URL: piraten-sachsen.de/tag/ak-vorrat/, Zugriff am 29.10.2014.
- Mai, Manfred* (2012). Die politischen Dimensionen der Zivilgesellschaft. In: Sozialwissenschaften Und Berufspraxis 35, 2, S. 233-248.
- Manne, Geoffrey A./ Wright, Joshua D.* (2011). Google and the Limits of Antitrust: The Case against the case against Google. In: Harvard Journal of Law & Public Policy 34, 1, S. 171-264.
- Martin-Jung, Helmut* (2014). Der Gorilla und die Regeln. In: Süddeutsche Zeitung vom 22.05.2014, S. 17.
- McCarthy, John/ Zald, Mayer N.* (1977). Ressource Mobilization and Social Movements: A Partial Theory. In: American Journal of Sociology 82, 6, S. 1212-1241.
- McMillan, Robert* (2012). Google: We're One of the World's Largest Hardware Makers. In: Wired, URL: www.wired.com/2012/06/google_makes_servers, Zugriff am 29.10.2014.
- Morozov, Evgeny* (2011). The Net Delusion. The dark side of internet freedom, First edition, Public Affairs New York.

- Müller, Ragnar/ Plieninger, Jürgen/ Rapp, Christian* (2013). Recherche 2.0. Finden und Weiterverarbeiten in Studium und Beruf, Springer Fachmedien Wiesbaden.
- Netzpolitik.org* (2014). Vielen Dank! Chaos Computer Club spendet an netzpolitik.org, URL: netzpolitik.org/2014/chaos-computer-club-unterstuetzt-netzpolitik-org-finanziell, Zugriff am 29.10.2014.
- Netzpolitik.org* (2013). Unser Blog soll schöner werden (V): Finanzierung, URL: netzpolitik.org/2013/unser-blog-soll-schoener-werden-v-finanzierung, Zugriff am 29.10.2014.
- Netzpolitik.org* (2010). Peter Schaar antwortet auf offenen Brief des AK-Vorrat, URL: netzpolitik.org/2010/peter-schaar-antwortet-auf-offenen-brief-des-ak-vorrat, Zugriff am 29.10.2014.
- Netzpolitik.org* (a). Über uns, URL: netzpolitik.org/about-this-blog, Zugriff am 29.10.2014.
- Netzpolitik.org* (b). Stellenanzeige buchen, URL: netzpolitik.org/stellenanzeige-buchen, Zugriff am 29.10.2014.
- Newthinking*. Netzwerk, URL: newthinking.de/about/network, Zugriff am 29.10.2014.
- Niedermayer, Oskar* (Hrsg.) (2013a). Die Piratenpartei, Springer Fachmedien Wiesbaden.
- Niedermayer, Oskar* (2013b). Parteimitglieder in Deutschland: Version 2013. In: Arbeitshefte aus dem Otto-Strammer-Zentrum Nr. 20, Freie Universität Berlin, URL: www.polsoz.fu-berlin.de/polwiss/forschung/systeme/empsoz/schriften/Arbeitshefte/ahosz20.pdf?1370258727, Zugriff am 29.10.2014.
- O'Reilly, Tim* (2005). What is Web 2.0. Desing Patterns and Business Models for the Next Generation of Software, URL: <http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0CGAQFjAH&url=http%3A%2F%2Ffacweb.cti.depaul.edu%2Fjnowotarski%2Fse425%2FWhat%2520Is%2520>

Web%25202%2520point%25200.pdf&ei=0QgkVLWcDMHg7Qak3IHACg&usg=AFQjCNGJRQaZiBySB_FXbvbj6JXl4Uq2mw&bvm=bv.76247554,d.ZGU, Zugriff am 29.10.2014.

Orle, Manfred (2014). Wegfall des Gatekeeper-Monopols der Journalisten. In: Deutscher Medienverband – Blog!, URL: blog.dmv-verband.de/wegfall-des-gatekeeper-monopols-der-journalisten, Zugriff am 29.10.2014.

