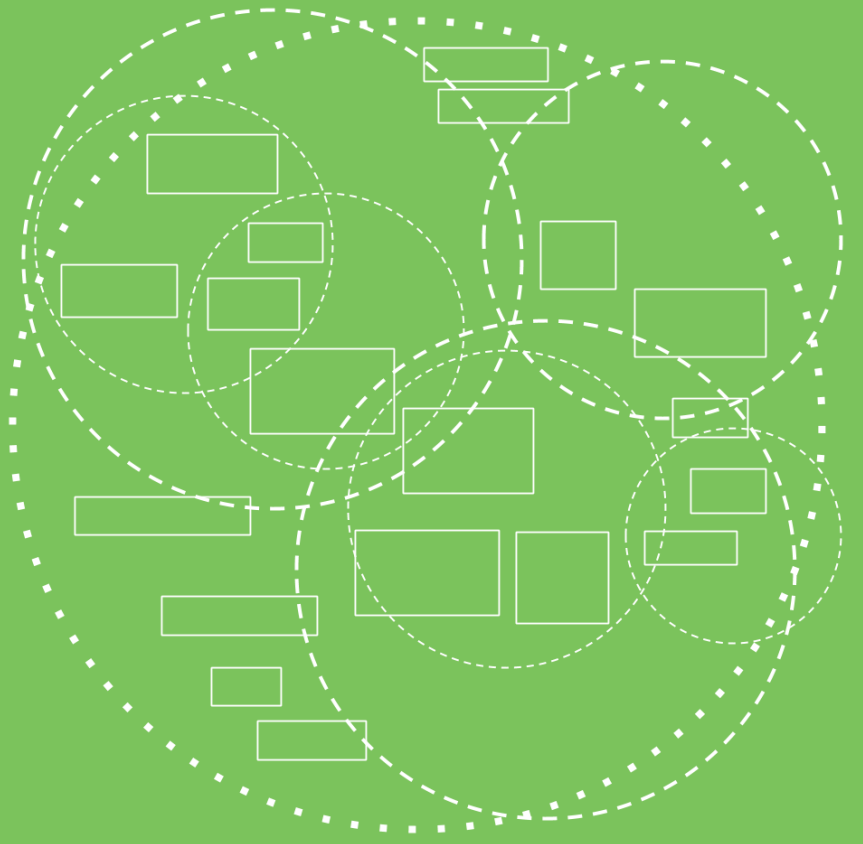

Die Reterritorialisierung des Digitalen

Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden

Barbara Büttner, Christian L. Geminn, Thilo Hagendorff,
Jörn Lamla, Simon Ledder, Carsten Ochs, Fabian Pittroff

kassel
university
press

Barbara Büttner, Christian L. Geminn, Thilo Hagendorff,
Jörn Lamla, Simon Ledder, Carsten Ochs, Fabian Pittroff

Die Reterritorialisierung des Digitalen

Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden

kassel university press

Das dieser Publikation zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS0096K gefördert. Die Verantwortung für den Inhalt der Veröffentlichung liegt bei den Autoren.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

ISBN 978-3-86219-106-2 (print)
ISBN 978-3-86219-107-9 (e-book)
DOI: http://dx.medra.org/10.19211/KUP9783862191079
URN: http://nbn-resolving.de/urn:nbn:de:0002-31078

www.upress.uni-kassel.de

Printed in Germany

Inhalt

1 Einleitung

Jörn Lamla

Die vorliegende Gemeinschaftsarbeit präsentiert den methodischen und theoretischen Forschungsansatz sowie Hypothesen und Ergebnisse aus der Explorationsphase eines BMBF-Verbundprojektes zur „Kartografie und Analyse der Privacy-Arena“.[1] An diesem Projekt sind die Disziplinen Soziologie (unter der Leitung von Jörn Lamla und Carsten Ochs, Universität Kassel), Rechtswissenschaft (unter der Leitung von Alexander Roßnagel und Silke Jandt, Universität Kassel) und Philosophie/Ethik (unter der Leitung von Regina Ammicht Quinn und Jessica Heesen, Universität Tübingen) beteiligt. Die zentrale Idee des Projektes besteht darin, Privatheit als umstrittenes Konzept nicht wissenschaftlich definieren zu wollen, sondern den Streit darum zum Ausgangspunkt der Analyse zu nehmen. Methodisch schließt es an soziologische Ansätze an, die sich dem Nachzeichnen komplexer Konfliktlandschaften und ihrer Wandlungsdynamik verschrieben haben. Hierzu zählen Ansätze des „Mapping of Controversies“, die aus den Science & Technology-Studies und der Akteur-Netzwerk-Theorie hervorgegangen sind, sowie die Mapping-Verfahren der Situationsanalyse von Adele Clarke (2012). Letztere greift auf die Theorie der Sozialen Welten und Arenen zurück, die Anselm Strauss (1978, 1993; vgl. Strübing 2007) entwickelt hat, um dem dynamischen Strukturwandel und der „Wissensorganisation in modernen Komplexgesellschaften“ (Schütze 2002) Rechnung zu tragen. Im Sinne dieses Ansatzes wird hier angenommen, dass sich auch um die Streitsache Privatheit eine komplexe Arena gebildet hat und dynamisch entwickelt, die durch eine Pluralität sozialer Welten konstituiert und vorangetrieben wird. Gegenwärtig kommt diese Arena insbesondere durch die Herausfor-

[1] Aus Gründen der sprachlichen Vereinheitlichung und Vereinfachung wurde auf ein Gendern verzichtet und nur die männliche Form verwendet. In der Regel sind alle Geschlechter angesprochen.

derungen der Digitalisierung stark in Bewegung und evoziert einen Strudel von Argumenten und Positionierungen seitens der Beteiligten und Betroffenen. Angesichts der Offenheit dieser Situation ist es für die interdisziplinäre Forschung zentral, die Figuration der Arena detailliert in den Blick zu nehmen, um tragfähige Hypothesen zu den sozialen, technischen, rechtlichen, politischen und ethischen Verschiebungen zu generieren, die mit dem gegenwärtigen Wandel der Privatheit im Zuge der Digitalisierung verknüpft sind.

Im Sinne der Grounded Theory hat sich der Projektverbund für einen spiralförmigen Forschungsprozess entschieden, um nach und nach zu generalisierenden Aussagen über die Privacy-Arena zu gelangen. Im Sinne dieses Vorgehens musste ein geeigneter und überschaubarer Zugang zum *Issue* Privatheit identifiziert werden. Daher stand am Anfang der nachfolgenden Exploration die forschungspragmatische Entscheidung, mit der Analyse einer spezifischen und überschaubaren Debatte in die Situationsanalyse einzusteigen. Ausgewählt wurde dafür die Kontroverse um *nationales Routing*, das in Reaktion auf die Enthüllungen Edward Snowdens und die dadurch aktualisierte Krise der Privatheit als Lösungsvorschlag ins Spiel gebracht wurde. Die Auswertung dieses empirischen Falles führte zu der Hypothese, dass sich im Vorschlag des nationalen Routings Bestrebungen zu einer *Reterritorialisierung des Digitalen* manifestieren, die mit Berufung auf den Wert der Privatheit und das (keineswegs deckungsgleiche) Recht auf informationelle Selbstbestimmung gerechtfertigt werden. Unklar und empirisch zu ermitteln ist dabei, wie diese Ausrichtung der Privacy-Politik motiviert ist: Resultiert sie aus vertieften Auseinandersetzungen mit den Problemen des Privatheitsschutzes im digitalen Zeitalter oder wiederholt sie nur die Routinen und Präferenzen etablierter sozialer Welten und politischer Traditionen? Der Verlauf der Auseinandersetzungen zeigt zwar, dass sich der Vorschlag eines nationalen oder europäischen Routings in der Arena nicht durchsetzen konnte und vorerst gescheitert ist, aber auch hierfür sind die Gründe nicht offensichtlich. Dieses Scheitern bedeutet jedenfalls nicht, dass auch die mit dem Vorschlag verbundene Logik der Reterritorialisierung

digitaler Netze und Kommunikationsströme vom Tisch ist. Die Analyse des Aushandlungsprozesses zum Vorschlag des nationalen Routings hat vielmehr zu allgemeineren Fragen und Hypothesen darüber geführt. Wie ist die Suche nach Antworten auf die Krise der Privatheit angesichts der Digitalisierung verbunden mit den bestehenden Institutionen, Routinen und Ressourcen des Rechts, der Staatlichkeit und der Demokratie? Welche Folgen werden die Reaktionen auf diese Krise für die Privatheit und das Verständnis von Freiheit und Selbstbestimmung zeitigen?

An dieser Stelle verschmilzt der wörtliche geopolitische Gehalt des Reterritorialisierungsbegriffs mit seiner abstrakteren metaphorischen Verwendungsweise in Philosophie und Sozialtheorie. Er bahnt einen Weg von den Niederungen der Router-Technologie und der nationalen Rechtsauslegungen des Telekommunikationsgeheimnisses hin zu Fragen der digitalen Neukonfiguration des Verhältnisses von Demokratie und Gesellschaft oder der Zukunft des Grundrechts auf informationelle Selbstbestimmung. Ausgehend vom Vorschlag des nationalen Routings meint Reterritorialisierung zunächst nicht viel mehr als den Versuch, problematischen Folgen der Digitalisierung mit einer Begrenzung digitaler Datenströme auf territorial bestimmte Rechtsräume zu begegnen. Während solche Rechtsräume derzeit laufend unkontrolliert überschritten und missachtet würden, sollen die Datenflüsse stattdessen an staatliche Grenzen zurückgebunden werden; entweder durch gesetzliche Vorschriften (etwa im Rahmen von Behördenkommunikation) oder durch die Bereitstellung infrastruktureller Möglichkeiten und deren freiwillige Nutzung (z.B. im privatwirtschaftlichen Bereich). Aber auf dem Spiel steht mehr als die räumliche Begrenzung von Datenpaketen, die Neutralität des Netzes gegenüber Inhalten oder die Wettbewerbsfähigkeit von Telekommunikationsunternehmen. In den Kämpfen und Debatten um ein nationales Routing artikulieren sich außerdem De- und Reterritorialisierungsbewegungen, die ganze Rechts-, Sozial- und Wissensordnungen

betreffen (vgl. Deleuze/Guattari 1994: 85-113, 1992).[2] Diese Bewegungen sind Anzeichen tektonischer Verschiebungen zwischen etablierten Institutionen und neu entstehenden territorialen Assemblagen (vgl. Sassen 2006).[3] Reterritorialisierung bedeutet daher mehr als

[2] Reterritorialisierung bedeutet bei Deleuze und Guattari nicht nur, dass politische Tendenzen oder Kraftvektoren, die eine bestehende staatliche Ordnung unter Druck setzen, dezentrieren oder erschüttern (Deterritorialisierung), unterbunden und an die alte Ordnung zurückgebunden werden. Vielmehr ist dies nur eine, nämlich die negative Variante von Reterritorialisierung. Dieser Variante stellen die Autoren eine positive, kreative Variante von Reterritorialisierung gegenüber, die auf Einbindung jener die alte Ordnung überschreitenden politischen Kräfte in eine neue Ordnung abstellt. Territorium ist dabei nicht allein als räumliche Ordnung zu verstehen, sondern als Metapher für Ordnung generell, kann also auch Wissensgefüge (Episteme), Rechtsordnungen o.ä. bezeichnen.

[3] Eine interessante Vergleichsfolie für die Untersuchung von Ambivalenzen der Reterritorialisierung des gesellschaftlichen Wandels bietet die Theorie von Sassen (2006). Sie argumentiert, dass die großen historischen Verschiebungen im Aufbau und in der Organisationslogik von Gesellschaften nicht als Nullsummenspiel zu verstehen sind, bei dem die Globalisierung nur durch einen entsprechenden Abbau von Nationalstaatlichkeit fortschreiten könnte. Vielmehr entstehe das Neue aus dem Alten, sogar als Reproduktion des Alten, also der Nationalstaatlichkeit, in die neue Elemente eingelassen werden oder aus der heraus einzelne Kapazitäten für neue Verbindungen abgezweigt werden. So entsteht etwa eine global agierende Zivilgesellschaft aus lokal gebundenen Initiativen, die keineswegs über kosmopolitische Werte oder Menschenrechte vorverständigt sind, sondern vom Boden des Nationalstaats und ausgehend von partikularen Problemen und Anliegen (z.B. Migrationsbewegungen, neuen Ungleichheiten, ökonomischen Interdependenzen oder digitaler Kommunikationstechnik mit neuen Mobilisierungsmöglichkeiten) den Rechts- und Handlungsraum partiell denationalisieren. Unter dem Aspekt der Dominanz gewichtiger sind mit Blick auf die Digitalisierung für Sassen (vgl. ebd.: 348-365) allerdings noch die globalen Netzwerke der Finanzzentren, die ihren lokalen Sitz in den *global cities* haben, von wo aus sie die territorialen Grenzen des Rechts und der (national-)staatlichen Autorität verschieben. (Im Konflikt zwischen der Deutschen Telekom und dem Internetknoten DE-CIX um das nationale Routing manifestiert sich auch der Konflikt unterschiedlicher gesellschaftlicher Organisationslogiken. So haben die genannten Unternehmen ihren Firmensitz oder Hauptstandort wohl nicht zufällig in Bonn bzw. Frankfurt am Main!) Auch das Recht bleibt einerseits nationalstaatlich gebunden, entwickelt andererseits aber durch Zunahme und Beschleunigung grenzüberschreitender Beziehungen und Interdependenzen eigene Geographien mit eigenen Gerichtsständen und außerstaatlichen Schiedsverfahren (vgl. ebd.: 386). Privatheit ist in diesem Zusammenhang nicht nur das von Überwachung und Datenmissbrauch bedrohte Schutzgut, sondern auch ein Kraftvektor der Verschiebungen, die sich in neuen Rechts- und Eigentumsordnungen und der Schwächung öffentlicher Gesetzgebungsverfahren gegenüber der Macht der Exekutive niederschlagen. Vor diesem Hintergrund sind auch die nationalstaatlichen Möglichkeiten, „through the indirect venue of hardware standards and whatever regulations of content circulation and intellectual property rights“ re-

Renationalisierung des Digitalen. In Verbindung mit den Kräften der Deterritorialisierung adressiert der Begriff den gesellschaftlichen Wandel im Zeitalter der Digitalisierung. Nicht nur Routing, auch Privatheit ist in diesem Sinne ein Senkblei, das in die Tiefen dieser Verschiebungen vordringen kann. Und erst die Analyse der maßgeblichen Kräfte dieses Wandels gestattet es, das ganze Ausmaß der Krise der Privatheit zu erfassen.

Was das nationale Routing und ähnliche Vorschläge für die Krise der Privatheit und die Zukunft demokratischer Selbstbestimmung genau bedeuten, wird letztlich ohne eine Analyse von Deterritorialisierungsbewegungen nicht zu beantworten sein. Denn die beteiligten und betroffenen sozialen Welten der Privacy-Arena sind in genau diese Prozesse verstrickt. Ist es wirklich das Grundrecht auf informationelle Selbstbestimmung, das hier gegen die immer weiter ausgreifende Erfassung und Auswertung personenbezogener Daten durch Unternehmen und Behörden geschützt, gestärkt und auf neue technische und rechtliche Grundlagen gestellt werden soll? Oder geht es den Vorschlägen in der Privacy-Arena nur vordergründig um den verfassungsrechtlichen Legitimationszusammenhang von informationeller Selbstbestimmung und robuster Demokratie? Verbergen sich hinter der Mobilisierung des Rechts womöglich andere Zwecke wie etwa der Schutz heimischer Industrien und privaten Kapitals im ökonomischen Standortwettbewerb der digitalen Revolution? Oder geht es darum, die Erschütterungen und Risse durch die kontinuierliche Anwendbarkeit des Rechts abzumildern, die die digitale Transformation von Kommunikationsströmen, Lebenspraktiken und Handlungsräumen dem nationalen Band zufügt? Geht es um eine Verteidigung nationalstaatlicher oder europäischer Souveränität, die im globalen Kampf um Verhandlungspositionen und Informationsvorteile kein Terrain an

territorialisierend auf den digitalen Raum einzuwirken (ebd.: 418), als ambivalent einzuschätzen. Folglich muss die Beobachtung, dass die Geltung des Rechts auf informationelle Selbstbestimmung breit bekräftigt wird (prevalence), keineswegs bedeuten, dass es auch noch die Kraft hat, die Gestaltung der digitalen Welt zu prägen (dominance). Es kann sich auch um ein Festklammern an längst verlorenes „Territorium“ handeln (vgl. ebd.: 421).

andere abgeben will? Oder wird auch die eigene Hinterzimmerpolitik, Datenerfassung und Überwachung im Innern der Nation als problematische Entwicklung für das normative Selbstverständnis angesehen? Kann eine Erneuerung der Privatheit und die Verteidigung ihres normativen Gehalts nur dann erreicht werden, wenn bei der Ausgestaltung des digitalen Rechtsraumes zunächst Transparenz, öffentliche Kontrolle und die politische Repräsentation der Betroffenen signifikant erhöht wird?

Diese Fragen sollten mitlaufen, wo es um die Kartographie und Analyse der Krise der Privatheit nach Snowden geht. Sie werden in der vorliegenden Publikation nicht abschließend beantwortet, sondern liegen der Fortsetzung des Projektverbunds in einer zweiten, noch laufenden Phase zugrunde. In dieser wird die empirisch vorgefundene Reaktion der Demokratie, mittels nationaler Reterritorialisierung auf die Krise der Privatheit zu antworten, mit anderen demokratischen Reaktionsweisen konfrontiert und auf ihre Transformationsfähigkeiten hin befragt. Im Schlusskapitel dieses Zwischenberichts werden dazu ausblickhaft einige systematische Überlegungen vorgestellt. Im Kern jedoch geht es in den folgenden Abschnitten darum, die interdisziplinäre Analyse und Kartographie der Privacy-Arena am Fall dieser nationalen Reterritorialiserungsstrategie vorzustellen. Hierzu stellt *Barbara Büttner* in einem ersten längeren Abschnitt die methodische Herangehensweise des Projektzusammenhangs und die Theorie der sozialen Welten und Arenen mit ersten Bezügen zum Untersuchungsgegenstand vor (2). Im Anschluss daran rekonstruieren *Christian L. Geminn, Simon Ledder* und *Fabian Pittroff*, welche Dynamik der Vorschlag des nationalen Routings zur Lösung der Krise der Privatheit in der Privacy-Arena entfaltet hat. Hierzu wird der Vorschlag selbst vorgestellt und zu den in der Arena engagierten sozialen Welten und dort vorhandenen Argumenten für und gegen nationales Routing sowie verfügbaren Rechtsmitteln in Beziehung gesetzt (3). Im vierten Kapitel liefern *Christian L. Geminn, Thilo Hagendorff* und *Simon Ledder* Hintergrundanalysen aus der Perspektive ihrer jeweiligen Disziplin (Rechtswissenschaft bzw. Philosophie/Ethik) zur Ideengeschichte der

Privatheit, zum Privatheitsbegriff in der Rechtswissenschaft und zur Rolle des Vertrauens für Privatheit (4). An diese Reflexionsschleifen schließt sich der Übergang von den empirischen Einsichten zur Verlaufskurve der Privacy-Arena hin zur generalisierenden Hypothesenbildung über die zugrundeliegende Strategie der Reterritorialisierung des Digitalen an. *Barbara Büttner, Simon Ledder, Carsten Ochs* und *Fabian Pittroff* zeigen auf, dass die Diskussionen und Kämpfe in der Privacy-Arena von bestimmten Zugriffsweisen auf den Wert der Privatheit geprägt sind, die ein protektionistisches Reaktionsmuster der Demokratie auf die Krise der Privatheit nach Snowden sichtbar werden lassen (5). Dies wiederum ist der Hintergrund, vor dem *Jörn Lamla* für den Projektverbund und dessen weiteren Forschungsprozess die Frage nach alternativen Reaktionsmöglichkeiten der Demokratie aufwirft, die nicht nur abstrakt und theoretisch durch idealtypische Kontrastierungen eingeführt werden, sondern letztlich auch als Auftrag für die weitere, expansivere Untersuchung der komplexen und hier nicht abschließend rekonstruierten Privacy-Arena zu verstehen sind (6).

2 Kartografie als Methode

Barbara Büttner

2.1 Strauss' Theorie sozialer Welten und Arenen

Methodisch orientiert sich das Projekt an der Situationsanalyse von Adele Clarke (2012), die das Konzept der sozialen Welten und Arenen von Anselm Strauss (1978, 1993) mit verschiedenen Formen der Kartierung verknüpft. Die Methode Clarkes wird dem Umstand des Umbruchs der normativen Ordnung von Privatheit im Zeitalter der Digitalisierung in mehrfacher Weise gerecht. Zum einen nimmt sie die Rolle von Technik in Wandlungsprozessen ernst, indem explizit auch nicht-menschliche Elemente in die Analyse miteinbezogen werden. Anstatt diese als natürlich gegeben anzunehmen, werden so die Wechselwirkungen zwischen Technik und sozialen Formationen berücksichtigt (Clarke 2012: 101 ff.). Zudem beschäftigt sich die Situationsanalyse mit „Sozialprozesse[n]" (Clarke/Keller 2011: 119), um den Wandel des Sozialen und die damit einhergehenden Konsequenzen für die normative (Neu-)Ordnung analysieren zu können. Zur Berücksichtigung dieser Wandlungsprozesse orientiert sich Clarke an der Theorie sozialer Welten und Arenen von Anselm Strauss (1978, 1993). Kennzeichnend für soziale Welten im Sinne Strauss' ist eine gemeinsame Kernaktivität, die sie von anderen Welten abgrenzt. Die Ausführung dieser Kernaktivität fußt auf einer ihr zugrundeliegenden Technologie,[4] die die Art und Weise der Ausübung bestimmt. Zudem gibt es bestimmte Orte, an denen diese Aktivitäten stattfinden (Strauss 1978: 122). Eine soziale Welt bestimmt sich demnach unter anderem aus der Kernaktivität, also dem *was* sie tut, dadurch *wie* sie es tut (zugrundeliegende Technologie), als auch dem *wo* sie es tut (Orte). Die Etablierung und Festigung einer sozialen Welt geht in der Regel mit

4 Mit Technologien sind in diesem Sinne nicht nur mechanische Verfahren gemeint, sondern auch bestimmte Handlungsabläufe- und verfahren.

der Herausbildung von Organisationen einher. Parallel dazu durchlaufen die Welten Prozesse der Authentisierung und Legitimation. Die Identifikation weltenrelevanter Spezifika, die bestimmen, worin sich diese von anderen Welten abgrenzen und wer oder was *authentische* Bestandteile und Praktiken dieser Welt sind, wird in fortgeführten kollektiven Aushandlungen eruiert. Eng damit verzahnt sind Legitimationsverfahren, die insbesondere während Wandlungsprozessen – sei es bei der Entstehung neuer Welten oder der Veränderung zwischen oder innerhalb Welten – virulent werden. Die Welten müssen sich gegenüber anderen Welten positionieren, gleichzeitig aber die Balance wahren zwischen Absonderung und Einbindung anderer Welten. Einerseits muss die eigene Glaubwürdigkeit und Abgrenzung gewährleistet werden, andererseits können neue Verbindungen den Zugang zu Ressourcen und Technologien bieten (Strauss 1978: 123f.; ders. 1982: 172 ff.; ders. 1993: 213). Die Begründung der eigenen Daseinsberechtigung stellt häufig den normativen Bezugspunkt weltenspezifischer Argumentations- und Diskursmuster. Boltanski und Thévenot (2007) sprechen hier von Rechtfertigungsordnungen, die sie idealtypisch bestimmten Welten zuordnen. Diese Verbindung wird im Explorationsprojekt genutzt, indem die unterschiedlichen weltenspezifischen Rechtfertigungsordnungen bei Boltanski und Thévenot als Heuristik für die Analyse der sozialen Welten herangezogen werden.

In Anlehnung an Strauss' Theorie sozialer Welten und Arenen stehen nicht die Handlungen oder Interaktionen Einzelner im Mittelpunkt; vielmehr geht es um die Rekonstruktion kollektiver Aushandlungsprozesse und deren Implikationen für die Neuordnung der Arena. Die Situation als Ganzes, d. h. auch die kontextualen Bedingungen und somit die situative Einbettung kollektiver Interaktionen rücken ins Zentrum der Analyse. Die Arena stellt den Schauplatz der Auseinandersetzung dieser kollektiven Aushandlungsprozesse, auf dem verschiedene soziale Welten aufeinander treffen. Die Formation um ein bestimmtes *Issue* (in unserem Falle „privacy") mündet in Diskussionen, Verhandlungen und Kämpfen. Die Relevanz einer sozialen Welt für die Arena setzt sich aus deren Größe, der Weltenhistorik sowie

der Ressourcenausstattung zusammen. Die Chance, eigene Interessen durchzusetzen und sich Gehör zu verschaffen, variiert mit dem Zugang zu materiellen oder immateriellen Gütern, der Anzahl und Zusammensetzung der Mitglieder und Organisationen, dem Entstehungshintergrund sowie den Beziehungen zu wichtigen, machtvollen Instanzen (vgl. Strauss 1993: 213).

2.2 Das Konzept der Kartografie in der Forschungsliteratur

Ausgangspunkt dieses Analyserahmens ist die Betrachtung der Situation als Ganzes, um so die Komplexität des Untersuchungsgegenstandes einzufangen. Die Kartografien im Sinne der Situationsanalyse nach Adele Clarke (2012) ermöglichen es, diese Komplexität handhabbar zu machen und zu verstehen, wie die einzelnen Elemente der Situation miteinander zusammenhängen. Um die Abgrenzung und Vorteile dieser Form der Kartierung zeigen zu können, sollen im Folgenden ergänzend zu den bisherigen Ausführungen die konzeptionellen Ansätze und Diskussionen in der sozialwissenschaftlichen Forschungsliteratur zur Visualisierung vorgestellt und beurteilt werden.

Das Konzept der Kartografie als Analyse und Darstellungswerkzeug findet sich in der Forschungsliteratur in verschiedenen Kontexten. Einen der ersten Versuche stellen die sozialökologischen Ansätze der Chicagoer Schule der Soziologie dar, die ihren Schwerpunkt auf Gruppen in bestimmten Situationen legen, um Prozesse wie Urbanisierung oder Ghettoisierung nachzeichnen zu können. Im Mittelpunkt dieser geografisch abgegrenzten Karten stehen Gemeinschaften, Organisationen, Schauplätze und Kollektive sowie deren Relationen zueinander (Clarke 2012, 1991). Im Gegensatz zu Ressourcen- und Mobilisierungstheorien,[5] die ebenfalls grafisch arbeiten, aber Interaktionen zwischen den (kollektiven) Akteuren weitestgehend unbeachtet lassen, beziehen sozialökologische Ansätze die verschiedenen

[5] Die Ansätze der Ressourcen- und Mobilisierungstheorien gehen von einem rationalen Handlungsmodell aus. Für soziale Bewegungen und Organisationen ist die Mobilisierbarkeit von Ressourcen handlungsleitend und entscheidet über deren Erfolg (McAdam/McCarthy/Zald 1996; Pfeffer/Salancik 1978).

sozialen Prozesse mit ein. Damit grenzen sie sich auch von populationsökologischen Ansätzen ab, die sich nur auf den Wettbewerb als den zentralen sozialen Prozess konzentrieren und alternative Prozesse wie Konflikte, Kooperation, Austausch oder Verhandlung ignorieren.[6] Die Herausbildung ökologischer Nischen sowie das ihnen zugrunde liegende Ökosystem sollen mit diesem Ansatz kartografiert werden. Eine Erweiterung erfuhr der Ansatz durch die Verlagerung von geografischer Grenzziehung auf funktionale Abgrenzungen. Diese Modelle untersuchen verschiedene Sektoren, wie beispielsweise den Gesundheitssektor (Clarke 1991). Das Problem bei all diesen Modellen liegt in der Grenzziehung des Gegenstandes a priori, anstatt das Feld empirisch festzulegen.

Eine weitere Möglichkeit zur Visualisierung stellen die soziologischen Netzwerkanalysen dar. Darunter sind verschiedene Ansätze gefasst, die das Netzwerk als Paradigma des Sozialen begreifen und versuchen, dieses anhand der Darstellung von Knoten und Beziehungen grafisch einzufangen. Die Bestimmung der Eigenschaften von Beziehungen, Knoten oder Netzwerken dient dem Ziel der Offenlegung von Strukturen, Prozessen und Konsequenzen von Interaktionen. Dennoch fällt es gängigen Netzwerkanalysen schwer, die Komplexität der Situation zu systematisieren. Die Zentriertheit auf Knoten und Kanten verstellt den Blick auf die Prozesse, in denen beide wechselseitig erst geschaffen werden. Eine Erweiterung erfuhr das Modell durch die Entwicklung der Akteur-Netzwerk-Theorie (ANT). Hierin finden nichtmenschliche Elemente wie beispielsweise Technik als Bestandteil des Netzwerks explizite Berücksichtigung, ebenso wie die Frage nach der wechselseitigen Konstitution von Akteuren und Netzwerk (vgl. Callon 1986; Latour 2005). Darin trifft sich die ANT mit der Heuristik der sozialen Welten und Arenen, die ebenfalls neben allen (kollektiven) Akt-

[6] Im Zentrum von populationsökologischen Ansätzen stehen nicht einzelne Organisationen, sondern Organisationspopulationen, d. h. Populationen von Organisationen, die in einem gleichen oder ähnlichen ökologischen Kontext eingebettet sind. Die Überlebenswahrscheinlichkeit einer Organisationspopulation hängt von deren Effizienz ab. Selektionsprozesse sorgen für das Aussterben ineffizienter Organisationspopulationen (Hannan/Freeman 1977).

euren Diskurse und nicht-menschliche Elemente einbezieht und darüber hinaus empirisch offen auf Teilnahme, Grenzen, Strukturen und Prozesse blickt: Die Situation als Ganzes wird untersucht und so eine voreilige Grenzziehung zwischen Akteuren und Umwelt vermieden. Grenzen zwischen den Welten sind stets durchlässig und die Art der Beziehung zueinander ist nicht vorab festgelegt.

Die ANT hat auch einen interessanten Ansatz zur Kartografie hervorgebracht, der unter dem Titel „Mapping of Controversies" läuft. Diese Art der Kartografie von Kontroversen wurde von Bruno Latour ursprünglich als didaktisches Mittel entwickelt, um seinen Studierenden die Untersuchung gegenwärtiger sozio-technischer Debatten mit Hilfe der Akteur-Netzwerk Theorie näher zu bringen. Mittlerweile wurde der Ansatz von zahlreichen anderen Forschungsinstituten aufgegriffen und weiter entwickelt (z.B. Venturini 2010). Beim Mapping von Kontroversen handelt es sich um öffentlich zugängliche Websites, die verschiedene Ebenen der Darstellung umfassen: Dazu gehören ein Glossar der nicht kontroversen Elemente, die vollständige Dokumentation des Forschungsprozesses, eine Analyse der wissenschaftlichen Literatur, eine Übersicht der Diskurse in den Medien und der öffentlichen Meinung, die Darstellung der Akteure und Akteur-Netzwerke sowie eine Chronologie der Kontroverse und deren Zusammenhang mit anderen Konflikten (Venturini 2012). In dem Verfahren wird auf visueller Ebene mit unterschiedlichen Zoomebenen gearbeitet. Zusätzlich besteht die Möglichkeit interaktive Elemente einzubauen, Textbausteine zu einzelnen Elementen als Hintergrundinformation einzublenden oder mit Bildern zu arbeiten.[7] Mit Hilfe dieser digitalen Tools sollen komplexe Zusammenhänge einer breiteren Öffentlichkeit zugänglich gemacht werden.

Hinter dem Mapping of Controversies steht keine einheitliche Analysemethode, vielmehr wird mit zahlreichen digitalen Technologien

[7] Beispiel eines deutschen Projekts des Mapping of Controversies stellt die „Nanotechnology Risk Cartography" dar (vgl. Münchner Projektgruppe für Sozialforschung e. V./Wissenschaftszentrum Umwelt der Universität Augsburg (ohne Datum)).

gearbeitet, die die Auswertung und Visualisierung erleichtern sollen.[8] Die Auswertungen basieren häufig auf komplexen Algorithmen, deren implizite Hintergrundannahmen ohne ausgeprägtes technisches Know-How jedoch nur schwer nachzuvollziehen sind. Ein weiterer Nachteil an diesen zum Teil vollautomatischen Analysetools besteht in der quantitativen Auszählung von Ergebnissen. Zwar ist es möglich, auf diese Weise sehr schnell Ergebnisse zu produzieren, eine tiefenscharfe Analyse der Situation bedarf jedoch eines qualitativen Methodeninstrumentariums, um komplexe Phänomene systematisch erfassen zu können. Als virtuelle Darstellungsform kann das Mapping of Controversies eine sinnvolle Ergänzung im Forschungsprozess darstellen, jedoch bietet es keinen methodisch-konzeptionellen Alternativpfad des Modells sozialer Welten und Arenen. Diskussionen rund um diese Methode greifen inhaltlich inzwischen auch auf die *Issues* Privatheit und Überwachung nach den Enthüllungen durch Edward Snowden zurück (vgl. Marres/Moats 2015).

Einen weiteren auf das Problemfeld Privatheit bezogenen Kartierungsversuch mit dem Ziel, die eigenen Ergebnisse einem breiteren Publikum vermitteln zu können, stellt die Landkarte der Phänomene zum Wandel von Privatheit und Öffentlichkeit des Internet & Gesellschaft Collaboratory e.V. dar. Dabei handelt es sich vor allem um eine Visualisierungsstrategie und nicht um einen spezifischen methodisch-konzeptionellen Ansatz. Der von Google initiierte Verein versteht sich selbst als offene Kollaborationsplattform, auf der Experten verschiedener Disziplinen zusammenkommen, um den digitalen Wandel zu analysieren und die Ergebnisse der Öffentlichkeit zur Verfügung und zur Diskussion zu stellen. In ihrer Landkarte der Phänomene sollen exemplarisch wichtige Aspekte des Wandels von Privatheit und Öffentlichkeit im Zuge der wachsenden Digitalisierung veranschaulicht

[8] Ein Beispiel eines solchen automatischen Analysetools ist das sogenannte Lippmannian Device. Es durchsucht in einem zweistufigen Prozess die Suchmaschine Google und erstellt auf der Grundlage der Suchergebnissen zu bestimmten Begriffen eine Übersicht über die Häufigkeit. Damit soll ermöglicht werden, die Wichtigkeit eines Themas zu bestimmen und dies in die Kartografie mit einzubauen. (vgl. MACOSPOL Project).

werden (Internet & Gesellschaft Collaboratory 2011: 15-17). Der Vorteil dieser Darstellungsweise liegt in dem Zugang zu einem gängigen geografischen Kartenverständnis, das an einem allgemeinen Wissensfundus über diese Art von Karten anknüpft und die Karte auf den ersten Blick intuitiv plausibel wirken lässt. Die Darstellung setzt dabei typische Elemente einer Landschaftskarte wie Berge, Buchten, Inseln, etc. metaphorisch ein, um die unterschiedlichen Aspekte von Privatheit und Öffentlichkeit plastisch darzustellen. Allerdings wird ein sehr starres Konzept des Phänomens vermittelt, das von eindeutigen Zuordnungen und Abgrenzungen ausgeht.[9] Zudem verfügt eine geografische Karte über kein systematisches Konzept bezüglich der Rolle von Akteuren und deren Verhältnis zur Umwelt. Um die vielfältigen Zusammenhänge besser in den Blick zu bekommen und zu systematisieren, eignen sich geografisch angelehnte Konzepte von Karten daher nur bedingt. Um nun dem Phänomen der Privatheit näher zu kommen, ohne die Stärken visueller Tools außer Acht zu lassen, erscheint der Ansatz der sozialen Welten und Arenen Theorie ein fruchtbareres Analyseinstrument.

2.3 Mapping sozialer Welten und Arenen nach Clarke als Visualisierungsstrategie

Soziale Welten und Arenen gestalten sich als komplexe Gebilde, in denen vielfältige Verstrickungen, Koalitionen oder auch Dissense zwischen den oder innerhalb der Welten entstehen. Die Situationsanalyse von Adele Clarke (2012) verspricht die Darstellung dieser komplexen Arena, in der unterschiedliche soziale Welten und ihre diversen Repräsentanten aufeinander treffen. Clarke verwendet für ihre Methode verschiedene Verfahren des Mappings. Neben den Situationsmaps und Positionsmaps spielt für die kartografischen Illustrationen unserer Untersuchung die Map sozialer Welten und Arenen eine

[9] Beispielsweise wird differenziert zwischen dem „Land der Privatheit“ und dem „Ozean der Öffentlichkeit“ und somit ein simples dichotomes Verständnis von Privatheit und Öffentlichkeit erzeugt (Internet & Gesellschaft Collaboratory 2011: 16 f.).

zentrale Rolle. Sie ermöglicht als Mittel der Visualisierung tendenziell am ehesten, die Vielschichtigkeit fassbar zu machen.

Maps sozialer Welten und Arenen sind nicht als statische Gebilde zu verstehen, ihre Grenzen und Ordnungen sind fluide. Welten können mit anderen Welten in Beziehung treten, sich austauschen, Verhandlungen eingehen, Kompromisse schließen bis hin zum Führen von harten Auseinandersetzungen und Kämpfen. Die so entstehenden Verknüpfungen zwischen verschiedenen Welten bezeichnet Strauss als „Intersektionen" (Strauss 1978: 122). Wenn sich hingegen Teile einer Welt absondern, spricht Strauss (ebda.: 123) von „Segmentationen". Eine Welt kann in sich widersprüchlich sein, aus Uneinigkeiten können neue Subwelten hervorgehen. Die Erstellung von Karten sozialer Welten und Arenen darf insofern nicht als Endergebnis eines Forschungsprozesses gesehen werden, vielmehr ist sie selbst Teil davon. Karten verändern sich, neue Aspekte treten hinzu, andere verschwinden. Das Wandlungspotential wird symbolisiert in den offenen Grenzen der Welten. Die Vielschichtigkeit visuell greifbar zu machen und dadurch zur Disposition zu stellen ist dabei die Stärke dieser Visualisierungsstrategie. Die beobachtbaren Prozesse der Makroebene können in ihrem Entstehungsprozess dokumentiert werden. Ziel ist es, deren Verankerung in Praktiken und Routinen auf der Mesoebene zu analysieren und sichtbar zu machen (Clarke/Keller 2011). Dies ermöglicht der Forschung Fragen zu stellen: Welche Welten hängen wie miteinander zusammen, wo befinden sich deren Verknüpfungspunkte, wo segmentieren sich einzelne Subwelten innerhalb einer Welt usw.?

Das Ziel unserer Untersuchung lag in der empirischen Rekonstruktion der Konstitution der Arena. Die Annäherung an die Situation erfolgte mit der Durchsichtung „sprachförmiger ‚natürliche[r]' Dokumente", wie Reden, Pressemitteilungen, Gesetzestexte, etc. sowie der Analyse des massenmedialen Diskurses (Keller 2011: 87). In unserer Vorgehensweise haben wir uns am Prinzip der Fallkontrastierung orientiert, d. h. es wurden Dokumente möglichst unterschiedlichen Ursprungs ausgewählt, um ein breites Spektrum an Positionen abgreifen zu

können. Ferner wurden weltenspezifische Argumentationsmuster und Praktiken herausgearbeitet (Strauss & Corbin 1996). Die hier exemplarisch dargestellte Map (Abb. 1) zeigt die Situation der Privacy-Arena ausgehend vom Konflikt um das nationale Routing, mittels derer ein analytischer Zugang zum Untersuchungsgegenstand gewonnen wurde. Die Akteure dieser Welten in der Arena sind ständig in fortgesetzten Aushandlungen und Diskursen eingebunden. Dennoch ist der Diskurs immer nur als ein Teil dieser Welten zu betrachten. Daneben spielen Fragen wie die Ressourcenmobilisierung (rechtliche Ressourcen, diskursive Ressourcen, etc.), fehlende Gemeinsamkeiten (Sammeln von Informationen als Aufgabe der Welt der Geheimdienste vs. Schutz der informationellen Selbstbestimmung durch die Welt der Rechtsanwendung) oder das Herausbilden gemeinsamer Praktiken (die Netzpolitik der Piratenpartei als Teil der Welt des Staates und der Welt der Netzgemeinde) eine Rolle. Gleichzeitig sollen auch Orte der Konfliktaushandlung (Uneinigkeit zwischen DE-CIX und Telekom in der Welt der Ökonomie) sowie ggf. Kompromissbildungen identifiziert werden.

Das Sichtbarmachen der Untersuchungssituation anhand einer Kartografierung dient dabei einem weiteren wichtigen Zweck. Die Grafiken können nicht nur als Arbeitswerkzeug innerhalb der disziplinären Teams, sondern auch für die *interdisziplinäre Zusammenarbeit* genutzt werden. Die Kartografien vermitteln anschaulich die bisherigen Ergebnisse und können als gemeinsamer Ausgangspunkt der Diskussion genutzt werden. Die Grafiken können als Teil eines Narrativs verstanden werden, d. h. sie sprechen nicht für sich selbst, ihre Stärke liegt in der Symbiose von Text und Bild. Über die kollaborative Arbeit an den Karten wird es gewissermaßen möglich und nötig, die dem disziplinären Denken zugrundeliegenden kognitiven oder auch moralischen Landkarten zu explizieren und abzugleichen (vgl. Rosa 1998: 98 ff.; Beetz et al. 2014). Eine ständige Reflexion darüber, welche Elemente, seien es Diskurse, nicht-menschliche Elemente oder zentrale Akteure, in der Situation eine Rolle spielen, wo sie in der Arena anzusiedeln sind und welche Funktion ihnen zuteilwird, wird durch die

Kartografie angeregt. Neue Erkenntnisse und Veränderungsprozesse können jederzeit eingebaut und so die Kartografien verbessert und an den gegenwärtigen Erkenntnisstand angepasst werden.

Abb.1: Darstellung der Privacy-Arena im Rahmen der Situationsanalyse der Auseinandersetzungen um den Vorschlag eines nationalen Routings.

2.4 Das Arena-Segment des nationalen Routings

Die Karten stehen nicht für sich selbst. Vielmehr sind sie eine Hilfe, um die dahinterliegenden Diskurse zu explizieren. Die Visualisierung veranschaulicht die Ordnung einer Arena räumlich; um diese Ordnung zu verstehen braucht es jedoch einen erklärenden Text. Anhand der *Abb. 1* sei kurz exemplarisch erläutert, wie eine solche Karte zu lesen ist: Der große, dick gepunktete Kreis stellt das nationale Routing

als Teilausschnitt der Privacy Arena dar. Die gestrichelten Kreise repräsentieren die Welten und ihre Subwelten. Die Kästen stehen für die Akteure. Eine der zentralen Welten in der Arena, die Welt der Ökonomie, befindet sich links oben. Die Unterteilung in die Subwelt der Industrie mit den großen Telekommunikationsunternehmen als deren Vertreter und die Subwelt des Marktes, allen voran die kleinen und mittleren Telekommunikationsunternehmen sowie Internetunternehmen als Repräsentanten dieser Welt, sollen eine Segmentation der Welt der Ökonomie in konfligierende Subwelten illustrieren (s.o.). Die Welt der Ökonomie steht in vielfacher Weise in Beziehung zu anderen Welten. Die Rechtsabteilungen von Firmen sind zugleich Teil der Welt der Rechtsanwendung. Die Welt der Wissenschaft und Technik wird teilweise durch Unternehmen finanziert oder steht im Wissensaustausch mit dieser. Staatliche Regulierungen betreffen auch die Welt der Ökonomie, gleichzeitig nimmt die Ökonomie beispielweise durch Lobbyarbeit Einfluss auf die Politik des Staates. Die Welt des Hauses wird durch den Verbraucher, der zugleich auch Kunde ist und dessen Vertrauen die Unternehmen anstreben wiederherzustellen, angesprochen. Die Welt der Netzgemeinde ist vor allem im Bereich der Technikinnovationen mit der Welt der Ökonomie verbunden, hängt jedoch auch mit der Welt des Hauses zusammen. Man denke an den durchschnittlichen Internetnutzer, der je nach Intensität der Auseinandersetzung mit dem Netz auch als Teil der Netzgemeinde betrachtet werden kann. Ebenso hängt die Welt der Netzgemeinde mit der des Staates zusammen. Die Piratenpartei zählt viele Mitglieder aus den Reihen der Netzgemeinde, die zugleich Politik betreiben. Nachrichten werden nicht mehr nur durch professionelle Journalisten erzeugt, sondern auch durch soziale Medien aufgegriffen und verbreitet. Die Welt der Nachrichten ist somit auch mit der Welt der Netzgemeinde verknüpft. Die Grenzen zwischen den Welten sind fließend und die Welten an sich sind nicht statisch sondern stets in Bewegung. Welten können sich wandeln, neue Verknüpfungen eingehen oder alte aufgeben. Akteure können Mitglieder verschiedener Welten sein; ein Mitarbeiter einer Firma kann als Familienvater auch Teil der Welt des Hauses und in der Netzgemeinde aktiv sein.

Damit zeigen sich freilich auch Grenzen dieses Mappingverfahrens. Nicht immer sind alle Verbindungen zwischen den Welten in einer solch zweidimensionalen Grafik abbildbar. Die Welt der Rechtsanwendung spricht das Rechtssubjekt an und müsste mit der Welt des Hauses grafisch verbunden werden. Ebenso die Welt des Staates, die sich an den Bürger wendet. Die Welt der Wissenschaft und Technik schließt an die Welt des Staates an. Um diesem Defizit entgegenzuwirken, wurde zusätzlich mit unterschiedlichen Zoomebenen gearbeitet. Einzelne zentrale Welten wurden genauer in den Blick genommen und separat abgebildet. In diesen Kartografien können weitere relevante Verbindungen und Kontroversen genauer aufgegriffen und spezifiziert werden. Entsprechend wurde zusätzlich mit verschiedenen Karten sozialer Welten gearbeitet. Zudem muss man sich vergegenwärtigen, dass es sich bei den Karten nicht um Ergebnisdarstellungen handelt. Die Karten werden im Forschungsprozess laufend angepasst, verändert und miteinander verglichen. Ihre Stärke liegt in der Verwendung als Kommunikations- und Interpretationsmedium. Die Karten dienen als Ankerpunkte, die Geschichten dahinter müssen aber expliziert werden. Dies wird im folgenden Kapitel versucht.

3 Routing und die Arena seiner Aushandlung

Christian L. Geminn, Simon Ledder, Fabian Pittroff

3.1 Schengen- bzw. nationales Routing als umkämpfter Lösungsvorschlag

Im Rahmen der Enthüllungen zu den Tätigkeiten der NSA und weiterer Nachrichtendienste wurden bewährte Sicherheiten erschüttert und normative Bestimmungen in Frage gestellt.[10] Programme wie PRISM und XKeyscore oder Tempora[11] wurden durch die Bemühungen des Whistleblowers Edward Snowden der Öffentlichkeit bekannt gemacht. Überraschend war dabei weniger die Tatsache, dass Geheimdienste grundsätzlich die Möglichkeit zum Mithören besitzen, als vielmehr das schiere Ausmaß der Praxis und die Vehemenz, mit der Programme zur Überwachung der „unverzichtbaren Basistechnologie" Internet (Schaar 2013: 224) verfolgt wurden und werden.[12]

Spätestens mit diesen Enthüllungen ist Privatheit zu einem der unsichersten und umstrittensten Konzepte der digitalen Welt avanciert. Als Reaktion und Lösungsvorschlag bezüglich dieser neuen Unsicher-

[10] Teile dieses Textes wurden bereits veröffentlicht in: Geminn 2015: 98 ff.

[11] Beispielhaft soll kurz das Tempora-Programm dargestellt werden: Hier werden unter anderem in einer gemeinsam von GCHQ und NSA betriebenen Anlage in Bude (Cornwall) Daten direkt aus dem in Norden (Niedersachsen) entspringenden Transatlantischen Telefonkabel (TAT) Nr. 14 und aus weiteren Unterseekabeln abgezapft („full take"). Siehe Rosenbach/Stark (2014: 125 ff.) Für eine Darstellung von XKeyscore siehe Greenwald 2014: 221 ff.

[12] So schreibt etwa Pohlmann (2014: 47): „Natürlich wussten wir, dass NSA und Co. uns ausspionieren. Aber der Umfang und die Tiefe, sowie das Geld, das dafür ausgegeben wird, haben die Grenzen unserer Vorstellungskraft deutlich überschritten." Siehe auch Hoffmann-Riem 2014: 53: „Die Annahme, die Kommunikation in den globalen Kommunikationsinfrastrukturen sei durch Qualitäten wie Vertraulichkeit und Integrität und hinreichende Möglichkeiten des Freiheitsschutzes gekennzeichnet, hat sich spätestens infolge solcher Erkenntnisse als Illusion erwiesen." sowie Hange (zit. in: Der Spiegel 32/2014: 32): „Wir wussten immer, dass die NSA enorme Fähigkeiten bei der strategischen Erfassung von Daten hat. Aber wir waren schon verblüfft, als wir in einem der veröffentlichten Dokumente gelesen haben, das Ziel für die kommenden Jahre sei, ‚anyone, anywhere, anytime' zu erfassen."

heit kam die Idee der Einführung eines nationalen Routings auf. Gemeint sind damit politische und technische Strategien, um die globalen Datenströme des Internets so zu leiten, dass sie bestimmte regionale Räume möglichst nicht verlassen. Die Ansätze wurden dabei häufig mindestens rhetorisch mit der Aussicht auf Verbesserung oder Wiederherstellung von Privatheit verknüpft. In die öffentliche Diskussion Deutschlands wurden solche Konzepte das erste Mal prominent eingebracht im Jahr 2013.

Ausgangspunkt der deutschen Debatte war ein Vorstoß der Deutschen Telekom AG aus dem Herbst 2013: Über das Internet versendete Daten sollen den Rechtsraum ihres Ursprungs nicht verlassen, sofern auch der Empfänger in diesem Rechtsraum angesiedelt ist. Je nachdem, ob hierbei auf die nationale Ebene oder die europäische Ebene Bezug genommen wird, spricht man von „nationalem Routing", „Deutschland-Routing" oder „Schengen-Routing", wobei durch die Begrenzung auf den Schengen-Raum bewusst Großbritannien ausgeschlossen werden soll.[13]

René Obermann, bis Ende 2013 Vorstandsvorsitzender der Telekom, beschrieb die Idee so: „Darum jetzt unser Vorschlag für ein Internet der kurzen Wege. Schengen-Routing heißt nur, wenn Sender und Empfänger innerhalb des Schengen-Raums sind, dass dann Daten nicht unnötig über Amerika oder Asien geroutet werden" (Obermann, zit. in: FAZ.net 2013).[14] Das nationale Routing sollte nach dem Willen

[13] Der Begriff „Routing" bezeichnet die „Vermittlung bzw. Weiterleitung von Datenpaketen zwischen Sender und Empfänger" (Brüne 2009: 224). Für eine ausführliche Erklärung siehe Dierichs/Pohlmann (2008). Da es sich auch beim Schengen-Routing bzw. beim „europäischen" Routing letztlich um eine Form des nationalen Routing handelt, sollen beide Begriffe in diesem Band weitgehend synonym verwendet werden. Im Unterschied dazu wird der Begriff der „Reterritorialisierung" immer dann verwendet, wenn ein breiteres Set an politischen und technischen Strategien gemeint ist, das Routing-Ansätze einschließt und darüber hinaus noch weitere Formen der Rückbindung von Datenströmen an bestimmte Räume umfasst.

[14] Eine detaillierte Beschreibung der hinter dem Vorschlag stehenden Problematik liefert Schaar: „Als globales Informationsnetz kennt das Internet (technisch) keine Grenzen. Dies ist insbesondere dann problematisch, wenn etwa deutsche Internetnutzer sich darauf verlassen, dass der durch deutsches Recht vorgesehene Schutz gewährleistet ist – ein angesichts der komplexen Struktur und Funktionsweise des

der Telekom durch Angebote wie „Clean Pipe“ und „Schengen-Cloud“ ergänzt werden.[15] Laut dem Magazin „Der Spiegel“ findet mit 40 Prozent ein beträchtlicher Teil des deutschen Internetverkehrs zwischen deutschen Computern statt (Dohmen/Traufetter 2013: 46). Nach Informationen des Fachmagazins „iX“ läuft im Durchschnitt jede fünfte (22%), mindestens aber jede achte (12%) Verbindung zwischen zwei deutschen autonomen Systemen über ein ausländisches autonomes System (Pohlmann/Siromaschenko/Sparenberg 2014: 114). Führt man die Zahlen zusammen, so würden im Durchschnitt 8,8 Prozent des deutschen Internetverkehrs von nationalem Routing profitieren.

Die Initiative der Deutschen Telekom wurde von Befürwortern als „einfach und einleuchtend“[16] sowie „richtig und überfällig“ (Federrath, zit. in: Pech 2014: 22) beschrieben, von Kritikern dagegen als „furchtbar“[17] und „nutzlos“[18] verhöhnt. Spott kam insbesondere aus der

---

Internets kaum erfüllbarer Anspruch. So führt etwa die Anwendung des ‚Best Effort‘-Prinzips Internetdienste heutzutage nicht zwangsläufig zur Nutzung des kürzesten Weges, der eine Information etwa innerhalb eines Staats und damit auch innerhalb eines Rechtsregimes halten würde. Die Regeln für das dynamische Routing von Datenpaketen folgen vor allem technischen und betriebswirtschaftlichen Kriterien. Die Frage, welche Wege ein Datenpaket nimmt, spielte bisher nur eine untergeordnete Rolle, sieht man einmal von den Überwachungs- und Zensurbestrebungen autoritärer Regimes ab. Seit ‚PRISM & Co.‘ wird aber zu Recht darüber diskutiert, ob die Provider ein Routing innerstaatlicher Kommunikation innerhalb des jeweiligen Rechtsraums sicherstellen sollten, um ausländische Nachrichtendienste an der Überwachung dieser Kommunikationsvorgänge zu hindern.“ (Schaar 2013a: 214). Siehe auch Waidner 2014: 11 ff. Konzernintern und bezogen auf den E-Mail-Verkehr hat die Telekom das Prinzip zwischenzeitlich umgesetzt. Höttges (zit. in: Heuzeroth 2014: 5): „Für unsere Privatnutzer in Deutschland haben wir das nationale Routing bereits umgesetzt. Sie können sicher sein, dass eine E-Mail auf dem Weg von Bremen nach München nicht das Land verlässt, wenn beide Nutzer bei der Telekom sind.“

15 Dabei handelt es sich um das Angebot einer sicheren Verbindung zu einem ebenfalls speziell gesicherten Cloud-Speicher über zertifizierte Hardware des deutschen Anbieters Lancom.

16 So der Gründer von Lancom, Koenzen (2014).

17 So die Digitalbotschafterin der Bundesregierung Joost (zit. in: Der Spiegel 28/2014: 74 f.).

18 So etwa vom Präsidenten des Bundesverbands IT-Mittelstand: „Weiterhin müssen wir aufpassen, dass keine rein symbolischen und technisch nutzlosen Konsequenzen aus dem NSA-Skandal gezogen werden – wie zum Beispiel ein nationales oder Schengen-Routing oder eine gesetzliche Meldepflicht bei IT-Sicherheitsvorfällen. Der Fokus muss auf der Stärkung der Qualität und Zukunftsfähigkeit unserer IT-

Netzgemeinde („#schlandnet"). Gewichtige Unterstützung kam indes etwa von Peter Schaar;[19] aber auch der Verband BITKOM und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfahlen, die Initiative zu prüfen.[20] Darüber hinaus fand das Vorhaben Eingang in den aktuellen Koalitionsvertrag.[21] Rechtlich festschreiben, wie von der Telekom angedacht,[22] wollte die deutsche Regierung ein nationales Routing am Ende allerdings nicht: Aus dem Bundeswirtschaftsministerium hieß es stattdessen, man befürworte „freiwillige Angebote" (Berke 2014a). In die Digitale Agenda 2014-2017 der Bundesregierung wurde der Vorschlag eines nationalen Routings konsequenterweise nicht aufgenommen. Demgegenüber forderte etwa Gaycken „harte gesetzliche Auflagen", um dafür zu sorgen, dass IT-Dienstleister Daten nicht über internationale Netze versenden.[23]

Versuche, Teile des Internets an staatlich verfasste Räume zurückzubinden, sind nicht selten mit der Hoffnung verbunden, verloren geglaubte Sicherheiten widerherstellen und neue Formen der Kontrolle etablieren zu können. Unterstellt wird dabei, es ließe sich ein vertrauenerweckender Schutzraum herstellen, in dessen Innerem Pri-

---

Produkte liegen, damit wir unabhängiger von ausländischen Produkten werden" (Grün, zit. in: Bundesverband IT-Mittelstand e.V. 2013). Aus dem Office of the United States Trade Representative heißt es besorgt, eine Umsetzung von Schengen-Routing „would decrease efficiency and stifle innovation" (United States Trade Representative 2014: 5).

19 Siehe Fußn. 11; „Wir werden um eine Restrukturierung des Internets nicht herumkommen" (Schaar, zit. in: Rosenbach/Stark 2014: 293).

20 BITKOM Positionspapier 2013: 5; 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2014. Zu beachten ist, dass sich die Telekom innerhalb des BITKOM-Verbandes dafür eingesetzt hatte, eine klare Befürwortung von nationalem Routing in das Positionspapier aufzunehmen. In das Papier schaffte es letztlich jedoch nur die Empfehlung, die Idee eines nationalen Routings zu prüfen. Grund dafür war massive Kritik insbesondere von Microsoft, Oracle und Amazon. Daran konnte auch ein Verweis der Telekom auf die Situation in den USA nichts ändern, wo nationales Routing „geübte Praxis" sei. Es sei „als rechtlich verbindliche Auflage in Verträgen fixiert […], die ausländische Investoren abschließen müssen". Siehe Berke 2014.

21 CDU/CSU/SPD 2013: 103.

22 „Aufgrund der Vielzahl von Anbietern und aus Gründen der Chancengleichheit werden wir das aber nicht auf Basis einer Branchenvereinbarung machen können, da ist der Gesetzgeber gefragt" (Obermann, zit. in: FAZ.net 2013).

23 Heute im Bundestag Nr. 340. Siehe auch Gaycken 2014.

vatheit vor äußeren Zugriffen bewahrt werden kann. In den Auseinandersetzungen um die Idee der Einführung eines nationalen Routings wurde der Ansatz gelobt als adäquates Mittel zur Rückeroberung von Privatheit, aber ebenso kritisiert als politisches Placebo oder Wirtschaftsförderung unter dem Deckmantel des Privatheitsschutzes. Es bleibt mithin die Frage, ob die Vorschläge zu einem nationalen oder europäischen Routing tatsächlich lediglich auf einer Anamnese des Status Quo von informationeller Selbstbestimmung im Internet basierten oder ob der Vorschlag nicht vielmehr von wirtschaftlichen Überlegungen geleitet wurde. Wurde hier eine Scheindebatte geführt, in der das berechtigte und geschützte Interesse der Bürger nach informationeller Selbstbestimmung und die Verunsicherung und Empörung über die durch Snowden aufgedeckten Aktivitäten lediglich zur Durchsetzung wirtschaftlicher Interessen missbraucht wurden? Jedenfalls mobilisierte die Debatte um ein nationales Routing sehr verschiedene Akteure und Interessen, die in politische Aushandlungsprozesse verstrickt sind. Eine Kartografie dieser Prozesse der Streitaustragung und Koalitionsbildung verspricht sichtbar zu machen, wie diverse Konzeptionen des *Issues* Privatheit aufeinandertreffen und welche Reaktionsmuster im Falle digitaler Krisen Resonanz finden.

3.2 Die beteiligten sozialen Welten und die Arena ihrer Aushandlungen

Entlang der Kompromisse und Kämpfe um Ansätze des nationalen Routings *versammeln* sich wichtige Instanzen und Akteure zur *Neuverortung* der Privatheit (vgl. zum Konzept der Neuversammlung von Kollektiven Latour 2005: 32, 2010: 210-229; Lamla 2013b: 98-107). Die Debatte kann in diesem Sinne verstanden werden als wichtiger Ausschnitt einer Arena, in der Repräsentanten sozialer Welten koalierend und konfligierend über die Zukunft der Privatheit verhandeln (Strauss 1978, 1993: 225-227; Clarke 1991; Lamla 2013b: 107-118). Die Lösungsstrategien des nationalen Routings können entsprechend als Versuche gedeutet werden, Allianzen zwischen wichtigen sozialen Welten dieser Privacy-Arena zu etablieren. Koalitionen werden ange-

bahnt zwischen den Welten des Staates (Netzausbau im Sinne des Bundesministeriums für Verkehr und digitale Infrastruktur), der Rechtsanwendung (Gewährleistung der Hoheit nationalen/europäischen Rechts über Datenströme), der Telekommunikationsindustrie (Festigung der Sonderstellung der Deutschen Telekom im deutschen Markt) sowie den europäischen Technologieunternehmen (mögliche Bevorteilung europäischer Unternehmen gegenüber US-amerikanischen). Gleichzeitig provoziert das nationale Routing Widerstände, die Aufschluss geben über weitere relevante Fluchtlinien der Privacy-Arena. So bringen Gegner der Idee alternative Werte (Offenheit des Internets bzw. Netzneutralität) oder Lösungsvorschläge (Ende-zu-Ende-Verschlüsselung) in die Arena ein, um sich gegen das nationale Routing zu positionieren. Außerdem werden im Zuge der Aushandlungen teils tiefsitzende Uneinigkeiten innerhalb beteiligter Welten brisant; etwa zwischen den Parteien der großen Koalition, politischen und unpolitischen Nutzern des Internets, verschiedenen Formen des Wirtschaftens oder entlang nationaler Grenzen. Diese hier nur angedeuteten Arena-Prozesse werden im Folgenden differenzierter entfaltet.

3.2.1 Die sozialen Welten der Ökonomie

Die Deutsche Telekom und ihr damaliger Vorstand René Obermann machten die Geheimdienstenthüllungen zum Anlass, die Idee des nationalen Routings als erfolgversprechende, einfache technische Lösung zur Erhöhung der Datensicherheit und der Privatheit in Deutschland und Europa in die Öffentlichkeit einzubringen. Obermann und die Telekom können als Repräsentanten der sozialen Welt der *Industrie* verstanden werden, deren Praktiken auf die Effektivität und Leistungsfähigkeit von technischen Lösungen ausgerichtet sind, wobei zentral organisierte Infrastrukturprojekte mehr zählen als dezentraler Wettbewerb (Boltanski/Thévenot 2007: 276-286). Es verwundert daher nicht, dass sich in direkter Reaktion auf den Vorschlag die DE-CIX Management GmbH als Repräsentantin der kleinen und mittleren Internetprovider kritisch zu Wort meldete. So bezeichnete der Geschäftsführer des DE-CIX und des Verbands der deutschen

Internetwirtschaft e.V. (eco), Harald A. Summa, die Pläne der Telekom als „öffentlichkeitswirksame Augenwischerei und einen Versuch, ihr altes Monopol in Deutschland de facto wieder herzustellen“ (DE-CIX 2013). Die kleineren Provider fürchteten, ihnen könnte eine gesetzliche Regelung des Routings mindestens in dem Maße schaden, wie sie dem ehemaligen Monopolisten Telekom bei der Festigung einer Zentralstellung am Markt helfen würde. Denn anders als im Fall der Telekom sind die Praktiken der kleineren Provider in der Subwelt des *Marktes* zuhause, in der es vordringlich um einen möglichst freien und unbeschränkten Wettbewerb geht (Boltanski/Thévenot 2007: 264-267). In diesem Sinne lässt sich die Abwehrhaltung der kleineren Provider verstehen als Ausdruck der Differenz unterschiedlicher Formen des Wirtschaftens und als Spaltung der sozialen Welten der Ökonomie, eben als Unterschied zwischen der Welt der Industrie und der des Marktes.

Diese Lesart erhält zusätzliche Plausibilität durch die Uneinigkeiten, die sich Medienberichten zufolge im IT-Branchenverband BITKOM manifestierten. So habe sich die Telekom im Verband dafür eingesetzt, in ein gemeinsames Positionspapier zum Thema „Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden, Datenschutz und Datensicherheit“ eine klare Befürwortung eines nationalen Routings aufzunehmen (Wirtschaftswoche 2014). Dagegen habe sich jedoch eine Allianz mehrerer US-Unternehmen formiert und erreicht, dass in der Endversion des Papiers nur eine Willensbekundung auftauchte, den Vorschlag des nationalen Routings zu prüfen. Auch hier aktualisierte sich die Differenz zwischen den Welten der Industrie und des Marktes, nämlich im Pochen der im Bereich Hardware-, Software- und Internetdienstleistungen dominanten US-Unternehmen auf einen freien Wettbewerb einerseits und der Hoffnung der Telekom andererseits, ihre Vormachtstellung auf dem deutschen Markt zu erhalten. Überlagert wird diese Konfliktlinie zugleich vom Konflikt zwischen europäischen und US-amerikanischen Technologieunternehmen.

3.2.2 Allianzen mit der sozialen Welt des Staates

Die Deutsche Telekom konnte zunächst hoffen, durch ihren Vorschlag eine Allianz mit der Welt des Staates zu etablieren. Im November 2013 schaffte es eine Befürwortung des nationalen Routings in den Koalitionsvertrag der Bundesregierung: „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings“ (CDU/CSU/SPD 2013: 103). Anfang 2014 sprach sich Alexander Dobrindt, Bundesminister für Verkehr und Digitale Infrastruktur, dann explizit dafür aus, Datenströme möglichst innerhalb des Schengen-Raums zu belassen (computerwoche.de: 2014). Daran wird sichtbar, wie Ansätze des nationalen Routings nicht nur zu den Praktiken der Industrie, sondern auch zu denen der Welt des Staates passen, da sie sich an der mit moderner Nationalstaatlichkeit einhergehenden Territorialität orientieren. Darüber hinaus geht ein nationales Routing mit dem Vorhaben eines innerdeutschen Netzinfrastrukturausbaus einher, wie er auf der Agenda des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) steht.

Minister Dobrindt forcierte den Vorschlag aber nicht nur als Repräsentant der Welt des Staates, sondern auch als Vertreter der Subwelt der Bundesregierung. Vor allem drei Ministerien[24] dieser Subwelt sind

[24] Für die Situationsanalyse sozialer Welten und Arenen (Clarke 2012) ist es wesentlich, auch solche Welten oder Subwelten in der Kartografie zu berücksichtigen, die nicht als offizielle Repräsentanten in der Arena auftreten, dort aber gleichwohl präsent sind. So ist zwar das in der Vorgängerregierung mit Fragen des Verbraucherschutzes in der Digitalen Welt beauftragte und ebenfalls von der CSU besetzte Ministerium für Ernährung und Landwirtschaft durch die neue Zuständigkeitsverteilung weitgehend zum Schweigen verdammt. Mit dem um den Verbraucherschutz erweiterten Justizministerium jedoch erfahren diese Fragen eine Aufwertung, die

relevante Akteure der Arena um Ansätze des nationalen Routings: das schon erwähnte BMVI, das Bundesministerium für Wirtschaft und Energie (BMWi) sowie das Bundesministerium des Innern (BMI). Als federführende Ministerien bei der Ausgestaltung der Digitalen Agenda 2014-2017 der Bundesregierung, die den Rahmen bilden soll „für das Handeln aller Ressorts der Bundesregierung bei der Digitalisierung aller Lebens- und Wirtschaftsbereiche“ (Bundesregierung 2014), haben sich alle drei explizit zum nationalen Routing positioniert: Im Gegensatz zur Befürwortung durch den Verkehrsminister lassen sich der Wirtschaftsminister und der Innenminister nicht in die Allianz einspannen und äußern öffentlich Zweifel am Verhältnis von Aufwand und Nutzen des nationalen Routings (Welt am Sonntag 2014) oder sprechen sich ausdrücklich gegen gesetzliche Regelungen aus (BMWi 2014). In der Folge findet sich – anders als noch im Koalitionsvertrag – in dem von den drei Ministerien herausgegebenen Dokument zur Digitalen Agenda keine Erwähnung eines nationalen oder europäischen Routings mehr.[25]

Was jedoch in der Arena bestehen bleibt, ist eine Neigung zur Suche nach neuen, alternativen Koalitionspotentialen und Kompromissformen. Dabei wird deutlich, dass Strategien der Reterritorialisierung nicht wie im Falle des nationalen Routings strikt an technische Lösungen gebunden sein müssen, sondern auch mit anderen Mitteln verfolgt werden können. Dies macht deutlich, inwiefern die Kontroverse

---

durch den Zuschnitt der Verantwortlichkeiten der Digitalen Agenda zugleich wieder relativiert worden ist. Das auch intern durch die Neuorganisation herausgeforderte Ministerium der Justiz und für Verbraucherschutz (BMJV) äußerte sich zwar nicht offiziell zum Deutschland- oder Schengen-Routing, setzt sich aber für eine gesetzliche Pflicht zur Ende-zu-Ende-Verschlüsselung ein, die in der Arena immer wieder gemeinsam mit bzw. als Alternative zum Schengen-Routing im Spiel ist. So greift das BMJV als Repräsentant der Welt des Staates (und insbesondere als Verfassungsressort) in indirekter Weise in die Privacy-Arena ein.

[25] In der Opposition unterstützen weder Die Grünen noch Die Linke noch die Piratenpartei das Schengen-Routing und auf europäischer Ebene herrscht Uneinigkeit über dessen Nützlichkeit. Während Angela Merkel mit europäischen Partnern zumindest darüber sprechen wollte, Kommunikationsnetzwerke innerhalb Europas aufzubauen, um den Datenschutz zu verbessern, votierte die EU-Kommissarin für die digitale Agenda, Neelie Kroes, gegen ein Schengen-Routing.

um Ideen des nationalen Routings für eine breitere und wesentlichere Auseinandersetzung stehen könnte, nämlich als Symptom für einen Streit um Strategien der Reterritorialisierung. Aufschlussreich ist hier ein Blick auf weitere soziale Welten der Privacy-Arena.

3.2.3 Unsicherheiten und Widersprüche in den sozialen Welten der Netzgemeinde, der Rechtsanwendung, des Hauses und der Geheimdienste

Die sozialen Welten der Netzgemeinde,[26] der Rechtsanwendung und des Hauses artikulieren vor allem bleibende Unsicherheiten bezüglich des Lösungsvorschlags nationales Routing. Repräsentanten der Welt der Netzgemeinde reagieren größtenteils verhalten auf die in der Arena diskutierten Ansätze, denn die Praktiken der Welt der Netzgemeinde setzen im Gegensatz zu Routing-Ansätzen auf Offenheit und Zugänglichkeit des Internets. Zusätzlich zu dieser diffusen Sympathie für ein offenes Netz zeigt sich die Welt der Netzgemeinde interessiert an individueller Informationskontrolle und persönlichen Schutzräumen vor Überwachung.

Die Ansätze des nationalen Routings ernten vor allem Kritik aus der Netzgemeinde; größtenteils wird Ablehnung und Spott geäußert gegenüber der Provinzialität der deutschen Politik oder den Geschäftsinteressen der Telekom. Auch der Negativbegriff der „Balkanisierung" als Metapher einer schädlichen Zersplitterung des Internets wird gebraucht. Die ablehnende Haltung der sozialen Welt gegenüber Ideen des nationalen Routings überrascht dabei nicht, insofern eine Reterritorialisierung dem Wert der Offenheit des Internets widersprechen könnte und die Bedingungen der Kernpraktiken der Netzgemeinde sabotiert werden könnten. Aber Strategien der Reterritorialisierung werden von Repräsentanten der Netzgemeinde nicht nur kritisiert. Es finden sich auch Vertreter, die ein nationales Routing (je nach Ausge-

[26] Wir verwenden hier den Begriff Netzgemeinde als umkämpfte und problematisierte Selbst- und Fremdbeschreibung. Insbesondere die Vielschichtigkeit des Begriffs Gemeinde zwischen räumlicher, politischer, administrativer und religiöser Kollektivität soll erhalten bleiben.

staltung) als hilfreichen Baustein bewerten und in einer Strategie der Reterritorialisierung des Netzes die Chance sehen, die Dezentralisierung des Internets voranzutreiben.[27] Politiken der Dezentralisierung könnten in diesem Sinne mit Strategien der Reterritorialisierung einhergehen.

Innerhalb der Arena unterhält die Netzgemeinde allerhand Verbindungen mit anderen Welten: Es gibt Kompromissversuche mit der Welt des Staates (Piratenpartei), Abhängigkeiten von der Welt der Industrie (Infrastruktur), Verstrickungen mit der Welt des Marktes (Internetunternehmen) und Allianzen mit der Welt der Rechtsanwendung (Datenschutzbeauftragte). Trotz dieser Verbindungen scheint es der Netzgemeinde aber oft schwer zu fallen, stabile Allianzen mit anderen Welten zu unterhalten und in der Arena hinreichend Resonanz für ihre Interessen zu finden. Relevant wird in dieser Hinsicht die Frage nach Politik und Politisierung der Netzgemeinde, das heißt nach den Arten und Weisen, wie die soziale Welt ihre Anliegen in der Arena formuliert und verfolgt. Dabei ist die soziale Welt der Netzgemeinde nicht identisch mit einer netzpolitischen Bewegung; letztere ist zu verstehen als politisch mobilisierter Teil der Netzgemeinde. In diesem Sinne ist die soziale Welt der Netzgemeinde dann relevant als Basis einer politisierten netzpolitischen Bewegung. Und während in der netzpolitischen Bewegung Kämpfe für Datenschutz und gegen staatliche Überwachung im Mittelpunkt stehen (vgl. auch Dobusch 2014: 8-10), geht es in der Netzgemeinde immer auch um die Offenheit und Neutralität des Internets und damit um die Bedingungen der Kernpraktik der sozialen Welt. Hier sollte die Frage weiterverfolgt

[27] „Mindestens was die Erzielung von technischer Sicherheit gegen die Massenüberwachung angeht, halte ich es für ein durchaus lösbares Problem. Dazu wird es rechtliche Vorschriften brauchen. Also, Schengen-Routing war zum Beispiel eines dieser Themen – ist nur ein klitzekleiner Baustein, wo es wieder auf die Details ankommt –, Vorschreiben von Ende-zu-Ende-Verschlüsselung. Mit all diesen Dingen kann man sicherlich eine Menge bewegen. Aber dazu gehört eben auch, tatsächlich deutsche Datensouveränität herzustellen“ (Rieger 2014: 16). „Zur Frage […] bezüglich der Kosten und Risiken des Schengen-Routings: Das Schengen-Routing kann in allem, was wir diskutieren, nur ein Baustein sein. Es ist halt ein kleines Element, wo wir versuchen, etwas rückgängig zu machen, was durch, sagen wir mal, eine strategische Deregulierungspolitik der Amerikaner entstanden ist“ (ebd.: 20).

werden, ob diese unterschiedlichen politischen Schwerpunkte sich produktiv ergänzen oder eher Widersprüche erzeugen, die eine oder beide Seiten schwächen. Es gibt zwar ein geteiltes Interesse an freien, offenen, neutralen Informationsflüssen; das allein scheint aber nicht zu genügen, um eine nachhaltige politische Organisiertheit innerhalb der Arena zu tragen. Möglicherweise blockieren die dezentralen, individualistischen Praktiken und die damit verbundenen Anliegen der Netzgemeinde eine Politisierung.

Attraktiv scheint ein nationales Routing zunächst für die Welt der Rechtsanwendung, da sie maßgeblich auf die national- und territorialstaatliche Rahmung ihrer Praktiken abhebt. Die Durchsetzung geltender Rechtsnormen könnte durch eine Rückbindung von Datenströmen an das deutsche oder europäische Territorium erleichtert werden. Insbesondere Unterschiede und Konfliktpotentiale im Verhältnis zum US-amerikanischen Rechtsraum könnten so abgeschwächt werden. Letztendlich handelt es sich beim nationalen Routing aber um ein Randthema innerhalb der Welt der Rechtsanwendung. Mit der Datenschutzgrundverordnung existiert bereits ein territorialer Lösungsansatz, der in der Welt der Rechtsanwendung diskutiert und in naher Zukunft zur Anwendung kommen wird. Davon abgesehen könnten sich aus einem nationalen Routing handfeste rechtliche Probleme ergeben. Fraglich ist für die Welt der Rechtsanwendung etwa, ob das nationale Routing der Deutschen Telekom AG zu einer marktbeherrschenden Stellung verhelfen könnte. Dazu passt, dass sich gerade die im Bundesverband IT-Mittelstand organisierten kleinen und mittelgroßen IT-Unternehmen der Welt des Marktes gegen die Pläne der Telekom wenden.

Auch die Welt des Hauses,[28] deren Praktiken auf Vertrauen und Intimität bauen, ist in der Arena einer Reihe von Unsicherheiten ausgesetzt. Die dieser Welt zuzuordnenden Nutzer des Internets, in ihrer

[28] Unter „Welt des Hauses" verstehen wir hier soziale Formationen, die dem Prinzip familiärer Lebensgemeinschaften folgen. Im weiteren Sinne bezieht sich der Ausdruck jedoch auch auf eine spezifische Logik der Rechtfertigung (Boltanski/Thévenot 2007).

Rolle als Privatanwender, werden zwar in der Arena als relevante Elemente ins Spiel gebracht, verfügen jedoch kaum über eigene Abgesandte. Stattdessen werden sie von den Vertretern anderer sozialer Welten je unterschiedlich repräsentiert, um die dort vorherrschenden Interessen besser durchsetzen zu können. Außerdem sieht sich die Welt angesichts neuer digitaler und vernetzter Kommunikationsformen mit teils unvermittelten Widersprüchen und Unsicherheiten konfrontiert. Einerseits sind für die soziale Welt neue kollektive Praktiken intimer und vertrauensvoller Kommunikation attraktiv, andererseits kann diese Vertraulichkeit in digital vernetzten Konstellationen nur allzu leicht unterlaufen werden. Unabhängig davon, dass das nationale Routing von der Welt des Hauses kaum reflektiert zu werden scheint, könnte eine Reterritorialisierung je nach Ausgestaltung ebenso nützlich wie schädlich für die Praktiken der Welt sein (verbesserter Datenschutz ohne Kompetenzanforderungen, höhere Telekommunikationskosten aufgrund veränderter Wettbewerbssituation).

Von Widersprüchen durchzogen scheint auch die soziale Welt der Geheimdienste. So zeichnen insbesondere Repräsentanten der Welt der Regierung im Rahmen der Arena-Aushandlungen wiederholt das Bild unsicherer, weil über außereuropäische Server geleitete Datenflüsse und betonen die Gefahr, die von nicht-deutschen Geheimdiensten ausgehe. Vertreter der Welt der Industrie stärkten diese diskursive Differenz zwischen ausländischen und deutschen Geheimdiensten. So würde die NSA großzügig viele Metadaten speichern, während sich der BND auf konkrete Inhalte ausgewählter Ziele konzentriere.[29] Kritisiert werden solche Argumentationslinien indes von Sicherheitsexperten, Vertretern der Oppositionsparteien und Repräsentanten der Netzgemeinde. Den Kritikern zufolge seien auch inländische Dienste an Abhörmaßnahmen beteiligt, deutsche Dienste ge-

[29] So wurde zu Beginn der Snowden-Enthüllungen häufig die Unterscheidung zwischen der „Schleppnetz-Methode“ der NSA und der „Harpunen-Methode“ des BND wiedergegeben, mit der der BND-Präsident Schindler die verschiedenen Maßnahmen „ansatzorientierter“ und „zielorientierter Erfassung“ veranschaulichte.

nerell unzureichend kontrolliert und die Zusammenarbeit und der Datenaustausch zwischen inländischen und ausländischen Behörden nachweisbar. Die Klassifizierung ausländischer Behörden als problematisch und inländischer als unproblematisch sei folglich hinfällig. Eine weitreichende Zusammenarbeit zwischen BND und NSA darf indessen spätestens seit den Medienberichten über die „Operation Eikonal" angenommen werden (Süddeutsche.de 2014).

3.3 Argumente und Bewertungen in der Arena

Als Schauplätze von Aushandlungen sind soziale Arenen nicht nur Versammlungen sozialer Welten, sondern immer auch „Strudel argumentativen Handelns" (Strauss 1993: 227), also Verstrickungen diverser diskursiver Positionen über mehrere soziale Welten hinweg. In diesem Sinne ist es hilfreich, die Analyse sozialer Welten (3.2) zu ergänzen durch eine Beschreibung und Verortung zentraler Positionen und Themen des Arenasegments (Clarke 2012: 165-167). Die folgenden Abwägungen der zahlreichen Argumente, die für und gegen ein nationales Routing vorgebracht wurden, zeigen demnach, welche (normativen) Diskurse in den Aushandlungen der Arena eine Rolle spielen.

Als Begründung für das nationale Routing wird vor allem die angenommene gesteigerte Abhörsicherheit genannt. Dieses wünschenswerte Ziel sei durch ein nationales Routing mit wenig technischem Aufwand zu erreichen.[30] Jedoch sei ein Ausbau von Leitungskapazitäten erforderlich, um Leistungsengpässe zu verhindern, die dadurch entstehen, dass nicht mehr auf ausländische Leitungsressourcen zurückgegriffen werden soll (Waidner 2014: 15). Das Argument der Abhörsicherung fungiert als Wegbereiter einer Allianz zwischen der Welt der Industrie und der Welt des Staates, die so dieses scheinbar gemeinsame Anliegen mit den jeweiligen weltenspezifischen Interessen verknüpfen können. Während eine Einführung des Routings für die Deutsche Telekom potentiell mit Wettbewerbsvorteilen einhergehen könnte, ergibt sich für die deutsche Bundesregierung die Mög-

[30] Siehe hierzu Federrath, zit. in: Pech 2014: 22.

lichkeit, deutsche und europäische Wirtschaftsförderung zu betreiben (vgl. Abschnitt 3.2). Die Gegenargumente sind indes vielfältig und werden im Folgenden genauer beleuchtet.

3.3.1 Internationale Abkommen als Alternative?

Eine erste ausführliche Stellungnahme aus der akademischen Fachwelt zum nationalen Routing haben Pohlmann, Siromaschenko und Sparenberg abgegeben (2014: 112). Als Vertreter der Welt der Wissenschaft und Technik stehen sie dem Vorhaben des nationalen Routings skeptisch gegenüber. Sie sprechen sich gegen die Idee des nationalen Routings aus und empfehlen stattdessen, auf verbindliche internationale Normen hinzuwirken und gleichzeitig die Internet-Provider und ihre Kunden durch Anreize wie Steuervorteile zur Implementierung von Sicherheitstechnologien zu motivieren (ebd.: 118). Dem kann zunächst entgegengehalten werden, dass die Aussichten auf den Abschluss solcher internationaler Abkommen als sehr gering einzustufen sind.[31] Insbesondere dürften die Verhandlungen um ein sog. „No-Spy-Abkommen" zwischen den USA und der Bundesrepublik Deutschland als gescheitert gelten.[32] Zudem ist zu beachten, dass ein solches Abkommen mit den USA nicht gegen die Tätigkeit russischer, chinesischer oder sonstiger Geheimdienste wirken würde. Wer nach internationalen Abkommen ruft,[33] der verkennt, dass solche Abkommen häufig nicht im Interesse der unterzeichnenden Staaten liegen.[34]

---

[31] So blieben bereits 2001 Forderungen des EU-Parlaments nach einem Abkommen zum Schutz von EU-Bürgern vor amerikanischen Geheimdiensten ungehört, die im Rahmen der Echelon-Affäre formuliert worden waren. Siehe zur Affäre den Bericht des Europäischen Parlaments A5-0264/2001 v. 11.7.2001. Die Affäre wurde schnell durch die Ereignisse des 11.9.2001 überdeckt.

[32] Ob von Seiten der USA überhaupt irgendeine Verhandlungsbereitschaft zum Abschluss eines solchen Abkommens bestanden hat und ob die Bundesregierung sich dieser Sache bewusst war, aus wahltaktischen Gründen jedoch öffentlich an der Möglichkeit eines Abkommens festhielt, wurde ab Frühjahr 2015 lebhaft diskutiert. Laut Recherchen von NDR, WDR und SZ war die Bundesregierung bereits im Januar 2014 sicher, dass es kein „No-Spy-Abkommen" geben wird. Frankreich bemühte sich 2012 ebenfalls erfolglos um ein No-Spy-Abkommen mit den USA.

[33] So etwa Rolofs 2014: 28.

[34] Eine weitere Erklärung liefern Rosenbach/Stark (2014: 145): Der Betrieb des Überwachungsapparats unter Zuhilfenahme privater Unternehmen (z.B. Booz Allen

Ein Staat hat – oftmals – nur ein Interesse am Schutz seiner eigenen Bürger. Das Wohlergehen der Bürger anderer Nationen gehört dann nicht zu den genuinen Aufgaben des Nationalstaates. Sofern Nationalstaaten miteinander in Verhandlungen treten, können folglich Interessenkonflikte auftreten. Ein internationales Abkommen gegen Abhörmaßnahmen und Datensammeln im Internet müsste spezielle Vorteile für alle Unterzeichnerstaaten mit sich bringen, sonst könnte es nur mit Druck durchgesetzt werden. Eine Allianz wie zwischen der Welt der Industrie und der Welt des Staates im Falle des nationalen Routings dürfte hier nur schwer vorzustellen sein, solange es nicht gelingt, einen gemeinsamen Nenner, im Sinne eines obligatorischen Passagenpunkts, zu finden, der es erlaubt, sowohl ein gemeinsames Interesse als auch eigene Interessen weiterhin verfolgen zu können.