Passig, Kathrin/ Lobo, Sascha (2012). Internet. Segen oder Fluch, Sonderausgabe für die Bundeszentrale für politische Bildung, Bundeszentrale für politische Bildung Bonn.

Pimpl, Roland (2013). Google: Philipp Justus folgt Stefan Tweraser als Deutschland-Chef. In: Horizont.net, URL: www.horizont.net/medien/nachrichten/-Google-Philipp-Justus-folgt-Stefan-Tweraser-als-Deutschland-Chef-114643, Zugriff am 29.10.2014.

Piratenforum (2014). Sync-Forum Piratenpartei Deutschland, URL: news.piratenpartei.de/forumdisplay.php?fid=334, Zugriff am 29.10.2014.

Piratenpartei (2014). Bundessatzung, URL: wiki.piratenpartei.de/Bundessatzung, Zugriff am 29.10.2014.

Piratenpartei (2013). Wahlprogramm, URL: www.piratenpartei.de/wp-content/uploads/2013/06/PP-Bund-BTW13v1.pdf, Zugriff am 29.10.2014.

Piratenwiki (2014). Mitglieder, URL: wiki.piratenpartei.de/Mitglieder, Zugriff am 29.10.2014.

Pirate Party International (2014). About the PPI, URL: www.pp-international.net/about, Zugriff am 29.10.2014.

Prantl, Heribert (2014). Totalverlust eines Grundrechts. In: Süddeutsche.de vom 04.10.2014, URL: www.sueddeutsche.de/politik/operation-eikon-al-totalverlust-eines-grundrechts-1.2157335, Zugriff am 29.10.2014.

- Probst, Lothar* (2007). Bündnis90/Die Grünen. In: Decker, Frank/ Neu, Viola (Hrsg.). Handbuch der deutschen Parteien. Bundeszentrale für politische Bildung Bonn, S. 173-188.
- Raab, Charles D.* (2010). Information Privacy: Networks of Regulation at the Subglobal Level. In: *Global Policy* 1, 3, S. 291-302.
- Redaktion der Datenschleuder* (2011). Geleitwort. In: Die Datenschleuder. Fachblatt Für Datenreisende #96, URL: ds.ccc.de/pdfs/ds096.pdf, Zugriff am 29.10.2014, S. 1-2.
- Re:publica* (2014). Michael Seemann, URL: www.re-publica.de/user/948/event/1, Zugriff am 29.10.2014.
- Reus, Jonathan* (2011). Fingerprint Forgery Workshop. In: Mediamatic, URL: www.mediamatic.net/213482/en/fingerprint-forgery-workshop; Zugriff am 29.10.2014.
- Röhr, Matthias* (2012). Ursprünge und Entwicklung des Chaos Computer Clubs in den 1980er Jahren, URL: blog.stummkonzert.de/wp-content/uploads/2013/09/Matthias-R%C3%B6hr-Urspr%C3%BCnge-und-Entwicklung-des-Chaos-Computer-Clubs-in-den-Achtziger-Jahren.pdf, Zugriff am 29.10.2014.
- Roßnagel, Alexander* (2012). Modernisierung des Datenschutzrechts. In: Schmidt, Jan-Hinrik/ Weichert, Thilo (Hrsg.). Datenschutz. Grundlagen, Entwicklungen und Kontroversen. Bundeszentrale für politische Bildung Bonn, S. 331-344.
- Roßnagel, Alexander* (2006). Datenschutz im 21. Jahrhundert. In: APuZ - Aus Politik und Zeitgeschichte 5-6, S. 9-15.
- Rzepka, Dominik* (2014). Austrittswelle aus der Piratenpartei. In: ZDF heute.de, URL: www.heute.de/austrittswelle-bei-der-piratenpartei-nach-lauer-und-hoefinghoff-geht-auch-domscheit-berg-35083984.html, Zugriff am 29.10.2014.
- Sabatier, Paul A.* (1988). An advocacy coalition framework of policy change and the role of policy-oriented learning therein. In: *Policy Sciences* 21, 2-3, S. 129-168.