Als Beispiel für diese Schwierigkeiten verweist Hoffmann-Riem auf den Umweltbereich, konkret auf das Kyoto-Protokoll und die Rio-Deklaration, um zu illustrieren, wie schwierig sich die Durchsetzung einer bestimmten Agenda auf internationaler Ebene gegen bestimmte nationale und wirtschaftliche Interessen regelmäßig gestaltet (Hoffmann-Riem 2014: 63).[35] In diesem Zusammenhang wird häufig auf die Verhandlungen um ein transatlantisches Freihandelsabkommen zwischen den USA und Europa verwiesen, die genutzt werden könnten, um entsprechenden Druck auszuüben.[36] Ob Deutschland, die Schengen-Staaten oder die Europäische Union als Ganzes jedoch tatsächlich in der Lage sind einen ausreichend starken Druck aufzubauen ist zumindest fraglich. Zudem könnte die innerstaatliche Durchsetzung eines Abkommens, das gerade für das notorisch intransparente Wirken von Geheimdiensten Wirkung entfalten soll, – sollte es zustande kommen – wohl kaum wirksam überprüft wer-

---

Hamilton) „ist ein Bombengeschäft".

[35] Trotzdem bestehe eine Pflicht, trotz geringer Erfolgsaussichten am Ziel eines internationalen Abkommens festzuhalten: „Die Aufgabe als solche entfällt aber nicht dadurch, dass ihre Erfüllung durch Interessengegensätze erschwert wird und in vielem noch Desiderat ist."

[36] Siehe beispielhaft Bendiek 2014.

den.[37] Den Bürgern bliebe letztlich nur, darauf zu vertrauen, dass andere Staaten, die ein solches Abkommen unterzeichnet haben, sowie ihre Dienste sich an für sie stark nachteilige Vereinbarungen halten. Eine Verletzung des Abkommens wäre mithin kaum feststellbar und wenn doch, fast unmöglich zu rügen.

Häufig wird ferner auf unterschiedliche kulturelle Vorstellungen und Werte zwischen Europa und den USA verwiesen, in denen verschiedene Konzepte von Privatheit miteinander konkurrieren würden, weswegen ein Abkommen oder gar eine rechtliche Harmonisierung unmöglich wäre. Das nationale ebenso wie das Schengen-Routing erscheinen unter dieser Perspektive als ordnende Praktiken, die ein an der Privatsphäre seiner Bürger interessiertes Deutschland bzw. Europa den in das Intimste eindringenden USA gegenüberstellen. Diese Darstellung der Auseinandersetzung, die in Anlehnung an Huntington gar als „Kampf der Kulturen" (Miller/Poscher 2013) bezeichnet wurde, lässt sich jedoch eher als eine „Politik der Verortung" (Lossau 2002) beschreiben, in der ein kulturell homogenisierter Raum konstruiert wird. Eine solche Darstellung verschleiert, dass sowohl in der BRD als auch in Europa insgesamt sehr unterschiedliche Vorstellungen von Privatheit vorherrschen und die Befugnisse auch der hiesigen Behörden umstritten sind.

3.3.2 Anreize und Hilfe zur Selbsthilfe

Ein prominenter Argumentationsstrang in der Debatte um ein nationales Routing sieht in dem Vorhaben bestenfalls eine Ergänzung zu weiteren Sicherheitsvorkehrungen, die auf Seiten der Nutzer oder der Provider – am besten gefördert durch staatliche Anreize – implementiert werden sollten (vgl. Abschnitt 3.2). Die Erfolgsaussichten von staatlichen Anreizen für Internet-Provider dürfen jedoch bezweifelt werden. Die Anreize müssten gewichtig genug sein, um Provider tatsächlich zum Handeln zu bewegen. Auf Nutzerebene ist zu beachten,

[37] So verletzten die USA und China durch umfassendes Ausspähen der Vereinten Nationen entsprechende Abkommen, die derartige Spionage eigentlich verbieten (Rosenbach/Stark 2014: 152 ff.).

dass eine Hilfe zur Selbsthilfe bei der Implementierung von Sicherheitsmaßnahmen häufig an den Fähigkeiten der Nutzer scheitern wird.

Zum einen setzt die Selbsthilfe voraus, dass die Möglichkeiten des Selbstdatenschutzes überhaupt gegeben sind. Zum anderen müssen die Nutzer dafür sensibilisiert werden, welche Gefahren vorliegen, wenn die eigenen Daten nicht gesichert sind. Schließlich dürften beispielsweise mit einer Ende-zu-Ende-Verschlüsselung von E-Mails etwa via GnuPG/PGP oder S/MIME nicht wenige Nutzer überfordert sein. So gestehen auch Pohlmann u.a. ein: „Um einen wirkungsvollen Schutz vor Traffic Snooping und MITM-Attacken [...] zu gewährleisten, sind allerdings profunde Fachkenntnisse erforderlich, die man beim typischen Durchschnittsnutzer nicht voraussetzen kann“ (Pohlmann/Siromaschenko/Sparenberg 2014: 118).[38]

So lobenswert das Ziel auch sein mag, die Bevölkerung bezüglich des Einsatzes von Sicherheitstechnologien zu sensibilisieren und Anleitungen zum Selbstschutz zur Verfügung zu stellen, so muss doch auch klar sein, dass dieser Ansatz allein nicht zum Ziel führen, sondern lediglich eine unterstützende Maßnahme sein kann.

Allerdings findet sich hier eine Ambivalenz im Verhältnis der Aufgabenverteilung zwischen Staat und Bürger. In der klassischen Staatstheorie ist der Staat zwar verpflichtet, sich um das Gemeinwohl zu sorgen. So legitimiert etwa für Thomas Hobbes der Schutz des Bürgers erst das Gewaltmonopol des Staates (Hobbes 1996: 141ff.). Es ist Aufgabe des Staates, für die Unversehrtheit seiner Bürger zu sorgen. Dies gilt nicht zuletzt gegen Angriffe von außen. Zugleich gibt es eine Pflicht zur aktiven Mitarbeit des mündigen Bürgers. Der Staat kann die ihm zugewiesenen Aufgaben nur durchführen, solange sich der Bürger kooperativ zeigt.

[38] Drastischer formuliert es Schneier: „Im Grunde genommen ist der durchschnittliche Anwender aufgeschmissen“ (Schneier 2013a).

In den aktuellen Vorschlägen der Selbsthilfe wird nun der Schwerpunkt der Verantwortung dem Bürger zugeschrieben. Dem einzelnen Bürger stehen gerade im direkten Vergleich zu den mächtigen Geheimdiensten aber nur verschwindend geringe Ressourcen zum Selbstschutz zur Verfügung. Wenn der Staat daher seine eigenen Ressourcen nicht einsetzt und seine Verantwortung auf das Individuum ablädt, ist dies insgesamt eine einseitige Verschiebung des Verhältnisses zu Lasten des Bürgers.[39]

Es ist ferner anzunehmen, dass etwa ein Aufruf zur Verschlüsselung von E-Mails – sei es aufgrund von Gleichgültigkeitseffekten oder einer „Nothing to hide-Grundhaltung“[40] – nicht den gleichen Effekt erzielt hätte, wie er durch die Kampagne „E-Mail made in Germany“[41] erzielt

---

[39] So scheinen sich bisher Reaktionen der Bundesregierung auf den NSA-Skandal vornehmlich auf Maßnahmen zur Eigensicherung zu reduzieren, die dem Bürger nicht zur Verfügung stehen. Siehe hierzu Amann u.a. 2014: 24 f.: So werden für sensible Kommunikation vermehrt sogenannte Kryptohandys benutzt. Steht dem gewünschten Gesprächspartner kein solches Gerät zur Verfügung, wird zu ungewöhnlichen Maßnahmen gegriffen: „Für heikle Telefonate in Berlin schickt [die Verteidigungsministerin] manchmal einen Bundeswehroffizier mit einem Krypto-Handy zu ihren Gesprächspartnern. Der wählt von dem verschlüsselten Mobiltelefon die Ministerin an und reicht das Gerät weiter. ‚Frau Ministerin, ich übergebe', heißt es dann.“ Handys und ähnliche Geräte werden bei wichtigen Besprechungen aus dem Raum verbannt. Weitere Maßnahmen sind neue Verhaltensvorschriften für Mitarbeiter und Überprüfungen der internen Kommunikationsnetze. Zudem habe das BSI „an zentralen Punkten im Bundestag und in Bundesministerien kleine Handy-Funkmasten installiert. Der Zweck dieser sogenannten Inhouse-Anlagen: Wer immer in deren Nähe mobil telefoniert, dessen Handy loggt sich in den vom BSI präparierten Minimasten ein – und nicht in einer Anlage, die auf dem Dach der US-Botschaft am Brandenburger Tor oder nebenan bei Briten und Russen stehen könnte“ (Amann u.a. 2014: 25).

[40] Vgl. hierzu die Ergebnisse der repräsentativen dimap-Studie „Untersuchung zur Wahrnehmung des ‚Snowden/NSA-Skandals' in Deutschland“ im Auftrag des DIVSI v. 8.5.2014. Danach sehen immerhin 22% der Befragten die Überwachung durch Geheimdienste als gerechtfertigt an, während 18% angeben, „das Vorgehen der Geheimdienste hat keinen Einfluss auf mein Leben und interessiert mich daher nicht“ (S. 8 f. der Studie). Nur jeder vierte gab an, sein Telefon, Mail- und Surfverhalten seit den Enthüllungen „sehr“ (9%) oder „etwas“ (14%) geändert zu haben; 44% identifizierten sich mit der Aussage „Es interessiert mich nicht, ob meine Telefonate oder Mails abgehört werden oder aufgezeichnet werden. Ich habe nichts zu verbergen und ich werde auch nichts ändern“ (S. 10 f. der Studie).

[41] Siehe hierzu Gerling 2014: 109. Im Gegensatz zu der von der Deutschen Telekom, United Internet mit 1&1, GMX und Web.de ins Leben gerufenen Initiative setzen der

wurde, bei der Nutzer gewissermaßen zum Einsatz von (Transport-) Verschlüsselung „gezwungen“ wurden. Überdies ist zu bedenken, dass – werden die Nutzer sich selbst überlassen – mit einer langen Vorlaufzeit zu rechnen ist, bis die Mehrheit der Bürger Sicherheitsmaßnahmen implementiert hat. Zudem wird auf diese Weise immer ein Rest verbleiben, der sich solchen Maßnahmen aus unterschiedlichsten Gründen gänzlich verweigern wird.

Ebenfalls zu beachten ist, dass der Nutzer keinen Einfluss darauf hat, ob an ihn adressierte Nachrichten verschlüsselt werden, sondern allenfalls den Empfang unverschlüsselter Kommunikation ablehnen oder blockieren kann, was jedoch erhebliche Folgeprobleme nach sich zieht. Unter Umständen ist ein Zugriff auf ausgehende Kommunikation deshalb gar nicht notwendig, um zumindest einzelne Informationen über einen Nutzer zu gewinnen, da diese auch in eingehender unverschlüsselter Kommunikation enthalten sein können.[42] Dadurch wird die Effektivität von Selbstschutzmaßnahmen einzelner Nutzer limitiert.

3.3.3 Unterlaufen durch geheimdienstliche Kooperation?

Insbesondere aus der sozialen Welt der Netzgemeinde wird das Argument eingebracht, nationales Routing sei wirkungslos, da auf diesem Wege zwar ausländische Geheimdienste vom Zugriff abgeschnitten wären, dies aber nicht die Zugriffsmöglichkeiten der deutschen Dienste beträfe. Diese gäben ihre Datensammlungen ohnehin an ausländische Partnerdienste weiter.[43] Damit laufe das nationale Routing als Maßnahme leer. Während solche Argumentationen in der transnational orientierten Netzgemeinde fruchtbar sind, greifen die territorial operierenden Welten des Staates und der Rechtsanwen-

---

Dienst Posteo und der Bund auf die Transportverschlüsselung DANE, einen offenen Standard, der ohne eine kostenpflichtige Zertifizierung auskommt (heise.de 2014).

42 Siehe zum Thema „Was Dritte über uns verraten“ Bager 2014: 76 ff.

43 So etwa Rieger 2013. Eine generelle Kooperation wird auch nicht geleugnet, sondern als Notwendigkeit formuliert: „Ohne internationale Zusammenarbeit könnte der Bundesnachrichtendienst noch nicht einmal ansatzweise seine gesetzlichen Aufgaben erfüllen“ (Schindler 2013).

dung eher zu Erklärungen, die sich auf die Ordnungs- und Kontrollpotentiale der Nationalstaaten beziehen. In dieser Logik ist der Verweis auf diffuse Ängste bezüglich der Tätigkeiten der deutschen Dienste wenig zielführend. Die deutschen Dienste sind in ihren Tätigkeiten an das deutsche Grundgesetz und einfachgesetzliches deutsches Recht gebunden. Sie stehen unter parlamentarischer Aufsicht und Rechtsverstöße können direkt sanktioniert werden. Ferner sind die Kompetenzen der deutschen Dienste klar durch den deutschen Gesetzgeber regelbar. Die derzeit geltenden Ermächtigungsgrundlagen für eine Telekommunikationsüberwachung sind zwar vielfältig,[44] aber es sind auch Schranken gezogen. Das G10-Gesetz begrenzt etwa die Tätigkeit des BND im Rahmen der strategischen Telekommunikationsüberwachung auf die Überwachung internationaler[45] Telekommunikationsbeziehungen bei einer Höchstquote von 20% (§ 10 Abs. 4 S. 4 G10-Gesetz).[46] Damit sind allerdings nicht 20% der tatsächlichen übertragenen Daten gemeint, sondern die angegebene Höchstquote bezieht sich auf den „Anteil der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität" (§ 10 Abs. 4 S. 3 G10-Gesetz). Da die Auslastung einzelner Übertragungswege regelmäßig unterhalb dieser 20% liege, ist trotz der Beschränkung davon auszugehen, dass im Normallfall der gesamte Datenverkehr auf den überwachten Übertragungswegen ausgespäht wird.[47] Zudem ist zu beachten, dass etwa datenintensive Unterhaltungsanwendungen ohnehin keine geheim-

---

[44] Siehe insbesondere § 9 Abs. 2 S. 1 BNDG, § 5 G10-Gesetz, sowie Sonderbefugnisse wie etwa Art. 3 des Zusatzabkommens zum NATO-Vertrag.

[45] Hier ist jedoch anzumerken, dass die vom BND eingesetzten Filter, welche abgefangene Kommunikation deutscher Personen herausfiltern sollen, nach Medienberichten keine „absolute und fehlerfreie" Trennung zwischen ausländischer und deutscher Kommunikation ermöglichen. Dadurch seien von 2003 bis 2008 in Frankfurt abgefangene Daten auch deutscher Bürger rechtswidrig an Partnerdienste weitergegeben worden (Süddeutsche.de 2014a).

[46] Siehe hierzu Roggan, in: Kommentar zum G-10-Gesetz 2012: § 10n, Rn. 12. Siehe auch BVerfGE 100, 313.

[47] Siehe hierzu die Ausführungen von Bäcker: Bäcker 2014a: 12 f.; Bäcker 2014: 558. Der Spiegel berichtet etwa, der BND höre „den gesamten Datenverkehr der von ihm in Afghanistan, Somalia und dem Nahen Osten angezapften Verbindungen" ab und speichere diesen in der Regel für die Dauer von sieben Tagen (Der Spiegel 37/2014: 16).

dienstliche Relevanz haben dürften (Heumann/Wetzling 2014: 15). Es stellt sich somit durchaus die Frage nach der Effektivität der Schranken der Überwachungstätigkeit deutscher Geheimdienste. Ferner haben die deutschen Dienste in der Vergangenheit selbst die weiten Schranken ihrer Tätigkeit überschritten.[48] Da es trotz des bestehenden Entdeckungs- und Sanktionsrisikos zu Kompetenzüberschreitungen gekommen ist, ist – wie in der Folge der NSA-Affäre verstärkt gefordert[49] – eine stärkere Kontrolle der Dienste[50] und wegen der Ineffizienz von Schranken wie § 10 Abs. 4 S. 4 G10-Gesetz auch eine Präzisierung[51] oder gar Neufassung der gesetzlichen Grundlagen ihrer

[48] Siehe zu deutschen Geheimdienst-Affären beispielhaft Foschepoth 2012: 232 ff.

[49] So werden die Vorschriften des G10-Gesetzes zur strategischen TKÜ für verfassungswidrig halten. Insbesondere gelte das Fernmeldegeheimnis auch bei der Tätigkeit des BND im Ausland. Siehe beispielhaft die Stellungnahme Bäckers vor dem NSA-Untersuchungsausschuss: Bäcker 2014a**.** Demgegenüber steht zuletzt die Entscheidung des Bundesverwaltungsgerichts vom 28.5.2014 (BVerwG 6 A 1.13), in der das Gericht erklärte, die Überwachungspraxis des BND sei „verfassungsrechtlich nicht zu beanstanden". Siehe BVerwG 2014: 997. Im April 2015 wurde bekannt, dass die Überwachung ausländischer Kommunikationsvorgänge durch den BND als Reaktion auf die bestehende Kritik, insbesondere an der sog. ,,Weltraumtheorie", neu geregelt werden soll (Der Spiegel 16/2015). Die SPD-Bundestagsfraktion stellte hierzu im Juni 2015 ein Eckpunktepapier vor mit dem Titel „Rechtsstaat wahren – Sicherheit gewährleisten". Auch BND-Präsident Schindler sprach sich für eine Neudefinierung der Rechtsgrundlagen der Arbeit seiner Behörde aus (siehe Heute im Bundestag Nr. 320 v. 18.6.2015).

[50] So hat der Bundestag schon 2014 400.000 Euro zusätzlich für die Arbeit des Parlamentarischen Gremiums zur Kontrolle der Geheimdienste bewilligt. Dieses soll auch persönliche Kontrollen vor Ort durchführen. „Wir habe uns zur Aufgabe gemacht, künftig zu schnüffeln, zu bellen und wenn nötig auch zu beißen" (Lischka, zit. in: tagesschau.de 2014). Zu den vielfältigen Mängeln bei der Kontrolle und Aufsicht amerikanischer Geheimdienste durch den Foreign Intelligence Surveillance Court und den Kongress siehe Greenwald 2014: 186 ff. Neue Zweifel an der Effektivität der Kontrolle des BND kamen im April 2015 auf, als Informationen über den Umgang des BND mit unzulässigen Suchanfragen durch die NSA im Rahmen geheimdienstlicher Kooperation publik wurden.

[51] So identifizieren Arnbak und Goldberg etwa „Loopholes" in den US-amerikanischen Regelungen, die der NSA auch die Überwachung von amerikanischen Bürgern trotz des vierten Verfassungszusatzes erlauben. Internet Traffic gelte nämlich bereits dann als „nicht-amerikanisch" und damit nicht von US-Recht geschützt, wenn er im Ausland gesammelt wird. Dies erlaube beispielsweise durch eine Umleitung des Traffic die massenhafte Überwachung auch von US-Bürgern (Arnbak/Goldberg 2014). Sollte auch das deutsche Recht entsprechende Schlupflöcher beinhalten, so sind diese zu schließen. Zum Reformbedarf des rechtlichen Rahmens der strategischen Auslandsüberwachung durch den BND siehe (Heumann/Wetzling 2014).

Arbeit wohl zwingend notwendig.[52] Ein Gesetzentwurf, der Anfang 2016 von der Bundesregierung eingebracht wurde, soll die parlamentarische Kontrolle der Dienste durch Einsetzung eines Ständigen Bevollmächtigten verbessern. Ein nationales Routing könnte indes zum Verhindern des Umgehens von Befugnisschranken beitragen, wobei bestimmte Daten, die dem Zugriff deutscher Dienste durch geltendes Recht entzogen sind, durch ausländische Dienste gesammelt werden und dann an deutsche Dienste im Wege der nachrichtendienstlichen Kooperation weitergeleitet werden („Befugnis-Hopping").[53] Ferner entfiele auch die Möglichkeit, eigentlich innerdeutschen Datenverkehr als „ausländisch" einzustufen und im Rahmen der Auslandsaufklärung abzuhören, wenn dieser über das Ausland geleitet wird.

Fraglich war zunächst auch, ob die Enttarnung eines BND-Mitarbeiters, der geheime Dokumente an die USA weitergab, nicht ohnehin zu einer Abkühlung des Verhältnisses zwischen deutschen und amerikanischen Diensten und zu einer Entflechtung führen würde.[54] In der Folge der Enttarnung sprach etwa Innenminister de Maizière erstmals davon, die Spionageabwehr des BND brauche zukünf-

---

[52] Auch in den USA wurde davon gesprochen, die US-amerikanischen Dienste hätten gesetzliche Kompetenzen überschritten (Sensenbrenner, zit. in: Rolofs 2014: 29). Siehe auch den von Conyers und Amash eingebrachten Gesetzesentwurf vom Juli 2013 (Amendment to the National Defense Authorization Act) sowie die Empfehlungen von Clarke et al. (2013). Die anhaltende Kritik an der Ausspähung auch amerikanischer Staatsbürger innerhalb der Grenzen der USA führte schließlich zum Erlass des sogenannten USA Freedom Act, der letztlich jedoch nur geringe Einschränkungen vorsieht. Insbesondere soll die Speicherung entsprechender Daten künftig nicht mehr durch die NSA, sondern durch die Telefongesellschaften erfolgen. Im Vereinigten Königreich wurde zuletzt eine mangelnde Aufsicht der nationalen Geheimdienste konstatiert (House of Commons 2014: 57 ff.). Siehe als Beispiel für historisch belegte Kompetenzüberschreitungen und illegale Aktivitäten der US-Geheimdienste die Berichte des sog. Church Committee aus dem Jahr 1975. Zu Überschreitungen im aktuellen NSA-Skandal siehe (Rosenbach/Stark 2014: 175 ff.). Zum Problem der „incidental collection" siehe Gellman/Tate 2014.

[53] Zum Begriff siehe BT Drs. 18/59.

[54] „Man stelle sich auf eine längere Eiszeit mit den Amerikanern ein, heißt es in Regierungskreisen" (Amann u.a. 2014: 25). In einem ähnlich gelagerten Fall in den 1960er Jahren gab es ebenfalls Überlegungen, die Geheimdienstzusammenarbeit einzuschränken. Siehe Baumgärtner u.a. 2014: 22 f.

tig einen „360-Grad-Blick“ (Bild.de 2014).[55] Nato-Staaten dürften künftig nicht mehr von entsprechenden Maßnahmen deutscher Dienste ausgenommen werden.[56] Von Seiten der USA wurde die Zusammenarbeit mit dem BND ohnehin ab Frühjahr 2015 laut Medienberichten deutlich eingeschränkt. Es dauerte allerdings nicht lange, bis die Zusammenarbeit etwa in Bad Aibling wieder "fast so wie früher" lief (tagesschau.de 2016). Als ein Grund hierfür wurde die Befürchtung genannt, dass aus dem deutschen NSA-Untersuchungsausschuss geheime Informationen an die Öffentlichkeit gelangen könnten.

Insbesondere ist jedoch die unterschiedliche Interessenlage deutscher und ausländischer Dienste hervorzuheben. Hierin deuten sich Segmentationen der Welt der Geheimdienste in nationale Subwelten an, die unterschiedlichen Logiken folgen. Die NSA etwa „sichert die Informationsüberlegenheit der USA“ (Ruhmann 2014: 43 f.).[57] Dies schließt neben dem Kampf gegen Terrorismus und Kriminalität (der Suche nach „Nadeln“ in einem „Heuhaufen“, der den gesamten globalen Datenverkehr und die gesamte globale Kommunikation umfassen soll) wohl auch politische und wirtschaftliche[58] Spionage mit ein. Der

---

55 Siehe auch BT-Drs. 18/3352.

56 Man beachte hierzu jedoch, dass der NATO-Staat Türkei wohl auch zuvor bereits im Visier deutscher Dienste stand. Siehe BT-Drs. 18/2599. Gleiches gilt für Frankreich.

57 Dieser Anspruch ist zunächst durch das Versagen der amerikanischen Geheimdienste angesichts der Ereignisse des 11.9.2001 bestimmt, lässt sich jedoch über Programme wie „Project Shamrock“ und „ThinThread“ bis zur Tätigkeit des 1919 gegründeten Cipher Bureau zurückverfolgen. Siehe hierzu detailliert Rosenbach/Stark 2014: 91 ff.

58 So wirft etwa Obermann der NSA vor, es gehe ihr um das Erarbeiten ökonomischer Vorteile und spricht in diesem Kontext von einer „Aushöhlung des fairen Wettbewerbs“ (Obermann, zit. in: Diersch 2014: 68). Auch Snowden hat der NSA Wirtschaftsspionage vorgeworfen: „Wenn es etwa bei Siemens Informationen gibt, die dem nationalen Interesse der Vereinigten Staaten nutzen – aber nichts mit der nationalen Sicherheit zu tun haben – dann nehmen sie sich diese Informationen trotzdem“ (Snowden, zit. in: NDR.de 2014). Anders der ehemalige National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism for the United States Richard Clarke, der auf die Frage nach Wirtschaftsspionage antwortet: „Der NSA ist das verboten, und sie macht es nicht. Ganz im Gegensatz zu dem was zum Beispiel China tut. Die NSA darf sich nicht bei Airbus einhacken, um das neueste Flügeldesign herauszufinden und es an Boeing weiterzureichen. Das wäre illegal und es passiert nicht. Dafür kann ich garantieren.“ (Clarke, zit. in: tagesschau.de 2014c). Auch die deutsche Bundesregierung und der Verfassungsschutz sehen in

BND und die anderen deutschen Dienste hingegen haben kein Interesse an Wirtschaftsspionage bei *deutschen* Firmen.

In Betrachtung der historisch gewachsenen Verbindungen der BRD mit den USA gibt es bestimmte Abhängigkeiten der Geheimdienste voneinander. Nicht alle Verträge und Absprachen sind derzeit öffentlich zugänglich. Eine Kooperation der Geheimdienste, wie sie praktiziert wird und auch weiterhin aufrechterhalten werden soll, steht daher immer in Gefahr, dass bestimmte Pfadabhängigkeiten zu einer problematischen Situation der deutschen Geheimdienste führen, die deutsche Wirtschaft zu schützen. Die Welt der Geheimdienste steht somit in einem ständigen Spannungsfeld zwischen der Segmentation in einzelne nationale Subwelten und der gegenseitigen Abhängigkeit zwischen den Subwelten, die eine völlige Loslösung verhindert und mitunter zu obskuren Verzahnungen und Verstrickungen führt.[59]

3.3.4 „Balkanisierung" des Internets?

Häufig wird vorgebracht, das nationale Routing führe zu einer Fragmentierung, einer „Balkanisierung" des Internets und gefährde damit

---

der Tätigkeit der NSA nach Presseberichten keine Gefahr für die deutsche Wirtschaft (heise.de 2014a). „Der Bundesregierung liegen aktuell keine Konkreten Hinweise auf Wirtschaftsspionage US-amerikanischer Nachrichtendienste gegen deutsche Unternehmen vor" (BT-Drs. 18/2281: 4). Zu beachten sind in diesem Zusammenhang jedoch Erkenntnisse aus der sog. Echelon-Affäre (siehe Rosenbach/Stark 2014: 166 ff., 206). Siehe auch Greenwald 2014: 195 ff.: „Etliches von dem, was die Snowden-Dokumente enthüllt haben, kann man nur als Wirtschaftsspionage bezeichnen." Auf das Thema angesprochen äußerte sich der ehemalige Leiter des französischen Inlandsgeheimdienstes Squarcini wie folgt: „Les Américains nous espionnent sur le plan commercial et industriel comme nous les espionnons aussi, puisqu'il est de l'intérêt national de défendre nos entreprises" (Squarcini, zit. in: Cornevin 2013). Siehe hierzu auch die Äußerung von Müller-Enbergs, wonach die Vorstellung, der französische Geheimdienst füge der deutschen Wirtschaft mehr Schaden zu als der chinesische oder der russische, „nicht weltfremd" sei (Müller-Enbergs, zit. in: zeit.de 2014). Weitere starke Indizien für Wirtschaftsspionage durch die NSA kamen im April 2015 auf im Zuge einer Affäre um die Weitergabe sog. „Selektoren" an den BND, sowie im Juli 2015 durch von der Enthüllungsplattform WikiLeaks veröffentlichte Dokumente, wonach insbesondere Mitarbeiter des deutschen Wirtschaftsministeriums durch die NSA abgehört wurden (tagesschau.de 2015).

[59] Strauss (1978) spricht hier von Intersektionen, die sich mitunter nicht nur in Allianzen, sondern auch in harten Auseinandersetzungen und Konflikten äußern können.

dessen „Offenheit“ (Kroes, zit. in: Schmundt/Traufetter 2014: 78), was zudem die „Renationalisierung des Datenschutzes und des Urheberrechtes“ mit sich bringe (Hartmann, zit. in: Pech 2014: 22). Im nationalen Routing wird gar ein Versuch gesehen, „potentiell das Netz selbst zu zerstören“.[60] Dabei soll die Wortwahl, insbesondere der Begriff der „Balkanisierung“, negative Assoziationen wecken, während etwa Obar und Clement mit „Repatriation“ (Obar/Clement 2013: 3) einen positiv besetzten Begriff wählten. Damit wird in der Debatte auch das Mittel der Negativetikettierung bzw. der Positivetikettierung zur Unterstützung des eigenen Standpunkts genutzt. Auch das BMWi erteilt einer gesetzlichen Verankerung des nationalen Routings eine Absage mit dem Argument, das offene und freie Internet bewahren zu wollen (BMWi 2014). Das BMWi scheint hier für die Interessen der Welt des Marktes einzutreten, deren Praktiken (der Netzgemeinde nicht unähnlich) von „freien“ und „offenen“ digitalen Netzwerken profitieren. Hoffmann-Riem erinnert in diesem Zusammenhang an traditionelle Strukturen des Brief- und Paketvertriebs (Hoffmann-Riem 2014: 56).[61] Ein in Deutschland aufgegebenes Paket, das auch an einen Empfänger in Deutschland adressiert ist, verlässt die Landesgrenzen nicht. Trotzdem können Pakete ins Ausland verschickt und aus dem Ausland empfangen werden. Letztlich handelt es sich beim nationalen Routing also um eine Rückkehr zu diesen hergebrachten Strukturen. Warum ein „nicht-balkanisiertes” Internet einen Wert in sich darstellen soll, ist vor diesem Hintergrund zumindest erklärungsbedürftig.[62]

---

[60] „a movement to balkanize the Internet – a long-standing effort that would potentially destroy the web itself […] In the pre-Snowden world, such a proposal would have been hooted down. But now Obermann was speaking to an audience that was all but armed with pitchforks, ready to storm the listening posts of American spooks” (Levy 2014).

[61] Hoffmann-Riem 2014a: 10.

[62] Hoffmann-Riem 2014a: 18: „Der Aufbau der globalen und hoch vernetzten Kommunikationsinfrastruktur des Internet war und ist eine großartige technologische und soziale Innovation. Dies anzuerkennen, schließt aber nicht das Nachdenken darüber aus, ob und wie die durch neue technologische Entwicklungen sowie neue Geschäftsmodelle bedingten neuen Gefährdungspotentiale auch durch Änderungen der ‚Netzphilosophie‘ reduziert werden und durch teilweisen Um-/Neubau der Netze die vielen Chancen der Informationsgesellschaft besser genutzt werden können.“

Aus der Netzgemeinde wird dem entgegen gehalten, die so genannte „Balkanisierung" sei das „Ende des freien Internets", dessen Erfolg gerade in den „Prinzipien der Offenheit, Transparenz und Neutralität" lägen und die durch Fragmentierung und Separierung bedroht würden (Internet Society German Chapter 2003). Erst diese Offenheit und Konnektivität gewähre eine Stabilität des Netzes, da dadurch Daten immer wieder Wege fänden, wenn einzelne Server ausfielen oder aus politischen Gründen behindert würden. Ferner wird angeführt, ein „balkanisiertes" Internet erleichtere die Kontrolle des Internetverkehrs. Dem gegenüber stehen die Zielsetzungen der NSA, die intern mit „Owning the Internet"[63] umschrieben werden und gerade auf einem „nicht-balkanisierten" Internet aufbauen (NSA-Dokument „SigInt Strategy 2012-2016", zit. in: Rosenbach/Stark 2014: 124). Bereits 2008 machte die New York Times auf die Entwicklung aufmerksam, dass immer weniger Datenverkehr durch die USA fließe (Markoff 2008). Dies werde von den US-amerikanischen Geheimdiensten mit Sorge beobachtet. In dem Artikel, in dem sich viele der im Zuge der NSA-Affäre in aller Deutlichkeit zutage getretenen Probleme bereits andeuten, wird CIA-Direktor Hayden schließlich mit den Worten zitiert: „Because of the nature of global telecommunications, we are playing with a tremendous home-field advantage, and we need to exploit that edge [...] We also need to protect that edge, and we need to protect those who provide it to us" (Hayden, zit. in: Markoff 2008). Diese andauernden Bestrebungen würden durch ein nationales Routing zumindest gestört. Zudem verweist die New York Times auf das Beispiel Ägypten: Dort führte im Januar 2008 der Ausfall eines Datenkabels im Mittelmeer zu massiven Störungen im nationalen Netzverkehr, da Daten nicht zwischen lokalen Providern gepeert[64] wurden, sondern stattdessen über europäische Anbieter geleitet wurden. Insofern findet sich hier eine normative Hierarchie zwischen den Wer-

[63] Der Begriff „to own something" wird allgemein mit „etwas besitzen" übersetzt. „To own something" beschreibt dabei einen individuellen Besitzanspruch an etwas, der mit niemand anderem geteilt wird.

[64] Unter „Peering" wird die Verbindung von Netzwerken zum Zweck des Datenaustauschs verstanden. Siehe zum Begriff auch Tanenbaum/Wetherall 2011: 480 f.

ten Stabilität des Netzes und gesellschaftlicher Sicherheit, die gegeneinander ins Feld geführt werden.

3.3.5 Wirtschaftliche Aspekte

Von besonderer Signifikanz ist das Argument, die Einrichtung eines nationalen Routings führe zu einer marktbeherrschenden Stellung der Deutschen Telekom AG. Entsprechende Einwände kommen dann vor allem aus der Welt des Marktes, deren Praktiken auf einen möglichst unregulierten Wettbewerb setzen. So fühlen sich gerade die kleineren Anbieter durch die Pläne der Telekom in ihren wirtschaftlichen Interessen bedroht. Sie könnten, so die Befürchtung, durch eine Verpflichtung gezwungen sein, kostenpflichtig mit der Telekom zu peeren. Hintergrund ist, dass die Telekom für das Peering von anderen Anbietern Gebühren verlangt, während ein Peering mit ausländischen Anbietern unter Nutzung von Leitungsüberkapazitäten im Ausland oft kostenlos oder zumindest kostengünstiger möglich ist. So sieht denn auch Telekom-Chef Höttges in den Kosten einen zentralen Grund für die Ablehnung eines nationalen Routings (Höttges, zit. in: Heuzeroth 2014: 5). Es wäre deshalb bei der Ausgestaltung darauf zu achten, dass ein nationales Routing oder ein Schengen-Routing nicht zu einer ungewollten Monopolisierung führt. So könnte etwa die Telekom umgekehrt dazu verpflichtet werden, unentgeltlich mit anderen europäischen Anbietern zu peeren. Dies fordern etwa die Betreiber des Internetknoten DE-CIX (Summa, zit. in: DE-CIX 2013; Rieger 2013). Gerade an dieser Stelle wird deutlich, dass hinter der Debatte um nationales Routing handfeste wirtschaftliche Interessen stehen.[65] Vor einer möglichen Einführung von nationalem Routing sollte mithin dessen Vereinbarkeit mit §§ 19 bis 21 GWB sowie mit Art. 56 bis 62 AEUV geprüft werden.

Eng verknüpft mit der Sorge um eine marktbeherrschende Stellung der Telekom ist der Vorschlag einer Stärkung nationaler IT-

[65] Trotz gegenteiliger Beteuerungen durch die Deutsche Telekom AG: „Das Ziel ist nicht, mehr Geld zu verdienen, sondern wieder Vertrauen in unsere Branche aufzubauen“ (Obermann, zit. in: FAZ.net 2013).

Unternehmen, verbunden mit dem Ruf nach Technologieführerschaft. In den Worten von Kommissarin Kroes: „Europe can become the safest cyber economy in the world. […] We need the best technology“ (Kroes, zit. in: Diersch 2014: 68). Gleichsam fordert der Bundesverband IT-Mittelstand: „Der Fokus muss auf der Stärkung der Qualität und Zukunftsfähigkeit unserer IT-Produkte liegen, damit wir unabhängiger von ausländischen Produkten werden.“ (Grün, zit. in: Bundesverband IT-Mittelstand e.V. 2013; United States Trade Representative 2014: 5). Hier fällt häufig der Verweis auf den Flugzeughersteller Airbus als Beispiel einer europäischen Erfolgsgeschichte. So „forderte Kanzlerin Angela Merkel einen Airbus für das Internet: eine gemeinsame europäische Initiative, um sich der Übermacht amerikanischer und chinesischer Hightech-Firmen zu erwehren, wie sich einst Airbus dem US-Flugzeugbauer Boeing entgegenstemmte.“ (Dohmen/Traufetter 2013: 46).[66] Dies verstärkt den Eindruck, dass ein Teil der Debatte um ein nationales Routing und um die NSA-Affäre insgesamt von wirtschaftlichen Interessen geprägt wird. So heißt es hinter nur halb vorgehaltener Hand aus der deutschen IT-Wirtschaft: „Unser bester Marketing-Mitarbeiter ist Edward Snowden.“ (Schmundt/Traufetter 2014: 78).[67]

---

[66] Vgl. hierzu die Empfehlungen von Rogers/Ruppersberger (2012: VI f.), die vor dem Hintergrund der NSA-Affäre und der Dominanz der USA im Bereich der Computertechnik verbunden mit der Fähigkeit zur Manipulation amerikanischer Produkte bereits auf dem Versandweg fast schon ironisch wirken: „Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.” Siehe auch Greenwald 2014: 212 ff.: „Doch während amerikanische Firmen vor angeblich nicht vertrauenswürdigen chinesischen Routern gewarnt wurden, waren ausländische Organisationen gut beraten, sich vor amerikanischen Geräten zu hüten.“ Getragen war die Warnung des o.g. Berichts wohl von dem „Wunsch zu verhindern, dass die amerikanische Technik durch chinesische ersetzt wird, da dies die Reichweite der NSA beschränken würde.“

[67] Man beachte in diesem Kontext auch die Beendigung der Verträge von Bundesregierung und Bundesrat mit dem US-Provider Verizon (heise.de 2014b). Zudem planten alle Bundesländer außer Hessen nach Medienberichten eine Anpassung ihrer

Ein weiteres wirtschaftliches wie auch technisches Argument liegt in dem Verweis auf den durch die Implementierung eines nationalen Routings wahrscheinlich nötigen Ausbau der Netzinfrastruktur. Nationales Routing führe zu insgesamt „schlechterer Service-Qualität wegen künstlich geminderter Ausfallsicherheit, da die Verbindungen zu ausländischen Systemen nicht als Backup-Leitungen für innerdeutsche Kommunikation dienen können“ (Pohlmann/Siromaschenko/Sparenberg 2014: 116). Der nötige Netzausbau führe zu Preissteigerungen für die Nutzergemeinde, durch die „einkommensschwache Bevölkerungsteile besonders betroffen“ seien (Pohlmann/Siromaschenko/Sparenberg 2014: 115 f.). Ein weiterer Ausbau der nationalen Infrastruktur dürfte jedoch unabhängig von nationalem Routing ohnehin im Interesse des Standorts Deutschland und auch der Anbieter sein; er steht auch weiterhin – unabhängig von Ideen zum nationalen Routing – auf der politischen Agenda (CDU/CSU/SPD 2013: 34 f.). Allerdings müssten gegebenenfalls die Ausbauquoten gesteigert werden, um mit dem Ausbau nicht nur das nationale Routing abzufangen, sondern auch eine tatsächliche Steigerung der Datenübertragungsraten zu erzielen.

Unter wirtschaftlichen Gesichtspunkten sind die Abwehr der NSA-Überwachung und der Schutz von Privatheit nicht mehr schützenswerte Güter per se, sondern dienen auch als Instrument, um eine ökonomische Vorherrschaft zu legitimieren. Damit findet eine Unterordnung grundrechtlicher und ethischer Aspekte unter wirtschaftliche Interessen statt.

3.3.6 Verschlüsselung als Alternative?

Verschlüsselung wird besonders als Alternative zum nationalen Routing beworben und sei diesem vorzuziehen.[68] So schreiben Pohlmann u.a.: „Schutzkonzepte sollten […] eher auf den Inhalt der Kommunika-

Vergaberichtlinien, um Unternehmen von öffentlichen Aufträgen auszuschließen, die Daten an ausländische Dienste weitergeben, oder haben derartige Anpassungen bereits vorgenommen. Auch auf Bundesebene ist seit April 2014 eine entsprechende „No-Spy-Klausel“ in Kraft (BT-Drs. 18/3337; tagesschau.de 2014b).

[68] Siehe beispielhaft Hange, zit. in: Diersch 2014: 72.

tion als auf die Transportweginfrastruktur abstellen. Sofern es gelingt, den Informationsgehalt von Daten vor Dritten zu verbergen, wird die Fähigkeit zum Abhören und Mitschneiden nahezu wertlos." (Pohlmann/Siromaschenko/Sparenberg 2014: 114). Dem gegenüber stehen Erkenntnisse über die Fähigkeiten von Geheimdiensten, Verschlüsselungen zu brechen oder mittels Hintertüren oder Generalschlüsseln zu umgehen. So verfügten die NSA und ihre Partnerdienste „allein in 2013 über insgesamt mindestens 12 Mrd. US-Dollar für die Datensammlung, -analyse sowie das Brechen von Chiffren und Sicherheitsvorkehrungen" sowie „Tausende von Entwicklern und IT-Spezialisten sowie spezielle Zugangsmöglichkeiten zu Unternehmensinterna" (Ruhmann 2014: 42). Ruhmann bezeichnet die NSA deshalb als die „am besten ausgestattete Hackerorganisation der Welt" (Ruhmann 2014: 42). Diese besitzt überdies Zugang zu einigen der weltweit bedeutendsten, nämlich der in den USA ansässigen IT-Unternehmen und hat bei diesen in der Vergangenheit die Herausgabe von Schlüsseln und das Einbauen von Hintertüren und Schwachstellen erreicht (Ruhmann 2014: 42).[69] Um diesen Vorteil nicht zu gefährden, haben die USA sich in der Vergangenheit gegen die Entwicklung von Verschlüsselungsmethoden ohne Generalschlüssel gestemmt (Ruhmann 2014: 45).[70] Ferner wurden wohl auch gezielt Sicherheitslücken ausgenutzt (Stichwort „Heartbleed") (zeit.de 2014a).[71] Gerade hierin spiegelt sich das permanente Wettrüsten zwischen der Welt der Geheimdienste und der Welt der Kryptotechnik, die in einem ständigen Wettkampf versuchen, dem jeweils anderen einen Schritt voraus zu sein. Jedoch ist fraglich, ob und wenn ja für wie lange aktuell verbreitete Verschlüsselungsmethoden für bestimmte Geheimdienste eine signifikante Hürde darstellen. Es sei derzeit „schwer,

[69] Vgl. Greenwald 2014: 169 ff. Nach den antisemitischen Anschlägen in Frankreich im Januar 2015 drohte der britische Premierminister Cameron etwa mit dem Verbot von verschlüsselten Messagingdiensten, solange diese keine Hintertüren für Sicherheitsbehörden enthalten (Cameron, zit. in: Tamblyn 2015). Ähnlich äußerte sich auch de Maizière (zit. in: heise.de 2015).