- Schmid, Josef/ Buhr, Daniel/ Roth, Christian/ Steffen, Christian*, (2006).
Wirtschaftspolitik für Politologen, Schöningh Paderborn.
- Schmidt, Jan-Hinrik/ Weichert, Thilo* (Hrsg.) (2012). Datenschutz. Grundlagen, Entwicklungen und Kontroversen, Bundeszentrale für politische Bildung Bonn.
- Schneider, Volker* (2003). Akteurkonstellationen und Netzwerke in der Politikentwicklung. In: Schubert, Klaus/ Bandelow, Nils C. (Hrsg.). Lehrbuch der Politikfeldanalyse, Oldenbourg München, S. 107-146.
- Schramm, Julia* (2011a) in: Grün Digital: Datenschutz, Post-Privacy und die Spackeria im Podcast, URL: folgen.politology.de/008_Politology_-_Ueber_Datenschutz_Post_Privacy_Spackeria.mp3, Zugriff am 29.10.2014.
- Schramm, Julia* (2011b), zitiert nach: Reißmann, Ole: Internet Exhibitionisten „Spackeria“: „Privatsphäre ist sowas von Eighties. In: Spiegel online vom 10.03.2014, URL: www.spiegel.de/netzwelt/netzpolitik/internet-exhibitionisten-spackeria-privatsphaere-ist-sowas-von-eighties-a-749831.html, Zugriff am 29.10.2014.
- Schröder, Michael* (Hrsg.) (2012). Die Web-Revolution. Das Internet verändert Politik und Medien, Olzog Verlag München.
- Schrutzki, R.* (2002). Hackerethik 2002. In: Die Datenschleuder. Fachblatt Für Datenreisende #77, S. 38-39.
- Schubert, Klaus/ Bandelow, Nils* (2003). Lehrbuch der Politikfeldanalyse. Oldenbourg München.
- Schuler, Karin* (2014). Wer nicht kämpft, hat schon verloren. In: FIF-Kommunikation 1/14, S.34-37, URL: www.datenschutzverein.de/wp-content/uploads/2014/04/FIF_01_14_Schuler.pdf, Zugriff am 29.10.2014.

- Schultze, Rainer-Olaf* (2008). Partizipation. In: Nohlen, Dieter/ Grotz, Florian (Hrsg.). Kleines Lexikon der Politik. Bundeszentrale für politische Bildung Bonn, S. 398-400.
- Seeman, Michael* (2011a). Was ist Postprivacy (für mich)? URL: www.ctrl-verlust.net/was-ist-postprivacy-fur-mich, Zugriff am 29.10.2014.
- Seemann, Michael* (2011b). The Rise of Spackeria, URL: www.ctrl-verlust.net/the-rise-of-spackeria, Zugriff am 29.10.2014.
- SKS Keyserver* (2014). Statistics, URL: sks-keyservers.net/status/key_development.php, Zugriff am 29.10.2014.
- SRIW e.V. (Selbstregulierung Internetwirtschaft e.V.)* (2014a): Ziele des Vereins, URL: www.sriw.de/, Zugriff am 29.10.2014.
- SRIW e.V. (Selbstregulierung Internetwirtschaft e.V.)* (2014b). Mitgliederverzeichnis, URL: www.sriw.de/index.php/home/organisation/mitgliederverzeichnis, Zugriff am 29.10.2014.
- Statista* (2014a). Umsatz von Google weltweit in den Jahren 2002 bis 2013 (in Milliarden US-Dollar), URL: de.statista.com/statistik/daten/studie/74364/umfrage/umsatz-von-google-seit-2002, Zugriff am 29.10.2014.
- Statista* (2014b). Nettogewinn von Google in den Jahren von 2001 bis 2013 (in Millionen US-Dollar), URL: de.statista.com/statistik/daten/studie/76456/umfrage/nettogewinn-von-google-seit-2001, Zugriff am 29.10.2014.
- Statista* (2014c). Top 20 soziale Netzwerke in Deutschland nach Anzahl der Visits* im Februar 2014 (in Millionen), URL: de.statista.com/statistik/daten/studie/70232/umfrage/soziale-netzwerke---nutzer-pro-monat, Zugriff am 29.10.2014.
- Staufenbiel* (2014). Google Deutschland GmbH, URL: www.staufenbiel.de/job-arbeitgeber/google/das-unternehmen.html, Zugriff am 29.10.2014