[70] Vgl. die sog. „Kryptodebatte" der 90er Jahre.

[71] Allgemein zum Heartbleed-Bug: Ries 2014: 16 f. Zur Ausnutzung von Schwachstellen im Sicherheitsmodell von Facebook siehe Greenwald 2014: 232 f.

angemessene Aussagen zum realen Sicherheitsniveau speziell von Kryptosystemen zu treffen“ (Ruhmann 2014: 44). So schreibt denn auch Schaar: „So wichtig und richtig derartige Schutzmaßnahmen sind, so sehr werden solche Bemühungen relativiert, wenn man Meldungen Glauben schenkt, nach denen auch Verschlüsselungstechniken für US-amerikanische und britische Geheimdienste keine Hürde darstellen. Auch deshalb sind Ratschläge skeptisch zu betrachten, die die Verantwortung für sichere Kommunikation vor allem den einzelnen Nutzern zuweisen.“ (Schaar 2013a: 216). Zudem bleibt die Problematik, dass, solange nur einzelne Personen oder Bevölkerungsteile Verschlüsselungstechnik nutzen, sich diese in den Augen der Geheimdienste verdächtig machen könnten (Schaar 2013a: 216).[72] Dieses Stigma würde erst dann gänzlich verschwinden, wenn die Mehrzahl der Nutzer verschlüsselt.

Zudem ist zu beachten, dass auch bereits eine Auswertung lediglich etwa des E-Mail-Headers signifikante Erkenntnisse bezüglich Kommunikationsgewohnheiten und sozialer Netzwerke liefern kann.[73] Diese Header-Informationen (From, To, Cc, Betreff und Zeitstempel) können aus Gründen der Funktionalität nicht verschlüsselt werden.[74] Grundsätzlich sind alle bei der Internetnutzung anfallenden Metadaten geeignet, durch ihre Auswertung Aufschlüsse über Nutzer und ihr Verhalten zu ermöglichen. Vor diesem Hintergrund ist die Aussage, durch Verschlüsselung von Inhalten werde „die Fähigkeit zum Abhö-

[72] Siehe auch tagesschau.de 2014. Nach Recherchen von NDR und WDR registriert die NSA bereits die Suchanfragen nach Verschlüsselungssoftware und Anonymisierungsdiensten wie dem Tor-Netzwerk und markiert entsprechende IP-Adressen. Betreiber und Nutzer solcher Infrastruktur werden als „Extremisten“ gekennzeichnet.

[73] Siehe hierzu beispielhaft das am MIT Media Lab entwickelte Analyseprogramm „Immersion“: https://immersion.media.mit.edu/. Zur Aussagekraft von Metadaten siehe auch Greenwald 2014: 191 ff. Diese seien überdies bei Sprachkommunikation wesentlich leichter automatisiert auswertbar als Kommunikationsinhalte.

[74] Die Entwicklung eines neuen Mail-Systems namens Dark Internet Mail Environment könnte diesen Zustand jedoch beenden (Kleinz/Krempl 2015: 17).

ren und Mitschneiden nahezu wertlos“ (Pohlmann/Siromaschenko/Sparenberg 2014: 114) kritisch zu betrachten.[75]

Dies ist freilich nicht als grundsätzliches Argument gegen Verschlüsselung zu werten. Vielmehr müsste Verschlüsselung weitaus stärker genutzt werden. Laut dem Magazin „iX“ laufen (Stand Dezember 2013) nur 23% der Datenpakete über HTTPS; lediglich 4% aller E-Mails waren verschlüsselt (Pohlmann/Siromaschenko/Sparenberg 2014: 116). Jedoch kann Verschlüsselung umgekehrt auch nicht als Argument gegen nationales Routing dienen. Vielmehr sollten sich beide Maßnahmen ergänzen.

3.3.7 Pflicht zur Implementierung von nationalem Routing?

Fraglich ist, ob nationales Routing im Falle Deutschlands durch staatliche Schutzpflichten geboten sein könnte. Diese könnten sich aus Art. 5 und 10 GG, dem Grundrecht auf informationelle Selbstbestimmung, aber auch aus Art. 12, 14, 87f und 91c GG ergeben (Hoffmann-Riem 2014: 57 f.). Mit Blick auf Art. 87f GG und speziell bezogen auf ein europäisches Routing schreibt Hoffmann-Riem: „Gegebenenfalls muss daher in Wahrnehmung des Gewährleistungsauftrags gesichert werden, dass die in Deutschland tätigen Anbieter eigene, von den globalen Kommunikationsnetzen abgeschottete (etwa kontinentaleuropäische, zum Beispiel auf den Schengenraum bezogene und begrenzte) Telekommunikationsnetze einrichten und den Nutzern als Alternative zur Kommunikation über die globalen Infrastrukturen anbieten.“ (Hoffmann-Riem 2014: 58) Der Handlungsspielraum bei der Wahrnehmung staatlicher Schutzpflichten ist indes denkbar groß.[76] Ein nationales Routing wäre nur dann geboten, wenn andere

[75] Man beachte hier insbesondere die folgenden Aussagen von Baker und Hayden zu Metadaten: „We kill people based on metadata.“ (Hayden, bei einer Debatte an der John Hopkins University 1.4.2014; Hayden, zit. in: Lobo 2014a); „If you have enough metadata, you don’t really need content.“ (Baker, bei einer Diskussion in New York; Hayden/Baker, zit. in: Cole 2014).

[76] „Die Verfassung schreibt den Staatsorganen nicht vor, wie sie die grundrechtliche Sicherheit gewährleisten. Sie gibt dem Gesetzgeber auf, die geeigneten Mittel zu bestimmen. Eine Vielzahl an Möglichkeiten steht bereit. […] Die Gesamtheit der Vorkehrungen (nicht notwendig eine isolierte Maßnahme) muss geeignet sein, dem

Maßnahmen evident unzureichend wären. Das Urteil zur Schleyer-Entführung (BVerfGE 46, 160)[77] illustriert beispielhaft, wie weit der Handlungsspielraum des Staates ist. Eine direkte Anrufung an die Welt des Staates nach Erfüllung der staatlichen Schutzpflicht mit Hilfe eines nationalen Routings findet sich in der Arena nicht.

3.3.8 Inhärente Probleme des Ansatzes

Einen Schutz vor dem Abhören von Internetverkehr ins und aus dem Ausland kann nationales Routing indes naturgemäß nicht bieten und ist auch nicht dessen Ziel. Problematisch ist in diesem Zusammenhang die Frage, wie der Nutzer erkennen soll, ob auch etwa beim Besuch einer vordergründig „deutschen" Webseite oder der Korrespondenz mit einer „deutschen" E-Mail-Adresse trotz einer Implementierung von nationalem Routing nicht doch Daten ins Ausland oder über das Ausland fließen, beispielsweise weil in die Seite Angebote ausländischer Anbieter eingebettet sind. Hierin liegt zugleich ein wesentliches Umsetzungsproblem, dem allenfalls durch eine automatisierte Warnung an den Nutzer, dass seine Daten den deutschen oder europäischen Rechtsraum verlassen, begegnet werden könnte. Doch auch eine solche Warnung würde den Nutzer wohl in aller Regel nicht davon abschrecken, Webseiten zu besuchen und Onlinedienste zu nutzen, bei denen Daten ins Ausland gehen oder über das Ausland

---

jeweiligen Rechtsgut tatsächlichen Schutz zu gewährleisten" (Isensee 1983: 38 ff.). Dem Untermaßverbot folgend, „müssen die Vorkehrungen des Gesetzgebers für einen – unter Berücksichtigung entgegenstehender Rechtsgüter – angemessenen und wirksamen Schutz ausreichend sein und auf sorgfältigen Tatsachenermittlungen und vertretbaren Einschätzungen beruhen" (Sachs, in: Sachs 2014, Art. 1 GG, Rn. 36). Zur Annahme einer Verletzung einer staatlichen Schutzpflicht müssten die getroffenen Maßnahmen allerdings „evident unzulänglich" sein (Hufen 2014, § 8 Rn. 13; vgl. BVerfGE 77, 170 (215)).

[77] Die Kläger in dem Fall hatten gefordert, die Bundesregierung müsse den Forderungen der Entführer nachgeben. Das Gericht entgegnete dem: „Wie die staatlichen Organe ihre Verpflichtung zu einem effektiven Schutz des Lebens erfüllen, ist von ihnen grundsätzlich in eigener Verantwortung zu entscheiden. Sie befinden darüber, welche Schutzmaßnahmen zweckdienlich und geboten sind, um einen wirksamen Lebensschutz zu gewährleisten" (BVerfGE 46, 160 (164)). Eine Ermessensreduktion auf Null liege nicht vor, denn auch in der Weigerung, den Forderungen der Entführer nachzugeben, liege eine Maßnahme zur Erhaltung der Sicherheit, da so zukünftige Entführer entmutigt würden (BVerfGE 46, 160 (164)).

geleitet werden. Denn viele dieser Seiten und Dienste haben eine derartige Popularität erreicht, dass kaum Bereitschaft bestehen wird, auf sie zu verzichten oder auf nationale Angebote umzuschwenken. Zudem werden solche nationalen Angebote häufig gar nicht verfügbar sein, sondern müssten – etwa mittels staatlicher Wirtschaftsförderung – erst etabliert werden.

Diese Problematik ist jedoch typisch für alle Formen der Implementierung neuer Ansätze: Ein genereller Wandel ist nicht ausgeschlossen, setzt aber ein gesteigertes Bewusstsein für die Notwendigkeit einer Veränderung voraus. Die Trägheit einzelner Nutzerinnen und Nutzer schließt einen sukzessiven Wandel nicht grundsätzlich aus.

Problematisch bliebe ferner auch nach der Einrichtung eines nationalen Routings die andauernde Präsenz zahlreicher US-amerikanischer Abhöreinrichtungen in der Bundesrepublik (z.B. der sog. „Dagger-Komplex" nahe dem hessischen Griesheim und diplomatische Vertretungen) und die damit verbundenen mutmaßlichen Möglichkeiten zum Abhören auch von innerdeutschem Datenverkehr,[78] sowie die Fähigkeit, in Deutschland tätige US-amerikanische Firmen zur Herausgabe von Daten zu verpflichten.[79]

Bereits damit steht fest, dass ein nationales oder europäisches Routing nicht die alleinige Antwort auf die Enthüllungen des NSA-Skandals sein kann.[80] Vielmehr kann es sich dabei nur um eine von vielen Maßnahmen[81] handeln, um den Internetverkehr vor Datensammelwut und Spionage zu schützen. Zugleich bleiben gewichtige

---

78 Siehe hierzu Becker u.a. 2014: 18 ff.

79 Siehe hierzu insbesondere das das Urteil des US District Court Southern District of New York v. 25.4.2014 – 13 Mag. 2814 (Nakashima 2014; heise.de 2014a).

80 Vgl. Schaar 2013a: 216: „Auf technischer Ebene gibt es für die unterschiedlichen Nutzungsarten nicht das eine ‚Rundum-Sorglos-Paket' zur Schaffung umfassender Sicherheit." Für eine Übersicht über gesetzliche Initiativen zur Cybersicherheit siehe Klett/Ammann 2014: 93.

81 Für einen Überblick über mögliche Maßnahmen siehe Hansen 2014: 442 ff. Diese werden dort unter den folgenden Überschriften zusammengefasst: Verschlüsselung, Schutz von Verkehrsdaten, Routing, vertrauenswürdige Zertifizierung von IT-Sicherheit und Datenschutz, Einbeziehung der Nutzenden, Ressourcen-Bereitstellung, Schutz der digitalen Menschenrechte.

rechtliche Fragen zur Zulässigkeit und der Ausgestaltung von nationalem Routing ungeklärt.

3.3.9 Exkurs: Nationales Routing im nicht-europäischen Ausland

Die Debatte um ein nationales Routing ist kein spezifisch deutsches Phänomen.[82] Vor allem in Brasilien wird über nationales Routing debattiert. Gleichzeitig wurde die Einrichtung einer direkten Telekommunikations-Kabelverbindung zwischen Brasilien und Europa geplant (Deutsche Wirtschaftsnachrichten 2014). Brasilien war ebenso wie Deutschland besonders von den Enthüllungen Snowdens betroffen: Auch die Kommunikation von Präsidentin Rousseff soll, genau wie die der deutschen Kanzlerin und weiterer Spitzenpolitiker, von der NSA abgehört worden sein. Zudem wurde offenbar der staatliche Ölkonzern Petrobras ausspioniert. Entsprechend heftig fiel die brasilianische Reaktion auf den Abhörskandal aus (Rosenbach/Stark 2014: 163 f.).[83]

Auch in Kanada ist nationales Routing unter den Begriffen der „Network Sovereignty"[84] und des „Boomerang Routing" ein Thema.[85] Zur

---

[82] Auch wenn der Bericht des Europäischen Parlaments zur NSA-Affäre vom 21.2.2014 (A7-0139/2014, 2013/2188(INI)) konstatiert: „Innerhalb der EU wird über Massenüberwachung in uneinheitlicher Weise debattiert. So wird in vielen Mitgliedstaaten kaum öffentlich debattiert, und auch der Umfang der Wahrnehmung des Themas durch die Medien stellt sich unterschiedlich dar. Auf das größte Echo sind dem Anschein nach die Enthüllungen in Deutschland gestoßen, wo die Diskussionen über deren Folgen unter großer Anteilnahme der Öffentlichkeit geführt werden" (54).

[83] Siehe hierzu auch die von Deutschland und Brasilien eingebrachte Resolution gegen Datenspionage (Das Recht auf Privatheit im digitalen Zeitalter, A/C.3/68/L.45/Rev.1, angenommen am 18.12.2013), sowie die brasilianische Marco Civil da Internet, Gesetz Nummer 12965 v. 23. April 2014, veröffentlicht im Gesetzblatt der Föderativen Republik Brasilien vom 24. April 2014 (deutsche Sprachfassung abrufbar unter: http://www.uni-muenster.de/Jura.tkr/oer/files/pdf/MarcoCivilDaInternetDeutscheÜbersetzungITM.pdf).

[84] „network sovereignty – the authoritative quality or process whereby an entity (such as the state) or set of entities distinguishes the boundaries of a network and then exercises a sovereign will or control within those boundaries"; (Obar/Clement 2013: 2). „[…] should a foreign body encroach upon the control of a Canadian telecommunications network and its operation, that action would constitute a violation of Canadian network sovereignty, and potentially threaten Canadian civil liberties." Diese Rechte sind in Section 8 der Canadian Charter of Rights and Freedoms sowie im Telecommunications Act 1993 und im Personal Information Protection and Elec-

Rückerlangung dieser „Netzsouveränität“ wurden von Obar und Clement zwei Ansätze vorgestellt: „1) strengthening and enforcement of Canadian privacy law […], and 2) repatriation of Canadian internet traffic by building more internet exchange points” (Obar/Clement 2013: 3). Als mögliche Maßnahmen unter Punkt 1 gelten eine Stärkung der Stellung des Office of the Privacy Commissioner, Breach Notifications, erweiterte Transparenz und Rechenschaftspflichten (Obar/Clement 2013: 2 f.).

Neben diesen Beispielen von Staaten, die als demokratisch gelten, wird in der Diskussion um nationales Routing häufig auf die als autoritär geltenden Staaten wie China und den Iran verwiesen. Anhand dieser Staaten sollen Möglichkeiten des Missbrauchs von nationalem Routing aufgezeigt werden. Das nationale Routing erleichtere die Kontrolle des Netzverkehrs, etwa in Form des Blockierens ausländischer Webseiten und Dienste. Zwar geht es beim nationalen Routings gerade nicht um das Aussperren von Daten, sondern lediglich darum, dass Daten, die sowohl aus einem bestimmten Rechtsraum stammen als auch an ein Ziel innerhalb dieses Raumes adressiert sind, diesen nicht verlassen sollen; mithin um Abhörsicherheit. Jedoch könne die so geschaffene Infrastruktur grundsätzlich auch zur Kontrolle des Netzverkehrs genutzt werden (Stichwort: Great Firewall of China).

tronic Documents Act normiert.

[85] „[…] one might assume that Canadian-to-Canadian communication remains within national jurisdiction. Contrary to that assumption, the IXmaps research makes visible a widespread phenomenon we call ‘boomerang routing’ whereby Canadian-to-Canadian internet transmissions are routinely routed through the United States. […] As a result, Canadian-to-Canadian internet transmissions that boomerang expose Canadian communications to potential U.S. surveillance activities – a violation of Canadian network sovereignty” (Obar/Clement 2013: 2 f.).

3.4 Recht als Ressource in der Arena

Christian L. Geminn

In der Arena stehen den verschiedenen Vertretern der einzelnen Welten in unterschiedlichem Maße Ressourcen zur Verfügung, um ihre Positionen publik zu machen, wissenschaftlich zu untermauern und auch gegen Widerstände durchzusetzen. Dieser Abschnitt untersucht die Verteilung rechtlicher Ressourcen in der Arena, wobei der Begriff der Ressource weit verstanden werden soll. Neben den rechtlichen Ressourcen, die zur Durchsetzung eines nationalen Routings zur Verfügung stehen, sollen auch jene Ressourcen betrachtet werden, die ein alternatives Vorgehen gegen die Bedrohung der informationellen Selbstbestimmung durch die im Rahmen der NSA-Affäre aufgedeckten Handlungen ausländischer Geheimdienste ermöglichen könnten.

3.4.1 Recht als Ressource

Der Begriff der Ressource ist definiert als der „natürlich vorhandene Bestand von etwas, was für einen bestimmten Zweck […] benötigt wird“ (Duden 2007).

Die „Ressource Recht“ taucht im rechtswissenschaftlichen Diskurs insbesondere dann auf, wenn über den Zugang zu den Gerichten als Kernelement des Rechtsstaats gesprochen wird.[86] Diese Ressource werde durch eine Normenflut (Sendler 1979: 227 ff.; Pfeiffer 1981: 122), eine Überlastung der Gerichte, lange Verfahrensdauer, sinkenden Personalstand und übermäßigen Rechtsmittelgebrauch, aber auch durch die vermehrte Nutzungs- und Konfliktbereitschaft durch den sozial und politisch aufgeklärten und dadurch weniger zur Hinnahme bereiten, sondern vielmehr anspruchsbewussten Bürger verknappt.[87] Gerd Pfeiffer, von 1977 bis 1987 Präsident des Bundesge-

[86] Siehe beispielhaft Hill 1981: 805 ff.

[87] Siehe Pfeiffer 1981: 121 ff.; Der Spiegel 29/1983: 29 f.; Greger 2000: 842; Rauscher, in: Münchener Kommentar zur ZPO 2013: Einleitung Rn. 44 ff.

richtshofs, prägte deshalb bereits 1981 den Begriff von der „knappen Ressource Recht“ (Pfeiffer 1981: 121 ff.).[88] Damit ist ein adäquater Zugriff auf die Ressource Recht nur dann gegeben, wenn die Möglichkeit besteht, einen Rechtsbehelf einzulegen und diese Möglichkeit auch faktisch wahrgenommen werden kann. Zudem muss sich die Verfahrensdauer in einem angemessenen Rahmen bewegen, womit auch eine zeitliche Dimension zu beachten ist. Fehlt eine dieser Komponenten, so ist der demokratische Rechtsstaat gefährdet (Pfeiffer 1981: 123). So verstanden handelt es sich beim Recht im wirtschaftswissenschaftlichen Sinne um ein Allmendegut und ist durch Übernutzung gefährdet (Tragik der Allmende[89]).

Für die Möglichkeit zum Einlegen eines Rechtsbehelfs ist von zentraler Bedeutung, wer die durch das Einlegen des Rechtsbehelfs entstehenden Kosten zu tragen verpflichtet ist. Im Falle der Klageerhebung vor Gericht gilt im deutschen Recht die sogenannte „English Rule“.[90] Nach der „English Rule“ trägt die unterliegende Partei die Kosten des Rechtsstreits (siehe § 91 Abs. 1 S. 1 ZPO, § 154 Abs. 1 VwGO).[91] Damit erhält der Zug vor Gericht eine ökonomische Komponente: Ob sich der Gang vor Gericht lohnt, hängt maßgeblich vom voraussichtlichen Erfolg der Klage, vom Streitwert und von den monetären Ressourcen der klagenden Partei ab. Instrumente wie die Prozesskostenhilfe sollen das Fehlen monetärer Ressourcen kompensieren helfen; Gebührenordnungen ein Ausufern der Kosten verhindern. Klagen Staaten gegen Staaten, kann der monetäre Aspekt vernachlässigt werden: Den Staaten stehen zum Führen von Rechtsstreiten im Grunde unbegrenzte Ressourcen zur Verfügung. Sie verfügen ferner über einen Pool von Rechtsexperten, um die eigene Position zu untermauern. Gleiches darf ab einer entsprechenden Größe auch für Unternehmen

88 „Wir machen da keine gute Figur“ (Der Spiegel 32/1981: 35 ff.).

89 Siehe hierzu Schäfer/Ott 2012: 595 f.

90 In Abgrenzung zur „American Rule“, bei der jede Seite die ihr entstandenen Kosten selbst zu tragen hat.

91 Eine Ausnahme hierzu gibt es vor den Arbeitsgerichten, wo in erster Instanz die Rechtsanwaltskosten unabhängig vom Verfahrensausgang von den Parteien selbst zu tragen sind.

angenommen werden. Demgegenüber benötigt der juristische Laie regelmäßig im Wortsinn „Rechtsbeistand“, um seine Interessen vertreten zu können. Er ist im Zugriff auf die Ressource Recht anderen Akteuren regelmäßig nicht nur aufgrund ökonomischer Faktoren unterlegen, sondern auch durch einen Fachwissensnachteil, der kompensiert werden muss.

Wie die Ressource Recht subjektiv wahrgenommen wird, hängt vom Vertrauen der Bürger in die Rechtsordnung, den ökonomischen Prozessrisiken sowie von der Verstehbarkeit und Akzeptabilität des Rechts ab (Pfeiffer 1981: 123). Auch dies hat potentiell starke Auswirkungen auf die Möglichkeit, aber auch auf die Bereitschaft zur Nutzung der Ressource Recht durch den Bürger.

Bereits eingangs wurde erwähnt, dass der Begriff der Ressource weit verstanden werden soll. Deshalb soll die Ressource Recht inhaltlich nicht auf den Rechtsbehelf begrenzt werden, sondern auch die Möglichkeit der Rechtsetzung berücksichtigen. Recht ist damit eine zentrale Ressource der Welt des Staates und mithin des politischen Systems als Ganzem (Voigt 1989: 115): „Im Mittelpunkt des Systems Politik steht die Produktion und Durchsetzung allgemeinverbindlicher Entscheidungen insbesondere mittels der Ressource Recht: Durch Gesetze und Verordnungen regelt das politische System Beziehungen innerhalb von und zwischen gesellschaftlichen Teilsystemen.“ (Jarren/Röttger 2009: 43). Doch der Zugriff auf die Ressource Recht wird oftmals als ultima ratio begriffen: „Es wird ‚zunächst einmal‘ (was vielfach aber bedeutet: dauerhaft) auf freiwillige Zusagen von Problemverursachern oder vertragsähnliche Vereinbarungen mit Unternehmen oder Wirtschaftsverbänden gesetzt. Ganz scheint es so, als würde zu Beginn des 21. Jahrhunderts die Ressource Recht in der Problembekämpfung künstlich verknappt.“ (Schetsche 2008: 167). Die Gründe dafür werden im Einzelfall ganz unterschiedlicher Natur sein. Mögliche Motivation ist beispielsweise der Wunsch, einer „Gesetzesinflation“ sowohl in Anzahl als auch in Umfang der Gesetze entgegenzuwirken, die zwar nicht zuletzt der zunehmenden technischen, aber auch sozialen Komplexität der Gesellschaft geschuldet ist, je-

doch auch für das Versagen von Recht als Steuerungsmittel verantwortlich gemacht wird (Voigt 1989: 118 f.). Auch Idealvorstellungen von der Rolle des Staates können zu einem restriktiven Zugriff auf die Ressource Recht führen, wenn etwa entsprechende Entscheidungsträger libertären Philosophien anhängen. Umgekehrt können Vorstellungen von einem „starken" Staat zu einer Übernutzung des Rechts führen. Ein weiterer Faktor sind die tatsächlichen Wirkungsgrenzen, denen das Recht unterliegt.

Zu beachten ist, dass die Ressource Recht in der Vergangenheit auch im Rahmen lediglich symbolischer Gesetzgebung fehlgebraucht worden ist. Hier verkommt Rechtsetzung zu einem reinen Tätigkeitsnachweis der legislativen Organe und der politischen Klasse. Diese symbolische Gesetzgebung kann durch ihre Ineffektivität bei gleichzeitiger Vergrößerung der Normenflut bestehende Aversionen gegen das Recht als solches sowohl auf Seiten der steuernden als auch auf Seiten der zu steuernden Personen und Institutionen verstärken und mithin ebenfalls zu einer Verknappung der Ressource Recht beitragen.

Es kann also letztlich in zweierlei Hinsicht zu einer Verknappung der Ressource Recht kommen, nämlich einerseits auf der Ebene des Rechtsbehelfs, andererseits auf der Ebene der Rechtsetzung.

Als dritte Option kann auch bereits der bloße Verweis auf das Recht eine bedeutende Wirkung entfalten. Recht kann also auch vorgelagert mobilisiert werden, etwa als Drohmittel oder als Argumentationshilfe. Damit können möglicherweise Rechtsstreite verhindert werden, beispielsweise indem der Gegner in der Auseinandersetzung von der vermeintlichen Aussichtslosigkeit des Einlegens von Rechtsmitteln überzeugt wird. Gleichermaßen können so Gesetzgebungsverfahren oder Debatten über den rechtlichen Status Quo angestoßen und in eine bestimmte Richtung gelenkt werden. Damit eine solche vorgelagerte Wirkung erzeugt werden kann, muss ein gewisser Einfluss auf entsprechende Entscheidungsträger bestehen oder erfolgreich gene-

riert werden; letzteres kann beispielsweise durch Petitionen oder durch die erfolgreiche Mobilisierung der Massenmedien erfolgen.

Von entscheidender Bedeutung ist damit letztlich die Frage, wer die Ressource Recht überhaupt mobilisieren kann. Dies sind unter Berücksichtigung der vorstehenden Überlegungen zunächst Akteure, die zugleich Betroffene sind, Akteure mit Rechtsetzungsbefugnissen, Akteure, die Einfluss auf die beiden erstgenannten Gruppen von Akteuren ausüben können, sowie die Organe der Rechtspflege. Diese Akteure nehmen schließlich am „Kampf ums Recht" (Voigt 1989: 116) teil.

3.4.2 Rechtliche Ressourcen in der Arena

Von zentraler Bedeutung in der Arena ist die Welt des Staates. Ihre wichtigste rechtliche Ressource ist – wie oben beschrieben – die (durch Verfassungsschranken begrenzte) Befugnis zur Rechtsetzung im Inneren. Diese Möglichkeit hat der Staat beispielsweise mit der Einrichtung der §§ 98 und 99 StGB wahrgenommen, die „landesverräterische" und „geheimdienstliche Agententätigkeit" unter Strafe stellen.

Von der grundsätzlichen Möglichkeit, ein nationales Routing per Gesetz vorzuschreiben, hat die deutsche Regierung indes keinen Gebrauch gemacht (Berke 2014a). Das Bundeswirtschaftsministerium befürwortete stattdessen „freiwillige Angebote". Damit verzichtet die Regierung im konkreten Fall des nationalen Routings auf den Rückgriff auf ihre zentrale Ressource der Rechtsetzungsbefugnis. Ein solches Unterlassen des Rückgriffs auf die Ressource Recht kann auf die anderen Akteure in der Arena Druck erzeugen. Der Verweis des Bundeswirtschaftsministeriums auf die Möglichkeit „freiwilliger Angebote" lässt sich auch als Hinweis lesen, solche Angebote seien politisch erwünscht. Somit ist das erklärte Unterlassen der rechtlichen Regelungssetzung auch als ein Versuch der Neuverteilung politischer, aber auch rechtlicher Verantwortlichkeiten und Risiken innerhalb der Arena zulasten der privatwirtschaftlichen Netzbetreiber zu verstehen.

Zugleich vermeidet der Staat auf diese Weise die Festlegung auf eine bestimmte technologische Ausgestaltung und kann sich selbst auf das Setzen technikneutraler Rahmenbedingungen beschränken.

Dem gegenüber stand die rechtspolitische Forderung der Deutschen Telekom AG nach der Schaffung rechtlicher Vorgaben und Rahmenbedingungen für ein nationales Routing, welche ebenfalls als Nutzung einer rechtlichen Ressource zu verstehen ist. Die von handfesten wirtschaftlichen Interessen motivierte und äußerst medienwirksam vorgetragene Forderung hat einen Diskurs ausgelöst und einen Handlungsdruck auf die Welten des Staates und der Politik ausgeübt, der letztlich jedoch in eine Zurückweisung der Forderung mündete. Dass die Forderung der Telekom überhaupt diese Wirkung hatte, liegt in ihrer großen Marktmacht und in ihrer Geschichte als aus der Privatisierung der Telekommunikationssparte der Deutschen Post heraus entstandenes Unternehmen begründet. Zudem hält die Bundesrepublik Deutschland (zum Teil über die Kreditanstalt für Wiederaufbau) fast ein Drittel der Telekom-Aktien.[92] Hier zeigen sich deutlich Verschränkungen zwischen den Welten und Interessenkreisen. Ein vergleichbarer Zugang zu den Welten des Staates und der Politik dürfte in der untersuchten Arena nicht noch einmal existieren. Auch der Ruf der Telekom nach dem Gesetzgeber war letztlich ein Versuch, Verantwortlichkeiten zu verschieben. Hintergrund ist, dass die Telekom durch eine gesetzliche Anordnung eines nationalen Routing zu hoffen schien, dass Anbieter, die derzeit nicht mit der Telekom peeren, gezwungen werden, dies kostenpflichtig zu tun. Es ging also letztlich um die Erlangung und die rechtliche Absicherung eines Wettbewerbsvorteils. Indes hätte die Forderung auch den von Seiten der Telekom höchst unerwünschten Effekt haben können, dass der Gesetzgeber umgekehrt die Telekom zu kostenfreiem Peering verpflichtet.

Ein Teilaspekt der Rechtsetzungsbefugnis liegt in der Möglichkeit der Aushandlung und Ratifizierung internationaler Abkommen und Ver-

[92] Siehe http://www.telekom.com/aktionaersstruktur.

träge. Hier kann der Staat tatsächliches oder vorgetäuschtes Verhandlungskapital nutzen, um auf für ihn und/oder seine Bürger vorteilhafte Vereinbarungen hinzuwirken. Er ist hierzu auf ein Nachgeben oder Entgegenkommen der anderen Verhandlungspartner angewiesen. Ein Beispiel hierfür ist die Entstehungsgeschichte des Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdaten und deren Übermittlung an das United States Department of Homeland Security (Rats-Dokument 17434/11). Sein Abschluss trotz kritischer Stimmen ist nicht zuletzt der Drohung der US-amerikanischen Behörden geschuldet, Fluggesellschaften, welche die geforderten Daten nicht übermitteln, nicht mehr auf amerikanischen Flughäfen landen zu lassen (Keiler/Kristoferitsch 2006: 487). Das Fluggastdatenabkommen ist mithin ein Beispiel für die Durchsetzung zwischenstaatlicher Maßnahmen zur Erreichung eines innenpolitischen Ziels, nämlich der durch die Datenübermittlung erwarteten Stärkung der inneren Sicherheit. Hierzu wurde Dank einer starken Verhandlungsposition ausreichend Druck aufgebaut, um ein Abkommen zu verwirklichen, dessen Hauptnutznießer sein Initiator ist. Es wurde gefordert, die Bundesregierung müsse in gleicher Weise auf ein No-Spy-Abkommen mit den USA hinarbeiten und hierzu – etwa über die Verhandlungen über ein transatlantisches Freihandelsabkommen zwischen den USA und Europa – Druck auf die Gegenseite aufbauen.[93] Der deutsche Staat hat jedoch bisher erfolglos versucht, diese rechtliche Ressource nutzbar zu machen: Die Verhandlungen über ein No-Spy-Abkommen dürfen als gescheitert gelten. Wäre es zum Abschluss eines solches Abkommens gekommen, bliebe jedoch das Problem einer fehlenden effektiven Nachprüfbarkeit der Einhaltung der Vorgaben des Abkommens.

Eng verbunden mit der Fähigkeit zur Mobilisierung der Ressource Recht ist die Fähigkeit, Rechtsbrüche aufzudecken, denn nur auf ein als solches erkanntes Problem kann mit einer Gegenmaßnahme ge-

[93] Siehe beispielhaft Rolofs 2014: 28.

antwortet werden. An dieser Fähigkeit fehlte es in der NSA-Affäre jedoch augenscheinlich. So war der deutsche Staat – zumindest bezüglich der Ausspähung des Mobiltelefons der Bundeskanzlerin – auf den NSA-Innentäter Edward Snowden angewiesen, um einen Anfangsverdacht zu generieren. Für den einzelnen Bürger fehlte die Möglichkeit zur Aufdeckung hingegen gänzlich.

Fraglich ist, welche Möglichkeiten für den deutschen Staat bestünden, Rechtsschutz gegen die im Rahmen der NSA-Affäre aufgedeckten Handlungen zu erlangen. Die fraglichen Handlungen fanden im Ausland statt oder von Örtlichkeiten auf Bundesgebiet aus, die den deutschen Strafverfolgungsbehörden unzugänglich waren und sind. Zudem ist das fragliche Vorgehen etwa der NSA nach US-amerikanischen Recht bisher nicht gerichtlich beanstandet worden. Damit handelt es sich um eine Auseinandersetzung zwischen Staaten und Rechtsordnungen. Die Möglichkeiten des deutschen Staates, Rechtsschutz zu erlangen, wurden bereits vor dem NSA-Untersuchungsausschuss des Deutschen Bundestags thematisiert. Der als Sachverständiger geladene Rechtsprofessor Douwe Korff räumte einer Staatenklage gegen Großbritannien vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) Chancen ein.[94] Die Ausspähung von Telekommunikation *innerhalb* der Bundesrepublik sei ein unrechtmäßiger Eingriff in das deutsche Hoheitsgebiet. Ferner könne der Europäische Gerichtshof (EuGH) eingeschaltet werden. Demgegenüber wandten die Sachverständigen Stefan Talmon und Helmut Philipp Aust ein, das Völkerrecht verbiete Spionage nur dann, wenn Botschaften oder Militärstandorte für Spionage genutzt würden.[95] Die Möglichkeit der Klageerhebung vor einem europäischen oder internationalen Gericht hat die Bundesregierung nicht genutzt. Die Zurückhaltung bei der Nutzung dieser rechtlichen Ressource lässt sich wohl mit den geringen Erfolgsaussichten und den diplomatischen Folgen ihrer Nutzung, aber auch mit fehlendem politischen

[94] Siehe dessen Sachverständigengutachten: Korff 2014.

[95] Siehe Aust 2014 und Talmon 2014a. Siehe auch Talmon 2014: 783 zum Hoheitsgewalterfordernis der einschlägigen Menschenrechtsverträge.

Willen erklären. Ein weiterer Erklärungsansatz könnte darin liegen, dass die deutschen Dienste selbst ähnliche Mittel wie die gerügten zur Auslandsaufklärung nutzen und vor Klagen geschützt werde sollen.[96] So wurde im Oktober 2015 schließlich bekannt, dass bis Oktober 2013 auch befreundete Staaten durch den BND ausgespäht wurden.[97]

Als rechtliche Ressource kommt möglicherweise auch der zwischen den regierenden Parteien vereinbarte Koalitionsvertrag in Frage, wo es heißt, die Koalitionäre „begrüßen auch Angebote eines nationalen bzw. europäischen Routings" (CDU/CSU/SPD 2013: 103). Bei Koalitionsverträgen handelt es sich jedoch nicht um rechtlich bindende Verträge, sondern lediglich um Absichtserklärungen. Dennoch kann der einmal ausgehandelte Koalitionsvertrag durchaus als politisches Druckmittel zwischen den Koalitionären genutzt werden und auch, um von außen Druck auf die Koalitionäre aufzubauen.

Die Möglichkeit der Aufnahme von Ermittlungen durch den Generalbundesanwalt beim Bundesgerichtshof als oberste Strafverfolgungsbehörde auf dem Gebiet des Staatsschutzes kann ebenfalls als rechtliche Ressource begriffen werden. Der Bundesanwalt entscheidet eigenverantwortlich über die Aufnahme von Ermittlungsverfahren, jedoch kann dieser Schritt auch politische oder diplomatische Folgen nach sich ziehen. Ferner ist zu beachten, dass es sich beim Generalbundesanwalt um einen „politischen Beamten" nach § 54 Abs. 1 Nr. 5 BBG handelt, der sein Handeln an den kriminalpolitischen Zielsetzungen und Ansichten der Bundesregierung ausrichten soll. Für die untersuchte Arena von einigem Gewicht war die Ankündigung des Ge-

[96] Vgl. hierzu Meldungen vom August 2014 zur Aufklärungstätigkeit des BND in der Türkei (Der Spiegel 34/2014: 22 ff.) sowie über Begehrlichkeiten der deutschen Dienste: So arbeite „der BND an einem System, um vor allem soziale Netzwerke künftig in Echtzeit überwachen zu können. Facebook & Co. rücken immer stärker in den Fokus des Bundesamtes für Verfassungsschutz. Auch der will unter dem Titel ‚Erweiterte Fachunterstützung Internet' künftig große Datenmengen aus dem Internet abgreifen und verarbeiten" (Amann u.a. 2014: 25).

[97] Diese Aktivitäten stehen in direktem Widerspruch zum Ausspruch von Kanzlerin Merkel: „Abhören unter Freunden – das geht gar nicht".

neralbundesanwalts vom 4.6.2014 ein „Ermittlungsverfahren gegen unbekannt wegen des Verdachts der geheimdienstlichen Agententätigkeit im Zusammenhang mit der möglichen Ausspähung eines Mobiltelefons der Bundeskanzlerin“ einzuleiten (§ 99 StGB) (Generalbundesanwalt 2014). Von der Möglichkeit des § 153d Abs. 1 StPO, von der Verfolgung von Straftaten abzusehen, „wenn die Durchführung des Verfahrens die Gefahr eines schweren Nachteils für die Bundesrepublik Deutschland herbeiführen würde oder wenn der Verfolgung sonstige überwiegende öffentliche Interessen entgegenstehen“, hat der Generalbundesanwalt keinen Gebrauch gemacht. Die „mögliche massenhafte Erhebung von Telekommunikationsdaten der Bevölkerung in Deutschland durch britische und US-amerikanische Nachrichtendienste“ hat indes mangels hinreichenden Tatverdachts nicht zur Einleitung eines Ermittlungsverfahrens geführt, blieb aber „unter Beobachtung“. Vor der Entscheidung war über die Medien erheblicher Druck auf den Generalbundesanwalt aufgebaut worden. Hier zeigt sich deutlich die Signalwirkung rechtlichen Handelns und wie rechtliches Handeln in die anderen beteiligten Welten hineinstrahlen kann. Im Mai 2015 erklärte Generalbundesanwalt Range schließlich, seine Behörde überprüfe, ob durch Hilfstätigkeiten des BND für die NSA ein Anfangsverdacht für eine Straftat vorliege. Das Ermittlungsverfahren bezüglich des Mobiltelefons der Bundeskanzlerin wurde indes im Juni 2015 mangels gerichtsfester Beweise eingestellt. Im Juli 2015 von der Enthüllungsplattform WikiLeaks veröffentlichte Dokumente führten indes nicht zu einer Wiederaufnahme des Verfahrens.

Für den einzelnen Bürger, aber grundsätzlich auch für kleine und mittelgroße Unternehmen und Verbände, ist die Ressource Recht im Kontext der NSA-Affäre nur schwer erfolgreich zu mobilisieren. Dies demonstriert beispielhaft der Versuch eines Berliner Anwalts, der auch Mandanten im Ausland betreut, gegen die sogenannte „strategische Telekommunikationsüberwachung“ internationaler Telekommunikationsbeziehungen durch den BND auf Grundlage des G10-Gesetzes vorzugehen. Der Kläger hatte das Bundesverwaltungsgericht mittels Feststellungsklage angerufen, weil er der Ansicht war,

durch die Überwachung von E-Mail-Kommunikation mit Auslandsbezug in seinen Rechten aus Art. 10 Abs. 1 GG verletzt worden zu sein.[98] Grundlage waren Berichte (BT-Drs. 17/8639), nach denen der BND im Jahr 2010 entsprechende Telekommunikationsverkehre nach bestimmten Begriffen durchsucht hatte und dabei insgesamt über 37 Millionen „Treffer"[99] erzielte. Dadurch sei die Wahrscheinlichkeit, dass auch die vielfach dem Anwaltsgeheimnis unterliegende Kommunikation des Klägers mit seinen ausländischen Mandanten und Kollegen sowie anderen Personen ins Visier des BND geraten sei, sehr hoch. Nachrichtendienstliche Relevanz hatten von den Treffern aus dem Jahr 2010 lediglich 213,[100] davon waren 12 E-Mails. Damit liege auch ein Verstoß gegen das Übermaßverbot vor.

Das Gericht wies die Feststellungsklage mangels eines konkreten Rechtsverhältnisses im Sinne von § 43 Abs. 1 VwGO als nicht zulässig ab. Die konkrete Betroffenheit des Klägers sei nicht mehr positiv feststellbar, da – mit Ausnahme der nachrichtendienstlich relevanten – die gesammelten Telekommunikationsverkehre inklusive zugehöriger Protokolldaten zwischenzeitlich – den Vorgaben des G10-Gesetzes folgend – gelöscht worden seien. Die verbleibende Wahrscheinlichkeit für die Erfassung der Kommunikation des Klägers sei „nicht so hoch, dass sie als überwiegend eingestuft werden müsste".[101] Dies ergebe sich aus der Beschränkung der Überwachung auf bestimmte, in der Anordnung bezeichnete Übertragungswege und die Beschränkung der Überwachung auf 20 Prozent der Übertragungskapazität.[102]

Der Kläger hatte angeführt, „eine stärkere Substantiierung der eigenen Betroffenheit sei ihm wegen der Heimlichkeit der Maßnahmen

---

98 BVerwG, Urteil vom 28.5.2014 – 6 A 1.13: Rn. 3 f. Siehe zum Urteil auch die Anmerkungen von Gärditz (2014: 998 ff.).

99 Im Vorjahr (2009) hatten sich hingegen weniger als sieben Millionen Telekommunikationsverkehre anhand der verwendeten Suchbegriffe qualifiziert (BT-Drs. 17/4278). Der drastische Anstieg im Jahr 2010 sei durch einen sehr hohen Spam-Anteil in diesem Jahr zu erklären (BVerwG, Urteil vom 28.5.2014 – 6 A 1.13: Rn. 2).