- Steiner, Falk* (2013). Die Enquete-Kommission „Internet und Digitale Gesellschaft“: Zivilgesellschaftlich ein Erfolg – oder ein Ausfall?. In: *Forschungsjournal Soziale Bewegungen* 26, 2, S. 83-88.
- Suda, Yuko* (2013). Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism. In: *Journal of Current Market Studies* 51, 4, S. 772-788.
- SZ-Redaktion* (2011). Enthüllungsportal: WikiLeaks verliert 480.000 EUR pro Woche, in *Süddeutsche.de* am 10.01.2011, URL: www.sueddeutsche.de/digital/enthuellungsportal-wikileaks-verliert-euro-pro-woche-1.1044633, Zugriff am 29.10.2014.
- Thiery, Peter* (2008). Zivilgesellschaft. In: Nohlen, Dieter/ Grotz, Florian (Hrsg.). *Kleines Lexikon der Politik*, Bundeszentrale für politische Bildung Bonn, S. 655-657.
- Tilly, Charles* (1998). Social movements and (all sorts of) other political interactions - local, national, and international - including identities. In: *Theory and Society* 27, 4, S. 453-480.
- Tilly, Charles* (1978). *From Mobilization to Revolution*. Addison-Wesley Publishing Company Reading/ Menlo Park u. A.
- Tor Project* (2014). Tor Metrics: Users, URL: metrics.torproject.org/users.html, Zugriff am 29.10.2014.
- Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein* (2014a). Chronik der Dienststelle des Landesbeauftragten für Datenschutz Schleswig-Holstein/ des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein ab 1978, URL: <https://www.datenschutzzentrum.de/ldsh/chronik>, Zugriff am 29.10.2014.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2014b). Thilo Weichert. Literaturübersicht zum Thema Datenschutz und Informationstechnik, URL: <https://www.datenschutzzentrum.de/ldsh/veroeffentlichungen-weichert.html>, Zugriff am 29.10.2014.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2014c). Pressemitteilung. OVG Schleswig-Holstein verhandelt in Sachen Facebook-Fanpages, URL: <https://www.datenschutzzentrum.de/presse/20140901-ovg-sh-facebook.htm>, Zugriff am 29.10.2014.

Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein (2013a). EuroPriSe - European Privacy Seal. Das Europäische Datenschutz-Gütesiegel beim ULD Schleswig-Holstein, URL: <https://www.datenschutzzentrum.de/europrise>, Zugriff am 29.10.2014.

Unabhängiges Landeszentrum Schleswig-Holstein (2013b). Tätigkeitsbericht 2013 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, URL: <https://www.datenschutzzentrum.de/material/tb/tb34/uld-34-taetigkeitsbericht-2013.pdf>, Zugriff am 29.10.2014.

Vise, David A. (2006). GOOGLE. In: Foreign Policy 154, S. 20-24.

von Lewinski, Kai (2012). Zur Geschichte von Privatsphäre und Datenschutz -- eine rechtshistorische Perspektive. In: Schmidt, Jan-Hinrik/ Weichert, Thilo (Hrsg.), Datenschutz. Grundlagen, Entwicklungen und Kontroversen, Bundeszentrale für politische Bildung Bonn, S. 23-33.

Voss, Kathrin (Hrsg.) (2014). Internet und Partizipation. Bottom-up oder Top-down? Politische Beteiligungsmöglichkeiten im Internet, Springer Fachmedien Wiesbaden.

- Vowe, Gerhard* (2014). Digital Citizens und Schweigende Mehrheit: Wie verändert sich die politische Beteiligung der Bürger durch das Internet? Ergebnisse einer kommunikationswissenschaftlichen Langzeitstudie. In: Voss, Kathrin (Hrsg.), Internet und Partizipation. Bottom-up oder Top-down? Politische Beteiligungsmöglichkeiten im Internet, Springer Fachmedien Wiesbaden, S. 25-52.
- Weidemann, Stefan* (2014). Freiheit unter Beobachtung?. In: APuZ - Aus Politik Und Zeitgeschichte 64, 18-19, S. 3-8.
- Wendelin, Manuela/ Löblich, Maria* (2013). Netzpolitik-Aktivismus in Deutschland. In: Medien und Kommunikation 63, 1, S. 58-75.
- WikiLeaks* (2011). About – What is WikiLeaks?, URL: wikileaks.org/About.html, Zugriff am 29.10.2014.
- Wiki Vorratsdatenspeicherung* (2014). URL: [wiki.vorratsdatenspeicherung.de /AktivCongrEZ_2014](http://wiki.vorratsdatenspeicherung.de/AktivCongrEZ_2014), Zugriff am 29.10.2014.
- Wilkens, Andreas* (2014). Justizminister: Kein nationaler Alleingang zur Vorratsdatenspeicherung. In: heise online, URL: <http://www.heise.de/newsticker/meldung/Justizminister-Kein-nationaler-Alleingang-zur-Vorratsdatenspeicherung-2218482.html>, Zugriff am 29.10.2014.
- Wong, Wendy H./ Brown, Peter A.* (2013). E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One. In: Perspectives on Politics 11, 4, S. 1015-1033.
- Zajácz, Rita* (2013). WikiLeaks and the problem of anonymity: A network control perspective. In: Media, Culture & Society 35, 4, S. 489-505.

Abkürzungsverzeichnis

ACF	Advocacy Coalition Framework
ACTA	Anti-Counterfeiting Trade Agreement
AK	Arbeitskreis
BAG	Bundesarbeitsgemeinschaft
BDI	Bund der Deutschen Industrie e.V.
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BND	Bundesnachrichtendienst
CCC	Chaos Computer Club
CEO	Chief Executive Officer
DVD	Deutsche Vereinigung für Datenschutz
EDRi	European Digital Rights
EG	Europäische Gemeinschaft
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
IKT	Informations- und Kommunikationstechnologien
NSA	National Security Agency

PET	Privacy Enhancing Technologies
PGP	Pretty Good Privacy
Quellen-TKÜ	Quellen-Telekommunikationsüberwachung
RBB	Rundfunk Berlin-Brandenburg
RMT	Ressourcenmobilisierungsansatz oder –theorie
SMI	Social Movement Industry
SMO	Social Movement Organisation
SMS	Social Movement Sector
SRIW	Selbstregulierung Informationswirtschaft e.V.
TTIP	Transatlantic Trade and Investment Partnership
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
VDS	Vorratsdatenspeicherung

ERKLÄRUNG GEM. § 7 Abs. 3
DER PRÜFUNGSORDNUNG
FÜR DEN
MASTERSTUDIENGANG POLITIKWISSENSCHAFT:
DEMOKRATISCHES REGIEREN UND
ZIVILGESELLSCHAFT

Hiermit versichere ich, dass ich die vorliegende Masterarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus Print- oder Online-Veröffentlichungen entnommen sind, sind als solche kenntlich gemacht.

Datum, Unterschrift