100 2009 waren es 278.

101 BVerwG, Urteil vom 28.5.2014 – 6 A 1.13: Rn. 28.

102 BVerwG, Urteil vom 28.5.2014 – 6 A 1.13: Rn. 29.

nicht möglich und könne deshalb auch nicht verlangt werden".[103] Eine Absenkung des Beweismaßes sei indes nicht geboten, denn das „Vorgehen des Bundesnachrichtendienstes entsprach Vorschriften, die verfassungsrechtlich nicht zu beanstanden sind".[104] Hier verweist das Gericht insbesondere auf die Pflichten zur unverzüglichen Löschung nachrichtendienstlich irrelevanter Kommunikation (§ 6 Abs. 1 S. 2 G10-Gesetz), auf die nach Ansicht des Gerichts „effektive"[105] Kontrolle des BND durch das Kontrollgremium des Bundestags und auf die Notwendigkeit der Verhinderung von Popularklagen nichtbetroffener Dritter.

In einem nächsten Schritt kündigte der Kläger an, das Bundesverfassungsgericht anrufen zu wollen (Gerber 2014: 36). Zur Zulässigkeit einer Verfassungsbeschwerde ist lediglich erforderlich, dass die Möglichkeit besteht, dass der Kläger von der Anwendung der Norm in einer grundrechtlich geschützten Position verletzt sein könnte (Möglichkeitstheorie). Das Bundesverfassungsgericht hat jedoch bereits 1999 in einem Urteil (BVerfGE 100, 313) die strategische Telekommunikationsüberwachung grundsätzlich für verfassungsgemäß erklärt.

Im Gegenzug stellt die Verfassungsbeschwerde vor dem Österreichischen Verfassungsgerichtshof gegen die Vorratsdatenspeicherung, die 2011 in Umsetzung der Richtlinie 2006/24/EG[106] in das österreichische Telekommunikationsgesetz 2003 aufgenommen worden war (§ 102a TKG 2003),[107] ein Beispiel dafür dar, wie Bürger im Kollektiv erfolgreich die Ressource Recht mobilisieren können. Die Gesetzesänderung war von heftigen Protesten begleitet worden: 106.067 Ös-

[103] BVerwG, Urteil vom 28.5.2014 – 6 A 1.13: Rn. 3.

[104] BVerwG, Urteil vom 28.5.2014 – 6 A 1.13: Rn. 34.

[105] BVerwG, Urteil vom 28.5.2014 – 6 A 1.13: Rn. 40 f.

[106] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105, S. 54). Zur Entstehungsgeschichte der Richtlinie siehe Moser-Knierim 2014: 147 ff.

[107] Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG geändert wird (BGBl. I Nr. 27/2011).

terreicher schlossen sich einer Petition gegen die Vorratsdatenspeicherung an;[108] 11.139 registrierten sich neben der Kärntner Landesregierung als Mitkläger der Verfassungsbeschwerde. Maßgeblich orchestriert wurde der Protest vom Verein „Arbeitskreis Vorratsdatenspeicherung Österreich“ (AKVorrat.at). Der Verfassungsgerichtshof rief (neben dem irischen High Court) den EuGH an, der am 8.4.2014 die Richtlinie 2006/24/EG für ungültig, da unvereinbar mit den in der Charta der Grundrechte der Europäischen Union fixierten Grundrechten auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten erklärte.[109] In der Folge kippte der Verfassungsgerichtshof auch die nationale österreichische Umsetzung.[110]

In einer ähnlichen Aktion in Deutschland erhoben infolge eines Aufrufs des deutschen Arbeitskreises Vorratsdatenspeicherung (AK Vorrat) insgesamt 34.443 Bürger[111] eine wortgleiche Verfassungsbeschwerde gegen die bundesdeutsche Umsetzung der Richtlinie 2006/24/EG.[112] Der Beschwerde gab das Bundesverfassungsgericht mit Urteil vom 2.3.2010 statt (BVerfGE 125, 260).[113] Damit war jedoch nur ein Teilerfolg erzielt, denn das Bundesverfassungsgericht erklärte, eine „sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienst“ sei „mit Art. 10 GG nicht schlechthin unvereinbar“ (BVerfGE 125, 260 (316)), sondern lediglich in der vom Gesetzgeber in Gesetzesform gegossenen Ausgestaltungsvariante unzulässig. Zudem blieb die Verpflichtung des deutschen Gesetzgebers zur Umsetzung der Richtlinie 2006/24/EG. Vor einer Neufassung wollten die jeweili-

[108] Siehe http://www.akvorrat.at/zeichnemit-100k.

[109] EuGH, Urteil v. 8. April 2014 in den verbundenen Rechtssachen C-293/12 und C-594/12.

[110] Österreichischer Verfassungsgerichtshof, Entscheidung G 47/2012 u.a. v. 27. Juni 2014.

[111] Siehe Krempl 2008.

[112] Siehe hierzu detailliert Hornung 2012: 384 ff. Besonders öffentlichkeits- und medienwirksam dürften die vom AK Vorrat organisierten Demonstrationen und die Übergabe von über hundert Aktenordnern mit anwaltlichen Vollmachten an das Bundesverfassungsgericht gewesen sein.

[113] Siehe zum Urteil auch Moser-Knierim 2014: 155 ff.

gen Regierungen, die grundsätzlich am Ziel der Einführung einer Vorratsdatenspeicherung festhielten,[114] aber die oben angesprochene Entscheidung des EuGH abwarten,[115] der letztlich die Richtlinie für ungültig erklärte. Im Mai 2015 wurde schließlich ein Referentenentwurf des Bundesjustizministeriums publik, mit dem ein neuer Anlauf zur Etablierung einer Vorratsdatenspeicherung unternommen wurde.[116] Das auf dem Entwurf basierende Gesetz ist schließlich am 18.12.2015 in Kraft getreten. Auch gegen das neue Gesetz wurden umgehend Klagen angekündigt.

Der Fall der Vorratsdatenspeicherung zeigt trotz ihres Wiederauflebens, dass Bürger durch Zusammenschluss die Kraft zur Mobilisierung der Ressource Recht unter Umständen erheblich steigern können.[117] Um einen solchen Zusammenschluss zu realisieren, können sie sich in Vereinen, Interessengemeinschaften und sonstigen, möglicherweise nur losen Organisationen zusammenschließen. Insbesondere Social Media erlauben dabei auch den spontanen Zusammenschluss ohne einen festen Organisationsrahmen. Bürger können sich direkt einer Organisation anschließen oder sich beispielsweise durch Spenden, das Leisten von Unterschriften, das Werben für bestimmte Anliegen oder die Übernahme kleinerer Hilfstätigkeiten mit einer Organisation oder ganz abstrakt einem Anliegen assoziieren. Durch den Zusammenschluss werden finanzielle Mittel gebündelt.

---

[114] Siehe für die seit Ende 2013 regierende schwarz-rote Koalition: CDU/CSU/SPD 2013: 102 f.

[115] Die blockierende bzw. abwartende Haltung insbesondere der Justizminister Leutheusser-Schnarrenberger und Maas wurde von den Unterstützern der Einführung einer Vorratsdatenspeicherung heftig kritisiert. Siehe beispielhaft: Der Spiegel 3/2014: 15; Der Spiegel 2/2014: 30 f.; Der Spiegel 51/2013: 17; Der Spiegel 21/2012: 15.

[116] Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 15.5.2015)

[117] Ein weiteres Beispiel ist die Rechtssache C-362/14 vor dem EuGH (Urteil v. 6. Oktober 2015). Hier stand mit dem Österreicher und Juristen Maximilian Schrems zwar eine Einzelperson im Mittelpunkt der medialen Aufmerksamkeit („Schrems vs. Facebook"), hinter Schrems stand jedoch unter anderem der von ihm gegründete Verein „europe-v-facebook.org", der zu unterstützenden Spenden aufrief. Über den Verein konnten Spenden in Höhe von knapp 70.000€ gesammelt werden (Stand Dezember 2015).

Gleiches gilt für juristischen Sachverstand, der entweder durch Mitglieder und Unterstützer repräsentiert wird oder durch die akkumulierten Finanzmittel „zugekauft" werden kann. Die Vorratsdatenspeicherung hat indes grundsätzlich das Potential, zum Modell auch für die NSA-Affäre zu werden.[118] Zwar ist jede Bündelung unterschiedlichster Individuen mit ganz individuellen Eigeninteressen mit Schwierigkeiten verbunden, jedoch bietet der erfolgreiche Zusammenschluss die Chance zur Steigerung der Mobilisierbarkeit der Ressource Recht. Gleichzeitig hilft der Zusammenschluss beim Aufbauen von politischem Druck im Sinne einer vorgelagerten Mobilisierung von Recht.

Zu beachten ist jedoch, dass bei der Klage gegen die Vorratsdatenspeicherung ein konkretes Gesetz angegriffen werden konnte, während es im Falle der NSA-Affäre sowohl an einem greifbaren Klagegegner als auch wegen Problemen bezüglich der Feststellbarkeit der konkreten Betroffenheit einer bestimmten Person an einem echten Angriffspunkt, mithin insgesamt an effektivem Rechtsschutz fehlt. Die Aktivitäten ausländischer Geheimdienste sind ferner im Regelfall durch nationales Recht im Heimatstaat gedeckt und auf internationaler Ebene existieren nur wenige und regelmäßig zahnlose Vereinbarungen zur Regulierung bestimmter Spionagetätigkeiten.[119] Talmon nennt als grundsätzliche Möglichkeiten eines individuellen Rechtsschutzes im Falle der NSA-Affäre die Individualbeschwerde vor dem

[118] So identifiziert Hornung die folgenden Faktoren als entscheidend für die Mobilisierungswirkung der Vorratsdatenspeicherung: „Mutmaßlich spielte die Ubiquität und Anlasslosigkeit der Vorratsdatenspeicherung eine Rolle [...] Der Grundrechtseingriff wird als maßlos und nicht in demokratisch legitimierter Weise begründet empfunden. Er hat Infrastrukturcharakter und eröffnet deshalb auch bei normkonformem Verhalten keine Möglichkeiten, sich der Kontrolle zu entziehen. Überdies kann er leicht auf andere Zwecke wie die Bekämpfung von Urheberrechtsverletzungen ausgedehnt werden. Schließlich trifft die Maßnahme die sogenannten ‚digital Natives' ins Mark, in deren Lebenswirklichkeit die neuen Kommunikationsformen des Internets eine viel größere Rolle spielen als für die maßgeblichen Politiker" (Hornung 2012: 385). Diese Faktoren lassen sich analog auch auf die durch die NSA-Affäre aufgedeckten Praktiken übertragen.

[119] Beispielsweise Art. 41 des Wiener Übereinkommens v. 18. April 1961 über diplomatische Beziehungen, der den Missbrauch von Botschaften zu Zwecken der Spionage verbietet.

Europäischen Menschenrechtsgerichtshof (nur gegen Vertragsparteien der EMRK wie das Vereinigte Königreich möglich; immerhin mit reduzierten Anforderungen für die positive Feststellung der Betroffenheit), die Individualbeschwerde vor dem Menschenrechtsausschuss der Vereinten Nationen nach Art. 2 des Fakultativprotokolls zum IPbpR (dem jedoch weder die USA noch das Vereinigte Königreich beigetreten sind) und die Individualbeschwerde vor der Interamerikanischen Menschenrechtskommission nach Art. 44 der Amerikanischen Menschenrechtskonvention (die jedoch nur unverbindliche Empfehlungen beschließen kann) (Talmon 2014a: 35 ff.). Die Möglichkeit einer gegen das Vereinigte Königreich gerichteten Beschwerde vor dem EGMR wurde indes bereits wahrgenommen.[120] Erwähnung finden muss zudem eine – schlussendlich abgewiesene – Beschwerde mehrerer Menschenrechtsgruppen[121] vor dem britischen Investigatory Powers Tribunal, an welches unter dem Regulation of Inverstigatory Powers Act 2000 (c. 23) Beschwerden gegen Überwachungsmaßnahmen auf Grundlage dieses Gesetzes gerichtet werden können.[122] Diese Gruppen legten schließlich im April 2015 ebenfalls Beschwerde beim EGMR ein. Die Arbeitspraxis des britischen Geheimdienstes GCHQ verletze Art. 8, 10 und 14 EMRK. Zudem habe das Verfahren vor dem Investigatory Powers Tribunal gegen Art. 6 EMRK verstoßen.

[120] Big Brother Watch and Others v. UK, Application no. 58170/13. Die Beschwerde wurde eingereicht von den Organisationen Big Brother Watch, English PEN und Open Rights Group sowie von CCC-Sprecherin Constanze Kurz.

[121] Liberty, Privacy International, Amnesty International, ACLU u.a.

[122] Liberty and Others v GCHQ and Others, Case No. IPT/13/77/H, IPT/13/168-173/H. Das Tribunal stellte zwar fest, dass in der Vergangenheit gegen europäische Grundrechte verstoßen worden sei. Jedoch sei die aktuelle Praxis nicht zu beanstanden.

3.5 Privatheit in den Diskursen der Arena

Simon Ledder, Fabian Pittroff

In allen sozialen Welten wird diskursiv auf Privatheit Bezug genommen. Dies zeigt sich an zahlreichen Äußerungen zu Themen wie Datenschutz, Datensicherheit, informationelle Selbstbestimmung, Persönlichkeitsrecht und Privatsphäre. Teilweise werden diese Begriffe nahezu synonym verwendet, obwohl sehr verschiedene Aspekte thematisiert werden.[123] Für genauere Beschreibungen können die in der Arena vorgefundenen sozialen Welten (vgl. Kapitel 3.2) unterschieden werden.

3.5.1 Welt des Staates

Privatsphäre wird in der sozialen Welt des Staates immer wieder als Argument verwendet. Sie wird beständig in den Aussagen aller Parteien betont. Im Fokus des Diskurses steht dabei jeweils die informationelle Selbstbestimmung,[124] die aus ethischer Perspektive als eine Ausprägung informationeller Privatheit verstanden werden kann. Es mangelt jedoch meist an konkreten Ausgestaltungen des Begriffs. Eine Ausformulierung der ethischen Bedeutung findet im Diskurs eher selten statt; teils finden sich jedoch Rückgriffe auf das Prinzip der Menschenwürde: „Zur Würde des Menschen gehört vor allem sein Selbstbestimmungsrecht auch und gerade über seine persönlichen Daten“ (Gabriel 2014).[125] Damit zusammenhängend wird auf die

[123] Dieser durchmischte Gebrauch von analytisch klar zu trennenden Begriffen (Steeves 2009) ist aber in den untersuchten Diskursen nicht verwunderlich, da hierbei Stellungnahmen, Vorträge und Interviews zugrunde lagen, in denen nicht immer mit der gebotenen Schärfe argumentiert werden kann oder soll.

[124] Zumindest impliziter Bezugspunkt für die Welt des Staates und des Rechts ist das sogenannte Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 (BVerfGE 65, 1). Hier legte das BVerfG das Recht auf informationelle Selbstbestimmung als eine Ausprägung von Menschenwürde und dem allgemeinen Persönlichkeitsrecht aus.

[125] Im Folgenden werden nur einzelne Sätze als Beispiele zitiert. Entsprechende Äußerungen finden sich im Untersuchungsmaterial zuhauf; die zitierten Sätze sind

freie Entfaltung der Persönlichkeit verwiesen: „Dem Einzelnen steht ein Recht auf informationelle Selbstbestimmung zu, damit er seine Persönlichkeit frei entfalten kann. Diese Prinzipien haben nach wie vor ihre Berechtigung." (Schaar 2014) In dieser Argumentation wird Privatheit als Teilaspekt von Menschenwürde verstanden. Die Menschenwürde gilt als unhintergehbarer Wert; ein rhetorischer Anschluss von Privatheit an Menschenwürde macht eine Infragestellung von Privatheit unmöglich. Privatheit wird als Wert an sich verstanden, den es zu verteidigen gilt. In der sozialen Welt des Staates sind solche Argumentationslinien eher selten. Versucht wird eher, Privatsphäre als Grundpfeiler demokratischer Ordnung zu legitimieren. Sofern die Gefahr bestehe, dass Aussagen, die im Privaten getroffen werden, abgehört werden, könne eine „Schere im Kopf" (Maas 2014) entstehen. „Wer keine Privatsphäre hat, hat weniger Freiheit" (ebd.). Dies verhindere die Partizipation der Bevölkerung an der Politik, weswegen Privatsphäre als notwendiger Bestandteil demokratischer Ordnung verstanden wird: „Unsere freiheitliche Demokratie braucht die Mitwirkung der Bürgerinnen und Bürger so sehr wie der Mensch die Luft zum Atmen" (ebd.). Privatheit gilt hier als Wert, der grundlegend für das Funktionieren von Demokratie ist. Damit wird an demokratietheoretische Überlegungen angeknüpft, in der Öffentlichkeit und Privatheit als notwendige dichotome Sphären gelten (vgl. Habermas 1990, Geuss 2002; kritisch dazu: Holland-Cunz 1998). In beiden Positionen wird auf ethische Prinzipien verweisen, die Privatheit einen hohen Stellenwert zuweisen.

In den Positionen der Repräsentanten der Welt des Staates wird informationelle Selbstbestimmung als Kernelement von Privatheit formuliert. Die informationelle Selbstbestimmung manifestiert sich entsprechend vor allem im Datenschutz, dessen Stellenwert beständig beschworen wird: „Datenschutz und Datensicherheit haben eine ganz

exemplarisch für diskursive Aussagen aus einer bestimmten Position heraus. Es sei an dieser Stelle zudem darauf hingewiesen, dass der Verweis auf einzelne Personen nicht darauf zielt, hier gezielt Individuen als Verantwortungsträger herauszustellen, sondern sie als Repräsentanten bestimmter diskursiver Positionen zu begreifen, die miteinander in Konflikt stehen (vgl. Link 2005).

neue Bedeutung bekommen“, so Thomas de Maizière (2014a). Es bleibt zwar vage, wie informationelle Selbstbestimmung konkret ausgestaltet werden soll; Verletzungen derselben scheinen dagegen leicht identifizierbar. Dazu gehöre etwa das Verhalten von Geheimdiensten, die „millionenfach elektronische Daten abgreifen“, „Kriminelle […, die] fremde Identitäten missbrauchen“ sowie der Fall, „wenn unsere Daten zur Ware werden“, da „Unternehmer die Daten ihrer Nutzer ungefragt ausbeuten“ (Maas, ebd.). Anstelle einer positiven Bestimmung von Privatsphäre wird vielmehr formuliert, wo und wann Eingriffe festzustellen sind.

Andere Argumentationslinien verweisen auf die Bedeutung von Sicherheit, sobald es um das Thema Privatheit geht. Eine der ersten Reaktionen auf die Enthüllungen Snowdens lieferte Stephan Mayer, der innenpolitische Sprecher der CSU-Landesgruppe im Bundestag: „Es steht fest, dass Hinweise von US-amerikanischen Geheimdiensten dazu beigetragen haben, Terroranschläge in Deutschland rechtzeitig zu verhindern.“ (Schuler/Solms-Laubach 2013) Innerhalb solcher Argumentationsmuster werden Mittel über zu erreichende Ziele gerechtfertigt. Ob andere Werte auf diesem Weg verletzt werden, darf in dieser Logik ignoriert werden. Aus eben dieser Perspektive erklärte der damalige Bundesinnenminister Friedrich nach den ersten Veröffentlichungen der NSA-Aktivitäten: „Sicherheit ist ein Supergrundrecht“ (Friedrich, zit. in: Bewarder/Jungholt 2013). Hier wird ein Grundrecht über die anderen Grundrechte gestellt. Friedrich verlangt, die bisherige politische und juristische Gleichwertigkeit aller Verfassungsrechte aufzugeben, und stellt stattdessen Sicherheit als zentrale Aufgabe der Verfassung dar.[126] Solche Argumentationsmuster, die konsequentialistisch Mittel durch Ziele rechtfertigen, sind fester Ausgangspunkt für viele Rechtfertigungen in der sozialen Welt des Staates. So versuchte Friedrich nach Gesprächen mit der US-Regierung

[126] In der Reflexion muss zwischen Grundrechten und Grundwerten unterschieden werden. Die Grundrechte werden von Grundwerten abgeleitet. Die Ausgestaltung der Grundrechte orientiert sich an den Grundwerten und darf diese nicht verletzen, sondern muss diese schützen. Entsprechend sind die Grundrechte vorrangig als Abwehrrechte des Individuums gegenüber dem Staat konzipiert.

beschwichtigend zu wirken: „Alle Verdächtigungen, die erhoben wurden, sind ausgeräumt. Fest steht: Es gab keine ‚massenhaften Grundrechtsverletzungen' amerikanischer Geheimdienste auf deutschem Boden, wie behauptet wurde" (Friedrich, zit. in: Bröcker 2013). Diese Anerkennung weiterer Werte neben der Sicherheit verbirgt nicht die generell nutzen-fokussierende Perspektive. So rechtfertigt Friedrich auch die Zusammenarbeit zwischen deutschen und US-Geheimdiensten mit einer Bedrohungslage: „Das geschieht zum Schutz unserer Soldaten in Afghanistan und zum Schutz der Bürger vor Terrorangriffen. Die Gefährdungslage ist ja nicht kleiner geworden, sondern eher größer" (Friedrich, zit. in: Bröcker 2013). Schließlich verwies er auf 45 vereitelte Terroranschläge – eine Zahl, die aufgrund von Kritik schließlich auf sieben reduziert werden musste.

Auch Angela Merkel selbst verknüpft Fragen bezüglich des Abhörens von Daten kontinuierlich mit der Notwendigkeit von Terrorbekämpfung: „Welche Daten der Bürgerinnen und Bürger werden abgegriffen, zur Terrorismusbekämpfung zum Beispiel? Hier müssen wir die Verhältnismäßigkeit wahren: zwischen der Freiheit der Information, der Freiheit des Bürgers und der Sicherheit des Bürgers" (Merkel 2014b). Und an anderer Stelle: „Deshalb brauchen wir eine umfassende Debatte über das Verhältnis von Freiheit und Sicherheit, die immer in einem gewissen Konflikt zueinander stehen, aber immer wieder in eine Balance gebracht werden müssen" (Merkel 2014). Ähnlich argumentiert Thomas de Maizière, sowohl Vorgänger als auch Nachfolger Friedrichs im Amt des Innenministers. So stellt de Maizière die Geheimdienstaktivitäten als die ehrenwerteren Eingriffe in die Privatheit dar: „Ich finde, ein womöglich übertriebenes Abgreifen von Informationen mit dem Motiv der Terrorbekämpfung ist weniger zu verurteilen als mit dem Ziel der privaten Gewinnmaximierung" (de Maizière, zit. in: Hoppe/Jakobs/Sigmund 2014). Auch wenn in dieser politischen Aussage zwar von einer Intentionalität gesprochen wird, steht das zu erreichende Ziel im Mittelpunkt. Insbesondere die Formulierung „womöglich übertriebenes Abgreifen" suggeriert die Zuläs-

sigkeit sehr fragwürdiger Handlungen, da diese durch die zu erreichenden Folgen legitimiert werden können.

Eine kurzzeitige Verschiebung der Argumentation war bemerkbar, als im Oktober 2013 bekannt wurde, dass die NSA Merkels Handy abhörte. Dies kommentierte die Bundeskanzlerin in einer Pressekonferenz mit den Worten: „Ausspähen unter Freunden – das geht gar nicht. […] Wir brauchen Vertrauen unter Verbündeten und Partnern, und dieses Vertrauen muss jetzt wieder hergestellt werden" (Merkel 2013). Hier wurde die Achtung von Privatheit als Basis eines Vertrauensverhältnisses präsent. Der Begriff des Vertrauens hat seit diesem „Handygate" (Birnbaum et al. 2013) im Diskurs erheblich an Bedeutung gewonnen (vgl. Kapitel 4.3).[127]

Grundsätzlich wird Privatheit in den Aussagen der Bundeskanzlerin und der beiden Innenminister als Freiheitsrecht verstanden, das geschützt werden muss, aber auch Unsicherheiten in sich birgt. Sicherheit steht dem Wert der Privatheit mindestens gleichberechtigt gegenüber. Hier wird das Private nicht näher bestimmt, sondern als Gegenteil von Sicherheit postuliert. Informationelle Selbstbestimmung wird dabei gegenüber einer herzustellenden Sicherheit abgewogen und häufig auch abgewertet. Die Anrufung einer solchen Balance steuert den Diskurs bereits in eine entsprechende Richtung, die Freiheit und Sicherheit als Einsätze in einem Nullsummenspiel darstellt. Damit wird eine Änderung der bisherigen Rechtsprechung forciert. So muss zum einen der Staat die Sicherheit aller Rechte gewährleisten, daher gibt es in der bisherigen Rechtsprechung Sicherheit nicht als eigenen Wert. Zum anderen gerät schnell aus dem Blick, dass Sicherheit bisher nur ein abgeleiteter Wert ist. In der bisherigen Auslegung der Verfassung ging es stets darum, Sicherheit für etwas anderes, konkretisiertes herzustellen. Sofern Sicherheit als allgemeingültiges Ziel anerkannt und von einem zu erreichen Ziel gelöst wird, wird es schließlich zu einem Selbstzweck (Bielefeldt 2004: 13-15). Der staatlichen Kraft ist es in dieser Abwägung von Freiheit und

[127] Ich danke Jutta Krautter für diese Feststellung.

Sicherheit schlussendlich nur möglich, auf Unsicherheiten durch verstärkte Restriktionen gegenüber der Zivilgesellschaft zu reagieren. In diesem Vorgang wird Sicherheit schnell zu einem Schlagwort, das andere Formen politischen Handelns verunmöglicht (Neocleous 2007). Dabei muss Privatheit auch nicht näher bestimmt werden, wie sich etwa in der Digitalen Agenda zeigt.

In der Welt des Staates dient Privatheit vornehmlich als rhetorische Figur, um andere politische Entscheidungen zu erleichtern. Zum einen geht es darum, die Außenpolitik in neue Wege zu lenken, zum anderen wird eine stärkere Förderung von IT-Technologien gefordert. So benennt Gabriel „Datenschutz als Wettbewerbsvorteil" (Gabriel 2013) und der Bundesverkehrsminister Alexander Dobrindt erklärt: „Das Sicherheitsthema ist im Innenministerium angesiedelt, aber Rechtsfragen alleine reichen auch da nicht mehr aus. Wir brauchen Technologieführerschaft, um bei Sicherheitsfragen überhaupt mitgestalten zu können" (Dobrindt, zit. in: Gaugele/Kade/Malzahn/Vitzthum 2014). Heiko Maas pflichtet ihm bei: „Mit der Digitalen Agenda begleiten wir unsere klassische deutsche Industrie durch die Digitalisierung. […] Unsere Unternehmen aus dem Automobilbau, dem Anlagen- oder Maschinenbau müssen bei der digitalen Transformation dabei sein. Sonst werden sie transformiert." (Maas 2014) Und schließlich erklärt de Maizière: „Mit dem IT-Sicherheitsgesetz wollen wir international Vorreiter und Vorbild für die Entwicklung in anderen Ländern sein und so nicht zuletzt auch die deutschen IT-Sicherheitsunternehmen stärken und ihnen verbesserte Exportchancen eröffnen" (de Maizière 2014). Eine Angst vor dem Verlust von Privatsphäre wird hier als Vehikel verwendet, um die Förderung der deutschen IT-Unternehmen zu stärken. Der Begriff der Sicherheit ist insofern eng verknüpft mit ökonomischem Wettbewerb: Sicherheit von Daten dient vornehmlich dazu, sich als wirtschaftlicher Akteur auf internationaler Ebene behaupten zu können. Hier steht weniger der Schutz der eigenen Bevölkerung vor dem Zugriff fremder Mächte im Vordergrund als vielmehr die Qualität des wirtschaftlichen Standortvorteils. Auch hier ist Privatheit kein Zweck an sich, sondern Mittel für andere Ziele.

3.5.2 Welt der Rechtsanwendung

In der Welt der Rechtsanwendung wird versucht, das Niveau der rechtlichen Regulierungsdichte den technologischen Entwicklungen anzupassen. Dies hat vor allem Kritik am herrschenden Umgang mit Begriffen wie Privatsphäre und Datenschutz zur Folge, da sich in unterschiedlichen Staaten bis zum Beschluss der europäischen Datenschutzgrundverordnung sehr unterschiedliche Gesetze finden. Das bislang noch „uneinheitliche Datenschutzrecht in Europa" (Reda 2014) wird als Problem genannt. Ziel hier sei die Homogenisierung des Rechts, das für jeden Staat – in der EU oder in Europa – eindeutige Grenzen des Erlaubten festlegt. Als grundlegend für die veränderten Verhältnisse werden Informations- und Kommunikationstechnologien und eine damit einhergehende „globale Realität" (Hoffmann-Riem 2014b) verstanden.[128] Das deutsche Datenschutzrecht wird in der Debatte immer wieder als besonders rigide gelobt. So sei zwar eine Homogenisierung angestrebt, dies sei aber problematisch, „weil manche Länder einen geringeren Datenschutz haben als Deutschland. Und wir wollen nicht, dass unser Datenschutz aufgeweicht wird" (Merkel 2014a). Zudem wird beständig auf unterschiedliche Vorstellungen über Privatheit zwischen Deutschland und den USA hingewiesen. Dies sei gar ein „Kampf der Kulturen", wie dies die beiden Juristen Russell Miller und Ralf Poscher (2013) in Anlehnung an Samuel Huntington formulieren.

Juristinnen innerhalb der Welt des Rechts argumentieren vorrangig deontologisch für Privatheit als Wert an sich. Ebenso wie Menschenwürde als absoluter Wert an sich gilt, kommt auch Privatheit als notwendiger Aspekt der Menschenwürde Wertigkeit zu. So formuliert Hans-Jürgen Papier, ehemaliger Präsident des Bundesverfassungsgerichts: „Dieser Menschenwürdegehalt des Grundrechts führt zu ei-

[128] In der untersuchten Arena wird jedoch nicht mehr behauptet, das Internet sei ein „rechtsfreier Raum", wie dies zuvor in netzpolitischen Auseinandersetzungen von einigen Akteuren regelmäßig gepflegt wurde (Möller 2012). Anscheinend zeigt diese Aussage im Diskurs keine Wirkmächtigkeit mehr und wird daher nicht länger als Argument verwendet.

nem absoluten – auch nicht mit hochrangigen Ermittlungsinteressen abwägbaren – Überwachungs- und Erhebungsverbot im Kernbereich privater Lebensgestaltung" (Papier 2014: 12). Dabei geht es vorrangig um die informationelle Privatheit. Daten gelten hier als Träger personenbezogener Merkmale und letztere machen ihre Schutzbedürftigkeit aus. Privatheit wird nicht nur als rhetorische Figur gebraucht, sondern der Begriff bezieht sich explizit auf informationelle Privatheit.

3.5.3 Welt der Geheimdienste

Der Diskurs der Welt der Geheimdienste dreht sich zunächst um Techniken. Die Rede ist von verschiedenen Software-Anwendungen, ihrer Reichweite und den damit verbundenen politischen und ethischen Konsequenzen. Zunächst wurden die Arbeiten von BND und NSA als gleichartig dargestellt. So beschrieb Ex-BND-Präsident Hans Georg Wieck: „Wir machen das in Gestalt des Bundesnachrichtendienstes im Ausland selbst. Da ist nicht mehr Illegales drin als in anderen geheimdienstlichen Tätigkeiten" (Wieck, zit. in: Mitteldeutsche Zeitung 2013). Doch kurz darauf wurde in etlichen Medien die Unterscheidung zwischen der „Schleppnetz-Methode" der NSA und der „Harpunen-Methode" des BND wiedergegeben, mit der BND-Präsident Schindler die verschiedenen Maßnahmen „ansatzorientierter" und „zielorientierter Erfassung" veranschaulichte. Die NSA würde dabei sehr großzügig Metadaten speichern, während der BND sich auf konkrete Inhalte ausgewählter Ziele konzentriere. Darüber hinaus müsse zwischen Metadaten und Inhalten differenziert werden.[129] Die Speicherung von Metadaten stellt in der Wahrnehmung der NSA keinen Eingriff in die Privatsphäre dar. So erklärte Dianne Feinstein, Vorsitzende des Geheimdienstausschusses im US-Senat: „Das sind nur Metadaten […]. Da sind keine Inhalte dabei" (Feinstein, zit. in: Kling 2013). Die Erfassung von konkreten Inhalten geschehe erst nach einer gerichtlichen Anordnung. Aus verschiedenen Richtungen wurde

[129] Als Metadaten gespeichert werden Telefonnummern, benutzte Geräte, Ort und Zeit. Bei Emails gelten Empfänger- und Absender-Adressen, der Betreff, Orte und Zeitpunkte als Metadaten.

Kritik an dieser Differenzierung geübt, mit der Folge, dass US-Präsident Barack Obama die Befugnisse der NSA zumindest leicht einschränken ließ.[130] Im Gegensatz dazu meldete der BND im Mai 2014 den Bedarf an, in Zukunft „Echtzeitanalyse von Streaming-Daten" betreiben zu müssen und veranschlagte dafür 300 Millionen Euro zur eigenen Aufrüstung bis ins Jahr 2020. Im Zuge dessen wird die Unterscheidung zwischen Harpunen- und Schleppnetz-Methoden aufgegeben und der BND legitimierte die Verstärkung der eigenen Aktivitäten durch dieselben Argumente, die auch die NSA nutzt: „Die Analyse von Metadaten sei ein weniger starker Eingriff in die Privatsphäre, weil man im Gegenzug auf das massenhafte Ausspähen von Inhalten zunächst verzichten könne" (Goetz et al. 2014). Dem BND wurde dennoch vorgeworfen, durch die Akkumulation auch von Inhaltsdaten die Privatsphäre der Menschen zu verletzen. Doch dies wurde u.a. durch den Innenstaatssekretär Ole Schröder entkräftet: „Es liegt kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter eingrenzbaren Personenkreis richten" (Schröder, zit. in: Handelsblatt 2014).

In diesem Sinne wird in der Welt der Geheimdienste Privatheit als Zugang zu Informationen bestimmt. Privat ist das, was anderen Menschen unzugänglich ist. Sofern eine Person Informationen über sich preisgibt, verlassen sie den geschützten Bereich des Privaten. Diese Zugangsdefinition argumentiert über individuellen Besitz von Informationen und lässt so andere Fälle einer Verletzung von Privatheit außen vor. Hier dient die diskursiv erzeugte Sorge um „die Privatsphäre" als Begründung für eine Zunahme an Überwachung. Die Geheimdienste geben keine eigene Definition, wie Privatsphäre zu bestimmen sei, sondern verweisen vage auf rechtliche Grundlagen. So wird vom BND immer wieder betont, er handle stets im Rahmen geltender Gesetze. Der BND sieht sich selbst als „fest im gesellschaft-

[130] Durch den USA FREEDOM Act v. 2.6.2015.

lichen System verankerter Dienstleister“ (Schindler 2014). Weitaus häufiger wird die Notwendigkeit von Eingriffen in die Privatsphäre behauptet, um drohende Terroranschläge abwehren zu können. Ex-BND-Präsident Wieck verweigert sogar, überhaupt Bezüge zur Fragen nach Privatheit herzustellen: „Das sind keine Überwachungsmaßnahmen, sondern das ist ein Beitrag zur Bekämpfung des Terrorismus auch in Deutschland“ (Wieck, zit. in: Mitteldeutsche Zeitung 2013). Im Rahmen dieser Argumentationslinie werden, wie in der Welt des Staates, die Werte Privatheit und Sicherheit gegenübergestellt, wobei Privatheit schließlich untergeordnet wird.

Diskutiert wird außerdem die Zusammenarbeit zwischen BND und nicht-deutschen Geheimdiensten. Dabei wird die Wichtigkeit solcher Kooperationen betont. Kritik begegnet der BND mit Verweis auf gesetzliche Regelungen, ohne jedoch auf Details einzugehen. „Es wurde zu keinem Zeitpunkt von den gesetzlichen Regelungen abgewichen“ (Kröger 2014). Laut BND laufen „alle Aktivitäten im Rahmen von Kooperationen mit anderen Nachrichtendiensten unter Einhaltung der Gesetze, insbesondere des BND-Gesetzes und des G-10-Gesetzes“ (Bundesnachrichtendienst, zit. in: Spiegel Online 2013). Die Zusammenarbeit zwischen den Geheimdiensten wird als Selbstverständlichkeit formuliert: „Ohne internationale Zusammenarbeit könnte der Bundesnachrichtendienst noch nicht einmal ansatzweise seine gesetzlichen Aufgaben erfüllen“ (Schindler 2013). Auch der Bundesinnenminister bekräftigt die Rolle der NSA und verweist noch einmal auf die Bedeutung von Sicherheit: „Denn wir brauchen und möchten eine gute Zusammenarbeit mit den USA – nicht zuletzt für die Sicherheit unseres Landes“ (de Maizière, zit. in: Hoppe/Jakobs/Sigmund 2014). Der frühere NSA-Chef Hayden pflichtet ihm bei: „Es gibt eine breite Zusammenarbeit zwischen befreundeten Nachrichtendiensten, ja. Das ist ein sehr wichtiger Aspekt für die Sicherheit jedes Landes […]“ (Hayden, in: Thevesen 2013). Die Kooperation von Geheimdiensten wird so zum Garanten nationaler Sicherheit und einer genaueren Analyse entzogen.

Während nach den Snowden-Enthüllungen nicht selten dazu aufgerufen wurde, Daten durch Verschlüsselung im Sinne der informationellen Selbstbestimmung zu schützen, begreift der Verfassungsschutz „die zunehmende Verwendung von Verschlüsselungssoftware“ als Teil der Sicherheitsvorkehrungen von „Extremisten“[131] (Bundesministerium des Innern (2014): 57).[132] Eigenmächtiges Ausüben von Verschlüsselung wird damit diskursiv jenseits des demokratischen Zusammenlebens positioniert.

3.5.4 Welt der Ökonomie

In der Welt der Ökonomie gilt Privatheit als hoch geschätztes Gut. So formuliert der Unternehmensverband BITKOM: „[Die Unternehmen der Netzwirtschaft sind] bestrebt, den Schutz von Daten und Kommunikation und die Unversehrtheit der Privatsphäre jederzeit sicherzustellen und Angriffe und Zugriffe von außen zu verhindern. In die Sicherheit der Daten ihrer Kunden investieren die Unternehmen der Netzwirtschaft jährlich weltweit einen zweistelligen Milliardenbetrag“ (BITKOM 2013). Privatheit wird dabei als Schutz von Informationen deklariert. „Informationen sind das Wichtigste, was wir haben. Das betrifft unsere Privatsphäre, zum anderen aber auch unsere Infrastrukturen und Technologien“, so der damalige Telekom-Vorstands-

[131] Zu einer Kritik des Extremismus-Begriffs vgl. Butterwege 2002, Oppernhäuser 2011.

[132] Im Verfassungsschutzbericht 2013 findet sich mit Verweis auf eine Veröffentlichung auf der ursprünglichen Graswurzel-Journalismus-Plattform linksunten.indymedia.org: „Nahezu zeitgleich […] forderten Anfang Juni 2013 Autoren, die sich selbst dem „cyberterrorism“ zuordnen, einen sensibleren Umgang mit Daten. Sie verweisen auf ein […] ‚Privacy-Handbuch‘, um verdeckter zu surfen, Anonymisierungsdienste zu nutzen und Daten zu verschlüsseln“ (Bundesministerium des Innern 2014: 57). Als Grundlage für diese Zuordnung der möglichen Autoren zum „Cyberterrorismus“ diente dem VS der frei wählbare Accountname. Davon abgesehen, dass es schwierig ist, aus dem gewählten Accountnamen bereits eine solch gravierende Zuordnung abzuleiten, wird dieser nicht einmal korrekt wiedergegeben. Der Accountname ist „cybererrorism“ und wird auch am Ende der Veröffentlichung noch einmal wiederholt (vgl. cybererrorism 2013). Während „cybererrorism“ als Wortspiel erkennbar ist („error“ (engl.) = Fehler), rahmen die Aussagen des Verfassungsschutzes das Privacy-Handbuch direkt in den Kontext terroristischer Aktivitäten. Ob dies bewusste Irreführung oder schlicht schlechte Arbeit ist, darüber kann an dieser Stelle nur spekuliert werden. Verschlüsselungstechnologien werden damit jedoch delegitimiert.

Vorsitzende René Obermann (in: FAZ.net 2013). Zugleich findet dabei eine Transformation statt: Daten und Informationen werden in der Welt der Unternehmen als Ware gehandelt. Sie werden erhoben, um Profit zu generieren. „Es ist nicht nur eine Frage von Privatsphäre und Bürgerrechten, sondern eine fundamental wirtschaftsstrategische Frage, um die es hier geht." (ebd.) Privatheit gilt hier nicht nur als moralische Frage, sondern ausdrücklich auch als ökonomische.

Der Begriff Privatheit wird von datensammelnden Unternehmenden genutzt, aber eher vage beschrieben. So wirbt Microsoft (ohne Datum), einer der ersten Teilnehmer am PRISM-Programm, nun mit dem Slogan: „Your privacy is our priority." Facebook-CEO Marc Zuckerberg reformulierte seine Vorstellungen von Privatheit aufgrund der Snowden-Dokumente. Nachdem er 2010 noch behauptet hatte, Privatheit sei als „soziale Norm" überholt (Zuckerberg 2010), bekräftigt er 2014, dass „das Schaffen privater Räume für Leute wo sie Dinge teilen und interagieren können wie nirgendwo sonst" (Zuckerberg 2014) eine der wichtigsten Maßnahmen seines Unternehmens ist. Gerade diese Unterbestimmtheit des Begriffs eröffnet Unternehmen die Möglichkeit, den Begriff zu Werbezwecken zu verwenden, ohne bestimmte Maßnahmen einzuleiten zu müssen.

3.5.5 Welt der Netzgemeinde

In der Welt der Netzgemeinde stehen Auseinandersetzungen mit Informations- und Kommunikationstechniken im Mittelpunkt. Darüber hinaus geben sich die Repräsentanten der Welt heterogen. Privatheit wird weitgehend als informationelle Privatheit bestimmt, wobei wenig Einigkeit darüber besteht, welche Handlungen sinnvoll sind. Handlungsbedarf wird anlässlich der Geheimdienstenthüllungen ausdrücklich postuliert. Im Zuge erster Reaktionen wurde auf die bereits seit langem laufenden Auseinandersetzungen rund um die Themen Datenschutz und Überwachung verwiesen. Generell lässt sich die Zunahme martialischer Vokabeln feststellen: es geht um das „zurückerkämpfen" (Beckedahl, zit. in: Bewarder 2014) und um das „zurück erobern" (Birk 2014). Diese Rhetorik findet Anschluss an das

Selbstverständnis der gut ausgebildeten, aber wenig einflussreichen gesellschaftlichen Gruppe, die sich in Opposition zu Staaten, Nachrichtendiensten und Konzernen sieht. Damit verbunden sind die geforderten politischen Aktionen: Aus der Netzgemeinde heraus werden verschiedene Demonstrationen und Kampagnen organisiert,[133] mal mit dem Ziel, auf die Gesetzgebung einzuwirken, mal mit dem Ziel, eine stärkere Sensibilisierung für das Thema Privatheit bei der Bevölkerung zu erreichen. Häufig wird auf Kontaktformulare verlinkt, über die Politiker über die eigenen Anliegen informiert werden sollen. Akte zivilen Ungehorsams wie etwa die Kommunikationsguerilla-Aktionen des Peng! Collective[134] werden als Bereicherung der politischen Arbeit anerkannt. Neben der politischen Arbeit wird außerdem an Techniken gearbeitet, die auf Datenschutz abzielen. Hauptsächlich werden Verschlüsselung und dezentrale Strukturen vorgeschlagen und entwickelt. In diesem Sinne stellen Vertreter der Netzgemeinde recht konkrete Forderungen oder materialisieren diese Ansprüche in Form von Software und Aktionen. Ein Großteil derer, die an technischen Lösungen arbeiten, beruft sich dabei auf die Notwendigkeit informationeller Selbstbestimmung. Als gemeinsamer Feind und entscheidendes Übel gelten die Geheimdienste. So formuliert Marcus Beckedahl auf der re:publica 2014: „Kriminell agierende Geheimdienste haben uns das Netz entrissen“ (Beckedahl, zit. in: Endert 2014). Der Vorschlag der Bundesregierung, diversen Sicherheitsorgangen mehr Kompetenzen zuzugestehen, wird entsprechend hart

[133] Stellvertretend sei hier auf die Kampagnen „Starker Europäischer Datenschutz jetzt“ (Campact 2013) und „Privacy International“ (ohne Datum) hingewiesen. Beiden Kampagnen wurden von Repräsentanten der Netzgemeinde initiiert. Während die erste sich darauf beschränkt, dass Erheben personenbezogener Daten verhindern zu wollen, liefert die andere zudem Begründungen über die ethischen und juristischen Grundlagen von Privatheit. Privatheit gilt hier als Grundrecht, das essentiell für Autonomie und den Schutz der Menschenwürde ist. Es wird im Folgenden als Freiheitsrecht gegen asymmetrische Machtverhältnisse in Stellung gebracht.

[134] Auf der re:publica 2014 traten zwei Aktionskünstler des Peng! Collective als Mitarbeitende des Google-Konzerns auf und stellten fiktive Produkte als neue Angebote vor, die massive Eingriffe in die informationelle Selbstbestimmung bedeutet hätten. Die Reaktionen aus der re:publica waren wohlwollend und die Anwesenden führten nach Auflösung der Fiktion diese noch mittels Tweets fort; Google hingegen drohte mit einer Unterlassungsklage.

kritisiert: „IT-Sicherheit ist eine Aufgabe, die sich schlicht nicht militärisch, polizeilich oder geheimdienstlich lösen lässt – im Gegenteil: Es besteht die Gefahr, dass hier, wie es so schön heisst, der Bock zum Gärtner gemacht wird“, so CCC-Lobbyist fukami (fukami 2014).

Hinsichtlich Privatheit postulieren Repräsentanten der Netzgemeinde eine Bedrohung und rufen in Reaktion zum Handeln auf. So war Teil des Mottos der re:publica 2014: „Wenn Algorithmen uns zu gläsernen, kontrollierbaren, weil berechenbaren Menschen machen, müssen wir vielleicht unberechenbarer werden?“ (re:publica 2014) Privatheit wird dabei zumeist als kategorisch schützenswert verstanden. Insbesondere informationelle Privatheit wird als Bedingung für Autonomie und Menschenwürde sowie als Basis einer bestimmten gesellschaftlichen Ordnung bezeichnet: „Demokratie braucht Privatsphäre und Sicherheit in der Kommunikation“, so Aktivist Sebastian Hahn (Hahn 2014).

Abgrenzungen gegenüber anderer Welten verlaufen unterschiedlich. So finden sich vehemente Kritiken an der „Datenkrake Google“, insofern ihr Geschäftsmodell vor allem auf der Erhebung personenbezogener Daten gründe. Eine Dichotomie zwischen bösen Konzernen und guten Netzbewohnern wird nicht von allen Akteuren der Netzgemeinde stark gemacht. Sascha Lobo etwa meint: „Internetunternehmen wie Google, Apple oder Facebook werden in der Öffentlichkeit oft dämonisiert. Das ist kontraproduktiv“ (Lobo 2014). In dieser Logik werden weniger einzelne Unternehmen kritisiert, sondern die unzureichende Regulierung bestimmter kapitalistischer Verhältnisse problematisiert. Wieder andere weisen auf die Bedeutung von Privatheit aus ökonomischen Gründen hin. Wie sich an den sinkenden Verkaufszahlen von IT-Produkten nach den Snowden-Veröffentlichungen zeige, sei der Schutz von Privatheit bereits aus wirtschaftlicher Perspektive relevant.

Die Auseinandersetzungen der Netzgemeinde beziehen sich auf eine Privatheit, die vor allem als informationelle Selbstbestimmung gefasst wird. Entsprechend wird auf Ebene der Rhetorik versucht, sich gegen

technologisch materialisierte Mechanismen zur Wehr zu setzen. Innerhalb der Netzgemeinde wird dieser Wandel diskursiv vorangetrieben und teils affirmativ begrüßt, etwa von der Splittergruppe der Post-Privacy-Bewegung. Die Gruppe beschäftigt sich mit der Idee, ein Verschwinden (bürgerlicher) Privatheit könnte hinsichtlich technologischer Entwicklungen langfristig nicht abzuwenden und möglicherweise sogar zu begrüßen sein. Privatheit wird hier als unzeitgemäßes Element einer bürgerlichen Gesellschaft verstanden: „Die derzeitige Disruption der Privatsphäre wird nur deswegen hingenommen, weil auch ihre gesellschaftliche Funktion weitgehend obsolet geworden ist“ (Seemann 2014). Während der übrige Teil der Netzgemeinde nur noch „Rückzugsgefechte“ (Heller, zit. in: Schönleben 2013) um die veraltete Idee des Datenschutzes führe, sei vielmehr eine andere gesellschaftliche Ordnung gefragt. Als Lösungsvorschlag wird teils die strategische Offenbarung personenbezogener Daten empfohlen. Hieraus ließen sich nicht zuletzt ökonomische Gewinne generieren. Die Post-Privacy-Bewegung betreibt damit eine diskursive Abwertung einer bestimmten Privatheit. Aus technologischen Entwicklungen und neuen Praktiken der Digitalvernetzung wird eine normative Kraft des Faktischen abgeleitet, die affirmatives Verhalten bezüglich des Wandels oder Verschwindens von Privatheit einfordert. Teils wird die hohe Effizienz technischer Lösungen betont und Effizienz zum entscheidenden Maßstab gemacht. Solche utilitaristischen Argumentationen vernachlässigen allerdings Machtasymmetrien, etwa wenn Formen der Privatheit Unterprivilegierte schützen helfen.

3.5.6 Zusammenfassung

Privatheit ist ein zentraler Begriff in allen sozialen Welten und wird vorrangig als informationelle Privatheit bestimmt. Andere Aspekte und Formen des Privaten werden eher selten aufgerufen. Die Argumentationslinien innerhalb der beteiligten sozialen Welten sind selten homogen. Dennoch treten verwandte Rechtfertigungsstrategien in unterschiedlichen Welten auf. Grob unterschieden werden können aus ethischer Perspektive deontologische und konsequentialistische Argumentationslinien: Im Zuge deontologischer Argumentationen

wird informationelle Privatheit absolut gesetzt und unter Rückgriff auf Werte wie Menschenwürde oder Demokratie als integrales Gut konstruiert. Die deontologische Argumentationslogik wird insbesondere in den Welten der Rechtsanwendung und der Netzgemeinde formuliert, aber auch in den Welten des Staates und der Ökonomie. Im Gegensatz dazu wird Privatheit in konsequentialistischen Argumentationslinien als Freiheitsrecht im Spannungsverhältnis zu Freiheit konzipiert. Einschränkungen bestimmter Aspekte von Privatheit werden entsprechend mit Anforderungen des Werts Sicherheit legitimiert. Solche Figuren der Rechtfertigung finden sich vor allem in den Welten der Geheimdienste und des Staates. Eine dritte zentrale Argumentationsstrategie der Arena rahmt Privatheit als ökonomischen Wert: Die Ermöglichung informationeller Selbstbestimmung wird übersetzt in die Entwicklung von Produkten, die einer Nachfragesituation entsprechen. Privatheit wird als Effekt ökonomischen Handelns konzipiert. Entsprechend wird diese Strategie insbesondere in der Welt der Ökonomie verfolgt, findet sich aber auch in den Welten des Staates, der Netzgemeinde und der Rechtsanwendung.

Dem Wert Privatheit kommen in der Arena insbesondere in den entscheidenden Welten des Staates und der Geheimdienste nur wenig positive Bestimmungen zu: Als Abwehrrecht, informationelle Selbstbestimmung und Gegenpol zum Wert Sicherheit wird Privatheit häufig negativ und im Falle von Verletzungen bestimmt. Diese Diskurslinie passt in eine Tradition liberalen Staatsverständnisses, in der Privatheit vor allem der Limitierung staatlichen Handelns dient. In diesem Sinne verbleiben wichtige Teile des Arena-Diskurses dieser liberalen Tradition verpflichtet. Gemein haben viele der Positionen des Arena-Diskurses außerdem, dass sie Privatheit in Form informationeller Selbstbestimmung und damit rückgebunden an individuelle Eigenschaften bestimmen. Kaum thematisiert wird Privatheit als relationaler Effekt, der immer wieder ausgehandelt werden muss. Neben den drei zentralen Diskurslinien der Arena finden sich auch solche, die die Notwendigkeit einer Neubewertung von Privatheit zu artikulieren versuchen. Hier wird Privatheit als krisenhaft, erhaltenswert

und reformbedürftig verstanden. Solche Positionen finden sich etwa in den Welten der Netzgemeinde und der Rechtsanwendung.

4 Begriffliche und theoretische Hintergründe

4.1 Privatheit – Ideengeschichte und theoretische Zugänge

Thilo Hagendorff

4.1.1 Ideengeschichte

Wie in den vorhergehenden Analysen bereits angeklungen, wird der Begriff des Privaten in den unterschiedlichen Welten der Privacy-Arena zwar durchgängig und mit großer Häufigkeit verwendet, jedoch in den allerseltensten Fällen genauer spezifiziert. Der Auseinandersetzung mit philosophischen Spezifizierungen des Begriffs des Privaten sowie einer ideengeschichtlichen Einordnung soll das folgende Kapitel nachkommen, bevor im anschließenden Kapitel 4.2 eine rechtswissenschaftliche Analyse und Aufschlüsselung des Privatheitsbegriffs folgt. Solche begrifflichen Klärungen können als Kontrastfolie dabei helfen, typische Rechtfertigungsmuster und Zugriffsweisen auf den Wert der Privatheit in der Privacy-Arena genauer zu identifizieren (Boltanski/Thévenot 2007).

Die moderne Unterscheidung zwischen Privatheit und Öffentlichkeit resultiert aus einer langatmigen historischen Entwicklung (Geuss 2013). Grob ausgehend von der in der griechischen Antike gründenden Unterscheidung zwischen den beiden Seinsordnungen Oikos und Polis, zwischen Hauswirtschaft und dem Bereich der Öffentlichkeit, entwickelt sich die spätere Differenzierung zwischen privat und öffentlich. Bereits in der griechischen Antike wurde der Raum des Privaten als Rückzugspunkt verstanden. Aristoteles etwa sah die Einsamkeit der Privatsphäre als wichtige Bedingung für eine ungestörte Kontemplation. Die Sphäre des Privaten galt zudem als der Bereich des Haushalts, des familiären Zusammenlebens sowie der Verrichtung der Lebensnotwendigkeiten. Während der Bereich der Polis als Reich

der Freiheit galt, so galt der Haushalt als ein von Notwendigkeiten durchherrschter Bereich, welcher jedoch die Voraussetzung dafür war, dass sich überhaupt eine Polis konstituieren konnte (Cancik/Schneider 2014).

Letztlich entwickeln sich ausgehend von der griechischen Antike viele Traditionen und Theorien, deren gemeinsamer Kern darin besteht, dass sie die Privatsphäre, worunter in erster Linie Familie und Haushalt fallen, in Abgrenzung zu dem bestimmen, was als Öffentlichkeit gilt. Dabei beschreibt der Bereich des Privaten einen Sozialraum, welcher sich durch bestimmte Handlungsnormen und Konventionen konstituiert. Dieser Sozialraum steht in der Hauptsache in Relation zu drei weiteren gesellschaftlichen Sphären oder Welten – zur eigenen Nah- oder Lebenswelt, zur Welt der Ökonomie sowie zur Welt des Staates. Der Wert der Privatsphäre besteht dann darin, dass sie einen geschützten Raum bildet, welcher die Voraussetzung dafür ist, dass Personen angesichts der invasiven Kräfte einer in die Lebenswelt eindringenden Welt der Ökonomie sowie eines mit weitreichenden Befugnissen ausgestatteten Staates eine selbstbestimmte Identität ausbilden und erhalten können. „Privacy, in short, provides principles for negotiating the legal management of personhood in a manner that facilitates the development and maintenance of a coherent individual identity essential to our liberal polity's commitment to human flourishing" (Kahn 2003: 373). Dabei variieren die Grundsätze zur Regulierung von Privatheit von Kultur zu Kultur (Altman 1977, Ess 2005). Kulturelle Varianzen betreffen sowohl die Art der Schließung der Privatsphäre als auch die Art der Integration anderer Personen in dieselbe. Unterschiedliche Interaktionen werden als „privat" oder „öffentlich" gekennzeichnet und in entsprechende Inszenierungsrahmen eingefasst. Um nur ein Beispiel zu nennen: Während es in Deutschland als verpönt gilt, Fragen zum Gehalt anderer Personen zu stellen, so ist dies in Schweden selbstverständlich. Das schwedische Finanzamt „Skatteverket" gibt Auskunft über die Gehälter jedes Schweden – mit Ausnahme des Königs.

Definitionen des Privaten spalten sich ferner auf in solche, welche das Private negativ in Begriffen der Abspaltung, Einsamkeit, Vermeidung und des Rückzugs definieren und solche, welche das Private positiv durch Begriffe der Kontrolle und Freiheit definieren. Räumliche Privatheitskonzepte betonen eher erstgenannte Begriffe und definieren Privatsphäre über den Schutz einer Person vor bestimmten sozialen „Inputs", während informationelle Privatheitskonzepte sich eher auf letztgenannte Begriffe berufen und Privatsphäre über die Kontrolle definieren, welche eine Person über soziale „Outputs" ausübt. Beiden Privatheitskonzeptionen ist im weitesten Sinne gemein, dass sie die Regulation der Privatheit als einen dialektischen Prozess definieren, welcher Zugangsbeschränkungen oder die „Permeabilität" zum eigenen „Selbst" entweder gezielt lockert oder verschärft. Mit „Selbst" kann die Innenwelt, die Subjektivität einer Person gemeint sein, die Intimsphäre als Sphäre der höchstpersönlichen Körperverrichtungen, Bindungen und Beziehungen oder die konkrete häusliche Sphäre (Hahn/Koppetsch 2011: 11). Privatheit wird verstanden „as a dialectic process involving both a closing off of the self and an opening of the self to others" (Altman 1976: 27). Zu einer stufenweisen Enthüllung des eigenen Selbst respektive der eigenen Person kommt es bereits innerhalb der Privatsphäre selbst. Gemeint sind Ausbalancierungsprozesse zwischen individuellen Autonomieansprüchen und der häuslichen Gemeinschaft. Familien- oder Paarbeziehungen sind nicht ohne ein bestimmtes Maß an Offenbarung des eigenen Selbst und eine gewisse Aufkündigung an Intimität möglich. „Perfekte" Privatheit wäre dementsprechend durch die vollständige Unzugänglichkeit einer Person definiert. Diese Unzugänglichkeit kann definiert werden über das vollständige Fehlen von Informationen über eine Person, über das vollständige Missachten einer Person oder über die Unmöglichkeit des physischen Zugriffs auf eine Person. Fakt ist aber: „Perfect privacy is, of course, impossible in any society. The possession or enjoyment of privacy is not an all or nothing concept, however, and the total loss of privacy is as impossible as perfect privacy" (Gavison 1980: 428). Von Bedeutung sind in der Regel weniger Zugewinne an Privatheit als vielmehr der Verlust derselben. Dies kann entsprechend

dem oben Gesagten durch das Herausfinden von bestimmten Informationen über eine Person geschehen, durch Eingriffe in die Handlungsfreiheit einer Person oder durch das Missachten von räumlichen Zugangsbeschränkungen. Dabei kommt es zu einer Verletzung von Geheimhaltungsinteressen, der Autonomie oder von Rückzugsräumen einer Person.

Der Begriff des Privaten ist jedoch auch der Kritik ausgesetzt. Es gibt reduktionistische Ansätze, welche davon ausgehen, dass Privatheitskonzepte letztlich Konglomerate anderer grundlegender Rechte wie etwa des Rechts auf Leben, Freiheit und Eigentum sind. Diese Konzepte gehen davon aus, dass kein eigenständiges Recht auf Privatheit ausgemacht werden kann (Davis 1959; Moore 2008; Thompson 1975). Kommunitaristische Ansätze kritisieren, dass Privatheitskonzepte dem Individuum das Primat vor der Gemeinschaft einräumen und damit einen Verfall „öffentlicher" Werte wie Sicherheit, Wohlfahrt, Verantwortungsbewusstsein etc. begünstigen (Etzioni 1999). Seitens feministischer Positionen wird kritisiert, dass die Privatsphäre der Verschleierung (häuslicher) Gewalt dienen kann und das hierarchische Herrschaftsverhältnis zwischen Männern und Frauen verhärtet (MacKinnon 1989; Olsen 1993).

4.1.2 Privatheit als Raum

Der Begriff der Privatheit kann Räume beschreiben. Eine gängige Definition lautet, dass etwas dann als privat gilt, „wenn man selbst den Zugang zu diesem ‚etwas' kontrollieren kann" (Rössler 2001: 23). „Privacy is often defined spatially as involving a realm placed beyond the reach or measure of certain social forces" (Kahn 2003: 388). Privatsphäre kann in diesem Sinne als eine räumliche Rückzugs- und Erholungsmöglichkeit verstanden werden, welche eine Spontaneität der Handlungen erlaubt, welche in öffentlichen Bereichen sanktioniert wird. Wer über einen privaten Raum verfügt, der kontrolliert und überwacht den Zutritt anderer Personen zu ebendiesem. Private Räume umfassen Lebensbereiche von Personen, die als verborgen oder nur eingeschränkt sichtbar gelten. „Außen" und „Innen" sind klar

voneinander getrennt. Während das „Außen" als die Sphäre der Gesellschaft konzipiert wird, gilt das „Innen" als der Sozietät gegenübergestellt, als Refugium, welches vor „sozialer Kälte" schützt. Idealisierend schreiben Hahn und Koppetsch: „Hier regiert Emotionalität und Intimität, hier kann das Individuum zu ‚sich selbst' kommen und wird in seiner ganzen Persönlichkeit angesprochen" (Hahn/Koppetsch 2011: 11). Private Räume gelten als Räume der Erholung von den Anforderungen, welche in öffentlichen Sphären an das (Rollen-)Verhalten einer Person gestellt werden. Man denke an Anforderungen der Affektunterdrückung, Distanziertheit, Disziplin, Funktionalität. Hier findet mitunter eine Stilisierung des Privaten als Geborgenheit, als Schutzraum vor einer rücksichtslosen, „kalten" Gesellschaft statt. In diesem Zusammenhang steht die Konzeption einer Lebenswelt, welche als positive Größe oder Gegengewicht bereitgehalten wird, um sich gegen „soziale Kälte" und Unübersichtlichkeit zu schützen. Die Frage ist aber, ob es angemessen ist, dass semantische Komplexe, welche sich um den Begriff des Privaten ranken, die Hyperkomplexität sozialer Systeme auf eingängige, scheinbar „primordiale" Codes wie vertraut/unvertraut oder eben privat/öffentlich reduzieren.

Räumliche Privatheitskonzepte gehen davon aus, dass gerade das „Nicht-beheimatet-Sein" in der Welt zu Sphärenbildungen führt (Sloterdijk 1998). Der Mensch tritt als Sphären-Architekt auf. Das „Sein-in-Sphären" bildet ein Grundverhältnis des Menschen, „freilich eines, das von Anfang an durch die Nicht-Innenwelt angetastet wird und das sich ständig gegen die Provokation des Außen behaupten, wiederherstellen und steigern muß. In diesem Sinne sind Sphären immer auch morpho-immunologische Gebilde. Nur in innenraumbildenden Immunstrukturen können Menschen ihre Generationenprozesse weiterführen und ihre Individuationen vorantreiben. [...] Sie [die Menschen] gedeihen nur im Treibhaus ihrer autogenen Atmosphäre" (Sloterdijk 1998: 46). Die Privatsphäre bildet, mit Sloterdijk gesprochen, ein die Menschen umschließendes Mikroklima, eine selbstbeherbergende Binnenwelt. Die Ausdifferenzierung von Privatheit als Sphäre oder Raum folgt einer Formatierung der sozialen Welt, wobei es weniger

um die klassische soziale Differenzierung zwischen „oben" und „unten" geht als vielmehr um „draußen" und „drinnen". Privatheit ist also im Hinblick darauf zu untersuchen, „wie, mit welchen Mitteln und in welchen Bereichen Grenzen zwischen ‚drinnen' und ‚draußen' etabliert werden und wie die Sphären vor und hinter der Grenze markiert und in Szene gesetzt werden" (Wohlrab-Sahr 2011: 36).

Private Räume – in der Regel versteht man darunter häusliche Räume – sind nichts anderes als, um weiterhin mit Sloterdijk zu sprechen, die Resultate sphärenschaffender Regungen und Maßnahmen. Dabei kommt privaten Räumen eine Art „Seinsvorrang" vor nicht-privaten, öffentlichen Räumen zu. Die Privatsphäre wird zum immunologisch wirksamen Sphäreninnenraum, zum angenehmen Mikroklima von Intimformen des In-Sphären-Seins, zum Sozialapriori, das ein Fundament des Vertrauten und Sicheren bildet, welches der hyperkomplexen Unübersichtlichkeit der Gesellschaft widersteht. Das Syndrom Privatheit fungiert oppositionell. Die Privatsphäre bildet eine vor den Systemimperativen zu schützende Sphäre. Administrative Steuerungssysteme, etwa Geld oder Macht, dürfen nicht bis in die originär unversehrten Bereiche der Lebenswelt hineinwirken (Habermas 1987a). Angelehnt an ein Konzept der Lebenswelt bilden private Räume ein sphärologisches Korrektiv zu den in den Systemen verordneten Sozialpathologien. Über die Privatsphäre wird so die Differenzierung von vertraut/unvertraut hypostasiert. Die soziale Welt wird aufgespalten in eine vertraute Welt der Privatsphäre und eine diskriminierte, unvertraute Welt. Privatheitskonzepte folgen dementsprechend trivialanthropologischen Konzepten, welche den Menschen in unterschiedlichen Sphären verorten. Nicht berücksichtigt wird gerade bei räumlichen Privatheitskonzepten, dass in modernen Gesellschaften eine stete Verwischung der Differenz von Vertrautem und Unvertrautem stattfindet. Der Code privat/öffentlich transformiert sich hier mitunter gar stillschweigend zur Differenz von vertraut/kritisierbar. Der vertraute Bereich der Privatsphäre ist jedoch kein „sakrosankter" Bereich, welcher von einer unübersichtlichen Öffentlichkeitssphäre trennscharf abgekoppelt werden könnte.

Die Privatsphäre formiert sich, sofern man sie in Verbindung mit der oben genannten Welt des Hauses sehen mag, als eine von produktiven Funktionen entlastete Institution der Familie, welche sich in erster Linie auf Sozialisationsaufgaben konzentriert. Privatsphäre in diesem Sinne wird typischerweise über das häusliche Leben oder häusliche Räume bestimmt. Sie kann aber gleichsam einen Raum der Verdrängung bilden, in den Personen abgeschoben und der sozialen Welt entzogen werden. Ein räumliches Verständnis von Privatsphäre geht davon aus, dass private Räume Blasen bilden, welche sich in erster Linie gegenüber öffentlichen Räumen abgrenzen. Während öffentliche Räume allgemein zugänglich sind, bilden die Blasen der Privatsphäre zutrittsbeschränkte sowie -geschützte Bereiche. Eine Verletzung der Privatsphäre findet statt, wenn es zu einer konkreten Nichteinhaltung gesetzter Zutrittsbeschränkungen durch bestimmte Personen kommt. Private Räume bilden eine Art soziale Hinterbühne, welche die Möglichkeit bietet, das Spiel der Eindrucksmanipulation und der öffentlichen Selbstdarstellung zu unterbrechen. Gleichzeitig dienen private Räume der Einübung der eigenen Identität. Um dabei möglichst nicht den Beobachtungen fremder Personen ausgesetzt zu sein, sind private Räume in der Regel blickgeschützt.

Dieser Umstand jedoch bedingt gleichzeitig einen Bemäntelungseffekt der Privatsphäre. Private Räume sind oft auch Räume der (häuslichen) Gewalt und der Unterdrückung (Allen/Mack 1989). So wird insbesondere seitens feministischer Positionen der Raum der Privatsphäre kritisch gesehen. „The law of marriage and family contributed to the problem of women's privacy within the home. That problem was the problem of too much of the wrong kinds of privacy – too much modesty, seclusion, reserve and compelled intimacy – and too little individual modes of personal privacy and autonomous, private choice" (Allen/Mack 1989: 477). Privatsphäre in diesem Sinne dient als Raum zur Abwehr legitimer Einmischungen, als Institution der Nicht-Thematisierung von Herrschaftsbeziehungen. Die perfekte Privatsphäre wäre ein für Dritte komplett unzugänglicher und geheimer Raum, welcher indes als Ort für die Begehung von Straftaten perfekt

geeignet wäre. „Any individual's decision to violate a social norm in the privacy of her home may contribute to the demise of that norm [...]" (Gavison 1992: 15). Dementsprechend tangieren Überwachungsmaßnahmen zur Steigerung von Sicherheit gesetzte Zugriffsbeschränkungen auf die Privatsphäre. Zwischen dem Wert der Sicherheit und dem Wert der Privatheit muss dementsprechend ein Abwägungsprozess stattfinden, da beide Werte gegeneinander ausgespielt werden können. Dabei finden Erwägungen darüber statt, inwiefern unterschiedliche, genuin private Handlungen Fremdbeobachtungen bzw. einer Überwachung ausgesetzt werden sollen. Einblicke in private Räume können also entweder mit dem Wissen und eventuell der Einwilligung der betroffenen Person in Form von Sicherheit schaffenden Überwachungsmaßnahmen geschehen oder ohne deren Wissen in Form von voyeuristischen Beobachtungen stattfinden.

Über eine Privatsphäre zu verfügen bedeutet für eine Person, gegenüber anderen Personen oder Personengruppen separiert zu sein und, so die Vorstellung, autonom handeln zu können. Dieser Rückzug von anderen Personen in private Räume steht im Wechselspiel mit Momenten der Zusammenkunft mit anderen Personen in der Öffentlichkeit. Letztlich geht es darum, unterschiedliche Level interpersonaler Kontakte managen zu können, wobei ein individuell befriedigender Mittelweg zwischen zu viel und zu wenig Privatsphäre gefunden werden muss. „Thus, ‚ideal' privacy is a position on a continuum of desired interaction, with deviations in either direction being unsatisfactory" (Altman 1976: 12). Zu viel Privatsphäre bedeutet Isolation bzw. zu wenig soziale Interaktion, zu wenig Privatsphäre bedeutet permanentes Eindringen anderer Personen in einen eigentlich geschützten Raum respektive zu viel soziale Interaktion. Private Räume schützen, abstrakter formuliert, vor einer Überstimulation mit Reizen (Wohlwill 1974).

Zur Aufrechterhaltung ihrer Privatsphäre bedienen sich Personen unterschiedlicher verbaler sowie nonverbaler Verhaltensweisen. Während verbale Verhaltensweisen in der Regel aus einfachen Hin-

weisen bestehen, mit denen eine Person andeutet, dass sie sich in geschützte Räume zurückziehen möchte, so bestehen nonverbale Verhaltensweisen zumeist in Flucht- oder Abwendungsbewegungen (Patterson/Mullens/Romano 1971; Felipe/Sommer 1966; Hall 1969). Im Rahmen eines Konzepts von Privatsphäre als Raum geschieht dies über die Kontrolle bzw. die freie Wahl der die eigene Person umgebenden materiellen Umwelt. Räumliche Privatheit geht mit einer entsprechenden, Privatsphäre gewährenden Architektur einher. Diese umfasst Türen, Fenster, Zäune, Schilder oder Arrangements von Möbeln oder Einrichtungsgegenständen. Gerade Fenster sind ein anschauliches Beispiel dafür, wie die Grenze zwischen Privatem und Öffentlichem justiert wird. Über Gardinen, Jalousien oder Vorhänge findet eine Blickschutzregulierung und visuelle Abgrenzung des Privaten statt (Harth/Scheller 2012: 40). Die Privatsphäre wird durch die Einkehr, ja gar durch den Rückzug in die Wohnung erlangt. Einrichtungsgegenstände wie Kühlschränke oder Waschmaschinen bedingen zudem, dass man keine gemeinsamen Vorratskeller oder Waschküchen mehr teilen muss. So sind private Räume auch Räume, welche in materieller Hinsicht ein ansatzweise autarkes Leben ermöglichen.

4.1.3 Privatheit als Entscheidungsfreiheit

Der Begriff der Privatheit kann Handlungsweisen beschreiben. Eine Privatsphäre zu besitzen bedeutet autonom handeln zu können. In diesem Sinn dient die Privatsphäre der Sicherung von Entscheidungs- und Handlungsspielräumen (Innes 1992: 140) sowie der Entwicklung von Lebensführungsmöglichkeiten. Es gibt private „Angelegenheiten", aus denen Dritte sich „herauszuhalten" haben. Der Schutz der Privatsphäre dient dem Schutz und der Sicherstellung der persönlichen, auch rechtlich gesicherten Handlungsfreiheit. Darunter fällt insbesondere die Zurückhaltung des Staates aus Bereichen des Privaten (Brunst 2011). So gilt die Privatsphäre als konstitutives Element des Liberalismus. Sie verankert sich in dessen philosophisch-politischem Rahmen. Eine geschützte Privatsphäre ist die Bedingung dafür, dass staatlich garantierte Freiheiten überhaupt wahrgenommen werden

können. Nur wenn der Staat eine gewisse Autonomie seiner Bürger akzeptiert und ein ausreichendes Maß an Privatsphäre gewährleistet, kann über die Wahrung individueller Freiheit eine Pluralität von Lebensentwürfen gesichert werden. Erst geschützte private Bereiche ermöglichen es, Selbstbilder auszubilden und einzuüben, welche wiederum die Voraussetzung dafür sind, ein selbstbestimmtes und autonomes Leben führen zu können. „[…] it is my assertion that privacy implicates that aspect of dignity grounded in the belief that a full realization of one's personhood requires the recognition of, and respect for, the conditions necessary for each person to realize her distinct individual identity" (Kahn 2003: 378). Eine intakte Privatsphäre ist in erster Linie als Schutz vor staatlichen Eingriffen in private „Angelegenheiten" und als Schutz vor Fremdbestimmung zu verstehen. Es gibt eine Privatheit eigener Entscheidungen und Handlungen. Welcher Kirche eine Person angehört, welche Kleidung sie trägt, welche Partei sie wählt und so weiter, all dies gilt heute als „Privatangelegenheit" und bedarf vorerst keiner öffentlichen Rechtfertigung. „Die Privatsphäre ist jener Raum, den das Individuum für die Kontrolle seiner Interessen benötigt. Sie zu verletzen bedeutet, dem einzelnen gegen seinen Willen die Kontrollmöglichkeit über all das zu nehmen, was er eigentlich kontrollieren sollte" (Margalit 2012: 200).

4.1.4 Privatheit als Informationskontrolle

Der Begriff der Privatheit kann ein bestimmtes Wissen beschreiben. Privatheit ist hier gleichbedeutend mit der Sicherung von Erwartungen, die das Wissen betreffen, das andere Personen über die eigene Person besitzen. „Privacy is the condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is diminished exactly to the degree that others possess this kind of knowledge about him" (Parent 1983: 269). „[…] privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967: 7). Die informationelle Privatheit schützt die Autonomie einer Person im Hinblick auf die Kontrolle über den Zugriff Dritter auf Informationen jene Person betref-

fend. In diesem Zusammenhang stehen Ansprüche auf den Schutz persönlicher Daten. Die Kontrolle über Informationen, welche die eigene Person betreffen, wird in der digitalen Welt insbesondere über Datenschutztechnologien geregelt. Als problematisch wird dabei die Weitergabe von Informationen über die eigene Person gegen den eigenen Willen an Dritte gesehen. In der alltäglichen Kommunikation betrifft dies etwa den „Klatsch" (Bergmann 1987), in informationstechnischen Kontexten etwa den Handel mit Verbraucherdaten, die Analyse des digitalen Fingerabdrucks oder das Ausspähen geheimer Daten. Bereits Warren und Brandeis, von denen die häufig sentenzartig zitierte, ursprünglich auf Thomas Cooley zurückgehende Definition von Privatheit als das Recht, alleine gelassen zu werden, stammt (Cooley 1906: 364; Warren, Brandeis 1890: 205), stießen sich an einer maßlosen Nutzung der Instrumente zur Informationserlangung der Presse. „The press is overstepping in every direction the obvious bounds of property and of decency" (Warren/Brandeis 1890: 196). Warren und Brandeis ging es um die rechtliche Fixierung einer informationellen Privatheit – und das, noch lange bevor es Datenschutzdebatten rund um Google oder Facebook gab. Die beiden Juristen sahen in der florierenden städtischen Presse und der freien Zirkulation und Publikation von Fotografien eine Verletzung der Privatsphäre. Bereits Cooley schreibt dementsprechend: „The right to privacy, conceding it to exist, is a purely personal one, that is it is a right of each individual to be let alone, or not to be dragged into publicity" (Cooley 1906: 364).

Letztlich wird informationelle Privatheit über eine Regulierung der Kommunikation hergestellt. Dies geschieht im einfachsten Fall durch eine klare Beschränkung der an einer Kommunikation teilnehmenden Personen. Dies kann die Kommunikation zwischen zwei Personen in Intimsystemen betreffen, aber typischerweise auch die Gemeinschaft der Familie, der Freunde oder den Bekanntenkreis. Hier werden private, virtuelle „Kommunikationsräume" aufgemacht, wobei gemeinsam geteilte, gegenseitige Geheimhaltungs- und Vertrauensnormen greifen. Ein Sonderphänomen stellen Klatschgespräche dar. Klatsch-

gespräche zeichnen sich durch die Nichteinhaltung jener Normen aus, jedoch ohne, dass die betroffenen Personen darüber Kenntnis erhalten. Alsbald Kommunikation nicht mehr zwischen Ego und Alter stattfindet, sondern zwischen Ego und Tertius das Verhalten Alters mit einer eigentümlichen Vertrautheit thematisiert werden kann, kann die taktgemäße Einhaltung von Geheimhaltungsnormen durch Opportunismus eingetauscht werden. Bei der Kommunikation mit Tertius kann auf die interaktionell notwendigen Rücksichten, welche Alter gegenüber angemessen wären, wenn er denn anwesend wäre, verzichtet werden. Was in der Kommunikation mit Alter offensichtlich zum Konflikt führen würde, kann mit Tertius unter Abwesenheit von Alter konfliktfrei besprochen werden. Klatschgespräche sind zwar „private" Gespräche, allerdings kennzeichnen sie sich durch die Vermengung von Geheimhaltung und Veröffentlichung. Klatsch bedeutet, dass eine diskrete Kommunikation unter den Anwesenden stattfindet, welche jedoch indiskret ist gegenüber Nicht-Anwesenden. Die Indiskretion wird dann an sich Geheimhaltungsnormen unterzogen, welche jedoch im nächsten Klatschgespräch prinzipiell wieder aufgebrochen werden können – und so weiter.

4.1.5 Entdifferenzierung und Post-Privacy

Während der Bereich des Privaten lange Zeit als Bereich des Häuslichen, des Weiblichen und der Versorgung der (männlichen) Gesellschaftsmitglieder und der Bereich des Öffentlichen als Bereich des beruflichen, gesellschaftlichen Lebens, der Männer und der Politik galt, so ist spätestens zum Ausgang des 20. Jahrhunderts eine sukzessive Auflösung und eine vermehrte Vermischung dieser Bereiche zu beobachten. Die soziale Idee über die Trennung von Privatheit und Öffentlichkeit findet nicht zwingend ihr Ende – aber sie wird pluralisiert und in unterschiedliche Kontexte ausdifferenziert.

Dies liegt zum einen an einem Wandel gängiger Subjektmodelle. Viele Autoren, für welche der Schutz der Privatsphäre gleichsam ein Schutz persönlicher Autonomie ist, ignorieren, dass die Autonomie eines Subjekts sowie deren vermeintlich sozial isolierter Bereich der Pri-

vatsphäre ein hochartifizielles Konstrukt ist. Demgegenüber argumentieren andere Theorien, dass Personen in ihren Handlungen in hohem Maße von Faktoren ihrer sozialen Umwelt determiniert sind (exemplarisch dazu Bourdieu 1987). Dementsprechend sei auch Privatheit nicht anders zu denken als eine Sphäre, welche von diversen „systemischen" Imperativen durchzogen und bestimmt ist (Gavison 1992: 18). Ansätze, welche Privatheit als Sphäre der Handlungs- bzw. Entscheidungsfreiheit sowie der Entwicklung von Lebensführungsmöglichkeiten beschreiben, ignorierten, dass in die allermeisten „persönlichen" Entscheidungen – etwa welchen Beruf man annimmt, wie man sich ernährt, welchen Partner man heiratet, wie man sich kleidet, welche Religion man wählt etc. – weniger autonom getroffen werden als vielmehr das Ergebnis wirkmächtiger, sozialer Diskurse sind.

Zum anderen erfährt die soziale Idee über die Trennung von Privatheit und Öffentlichkeit eine Pluralisierung, da es, ausgelöst durch die massenhafte Verbreitung informationstechnischer Systeme, zu einer offensichtlichen Entgrenzung dieser Bereiche kommt. Freilich kann auch im Rahmen ebendieser Systeme Privatheit über die Kontrolle definiert werden, welche eine Person darüber ausüben kann, wer Zugang und Zugriff auf personenbezogene Daten und Informationen hat. Diese Kontrolle jedoch wird den Anwendern informationstechnischer Systeme sukzessive entzogen (Seemann 2014). Die dafür verantwortlichen Dienste, Behörden und Unternehmen – Google, Facebook, Microsoft, NSA, GCHQ etc. – suggerieren zwar, dass ein strenger Datenschutz Anwendung findet. Wer seine Daten jedoch an Dienste wie Facebook oder Google weitergibt, hat nur eingeschränkt Kontrolle darüber, was mit den Daten geschieht, wie sie ausgewertet werden (Das/Kramer 2013) und wer sie evtl. individuell einsehen kann. „In using the Internet you lose control over information about your site preferences and this loss of control often occurs without your knowledge. [...] Loss of control of information about you without your knowledge is a paradigm case of a loss of privacy" (Bowie 2013: 4113).

Neben einer durch informationstechnische Systeme verursachten Auflösung des Privaten kommt es in dieser Theorieperspektive auch zu einer in erster Linie durch die Massenmedien induzierten Veränderung der die Privatsphäre konstituierenden Handlungsnormen. Privates wird, angeregt durch die Vorbildfunktion insbesondere der Boulevardmedien, in zunehmendem Maße in der Öffentlichkeit besprochen und verhandelt. Dazu werden entsprechende Sprachspiele erlernt. „Eine Grammatik des Innern wird für die breite Bevölkerung verfügbar", schreibt Ehrenberg (2004: 134). Die Massenmedien wirken maßgeblich mit an der kollektiven Wirklichkeitskonstruktion, welche es legitimiert, dass öffentlich über Privates, etwa über psychische Probleme, gesprochen wird (Han 2012: 57 ff.; Illouz 2009; Sennet 1987). Es entsteht eine Kultur der Innerlichkeit, in welcher Ereignisse aus dem Bereich des Privaten öffentlich geteilt werden. Öffentlichkeit und Intimität verschränken sich, sodass Grenzziehungen zwischen Öffentlichkeit und Privatheit generell aufweichen.

In manchen Fällen entschließen sich Personen freiwillig dazu, Teile ihrer Privatsphäre (kontrolliert) aufzugeben und Privates in die Öffentlichkeit zu bringen oder personenbezogene Informationen in nicht-private Bereiche auszulagern. Die individuelle Bereitschaft, auf Privatheit zu verzichten, darf jedoch nicht verallgemeinert werden. Im Zuge mächtiger gesellschaftsstruktureller Veränderungsprozesse findet eine gesellschaftsweite Auflösung der Privatsphäre statt, welche als unausweichliche Folge der immer breiteren Implementierung informationstechnischer Systeme verstanden wird. Je mehr Informationen kapitalisiert und zur tauschbaren, wirtschaftlichen Ressource werden, desto mehr werden etablierte Beschränkungen zur Weitergabe von Informationen aufgelöst. „It seems quite evident that our right to informational privacy has been sacrificed for the sake of economic efficiency and other social objectives" (Spinello 1997: 9). Für Wirtschaftsunternehmen sind personenbezogene Informationen von großem Wert, schließlich erlaubt der Besitz dieser Informationen, dass sehr zielgenaue Kaufanreize gesetzt werden können.

Aus dem Zusammenspiel des Interesses der Wirtschaft an personenbezogenen Daten sowie den Möglichkeiten informationstechnischer Systeme entsteht eine Dynamik, welche die radikale Auflösung der Privatsphäre begünstigt. „[…] privacy is regularly challenged by a desire or need for greater efficiency, which has been a significant driver in the collection, aggregation, and analysis of personal information. One of the most common applications has been marketing; businesses wishing to identify suitable customers seek as much information as possible about the demographics of a population, as well as the habits, socioeconomic standing, interests, past activities, and purchasing choices of identifiable members" (Nissenbaum 2010: 109). Ging man klassischerweise immer von einer strukturellen Aufspaltung der Gesellschaft in private, nicht-ökonomisierte Bereiche einerseits und öffentliche, ökonomisierte Bereiche andererseits aus, so muss in neuester Zeit die Frage gestellt werden, inwieweit eine solche Eigensinnigkeit und Autonomie des privaten Bereichs gegenüber der Wirtschaft noch feststellbar ist. Dabei wird das Ausmaß der Entdifferenzierung im Hinblick auf Privathaushalte jedoch oftmals überschätzt. „[…] der private Bereich als Rückzugsraum und Kern individueller Autonomie wird als so bedeutsam eingeschätzt, dass er nach wie vor (gerade wegen des ‚Eindringens' von Dienstleistungsanbietern) verteidigt und aufrechterhalten wird. Der Privathaushalt erfüllt anscheinend nach wie vor eine Komplementärfunktion zur Erwerbsbereich" (Bergmann 2010: 182).

Außerhalb eines Kontextes von Privathaushalten und räumlicher Privatheit dürften sich Entdifferenzierungsbewegungen jedoch weitaus wirkmächtiger zeigen. Gerade Grenzziehungen im Hinblick auf die informationelle Privatheit fallen zunehmend diffuser aus. Konzepte, welche zwischen einer privaten und einer öffentlichen Sphäre differenzieren, sind insbesondere in Bezug auf informationstechnische Systeme obsolet. „[…] people often are not fully aware that at certain critical junctures information is being gathered or recorded. Nor do they fully grasp the implications of the informational ecology in which they choose and act" (Nissenbaum 2010: 105). Demnach kann die

Nutzung informationstechnischer Systeme, welche Informationen über eigene Emails, Kontakte, Termine, Aufenthaltsorte, Kaufgewohnheiten etc. speichern, als private Angelegenheit wahrgenommen werden, da ja bestimmte Informationen und Daten nur von einem selbst eingesehen werden können, während gleichzeitig die Benutzung ebendieser Systeme hochgradig nicht-privat ist, da die geteilten Informationen und Daten auf elektronischem Weg potentiell unkontrolliert und in Sekundenschnelle weitergereicht und verbreitet werden können (Pörksen/Detel 2012). „The problem with many of the controversial socio-technical systems [...] is that they flout entrenched informational norms and hence threaten contextual integrity" (Nissenbaum 2010: 127). Datenschutzrechtliche Bedenken gegenüber informationstechnischen Systemen werden in Form von Nichtbenutzungsempfehlungen formuliert, jedoch bleibt hier einzuräumen, dass die Nichtbenutzung bestimmter Dienstleistungen und Hardwaresysteme wie etwa einer Kreditkarte, einer Suchmaschine oder eines Handys zwangsläufig zur Folge hätte, dass große Nachteile in Kauf zu nehmen sind. Die Nichtbenutzung bestimmter Techniken führt in vielen sozialen Bereichen zu einer Zwangsentschleunigung anstehender Interaktionen und damit zu latenten oder manifesten Exklusionsbewegungen (Rosa 2005). Es besteht demnach ein gewisser struktureller Zwang, entwickelte und allgemein verbreitete informationstechnische Systeme gleichsam in Anspruch zu nehmen.

Während eine Grenzziehung zwischen dem Bereich des Privaten und dem Bereich des Öffentlichen in räumlichen Konzepten noch Sinn macht, so wird es schwierig, eine solche Grenzziehung in informationellen Konzepten unterzubringen. Eine Dichotomisierung von Informationen gemäß der Differenz von privat und öffentlich scheint mit Schwierigkeiten verbunden zu sein. Zwar gibt es Ansätze, welche dafür plädieren, dass bestehende, kontextabhängige „informational norms" berücksichtigt werden sollen, also dass Informationen aus einem bestimmten Kontext nur so weit verbreitet und geteilt sowie mit Informationen eines anderen Kontextes in Verbindung gebracht werden, wie dies allgemein sozial akzeptiert ist (Nissenbaum 2010).

Allerdings ist es bei der zunehmenden Durchdringung der Gesellschaft mit informationstechnischen Systemen stets schwieriger, zu bestimmen, wo und wie sich Kontexte situieren, wo deren Grenzen sind und wann diese überschritten werden. „Sensoren, Kameras, GPS-Apparaturen etc. [...] CCTV-Kameras überwachen den öffentlichen Raum, Handys mit Kamera und GPS sind allgegenwärtig, Kreditkartenlesegeräte erfassen beinahe alle Transaktionen und durch die Straßen fährt das Google-Street-View-Auto. Alle diese Geräte schicken immer mehr Daten auf immer größere Festplatten, in immer mehr Geräte und immer mehr ins Internet" (Seemann 2011: 75). Dabei werden die Daten immer „agiler" und immer ausgefeiltere Verknüpfungssysteme extrahieren Informationen aus größeren Datenmengen. Diese Verknüpfungssysteme sind die Bedingung dafür, dass mit der schieren Menge an Daten und Informationen überhaupt sinnvoll umgegangen werden kann. Gleichzeitig werden die Daten, welche Nutzer an unterschiedliche Internetangebote übermitteln, nicht unbedingt in der Weise genutzt, wie die Nutzer sich dies vorstellen. Über geschickte Algorithmen lassen sich in einer Weise Informationen aus Datenbanken gewinnen, welche einzelne Nutzer als nicht legitim erachten dürften (Jernigan/Mistree 2009).

In diesem Zusammenhang stehen weitere Probleme, denen sich gerade die Nutzer von Social Media-Angeboten stellen müssen. Auf Seiten der Anwender aber auch auf der der Anbieter kommt es, ausgelöst durch firmeneigene Datenauswertungsprozesse oder geheimdienstliche Interventionen, verstärkt zu einem Verlust der informationellen Kontrollierbarkeit der eingesetzten Systeme. Dieser Kontrollverlust wird unter datenschutzrechtlichen Fragen verhandelt. Den Hintergrund des Datenschutzdiskurses bieten Bemühungen um die Wahrung der Persönlichkeitsrechte sowie der Privatsphäre (Karg 2013). Während Privatsphäre in diesem Zusammenhang als konstitutives Element des Liberalismus, ja als Voraussetzung einer freiheitlichen Demokratie gesehen wird, so gibt es aber auch der „Post-Privacy"-Bewegung nahestehende Positionen, welche von einem allgemeinen Wertewandel ausgehen, in dessen Zuge es zu einer suk-

zessiven Auflösung des Privaten kommt – welche, wie oben bereits erwähnt, in bestimmten Subwelten der Netzgemeinde mitunter aktiv befürwortet wird. Dies wiederum soll anmahnen, dass datenschutzrechtliche Bedenken zumeist überbewertet werden. Unterschiedliche Auffassungen von Privatheit führen demnach zu unterschiedlichen Ansätzen, mit welcher Strenge und Intensität datenschutzrechtliche Gefährdungsanalysen getätigt werden sollen. Einigkeit besteht zwischen den Positionen insoweit, als dass erkannt wird, dass es unter den Bedingungen moderner Datenverarbeitung zu einer mehr oder minder starken Auflösung des Privaten kommt, wobei dieser Prozess jedoch nicht durchgehend negativ bewertet wird. Ganz im Gegenteil wird argumentiert, dass eine Schwächung des Wertes des Privaten letztlich zu einer transparenteren Gesellschaft führt (Brin 1998). Eine transparente Gesellschaft jedoch, so kann man entgegnen, ist eine perfekt überwachbare Gesellschaft. „Google und soziale Netzwerke, die sich als Räume der Freiheit präsentieren, nehmen panoptische Formen an. Heute vollzieht sich die Überwachung nicht, wie man gewöhnlich annimmt, als Angriff auf die Freiheit. Man liefert sich vielmehr freiwillig dem panoptischen Blick aus. Man baut geflissentlich mit am digitalen Panoptikum, indem man sich entblößt und ausstellt. Der Insasse des digitalen Panoptikums ist Täter und Opfer zugleich“ (Han 2012: 81).

4.2 Der Begriff der Privatsphäre in der Rechtswissenschaft

Christian L. Geminn

Der Privatsphäre kommt in der NSA-Affäre eine zentrale Stellung zu.[135] So beschreibt Whistleblower Snowden die Erkenntnis, die ihn zu seinen Enthüllungen motiviert habe, mit den folgenden Worten: „Ich begriff, dass sie ein System aufbauten mit dem Ziel, jegliche Privatsphäre abzuschaffen, weltweit. So dass niemand mehr elektronisch kommunizieren konnte, ohne dass die NSA diese Kommunikation sammelte, speicherte und analysierte." (Snowden, zit. in: Greenwald 2014: 75). Die Bedeutung solcher Maßnahmen der Geheimdienste fasst Greenwald pointiert zusammen: „Insbesondere für die jüngere Generation ist das Internet keine Domäne, die nur für bestimmte Zwecke benutzt wird. Es ist nicht nur unser Postamt und unser Telefon, sondern das Epizentrum unserer Welt – der Ort, wo sich praktisch das ganze Leben abspielt. Im Internet werden Freundschaften geschlossen, Lektüre und Filme ausgewählt, politische Aktionen organisiert, die privatesten Daten erstellt und gespeichert. Dort entwickeln wir unsere Persönlichkeit und unser Selbstgefühl und bringen es zum Ausdruck." (Greenwald 2014: 15).

Der Begriff der „Privatsphäre" ist ein für die Rechtswissenschaften schwer fassbarer. Er entspricht dem englischen Begriff „Privacy", der vornehmlich mit Warren und Brandeis als „Right to be le(f)t alone" beschrieben wird (Warren/Brandeis 1890: 193).[136]

[135] Eine veränderte Fassung dieses Textes wurde bereits veröffentlicht in Geminn/Roßnagel 2015.

[136] Siehe auch Olmsted v. United States, 277 U.S., 438, 478.

4.2.1 Privatsphäre in unterschiedlichen Rechtsordnungen

4.2.1.1 Privatsphäre im deutschen Recht

Im bundesdeutschen Recht taucht er nur in sehr wenigen Rechtsnormen auf, die auch vorwiegend neueren Datums sind.[137] Dem deutschen Grundgesetz ist er gänzlich fremd; ebenso wie die verwandten und häufig synonym gebrauchten Begriffe „Privatheit" und „Privatleben"[138].[139] Auch im sogenannten „Herrenchiemseer Entwurf" von 1948 kommt er nicht vor. Vielmehr durchwirkt das, was man umgangssprachlich als „Schutz der Privatsphäre" bezeichnen könnte, eine Vielzahl von grundrechtlichen Normen, insbesondere das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, das Post- und Fernmeldegeheimnis aus Art. 10 GG und die Unverletzlichkeit der Wohnung aus Art. 13 GG[140].

Auch die Verfassungen der Deutschen Demokratischen Republik kannten die Begriffe „Privatsphäre", „Privatheit" und „Privatleben" nicht. Jedoch waren auch hier Aspekte eines Privatsphäreschutzes grundsätzlich vorhanden. So erkennt Art. 37 Abs. 3 VerfDDR[141] die Unverletzlichkeit der Wohnung an, während Art. 19 Abs. 2[142] und 30

---

[137] Beispielsweise in § 62a Abs. 1 S. 4 Aufenthaltsgesetz; § 21 Abs. 2, 3 Flugunfall-Untersuchungs-Gesetz; § 2 Abs. 3 Jugendarrestvollzugsgesetz NRW. In der von Deutschland und Brasilien eingebrachten UN-Resolution gegen Datenspionage (Das Recht auf Privatheit im digitalen Zeitalter, A/C.3/68/L.45/Rev.1, angenommen am 18.12.2013) etwa wird in der englischen Sprachfassung von „Privacy" gesprochen, in der deutschen von „Privatheit".

[138] So wird der Begriff „Privacy" in Art. 12 der Allgemeinen Erklärung der Menschenrechte in der offiziellen deutschsprachigen Fassung mit „Privatleben" übersetzt. In Art. 8 Abs. 1 EMRK und Art. 7 GRCh findet sich hingegen in der jeweiligen englischen Sprachfassung der Begriff „Private Life" für „Privatleben".

[139] Auch diese beiden Begriffe tauchen nur in sehr wenigen Rechtsnormen auf, so etwa in § 1 Abs. 1 Nr. 2 des schleswig-holsteinischen Selbstbestimmungsstärkungsgesetzes und § 1 Abs. 1 Nr. 1 des baden-württembergischen Wohn-, Teilhabe- und Pflegegesetzes.

[140] Welche auch ein Abwehrrecht gegen das Anbringen von Abhöreinrichtungen in der Wohnung enthält. Siehe BVerfGE 109, 279 (309 ff.) (Großer Lauschangriff).

[141] Verfassung der Deutschen Demokratischen Republik v. 6. April 1968 in der Fassung v. 7. Oktober 1974.

[142] „Achtung und Schutz der Würde und Freiheit der Persönlichkeit sind Gebot für alle staatlichen Organe, alle gesellschaftlichen Kräfte und jeden einzelnen Bürger."

Abs. 1[143] VerfDDR die Persönlichkeit schützen. Mangels jedweder Durchsetzungsgarantien (Frotscher/Pieroth 2013: Rn. 810) und einer Gewaltenteilung hatten solche Grundrechte jedoch rein deklaratorischen Charakter und standen in krassem Gegensatz zur gesellschaftlichen Wirklichkeit eines autoritären Überwachungsstaats. Kern des Grundgesetzes ist die Menschenwürde. Demgegenüber ist der Kern der Verfassungen der DDR die Verwirklichung einer sozialistischen Gesellschaft (Gauck 1999: 214). Grundrechte werden in diesem Sinne lediglich als Instrumente zur Erreichung dieses Ziels begriffen und sind damit anders als im Grundgesetz nicht als Abwehrrechte ausgestaltet,[144] weshalb den Grundrechten auch Grundpflichten der Bürger gegenüber gestellt werden. Gauck schreibt: „Bei der Textlektüre aber konnte man den Eindruck gewinnen, die DDR habe mit den modernen Demokratien vieles gemein." (Gauck 1999: 215). Gleiches gilt auch für die DDR-Vorgängerverfassung von 1949. Auch sie erklärt: „Persönliche Freiheit, Unverletzlichkeit der Wohnung, Postgeheimnis [...] sind gewährleistet."[145] Im April 1990 wurde von einer vom Zentralen Runden Tisch eingesetzten Arbeitsgruppe ein Entwurf für eine demokratische Verfassung der DDR vorgelegt, der jedoch wenig Beachtung fand und die seit 1974 geltende Verfassung nicht mehr ablöste. Der Entwurf enthält in seinem Art. 8 Abs. 1 den Begriff „Privatheit": „Jeder hat Anspruch auf Achtung und Schutz seiner Persönlichkeit und Privatheit." Zudem enthält Art. 8 Abs. 2 des Entwurfs ein dezidiertes Datenschutzrecht.[146]

Fremd sind die fraglichen Begriffe auch der Weimarer Reichsverfassung, die einen allerdings lediglich als unverbindliche Programmsätze verstandenen Katalog von Grundrechten und Grundpflichten enthielt

[143] „Die Persönlichkeit und die Freiheit jedes Bürgers der Deutschen Demokratischen Republik sind unantastbar."

[144] Vgl. Art. 19 Abs. 3 VerfDDR v. 6. April 1968 i. d. Fassung v. 14. Oktober 1974.

[145] Art. 8 Abs. 1 S. 1 VerfDDR v. 7.10.1949.

[146] „Jeder hat das Recht an seinen persönlichen Daten und auf Einsicht in ihn betreffende Akten und Dateien. Ohne freiwillige und ausdrückliche Zustimmung des Berechtigten dürfen persönliche Daten nicht erhoben, gespeichert, verwendet, verarbeitet oder weitergegeben werden. Beschränkungen dieses Rechts bedürfen des Gesetzes und müssen dem Berechtigten zur Kenntnis gebracht werden."

(Frotscher/Pieroth 2013: Rn. 542). Deren Rechte auf Unverletzlichkeit der Freiheit der Person,[147] auf Unverletzlichkeit der Wohnung[148] und auf Unverletzlichkeit des Post-, Telegraphen- und Fernsprechgeheimnis[149] wurden schließlich im Februar 1933 mit der sogenannten „Reichstagsbrandverordnung" außer Kraft gesetzt.[150]

4.2.1.2 Privatsphäre im angloamerikanischen Recht

Fraglich ist, ob sich für den angloamerikanischen Rechtsraum bezogen auf den Begriff „Privacy" ein ähnliches Bild ergibt. Tatsächlich ist der Begriff „Privacy" im Text der Verfassung der Vereinigten Staaten von Amerika und ihrer Zusätze schlicht nicht enthalten; gleiches gilt für den Begriff „Private Life". Vielmehr finden sich einzelne Aspekte von Privatheit, die sich zu einem Schutz der Privatsphäre vor staatlichen Eingriffen summieren im First, Fourth, Fifth, Ninth und Fourteenth Amendment. Hervorzuheben ist vor allem der 1791 ratifizierte vierte Verfassungszusatz, der ein Abwehrrecht gegen unangemessene Durchsuchungen, Festnahmen und Beschlagnahmen enthält.[151] Die „Invasion of Privacy" spielt insbesondere im amerikanischen Deliktsrecht eine Rolle. Hier arbeitete Prosser 1960 vier Kategorien heraus: „1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness" (Prosser 1960: 389). Als Auslöser für die Entwicklung eines „Right to Privacy" im amerikanischen Deliktsrecht gilt ein Artikel von Warren und Brandeis aus dem Jahr 1890. Die Autoren beklagten, die Presse übertrete „in every direction the obvious bounds of property and decency. Gossip is no longer the re-

[147] Art. 114 WRV: „Die Freiheit der Person ist unverletzlich."

[148] Art. 115 WRV: „Die Wohnung jedes Deutschen ist für ihn eine Freistätte und unverletzlich."

[149] Art. 117 WRV: „Das Briefgeheimnis sowie das Post-, Telegraphen- und Fernsprechgeheimnis sind unverletzlich."

[150] § 1 der Verordnung des Reichspräsidenten zum Schutz von Volk und Staat v. 28. Februar 1933 (RGBl. I 1933, 83).

[151] „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated [...]."

source of the idle and the vicious, but has become a trade, which is pursued with industry" (Warren/Brandeis 1890: 193). Der Artikel von Warren und Brandeis stieß auch im Vereinigten Königreich eine Entwicklung hin zu einem deliktsrechtlichen „Right to Privacy" an. Jedoch bleibt umstritten, ob ein solches heute bereits als anerkannt gelten kann oder nicht.[152]

In Kanada enthalten weder die Canadian Charter of Rights and Freedoms als Teil des Constitution Act von 1982 noch deren Vorgänger, die Canadian Bill of Rights,[153] die Begriffe „Privacy" oder „Private Life". Auf Ebene der Provinzen enthält jedoch Absatz 5 der Quebec Charter of Human Rights and Freedoms ein Recht auf Achtung des Privatlebens.[154]

Insgesamt kann festgestellt werden, dass Privacy im angloamerikanischen Raum vor allem von der sogenannten „Castle Doctrine" her gedacht wird. Diese geht zurück auf einen Ausspruch von Coke aus dem Jahr 1628: „For a man's house is his castle – et domus sua cuique est tutissimum refugium" (Coke 1628: 162).[155] Die Formulierung von Art. 115 WRV, wonach die Wohnung jedes Deutschen für ihn „eine Freistätte und unverletzlich sei", deutet an, dass sich das Verständnis von Privatsphäre auch in Deutschland ausgehend von der Vorstellung der eigenen Wohnstätte als vor Eingriffen geschütztem Rückzugsraum entwickelt hat. Im Gegensatz zu Deutschland hat sich im angloamerikanischen Raum jedoch ein eigenes „Privacy Law" herausgebildet, das insbesondere in der Schaffung von „Privacy Acts" Niederschlag gefunden hat, die vornehmlich mit personenbezogenen Daten

[152] Für weitere Erläuterungen zum „Right to Privacy" im Recht des Vereinigten Königreichs siehe Geminn 2014: 300 ff.

[153] S.C. 1960, c. 44.

[154] „Every person has a right to respect for his private life."

[155] Siehe auch Semayne's Case (1604) 5 Co. Rep. 91a, All ER Rep 62: „The house of everyone is to him as his castle and fortress." 1763 illustrierte William Pitt dies sehr anschaulich in einer Parlamentsdebatte: „The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England cannot enter – all his forces dare not cross the threshold of the ruined tenement!" (zit. in Miller v. United States, 357 I.S. 301 (1958)).

befasst sind.[156] Der Begriff „Privacy Law" ist demnach häufig auf die Erhebung und Verwendung personenbezogener Daten reduziert, also „Information Privacy". Daneben lassen sich jedoch noch die Bereiche der „Bodily Privacy", der „Privacy of Communication" und der „Territorial Privacy" identifizieren.[157] Abweichend hiervon unterscheidet das britische Information Commissioner's Office zwischen „Privacy of Personal Information", „Privacy of the Person", „Privacy of Personal Behaviour" und „Privacy of Personal Communications"(Information Commissioner's Office 2007: Part I, Chapter II). In diesen abweichenden Unterteilungen zeigen sich die Schwierigkeiten beim Finden einer allgemeinen Definition des Begriffs. Ferner ist der Begriff „Privacy" eng mit dem Kampf zwischen Prominenten und Boulevardpresse verbunden.[158]

4.2.1.3 Privatsphäre im europäischen und internationalen Recht

Im Unterschied hierzu wird in den grundlegenden Dokumenten zu Menschen- und Bürgerrechten auf europäischer und internationaler Ebene die Privatsphäre direkt adressiert. So heißt es in Art. 12 AEMR:[159] „Niemand darf willkürlichen Eingriffen in sein Privatleben,[160] seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden." Es handelt sich bei dem Dokument aus dem Jahre 1948 um die erste völkerrechtliche Festsetzung eines Rechts auf Privatsphäre. Gleichartig ist Art. 17 Abs. 1 IPbpR[161] formuliert: „Niemand darf willkürlichen

[156] Kanada: Privacy Act (R.S.C., 1985, c. P-21); USA: Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a); Australien: Privacy Act 1988 (No. 119, 1988 as amended); Neuseeland: Privacy Act 1993 (No. 28).

[157] So jedenfalls die Australian Law Reform Commission (2007: 114).

[158] Privacy als ein „good highly desired by the rich and famous" (Schafer 2011: 635). Siehe beispielhaft Kaye v Robertson [1991] FSR 62; Douglas and Others v Hello! Ltd [2001] QB 967; Campbell v MGN Ltd [2004] 2 AC 457; Venables and Thompson v News Group Newspapers Ltd [2001] 2 WLR 1038; Mosley v News Group Newspapers Ltd [2008] EWHC 1777 (QB).

[159] Allgemeine Erklärung der Menschenrechte, Resolution 217 A (III) der Generalversammlung vom 10.12.1948.

[160] In der englischen Sprachfassung: „Privacy".

[161] Internationaler Pakt über bürgerliche und politische Recht v. 19. Dezember 1966. Von der Bundesrepublik Deutschland wurde der Pakt im Jahre 1973 ratifiziert: BGBl. 1973 II 1553.

oder rechtswidrigen Eingriffen in sein Privatleben,[162] seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden." Art. 8 Abs. 1 EMRK gesteht jeder Person ein „Recht auf Achtung ihres Privat- und Familienlebens,[163] ihrer Wohnung und ihrer Korrespondenz" zu. Art 7 GRCh ist nahezu wortgleich formuliert[164] und enthält somit ebenfalls ein Recht auf Achtung des Privat- und Familienlebens.[165] Zudem enthält die Charta als Besonderheit in Art. 8 Abs. 1 GRCh ein eigenständig aufgeführtes Recht auf den Schutz personenbezogener Daten als lex specialis zu Art. 7 GRCh.

Fraglich ist, was unter dem Begriff des Privatlebens in AEMR, IPbpR, EMRK und GRCh gemeint ist. Bezogen auf die EMRK schreibt Bernsdorff: „Der Begriff des Privatlebens entzieht sich dem Versuch einer allgemeingültigen Definition. Jedenfalls versteht der EGMR unter dem Recht auf Achtung des Privatlebens mehr als ein bloßes ‚right to be let alone'. In einem weiten Sinne sind alle Bereiche des Lebens, die andere nicht betreffen, der Privatsphäre zuzuordnen." (Bernsdorff, in: Meyer 2014: Art. 7 GRCh, Rn. 19).[166] Damit wird klar, dass Art. 8 Abs. 1 EMRK anders als Art. 2 Abs. 1 GG keine allgemeine Handlungsfreiheit ermöglichen soll (Bernsdorff, in: Meyer 2014: Art. 7 GRCh, Rn. 15). Dennoch handelt es sich beim Recht auf Achtung des Privatlebens um ein weit gefasstes Grundrecht zu dem neben dem Schutz persönlicher Daten auch der Schutz der physischen wie psychischen Integrität einer Person gehört, soweit nicht bereits durch andere Rechte erfasst.[167]

---

[162] Auch hier verwendet die englische Sprachfassung den Begriff „Privacy".

[163] Englisch: „private and family life".

[164] Allein das Wort „Korrespondenz" wurde durch den Begriff der „Kommunikation" ersetzt. Die Ersetzung ist lediglich der fortschreitenden technischen Entwicklung geschuldet (Dok. CHARTE 4487/00 CONVENT 50: 10).

[165] Auch hier englisch: „private and family life".

[166] So auch Meyer-Ladewig (2011: Art. 8 EMRK, Rn. 7): „Der Begriff wird umfassend verstanden und ist einer abschließenden Definition nicht zugänglich."

[167] EGMR, Fall S und Marper vs. Vereinigtes Königreich, 4.12.2008 – 30562/04 und 30566/04, DÖV 2009, 209.

4.2.2 Privatsphäre in der deutschen Rechtspraxis

In der Rechtspraxis in Deutschland spielen die Begriffe „Privatheit" und „Privatleben" kaum eine Rolle, wohl aber der Begriff der „Privatsphäre". Er findet insbesondere dann Anwendung, wenn es um die Feststellung der Intensität der Rechtfertigungsbedürftigkeit eines Eingriffs in das allgemeine Persönlichkeitsrecht geht.

4.2.2.1 Das allgemeine Persönlichkeitsrecht

Bis zur Volkszählungsentscheidung des Bundesverfassungsgerichts (BVerfGE 65, 1) wurde hierzu in aller Regel auf die sogenannte „Sphärentheorie" (Di Fabio, in: Maunz/Dürig 2015: Art. 2 GG, Rn. 158 ff.) zurückgegriffen. Das allgemeine Persönlichkeitsrecht ist eine „Besonderheit des deutschen Verfassungsrechts" (Hufen 2014: § 11, Rn. 28). Es handelt sich um ein unbenanntes Freiheitsrecht, um ein „Grundrecht im Grundrecht" (Di Fabio, in: Maunz/Dürig 2015: Art. 2 GG, Rn. 127). Es wurde aus dem Recht auf freie Entfaltung der Persönlichkeit und der Würde des Menschen entwickelt, ist jedoch primär in Art. 2 Abs. 1 GG verankert, während Art. 1 Abs. 1 einen „uneinschränkbaren Kern des Rechts fixiert" (Jarass/Pieroth 2012: Art. 2 GG, Rn. 36).[168] Sein Ziel ist der Schutz der Integrität der menschlichen Persönlichkeit. In Abgrenzung zur allgemeinen Handlungsfreiheit schützt das allgemeine Persönlichkeitsrecht „das Sein der Person im Unterschied zum Tun" (Murswiek, in: Sachs 2014: Art. 2 GG, Rn. 59).[169]

Der sachliche Schutzbereich des allgemeinen Persönlichkeitsrechts ist bei Beeinträchtigungen der engeren persönlichen Lebenssphäre, der Selbstbestimmung und der Grundbedingungen der Persönlichkeitsentfaltung eröffnet (Di Fabio, in: Maunz/Dürig 2015: Art. 2 GG, Rn. 147). Damit liegt die Aufgabe des Grundrechts darin, „die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen" (BVerfGE 54, 148

[168] „Sitz des Grundrechts" ist jedoch Art. 2 Abs. 1 GG (Starck, in: v. Mangoldt/Klein/Starck 2010: Art. 2 Abs. 1 GG, Rn. 57).

[169] Siehe auch Starck, in: v. Mangoldt/Klein/Starck 2010: Art. 2 Abs. 1 GG, Rn. 86.

(153)).[170] Kern des Grundrechts sind der Schutz der Privatsphäre und der Schutz der Selbstdarstellung. Auf der einen Seite garantiert das allgemeine Persönlichkeitsrecht jedem Menschen einen autonomen Bereich zur privaten Lebensgestaltung und zur individuellen Entfaltung. Auf der anderen Seite soll der Einzelne „selbst darüber befinden dürfen, wie er sich gegenüber Dritten oder der Öffentlichkeit darstellen will, was seinen sozialen Geltungsanspruch ausmachen soll und ob oder inwieweit Dritte über seine Persönlichkeit verfügen können, indem sie diese zum Gegenstand öffentlicher Erörterung machen" (BVerfGE 63, 131 (142)).[171] Es geht also einerseits um die „Abgrenzung eines autarken Privatbereichs", andererseits um den „Schutz vor Einsicht- oder Kenntnisnahme durch Dritte" (Dreier, in: Dreier 2013: Art. 2 I GG, Rn. 71).

Eingriffe in das Grundrecht können rechtliche wie faktische Einwirkungen durch Grundrechtsverpflichtete sein. Erfasst wird auch die herabwürdigende Behandlung (Jarass/Pieroth 2014: Art. 2 GG, Rn. 53). Die Intensität der Rechtfertigungsbedürftigkeit eines Eingriffs richtet sich nach der Sphärentheorie danach, auf welchen Lebensbereich eines Menschen der Eingriff gerichtet ist. Dazu wird eine Einteilung in „Sphären unterschiedlicher Privatheit und damit auch unterschiedlicher Schutzbedürftigkeit" (Hufen 2014: § 11, Rn. 4)[172] vorgenommen. Die innerste Sphäre beinhaltet die Identität, Intimsphäre und körperliche Integrität eines Menschen.[173] Sie ist absolut unantastbar, denn sie repräsentiert den Würdekern des Grundrechts.[174]

---

[170] Vgl. BVerfGE 72, 155 (170); BVerfGE 96, 56 (61).

[171] Vgl. BVerfGE 35, 202 (220); BVerfGE 54, 148 (155).

[172] BVerfGE 6, 32 (41); 35, 202 (220); 80, 367 (373 f.); kritisch Starck, in: v. Mangoldt/Klein/Starck 2010: Art. 2 Abs. 1 GG, Rn. 16: „Diese Unterscheidung ist dogmatisch unklar und praktisch nicht verwertbar. Denn es liegt allzu nahe, im Einzelfall den absolut geschützten Intimbereich dann nicht als berührt anzusehen, wenn eine Einschränkung für notwendig erachtet wird."

[173] Siehe zur Differenzierung der Begriffe „Intimsphäre" und „Kernbereich" auch Desoi/Knierim 2011: 398.

[174] Mallmann hingegen bezeichnet die Vorstellung von der absolut unantastbaren innersten Sphäre jedoch als „illusorisch" und verweist hierzu auf die Klärung von Sachverhalten im Strafprozess und die Meldepflicht bei bestimmten Krankheiten (heute geregelt in § 6 Infektionsschutzgesetz) (Mallmann 1977: 25).

Die zweite Sphäre ist die Privatsphäre, also der engere persönliche Lebensbereich. Als privat sind alle Angelegenheiten einzustufen, die nicht in die Öffentlichkeit getragen werden sollen.[175] Hier sind Eingriffe im Gegensatz zur innersten Sphäre durchaus möglich, jedoch stärker rechtfertigungsbedürftig als solche Eingriffe, die in die dritte Sphäre, die Sozialsphäre fallen. Diese beinhaltet das Ansehen des Einzelnen in der Öffentlichkeit. Wo die Grenze zwischen Privatsphäre und Sozialsphäre verläuft, lässt sich nur schwer definieren. Befindet sich eine Person an einem Ort, an dem sie unter einer Vielzahl anderer Menschen ist, so kann jedenfalls nicht von Privatsphäre gesprochen werden: „Wo die Grenzen der geschützten Privatsphäre außerhalb des Hauses verlaufen, lässt sich nicht generell und abstrakt festlegen. Sie können vielmehr nur aufgrund der jeweiligen Beschaffenheit des Ortes bestimmt werden, den der Betroffene aufsucht. Ausschlaggebend ist, ob der Einzelne eine Situation vorfindet oder schafft, in der er begründetermaßen und somit auch für Dritte erkennbar davon ausgehen darf, den Blicken der Öffentlichkeit nicht ausgesetzt zu sein. […] Plätzen, an denen sich der Einzelne unter vielen Menschen befindet, fehlt es von vornherein an den Voraussetzungen des Privatsphärenschutzes […] Sie können das Rückzugsbedürfnis nicht erfüllen." (BVerfGE 101, 361 (384)).

Das Bundesverfassungsgericht hat unterdessen zwar Kriterien für die Einstufung eines Eingriffs entwickelt – maßgeblich sind danach der Geheimhaltungswillen, der höchstpersönliche Charakter eines Sachverhalts und der Charakter und die Bedeutung seines Inhalts[176] – letztlich hängt die Einstufung aber von den Umständen des zu entscheidenden Einzelfalls ab.[177] Damit verschwimmt auch die Grenze zwischen innerster Sphäre und Privatsphäre: „Fasst man die Recht-

[175] „Die Privatsphäre ist der Bereich, den der Einzelne für die Öffentlichkeit unzugänglich hält, in den er nur Menschen seines Vertrauens hineinlässt" (Starck, in: v. Mangoldt/Klein/Starck 2010: Art. 2 Abs. 1 GG, Rn. 173).

[176] Vgl. BVerfGE 80, 367 (374 f.).

[177] Di Fabio, in: Maunz/Dürig 2015: Art. 2 GG, Rn. 161. Kritiker sehen in diesen Kriterien jedoch eine Aufweichung oder sogar eine Abkehr von der Sphärentheorie; siehe beispielhaft das Sondervotum zum sogenannten Tagebuchfall: BVerfGE 80, 367 (382).

sprechung des Bundesverfassungsgerichts zusammen, ist nicht mehr allein der äußerlich erkennbare, vom Verfasser bestimmte intime Verwendungszweck einer Aufzeichnung ausschlaggebend für die Zuordnung zum unantastbaren Intimbereich, sondern die Sozialgerichtetheit des Inhalts eines Gesprächs oder einer persönlichen Aufzeichnung und dabei wiederum maßgeblich die Wertigkeit der dadurch gefährdeten Belange der Allgemeinheit." (Di Fabio, in: Maunz/Dürig 2015: Art. 2 GG, Rn. 162).

Die Rechtfertigung eines Eingriffs kann zunächst durch Einwilligung erfolgen. Jedoch: „Die Wirksamkeit der Einwilligung entfällt, wenn dem Grundrechtsträger auf Grund einer Zwangslage keine wirkliche Wahlfreiheit verbleibt." (Di Fabio, in: Maunz/Dürig 2015: Art. 2 GG, Rn. 229).[178] Ferner greift der Gesetzesvorbehalt des Art. 2 Abs. 1 GG, allerdings nur für Eingriffe in die Sozial- und Privatsphäre, denn die innerste Sphäre ist, wie beschrieben, unantastbar: „Geht es allerdings um den Persönlichkeitskern, der zugleich durch Art. 1 Abs. 1 GG geschützt ist, ist jeder Eingriff verboten und kein öffentlicher Belang gewichtig genug, um selbst auf gesetzlicher Grundlage einen Eingriff zu rechtfertigen." (Hufen 2014: § 11, Rn. 23).[179] Zudem kann ein Eingriff durch andere Grundrechte als verfassungsimmanente Schranken gerechtfertigt sein, jedoch ebenfalls nur, wenn nicht die innerste Sphäre betroffen ist. Grundsätzlich gilt, dass Beschränkungen des allgemeinen Persönlichkeitsrechts unter Wahrung des Verhältnismäßigkeitsprinzips und unter Achtung des Würdekerns zum Schutz öffentlicher Interessen in Kauf genommen werden müssen (BVerfGE 67, 1 (41); 71, 183 (196)).

---

[178] Vgl. zum Beispiel der Einwilligung im Falle von Videoüberwachung BVerfG, Urteil vom 23.2.2007, 1 BvR 2368/06, DÖV 2007, 606, Rn. 40: „Von einer einen Eingriff ausschließenden Einwilligung in die Informationserhebung kann selbst dann nicht generell ausgegangen werden, wenn die Betroffenen aufgrund einer entsprechenden Beschilderung wissen, dass sie im räumlichen Bereich der Begegnungsstätte gefilmt werden. Das Unterlassen eines ausdrücklichen Protests kann nicht stets mit einer Einverständniserklärung gleichgesetzt werden."

[179] Vgl. Starck, in: v. Mangoldt/Klein/Starck 2010: Art. 1 Abs. 1 GG, Rn. 38; BVerfGE 75, 369 (380): „Soweit das allgemeine Persönlichkeitsrecht allerdings unmittelbarer Ausfluss der Menschenwürde ist, wirkt diese Schranke absolut ohne die Möglichkeit eines Güterausgleichs."

4.2.2.2 Die informationelle Selbstbestimmung

Das Bundesverfassungsgericht hat mehrfach die Offenheit der Norm für zukünftige Entwicklungen betont.[180] Es überrascht deshalb nicht, dass mit fortschreitenden technischen Neuerungen weitere Ausprägungen des allgemeinen Persönlichkeitsrechts entwickelt wurden. Eine dieser Ausprägungen, das Recht auf informationelle Selbstbestimmung, brachte mit sich eine Abkehr von der Sphärentheorie soweit der Schutzbereich des seit dem Volkszählungsurteil anerkannten Rechts betroffen ist. Das Recht auf informationelle Selbstbestimmung schützt vor der unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten (BVerfGE 67, 100 (142); 77, 1 (46)). Es „gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" (BVerfGE 65, 1 (43)) und damit „selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden" (BVerfGE 65, 1 (42)).[181] Denn: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden." (BVerfGE 65, 1 (43)).

Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist auf den Umgang mit personenbezogenen Daten beschränkt (Jarass/Pieroth 2014: Art. 2 GG, Rn. 43). Maßgeblich ist hier die Definition des § 3 Abs. 1 BDSG (Di Fabio, in: Maunz/Dürig 2015: Art. 2 GG, Rn. 175): „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person." Auf die Qualität des Datums kommt es dabei nicht an. Vielmehr stellt das Bundesverfassungsgericht fest, dass es gerade durch den technischen Fortschritt und der damit verbundenen Möglichkeit des Sammelns und des Kombinierens von Daten

[180] BVerfGE 54, 148 (153 f.); 65, 1 (41); 72, 155 (170); 79, 256 (268).

[181] BVerfGE 103, 23 (33); 113, 29 (46); vgl. Dreier, in: Dreier 2013: Art. 2 I GG, Rn. 79.

„kein belangloses Datum“ mehr gibt (BVerfGE 65, 1 (45)), „denn auch eine für sich unerhebliche Information kann in Verknüpfung mit anderen Daten Rückschlüsse auf den Betroffenen, seinen Lebensweg und seine Persönlichkeit zulassen“ (Dreier, in: Dreier 2013: Art. 2 I GG, Rn. 81). Einzelinformationen können heute zu einem „weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden“ (BVerfGE 65, 1 (42)). Unterschiedliche Sphären existieren beim Recht auf informationelle Selbstbestimmung mithin nicht; vielmehr ist jede Information über den Einzelnen in gleichem Maße schutzwürdig (Dreier, in: Dreier 2013: Art. 2 I GG, Rn. 93).

Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt in jeder fremdbestimmten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (BVerfGE 100, 313 (366)). Kein Eingriff soll lediglich dann vorliegen, „wenn Daten nach der Erfassung technisch spurenlos und anonym ausgesondert werden“ (Jarass/Pieroth 2012: Art. 2 GG, Rn. 53).[182] Für einen Eingriff ist stets eine hinreichend bestimmte gesetzliche Grundlage erforderlich, die den Zweck der Maßnahme genau festlegt (Di Fabio, in: Maunz/Dürig 2015: Art. 2 GG, Rn. 182). Beschränkungen der informationellen Selbstbestimmung bedürfen also einer „(verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht“ (BVerfGE 65, 1 (44)). Ferner ist zu beachten, dass jeder Umgang mit personenbezogenen Daten einen separaten Eingriff in die informationelle Selbstbestimmung darstellt.

4.2.3 Vergleich „Privatsphäre“ und „informationelle Selbstbestimmung“

Mit dem Volkszählungsurteil und der Anerkennung des Rechts auf informationelle Selbstbestimmung ging der Anwendungsbereich der

[182] BVerfGE 120, 378 (399). Diese Ansicht muss jedoch unter anderem mit Blick auf die potentiell verhaltenssteuernde Wirkung auch lediglich technikbedingter Erfassung kritisch gesehen werden.

Sphärentheorie stark zurück. Er ist heute weitgehend auf „Paparazzi-Fälle" reduziert, in denen sich das allgemeine Persönlichkeitsrecht und die Pressefreiheit gegenüberstehen, in denen also Prominente gegen die Veröffentlichung bestimmter Informationen über ihr Leben vorgehen wollen oder Schadensersatz fordern. Denn das allgemeine Persönlichkeitsrecht ist in seiner zivilrechtlichen Ausprägung als „sonstiges Recht" im Sinne des § 823 Abs. 1 BGB anerkannt,[183] womit die Privatsphäre[184] neben der Intim-, Geheim- und Sozialsphäre vor allem im deutschen Deliktsrecht eine Rolle spielt.[185]

Insgesamt ist festzuhalten, dass hinter der Sphärentheorie und der informationellen Selbstbestimmung zwei gänzlich unterschiedliche dogmatische Ausgangspunkte stehen. Zentrale Frage ist dabei, in welcher Weise das jeweilige Schutzgut bestimmt wird. Die Sphärentheorie folgt einem ordnungsorientierten, paternalistischen Ansatz. Hier legen Dritte, nämlich der Staat, die Justiz und auch die Rechtswissenschaften fest, was privat ist. Diese Vorstellung wird gleichsam der Gesellschaft aufoktroyiert. Ausgangspunkt dieses Ansatzes ist mithin der Staat; er legt die Grenzen der Privatheit fest.

Demgegenüber steht hinter der informationellen Selbstbestimmung ein freiheitsorientierter Ansatz. Hier darf der einzelne Bürger selbst festlegen, was er als schützenswert erachtet. Da mithin das Individuum zum Ausgangspunkt wird, kann es „die eine" Privatheit nicht geben. Ausfluss hiervon ist das Verbotsprinzip bezüglich der Verarbeitung personenbezogener Daten. Die Verarbeitung ist nur dann erlaubt, wenn eine Einwilligung hierzu vorliegt. Damit gesellschaftliches Zusammenleben trotzdem möglich bleibt, kann das Recht zudem

---

[183] Seit 1954: BGHZ 13, 334; BGHZ 20, 345; BGHZ 24, 200.

[184] „Die Privatsphäre umfasst denjenigen sowohl thematisch wie räumlich zu bestimmenden Lebensbereich, zu dem andere Menschen nach der sozialen Anschauung nur mit Zustimmung des Betroffenen Zugang haben, insbesondere das Leben im häuslichen oder Familienkreis und das sonstige Privatleben im eigenen häuslichen Bereich sowie je nach den Umständen auch außerhalb" (Sprau, in: Palandt 2014: § 823 BGB, Rn. 87).

[185] Daneben hat der BGH auch bereits die Begriffe „Eigensphäre" (BGHZ 27, 284, 288), „Individualsphäre" (BGHZ 26, 349, 355) und „persönliche Sphäre" (BGHZ 36, 77, 80) benutzt. Siehe auch Mallmann 1977: 25.

vom Staat eingeschränkt werden. Dann ist eine Verarbeitung auch aufgrund der so geschaffenen Erlaubnisnorm zulässig. Insgesamt handelt es sich bei der informationellen Selbstbestimmung um den vorzugswürdigen Ansatz.

Das Fortschreiten der technischen Entwicklung und insbesondere die weiter wachsende Fähigkeit zur Sammlung und Auswertung gigantischer Datenmengen sowie die Fähigkeit zur Überwachung von Datenströmen und Kommunikation bringen neue Gefahren für die Privatsphäre mit sich. Der in der Rechtswissenschaft vorherrschende Ansatz, wie diesen Bedrohungen zu begegnen ist, liegt in der Schaffung technologisch flexibler Regelungen zum Schutz personenbezogener Daten, deren Grundlage das Verbot mit Erlaubnisvorbehalt ist. So wurde bereits 1970 in Hessen das älteste formelle Datenschutzgesetz der Welt erlassen (Simitis, in: Simitis 2014: Einf. BDSG, Rn. 1), während sich das Bundesverfassungsgericht deutlich gegen eine Totalüberwachung des Bürgers ausgesprochen hat.[186]

Dem gegenüber stehen Stimmen, insbesondere in den USA, die einen anderen Ansatz verfolgen, der eine totale Erfassung des Bürgers zulassen möchte. So forderte Rubenfeld Anfang 2014 eine „New Jurisprudence of Anonymity". Danach soll das Sammeln und Speichern von Daten („Data Mining") und die Zuordnung zu einem Pseudonym noch kein Eingriff in die Rechte der Bürger sein, sondern erst das bedarfsorientierte „Anfassen" der Daten durch staatliche Behörden etwa zur Verbrechensaufklärung.[187] Das Bundesverfassungsgericht hat eine breite Erfassung am Beispiel des Scannens von Kfz-Kennzeichen hingegen lediglich dann für zulässig erklärt, wenn nach

[186] Siehe beispielhaft: BVerfGE 27, 1 (6); 65, 1 (42 f.); 109, 279 (323); 112, 304 (319 f.); 115, 320 (347).

[187] „Privacy was key when the question was whether, or how much of, our private lives could be monitored or recorded. That train has left the station. Today, most of us allow a great deal of our lives to be monitored and recorded – whenever we use a search engine, for example, or buy something online. Even the content of our private communications, such as e-mails and chats, is now routinely exposed to and stored by people at Facebook or Google. The key question isn't how to keep information about us from getting out into the world; it's how that information can be used" (Rubenfeld 2014).

einer automatisierten Auswertung die erhobenen Daten sofort automatisiert wieder gelöscht werden und gleichzeitig die Streubreite der Maßnahme begrenzt ist (BVerfGE 120, 378). Der von Rubenfeld verfolgte Ansatz ist mit deutschem Recht mithin erkennbar inkompatibel.

In der Gesamtschau zeigt sich, dass die Nutzung der Begriffe „Privatsphäre“, „Privatheit“ und „Privatleben“ gerade im deutschen Rechtsraum mit starken Problemen behaftet ist. Als Rechtsbegriffe tauchen sie im deutschen Recht kaum auf. Insbesondere besteht keine Deckungsgleichheit zwischen allgemeinem Persönlichkeitsrecht und Schutz der Privatsphäre. Vielmehr werden die Begriffe auf Ebene der Grundrechte in einzelne Teilaspekte aufgebrochen, die sich rechtlich besser fassen lassen wie etwa die Unverletzlichkeit der Wohnung. Tatbestände, die nicht diesen Teilaspekten unterfallen, aber dennoch als von der Privatsphäre erfasst angesehen werden, werden vom allgemeinen Persönlichkeitsrecht aufgefangen. Hier adressiert die Sphärentheorie den Begriff der „Privatsphäre“ direkt, deren Bedeutung jedoch auf einen eng begrenzten rechtlichen Raum reduziert ist. Möglich ist jedoch, dass die Bedeutung der Begriffe durch ihre Verwendung in europäischen oder internationalen Rechtsakten in Zukunft ansteigen wird.

Für die untersuchte Arena und die aktuelle Diskussion folgt daraus eine gewisse begriffliche Sprachbarriere, aus der wiederum eine reduzierte Anschlussfähigkeit des rechtswissenschaftlichen Diskurses resultiert.

4.3 Vertrauen ins Netz

Thilo Hagendorff

Die durch die Snowden-Enthüllungen losgetretene, breite Thematisierung bislang geheimer nachrichtendienstlicher Tätigkeiten in der Öffentlichkeit hat die Vorstellungen darüber, welche Bedeutung das Internet bei der staatlichen Überwachung spielt, drastisch verändert. Es besteht nun ein breites Wissen darüber, dass das technisch Mögliche zur Überwachung und Ausspähung der digitalen Welt weitestgehend ausgeschöpft wird. Dies erwirkt einen Vertrauensverlust innerhalb der Bevölkerung, welcher die Geheimdienste, die Regierungen insgesamt, aber auch die Internetkonzerne betrifft. Die Vertrauenskrise ist handfester Art, wie etwa an den monetären Verlusten amerikanischer Cloud-Anbieter zu erkennen ist, aber auch auf der Ebene der politischen und wirtschaftlichen Diskursführung zu lokalisieren. Eben weil die Snowden-Enthüllungen ein starkes Misstrauen gegenüber den Akteuren der Überwachung initiiert haben, bedarf es eines Ausgleichs des Vertrauensverlusts, welcher insbesondere über die Anwendung einer starken „Vertrauensrhetorik“ geführt wird (Krempl 2014). „Vertrauen [kommt] als eine Gefühlshaltung daher, die mit zwischenmenschlicher Wärme, Harmonie, Eintracht, Verständnis, Anerkennung, Achtsamkeit assoziiert wird." (Frevert 2013: 218) Vertrauensverhältnisse und das rhetorische Markieren von Vertrauen sind demnach zentraler Bestandteil „reibungslos“, produktiv und kooperativ funktionierender Interaktionen, wie sie sich innerhalb sozialer Welten, aber auch in der Beziehung ebendieser untereinander manifestieren. Tatsächlich aber spielt Vertrauen, gemessen an makrosoziologischen Kontexten, kaum eine Rolle – schließlich kann, spätestens nach Bekanntwerden des Ausmaßes und der Eingriffstiefe der geheimdienstlichen Überwachungstätigkeiten, weder davon gesprochen werden, dass Regierungen der Bevölkerung allgemein vertrauen, noch, dass die Bevölkerung der Welt des Staates allgemein

vertraut. Es geht um eine wachsende „Misstrauenskultur“, welche Meinungsbilder, politische Entscheidungen und Legitimitätsniveaus beeinflusst.

Doch wie kann Vertrauen als soziologisch zu identifizierendes Phänomen überhaupt theoretisch umrissen und einer sozialwissenschaftlichen Analyse zugeführt werden? Abstrakt gesagt dient Vertrauen dazu, eine soziale Ordnungsleistung zu erbringen. Es geht darum, dass soziale Akteure prinzipiell unberechenbar sind. Diese Unberechenbarkeit bedeutet eine im wahrsten Sinne des Wortes ungeheure Komplexität, auf welche man sich einstellen müsste – gäbe es kein soziales Vertrauen. „Auf der Grundlage sozial erweiterter Komplexität kann und muß der Mensch wirksame Formen der Reduktion von Komplexität entwickeln“, schreibt Luhmann (1973: 7). Vertrauen markiert einen Schnitt zwischen dem Sicheren und Unsicheren, Fremden oder Unheimlichen. Vertrauen erlaubt es, Unsicherheitsmomente zu unterdrücken, stabile Erwartungen aufzubauen und Risiken ausblenden zu können. Das bedeutet nicht, dass Vertrauen an sich nicht ein riskantes Unterfangen wäre. Schließlich kann der Vorteil, welchen man aus einem Vertrauensverhältnis zieht, im Fall eines Vertrauensbruchs mit hoher Wahrscheinlichkeit nicht den Nachteil aufwiegen, welchen man dadurch erleidet. Vertrauenserweise sind immer zu einem gewissen Grad leichtsinnig. Vertrauen reduziert soziale Komplexität zum Preis der Übernahme eines Risikos. Entscheidend ist, welche Schäden im Fall des Vertrauensbruchs anfallen und wie diese „absorbiert“ werden können.

Die Schadenshöhe steht in Beziehung zum Vertrauensobjekt. Geht es um das Vertrauen in eine bestimmte Person, in eine Gruppe von Personen oder in abstrakte Leistungsgefüge, Institutionen oder Infrastrukturen? Je nach Akteur gehen der Vertrauensbeziehung unterschiedliche Lernprozesse voraus, in Laufe derer anhand von Informationen über den Akteur dessen Vertrauenswürdigkeit bewertet und entsprechend Vertrauen aufgebaut wird. Die Vertrauenswürdigkeit eines Akteurs kann dabei auf der Grundlage dreier Aspekte eingeschätzt werden. Es können die Kompetenzen oder Fähigkeiten eines

sozialen Akteurs bewertet werden, seine Intentionen oder seine moralische Integrität (Mayer et al. 1995: 715). Das Sammeln von Informationen über die Vertrauenswürdigkeit eines sozialen Akteurs fällt jedoch immer lückenhaft aus. Man ist nie vollständig informiert und hat daher nie absolute Sicherheit über die Zuverlässigkeit des Akteurs.

Je stärker wechselseitige Abhängigkeiten ausgeprägt sind, desto einfacher können sich Vertrauensverhältnisse entwickeln. Ausgewogene Abhängigkeitsbeziehungen ermöglichen eher, dass Vertrauensbrüche sanktioniert werden können – und machen sie so unwahrscheinlicher. Allerdings sind gegenseitige Interdependenzen zwischen Personen und abstrakten sozialen Strukturen in der Regel kaum auszumachen – zumal auch Schuldzurechnungen und Sanktionsmöglichkeiten für Vertrauensbrüche hier nur schwer ausgemacht werden können. Man vertraut schlicht dem Funktionieren undurchschaubarer, hochkomplexer Systeme. Ist man gar auf die Systeme angewiesen, bekommt das Vertrauen einen eigentümlich zwanghaften Charakter.

Vertrauensverhältnisse können immer auch enttäuscht werden. Vertrauen wird dann zu Misstrauen. Sowohl das Aufbauen von Vertrauensverhältnissen als auch die Entstehung von Misstrauen folgt subjektiven Prozessen einer bestimmten Erlebnisverarbeitung. Man orientiert sich an Schlüsselerlebnissen. Diesen wird eine besondere Relevanz zugesprochen, sie werden zu Gründen, um Vertrauen oder Misstrauen zu rechtfertigen. Die Frage, welche dann aufkommt, ist eine ethische: Unter welchen Umständen soll man Vertrauen schenken? Ist Vertrauen nur dann richtig, wenn es hinreichend gerechtfertigt ist? Hierbei fällt auf, dass Vertrauen, welches auf sicheren Erwartungen beruht, viel instabiler ist als Misstrauen. Erwartungen können rasch enttäuscht werden, während erlittene Enttäuschungen nur sehr langsam wieder durch sichere Erwartungshaltungen überlagert werden können.

Jenseits einer systemtheoretischen, eher mikrosoziologisch orientierten Begriffsklärung steht der Vertrauensbegriff im Kontext der politischen Kulturforschung, welche sich auf einer eher makrosoziologi-

schen Ebene mit nichts geringerem als der „Überlebensfähigkeit“ demokratisch verfasster Gesellschaften beschäftigt. Dabei hat Vertrauen die Funktion, Handlungszusammenhänge produktiver zu machen und Kooperationen – nicht allein solche politischer Art – zu erleichtern. Neben der Dimension der Legitimität steht die Dimension des Vertrauens. Beide unterstützen politische Operationen. Legitimität erwächst aus dem Abgleich eigener Wertvorstellungen und Interessen mit politischen Entscheidungen. Vertrauen wiederum resultiert aus positiven Erfahrungen mit politischen Leistungen. Ein hohes Maß an sozialem, also generalisiertem Vertrauen fördert die Bereitschaft zur politischen Kooperation. Die Akzeptabilität politischer Aushandlungsprozesse, Entscheidungen und Ziele korreliert mit dem Vertrauensniveau, welches der Politik seitens der Bevölkerung entgegen gebracht wird. Ein hohes Vertrauensniveau fördert eine „lebendige“ Zivilgesellschaft. „Vertrauen äußert sich demnach in der Überzeugung, dass die eigenen Interessen in der Politik Resonanz erfahren, ohne dass dies durch persönlichen Einsatz überwacht und kontrolliert werden muss“ (Frings 2010: 44). Vertrauen spart, allgemein gesprochen, Ausgaben ein, insbesondere Kontroll- und Prüfausgaben.

Inwiefern können nun die beschriebenen Ansätze zum Phänomen Vertrauen im Kontext der Frage um das „Vertrauen ins Netz“ zur Anwendung kommen? Das „Internetvertrauen“ spielt eine wichtige Rolle, schließlich kann kaum ein Internetnutzer gänzlich verfolgen und kontrollieren, in welcher Weise sich Daten durch das Internet bewegen und an welchen Stellen sie in unzulässiger Weise kopiert oder manipuliert werden. „Indem das Internet auf jeder Ebene untergraben wurde, um es zu einer großen, vielschichten und robusten Überwachungsplattform zu machen, hat die NSA einen wesentlichen Gesellschaftsvertrag gebrochen. Die Unternehmen, die die Infrastruktur unseres Internets bauen und pflegen, die Unternehmen, die Hard- und Software herstellen und an uns verkaufen, oder die Unternehmen, die unsere Daten hosten: Wir können ihnen nicht länger vertrauen, dass sie moralische Ordner des Internets sind“ (Schneier 2013: 217). Anscheinend geht es bei der Debatte um das „Vertrauen

ins Netz“ um ein asymmetrisches Systemvertrauen in Akteure insbesondere aus der Welt der Ökonomie und der Welt des Staates, welches deutlich von einem psychologisch gesteuerten, typischerweise symmetrisch bzw. gegenseitig gelagerten interpersonalen Vertrauen differenziert werden muss. Während sich das Vertrauen in Personen über die Bewertung des Verhaltens einer potentiell vertrauenswürdigen Person generiert, entwickelt sich Systemvertrauen über die Beobachtung anhaltend regelbasiert und kontrolliert ablaufender Prozesse in Organisationen insbesondere in den erwähnten Welten. Dabei führt speziell die Nutzung des Internets „für Kooperationsprozesse zu Entbettungen aus dem [sic!] sozialen Bezügen mit Kopräsenz und einem physischen Kontext, und damit zu spezifischen Vertrauensproblematiken“ (Kumbruck 2012: 178).

Vertrauen hat die Funktion, Kooperationen zu erleichtern. Sinkt das Vertrauensniveau, so steigen Unsicherheitsmomente an, welche wiederum Handlungsmöglichkeiten, welche Vertrauen voraussetzen würden, vereiteln. Bezogen auf das Vertrauen in informationstechnische Systeme bedeutet dies, dass gebotene Anwendungen weniger genutzt werden, dass das Kommunikationsverhalten sich ändert oder dass Transaktionen nicht stattfinden können. „In some ways, trust works like oxygen in the atmosphere. […] Trust gives people the confidence to deal with strangers: because they know that the strangers are likely to behave honestly, cooperatively, fairly, and sometimes even altruistically. The more trust is in the air, the healthier society is and the more it can thrive. Conversely, the less trust is in the air, the sicker society is and the more it has to contract. And if the amount of trust gets too low, society withers and dies” (Schneier 2012: 6). Eine gewisse Vertrauensgrundlage ist auch im Kontext vieler Anwendungen des Internets notwendig. Nimmt das Niveau des Systemvertrauens ab, muss das Medium Vertrauen durch andere Absicherungs- oder Ordnungsmedien substituiert werden. „Vertrauen […] segelt gleichsam im Windschatten moderner Sicherheitsarchitektur.“ (Frevert 2013: 220) Wo es kein oder wenig Vertrauen gibt, braucht es Sicherheit.

Während in diesem Zusammenhang auf der einen Seite neue Geschäftsfelder erschlossen werden und in Bereichen neuer Sicherheitsmärkte große Gewinne erzielt werden, entstehen auf der anderen Seite hohe Kosten, welche unter den Bedingungen eines hohen Niveaus des Systemvertrauens nicht anfielen. Verluste in Milliardenhöhe entstehen etwa für die zahlreichen, vor allem US-amerikanischen Cloud-Anbieter, da die Internetnutzer kein Vertrauen mehr in die US-amerikanische Netzinfrastruktur haben. Allerdings sind die im Zuge der NSA-Affäre entstehenden Kosten nicht nur monetärer, sondern auch nicht-monetärer Art. Hier geht es um soziale Kosten. Es geht um die Verletzung der informationellen Privatheit, um schwindende Handlungsspielräume, um Risiken und Unsicherheiten. „It's less stressful to live in a world where you trust people. Once you assume people can, in general and with qualifications, be trusted to be fair, nice, altruistic, cooperative, and trustworthy, you can stop expending energy constantly worrying about security. Then, even though you get burned by the occasional exception, your life is still more comfortable if you continue to believe" (Schneier 2012: 224).

Man braucht, so heißt es, „dringend einen substantiellen und systematischen Vertrauensaufbau für das Heute der Informationsgesellschaft, ein Leitbild ‚Informationelles Vertrauen für die Informationsgesellschaft', das ein zielorientiertes und koordiniertes Streben nach Reduktion existierender Unsicherheiten, Ungewissheiten, Unabwägbarkeiten einer informations- und kommunikationstechnisch vernetzten Welt umfasst." (Klumpp, Kubicek et al. 2008: 3) Sofern man also von einem „Vertrauen ins Netz" spricht, geht es um ein Vertrauen in Organisationen, welche zusammengenommen das „System" Internet in seiner Gesamtheit bilden. Es geht, mit anderen Worten, um ein Vertrauen in ein abstraktes System, welches durch Konglomerate von Organisationen aus unterschiedlichen sozialen Welten abgebildet wird. Erwartet wird eine bestimmte Kompetenz, Absicht oder Leistung dieser Organisationen. Ein abstraktes Systemvertrauen wird flankiert von einem Kompetenzvertrauen einerseits – erwartet wird hier die korrekte Funktionsfähigkeit und Sicherheit von Programmen

und Infrastrukturen – und um ein Absichtsvertrauen andererseits – erwartet wird, dass bestimmte Akteure gemäß den Intentionen, welche sie nach außen kommunizieren, handeln. Im Kontext der Debatte um das „Vertrauen ins Netz“ ist sowohl das System-, das Kompetenz- als auch das Absichtsvertrauen aus unmittelbaren Interaktionsverhältnissen, welche personale Vertrauensverhältnisse begründen, losgelöst. Die Interaktionsverhältnisse werden substituiert durch ein wenig greifbares Reputationskapital.

„Trust is […] involved in a fundamental way with the institutions of modernity. Trust here is vested, not in individuals, but in abstract capacities.“ (Giddens 1990: 26) Das System- und Kompetenzvertrauen, welches der Technologie Internet beziehungsweise genauer den mit dem Internet befassten Organisationen entgegengebracht werden muss, ist insofern ein notgedrungenes Vertrauen, als dass die Kommunikation über das Internet einen hochkomplexen technischen Apparat voraussetzt, dessen Funktionalität in seiner Gesamtheit nicht durchschaut werden kann. Giddens führt hier einen parallelen Fall an: „When I go out of the house and get into a car, I enter settings which are thoroughly permeated by expert knowledge – involving the design and construction of automobiles, highways, intersections, traffic lights, and many other items. Everyone knows that driving a car is a dangerous activity, entailing the risk of accident” (Giddens 1990: 28). Dasselbe gilt für die Benutzung des Internets. Spätestens nach den Enthüllungen rund um die Spähaktivitäten amerikanischer und britischer Geheimdienste besteht ein gesellschaftliches Wissen darüber, dass die Benutzung des Internets mit gewissen Risiken verbunden ist. Das Risiko etwa, dass die eigene Internetkommunikation von Dritten ohne Einwilligung gespeichert und ausgewertet wird, ist immer gegeben. Hier setzt man sich einem möglichen Schadenseintritt aus, welcher gegen den Nutzen der Internetkommunikation abgewogen werden muss. „Trust operates in environments of risk, in which varying levels of security (protection against dangers) can be achieved.“ (Giddens 1990: 54)

Durch das Bekanntwerden der geheimdienstlichen Überwachungstätigkeiten sind auf Seiten der Endanwender digitaler Medien erhebliche Sicherheitsbedenken aufgekommen. Trotz der Initiativen rund um die Idee des nationalen Routings, aber auch rund um Kryptosysteme oder andere technische Datenschutzwerkzeuge, ist davon auszugehen, dass es letztlich wenige Möglichkeiten geben wird, das allgemeine „Systemvertrauen" in der Form wiederherzustellen, wie es vor den Snowden-Enthüllungen Bestand hatte. Ein gewisses „Vertrauen ins Netz" wird unumgänglich sein, solange man auf die Benutzung des Internets mehr oder weniger angewiesen ist. Allerdings wird das gegebene Vertrauen von großen Risiken begleitet und daher immer unter gewissen Vorbehalten stehen. Denkbar ist, dass das angeschlagene Systemvertrauen verstärkt durch vertrauensäquivalente Absicherungsstrategien gestützt wird. Hier greift insbesondere das Rechtssystem ein. Doch auch hier ist freilich nicht garantiert, dass Regierungen, Geheimdienste oder Konzerne ihre Operationen entgegen ihrer eigenen Systemlogik gemäß dem geltenden Recht limitieren. Auch das Recht kann die Verlässlichkeit und die erwartete Funktionalität der Infrastruktur des Internets nicht zwangsläufig garantieren.

Letztlich ist zu konstatieren, dass es eine handfeste Vertrauenskrise gibt. Die Vertrauensnehmer – Internetkonzerne, Geheimdienste, Regierungen – haben es nicht geschafft, angemessene Maßnahmen zur Erlangung von Vertrauenswürdigkeit zu ergreifen und den Vertrauensgebern – den Bürgern und Internetnutzern – entsprechend verlässliche Signale zu schicken (Kubicek 2008: 22). Bisherige Maßnahmen zur Vertrauensgewinnung seitens der Vertrauensnehmer – die Darbietung von „informationeller Wellness" oder von kontinuierlich zuverlässigen, stabilen, ästhetisch ansprechenden Systemleistungen (Kuhlen 2008: 50) – können den durch die NSA-Affäre erlittenen Vertrauensverlust nicht mehr wettmachen. Es verwundert daher nicht, dass Vertrauen in der Privacy-Arena ein vorherrschendes Thema ist.

4.4 Vertrauen in der Arena

Simon Ledder

In allen Welten wird gleichermaßen betont, dass Vertrauen wiederhergestellt werden müsse. Wie oben bereits zitiert, kritisiert Merkel das Abhören ihres Handys als eine kategorische Verletzung der zwischenstaatlichen Beziehung. Auch der BND betont einen Wandel in seiner Öffentlichkeitsarbeit. So erklärt der Präsident Schindler: „Ich habe kein Problem damit, wenn die Politik uns auf die Finger schaut" (Schindler, zit. in: Lau 2013). Es ginge nun um die „Schaffung von mehr Transparenz und einer breiteren gesellschaftlichen Vertrauensbasis [...]. Ich wiederhole mich gerne: Es ist für mich die wichtigste Herausforderung." (Schindler 2013).

Auch Mitglieder der Netzgemeinde beschwören Vertrauen und Transparenz. So betont Frank Rieger: „Ein erster, wichtiger Schritt ist, Transparenz herzustellen. Wenn Unternehmen ihre Services gegen die Preisgabe von Nutzerdaten anbieten, muss dieser Deal transparent gemacht werden" (Rieger, zit. in: FAZ.net 2013). Und an anderer Stelle: „Verlorengegangen ist das Vertrauen in die digitalen Technologien und in die politischen Prozesse, wenn es um den Schutz von Vertraulichkeit, Privatsphäre und Datensouveränität geht" (Rieger 2014a).

Das Vertrauen wird ebenso in der Welt der Unternehmen in den Fokus gerückt: „Die Unternehmen in Deutschland und in Europa müssen jederzeit im Stande sein, ihre kritischen Daten und die Daten ihrer Kunden in der Art zu schützen, dass das Vertrauen in die IT-Wirtschaft nicht beschädigt wird und idealer Weise ausgebaut werden kann" (BITKOM 2013). Der damalige Telekom-Chef ging sogar so weit, zu behaupten, die eigene Kernpraktik vernachlässigen zu können: „Das Ziel ist nicht, mehr Geld zu verdienen, sondern wieder Vertrauen in unsere Branche aufzubauen." (Obermann, zit. in: FAZ.net 2013).

Nun verschwimmt hierbei, dass Vertrauen die Vorbedingung ist, um überhaupt Umsatz erwirtschaften zu können; das ursprüngliche Ziel bleibt durchaus erhalten. Cisco-Vorstand und CEO John Chambers (2014) wandte sich gar mit einem offenen Brief an Barack Obama, in dem er neue Regulierungen der NSA fordert, da die US-Technologie-Konzerne Vertrauen eingebüßt und dadurch Kundschaft verloren habe.

Die wirtschaftliche Bedeutung des Vertrauens wurde von Thomas de Maiziere ebenfalls explizit gemacht, der mit „Schutz – Sicherheit – Vertrauen" als Titel bereits den „Auftrag der Politik im digitalen Zeitalter" beschrieb: „Denn was für jede dauerhafte Kommunikation gilt, gilt auch hier: Ohne Vertrauen geht es nicht. Vertrauen ist ein Wert, auch ein ökonomischer Wert" (de Maizière 2014a). Und weiter: „Die Unternehmen wissen: Das Vertrauen der Nutzer ist die Basis ihres geschäftlichen Erfolgs" (ebd.).

Zunächst ist der Fokus auf das Vertrauen eine Verschiebung im Diskurs. Wie Michael Nagenborg in einer Betrachtung des Trusted Computing noch 2010 festgestellt hat: „Erstaunlich an all diesen Vorschlägen zur Überwachung von Online-Medien und von Informations- und Kommunikationstechnologien zu Überwachungszwecken im Rahmen der Herstellung von Sicherheit ist, dass die Frage nach dem Vertrauen der Bürger(innen) in die entsprechenden Technologien oder diejenigen, welche sie einsetzen wollen, nicht gestellt wird. Dabei sind es die Daten der Bürger(innen), die nun ein weiteres Mal mit ungewissem Ausgang ausgewertet werden" (Nagenborg 2010: 165).

Wenn wir davon ausgehen, dass Vertrauen eine ordnungsstiftende Funktion hat, zeigt sich, dass im Diskurs eine Einschränkung dieser Funktion durch die nun offenbarten NSA-Aktivitäten behauptet wird. Infrage gestellt wird, wie sehr Bürgerinnen und Bürger dem Staat, den Geheimdiensten oder den Unternehmen vertrauen dürfen, wie sehr sich Staaten untereinander noch vertrauen können, wie sehr Unternehmen den Staaten vertrauen sollen. Von Merkels kategorischem Verweis auf ein „Abhören unter Freunden" abgesehen, betref-

fen alle anderen Aussagen Beziehungen auf Systemebene. Dabei lassen sich zwei verschiedene Grundlagen ausmachen: Entweder Vertrauen soll wiederhergestellt werden, um die Legitimation der betreffenden Institution zu gewährleisten, oder Vertrauen wird als Voraussetzung wirtschaftlicher Beziehungen verstanden.

Einige Akteure behaupten, dass die Integrität der beteiligten Institutionen ins Wanken geraten. Demokratietheoretisch wird darauf referiert, dass die Bevölkerung als Souverän über das Handeln des Staates, also der Legislative wie der Exekutive, informiert sein muss, um Entscheidungen fällen zu können. Es muss ein Vertrauensverhältnis bestehen. Daher wird Transparenz als Lösungsvorschlag vorgebracht. Die genaue Ausgestaltung wird im Diskurs jedoch selten ausgeführt, außer von Repräsentanten der Netzgemeinde. Diese artikulieren sehr konkrete Vorschläge, etwa die Offenlegung des unternehmerischen Umgangs mit erhobenen Daten.

Andere Akteure verweisen auf den ökonomischen Wert des Vertrauens. Vertrauen gilt in der Ratgeberliteratur zur Unternehmenskommunikation als Fundament für erfolgreiches Wirtschaften (vgl. Esch 2011; Meffert et al. 2012). Auch wenn es wirtschaftsethisch umstritten ist, inwiefern an Unternehmen moralische Ansprüche herangetragen werden können (Süßbauer 1991; Werhane 1992), führen die wirtschaftsethischen Prämissen zur Notwendigkeit funktionierender Vertrauensverhältnisse. So gründen verschiedene wirtschaftsethische Ansätze auf der Prämisse, dass durch den Wettbewerb der gesellschaftliche Wohlstand insgesamt steige, was ein wünschenswertes Ziel sei. Der Wettbewerb kann jedoch nur unter Einhaltung bestimmter Normen funktionieren, weswegen hier von einer Ordnungs- anstatt einer Individualethik ausgegangen werden muss. Nur dadurch, dass Erwartungen regelmäßig erfüllt werden, bleiben die Teilnehmenden Akteure im Wettbewerb und werden nicht exkludiert. Diese Form des Vertrauens würde jedoch gerade in Zweifel gezogen. Im Insistieren auf den Begriff des Vertrauens postulieren die Akteure die Angst davor, dass es zu einer generellen Abwendung der Bürger von Informationstechnologie kommen könne.

Unabhängig von der Grundlage wird der Einbruch des Vertrauens als erhebliches Problem charakterisiert. Dies gilt sowohl für die Legitimation der staatlichen Organe als auch für die Technologiebranche insgesamt. Für Gesellschaften wie der deutschen, in der der Glaube an Fortschritt und Technologie Teil der nationalen Identität ist, der Bereich Informationstechnologie aber stets als vergleichsweise rückständig gilt (vgl. Evans/Kelly 2002: 311-315, Stuhr 2010: 231-284), ist eine solche Darstellung rhetorisch wirkungsvoll. Dadurch lässt sich ein Bedrohungsszenario ankündigen, dass langfristig einen Zusammenbruch der aktuellen gesellschaftlichen Ordnung kommen sieht, sofern nicht bestimmte Maßnahmen eingeleitet werden.

5 Reterritorialisierung und Privatheit

Barbara Büttner, Simon Ledder, Carsten Ochs, Fabian Pittroff

Die Kartografie und Analyse des Arena-Segments, welches sich um den Problematisierungs-/Lösungsvorschlag des nationalen Routings aufspannt, haben bis an diesen Punkt eine Vielzahl von Einsichten und Erkenntnissen erbracht. Mit den methodischen Mitteln der Arena-Kartografie (s. Kap. 2) wurden die Akteure bzw. sozialen Welten, ihre Argumente und Positionierungen sowie ihre diskursiven Privatheitskonstruktionen sichtbar gemacht (s. Kap. 3). Zudem wurden der Privatheits- und Vertrauensbegriff theoretisch reflektiert (Kap. 4). In diesem Kapitel wird es nun darum gehen, die so generierten Forschungsresultate zusammen- und einer verdichtenden Analyse zuzuführen. Dies erfolgt in zwei aufeinanderfolgenden Schritten: Zunächst werden die Teilergebnisse in Hinblick auf das dominante Privatheitsverständnis und Wertegefüge innerhalb der Arena in Bezug zueinander gesetzt, um schließlich in die Bestimmung von idealtypischen Zugriffsweisen auf den Wert der Privatheit zu münden (5.1). Die Typisierung der Zugriffsweisen wird dann genutzt, um die weiter oben vorgestellte Fallschilderung in eine analytische Rekonstruktion der Verlaufskurve des untersuchten Segments zu überführen (5.2). Wie sich zeigen wird, tritt dabei eine spezifische Logik der gesellschaftlichen (Re-)Produktion zutage, wie sie für das untersuchte Segment typisch ist. Diese Logik hat politische Qualität und wird im Schlusskapitel diskutiert werden.

5.1 Zugriffsweisen auf den Wert der Privatheit

5.1.1 Welche Privatheit?

Um in die Zusammenführung der Forschungsresultate einzusteigen, bietet es sich zunächst an, auf einer sehr abstrakten, begriffstechnischen Ebene anzugeben, welche Form der Privatheit den Gegenstand

der in der *Privacy Arena* ausgefochtenen Kämpfe bildet: Um welche Privatheit geht es? Die Antwort hierauf scheint auf den ersten Blick recht leicht zu fallen. Halten wir uns an die in Kap. 4 in Anlehnung an Beate Rössler ausbuchstabierte dreifache Differenzierung der Privatheit in eine räumliche, dezisionale sowie informationelle Form, so erweist sich die letztere eindeutig als die im Routing-Segment dominante. Schaut man genauer hin, so wird jedoch ebenso schnell deutlich, dass das empirische Auftreten des Prädikats und des Werts des Privaten den begrifflichen Rahmen des genannten Dreiklangs bei weitem übersteigt. So wird Privatheit im empirischen Fall etwa im Zusammenhang mit der Verletzung von Schutzräumen (Kap. 3.2), von Eigentumsrechten sowie von Möglichkeiten der persönlichen Entfaltung thematisiert (Kap. 3.5). In diesem Sinne übersteigen die empirisch anzutreffenden Semantiken der Aushandlungspraxis übermäßig enge Konzeptionen. Dass in den Aushandlungen in der Arena oftmals unbestimmt gelassen wird, was denn nun genau unter Privatheit verstanden werden soll, fügt sich nur allzu gut in dieses Bild, denn es ist genau dies, was es den beteiligten Akteuren und ihrer Vielzahl von Kernpraktiken, Weltbildern und Interessen erlaubt, in den Aushandlungsprozess einzusteigen. Hieran wird somit einerseits die Pluralität von Semantiken und Praktiken der Privatheit sichtbar, was andererseits jedoch nicht darüber hinweg täuschen soll, dass das in dieser Pluralität vorfindliche dominante Privatheitsverständnis des Routing-Segments durch die Figur der informationellen Privatheit bestimmt ist.

5.1.2 Privatheit im Gefüge der Werte

Direkt an diesen Befund lässt sich die Erkenntnis anschließen, dass der Begriff der Privatheit – unabhängig davon, wie der Begriff jeweils semantisch aufgeladen wird – empirisch nur dann in seiner Wirkungsweise zu bestimmen ist, wenn er im Gefüge der Werte beleuchtet wird, in welches er sich jeweils situativ eingelassen findet. Empirisch findet man beispielsweise, dass Privatheit ethisch mit Vorstellungen einer unveräußerlichen Würde des Menschen aufgeladen, oder normativ mit der Idee der freien Persönlichkeitsentfaltung in

Bezug gesetzt wird. Wie weiter oben (Kap. 3.5.6) deutlich gemacht wurde, wird Privatheit in solchen Fällen deontologisch als ein Wert an sich konzipiert, der mit anderen in positiver, negativer oder paradoxer Beziehung stehen mag. Vielen gilt die Realisierung dieses Wertes indes als Voraussetzung einer bestimmten politischen Ordnung, namentlich der der Demokratie. In solchen Fällen herrscht ein stärker instrumentelles Privatheitsverständnis vor, was auch im Falle von Vorstellungen der Privatheit als ökonomischer Wert gelten dürfte. Tritt Privatheit hier in ein Spannungsverhältnis zu anderen Werten, wie etwa Sicherheit, so herrscht eine konsequentialistische Argumentationsweise vor, die den Wert der Privatheit schnell zu relativieren droht. Wie zu sehen war, werden die verschiedenartigen Werte in den Kämpfen der Privacy Arena vielfach aufgegriffen und ins Feld geführt – ob „für" oder „gegen" bestimmte Formen des Privatheitsschutzes. Sie werden dabei mit bestimmten Zugriffsweisen auf den Wert der Privatheit verknüpft. Diese werden im Folgenden genauer bestimmt.

5.1.3 Zugriffe auf Privatheit

Vorstellungen von Privatheit und die Aufladung mit bestimmten Werten oder Wert-Arrangements schnüren mitunter zu relativ stark verdichteten Zugriffweisen auf den Wert der Privatheit zusammen. Semantik und Wert-Bezug treten dann in ein relativ stabiles Verhältnis, mit der Folge, dass idealtypische Zugriffsmuster entstehen, deren Auftreten in zumindest sehr ähnlicher Form immer wieder beobachtbar ist. Der folgende Katalog von Zugriffsweisen erhebt keinerlei Anspruch auf Vollständigkeit, zeigt aber auf, dass empirisch tatsächlich unterschiedliche Zugriffsweisen in der Privacy Arena identifizierbar sind, welche wiederum verschiedenartige politische Qualitäten aufweisen.

5.1.3.1 Instrumenteller Zugriff

Der instrumentelle Zugriff ist dadurch charakterisiert, dass er mit einem entweder offenen oder impliziten Privatheitsverständnis operiert. Auf Privatheit wird lediglich Bezug genommen, um die Realisierung anderer Werte des Werte-Gefüges zu realisieren oder die Legi-

timität von Praktiken mit Hilfe des Wertbezugs sicherzustellen. Während rhetorisch die Privatheit in den Vordergrund gestellt wird, kann es z.B. darum gehen, Geschäftsmodelle zu stabilisieren[188] oder bestimmte Politiken zu legitimieren.[189] Dieser Zugriffsweise sind Akteure zuzuordnen, die den Wertbezug nutzen, um andere Interessen zu verfolgen, welche das Wertpostulat im Extremfall konterkarieren oder unterlaufen. Gerade in Kontexten, in denen Privatheit als rhetorische Figur eingesetzt wird (vgl. Kap. 3.5), scheint sie mehr Mittel zum Zweck zu sein. Wenn also sowohl aus Teilen der Welt des Staates als auch der Welt der Industrie Privatheit im gleichen Atemzug mit Innovation und Wettbewerbsvorteil genannt wird, so mag ein solcher Zugriff vorliegen.

5.1.3.2 Parametrischer Zugriff

Ein parametrischer Zugriff begreift Privatheit als immer mitzudenkende Anforderung soziotechnischer Systeme, eben als Parameter. Folgerichtig bleibt es in diesem Fall keineswegs offen, was genau unter Privatheit verstanden werden soll, erzwingt doch das „Parameterverständnis" eine relativ klare semantische Bestimmung. Charakteristisch für diese Zugriffsweise ist des Weiteren die Annahme, dass es keine per se privatheitsunverträglichen Systeme gäbe. Kompatibilität mit Privatheit müsse, könne und solle vielmehr immer in die Gesamtkomposition soziotechnischer Systeme integriert werden, etwa im Zuge von „Privacy by Design". Dementsprechend liegt der Vorstellung, ein beliebiges System „privatheitsfest" machen zu können, die Prämisse zugrunde, Privatheitsanforderungen ließen sich a priori und noch vor der Konstruktion eines spezifischen Systems formal be-

[188] Ein Beispiel hierfür wäre, wenn rhetorisch auf die hohe Relevanz verwiesen wird, die ökonomische Organisationen der Privatheit einräumen, um dann die Einwilligung in ihre Allgemeinen Geschäftsbedingungen zu erbitten. Im Zweifelsfall geht es dabei lediglich um die juristische Absicherung privatheitsunfreundlicher Geschäftsmodelle durch rhetorische Instrumentalisierung des Werts der Privatheit, wobei offenkundig nicht letzterer, sondern der ökonomische Wert der Profitmaximierung realisiert werden soll.

[189] Beispiel hierfür wäre das Agieren der Telekom im Routing-Segment der Arena: wiederholt wird auf den Wert der Privatheit verweisen, um das politisch-ökonomische Unternehmen des nationalen Routings voranzubringen.

stimmen bzw. seien schon bestimmt (etwa als „informationelle Selbstbestimmung"). Damit kann ein Beharren auf Bewährtem (Recht, Normen, Vorstellungen) verbunden sein, das mit Innovationen versöhnt werden kann und soll. Im Resultat droht diese Zugriffsweise jedoch die Aushandlung der Privatheitssemantik still zu stellen.

5.1.3.3 Relativierender Zugriff

Die relativierende Zugriffsweise ist typisch für jene Diskurse, die weiter oben (Kap. 3.5) als konsequentialistisch charakterisiert wurden. Sie stellen Privatheit in güterabwägende Konkurrenz zu anderen Werten, insbesondere zu Sicherheit oder der Produktion von ökonomischem Mehrwert. Im konkurrenzhaft bestimmten Wertegefüge wird der Wert der Privatheit etwa dann relativiert, wenn das „Supergrundrecht" der Sicherheit als höher-relevanter Wert behauptet wird. Ein relativierender Zugriff geht folglich einher mit der rhetorischen oder praktischen Hierarchisierung von Grundwerten. Innerhalb und außerhalb des Arena-Segments praktizieren Geheimdienste und deren staatliche Fürsprecher einen relativierenden Zugriff. Dieser kann aber auch im Modus verfassungsrechtlicher Abwägungen auftreten.

5.1.3.4 Ethischer Zugriff

Eine ethische Zugriffsweise rekurriert auf den Wert der Privatheit in dessen Verhältnis zu den Bedingungen „des guten Lebens." Typisch für das empirische Auftreten dieses Wertes ist, dass Privatheit entweder, sofern der Wert als Grundvoraussetzung des guten Lebens perspektiviert wird, deontologisch als Wert an sich verteidigt wird, der nicht durch höherstufige Werte relativiert werden dürfe; Überwachungskritiker und datenschutzbefürwortende Teile der Welt der Netzgemeinde praktizieren eine solche Zugriffsweise dementsprechend dann, wenn sie Privatheit als Voraussetzung für ein gelungenes Lebens universalisieren. Oder aber der Wert wird, basierend auf einem gleichermaßen wesensmäßig orientierten Privatheitsdenken, verworfen, z.B. wenn datenschutzkritische Anhänger der Post-Privacy-Idee die genau entgegengesetzten Schlüssen ziehen und Privatheit als Hindernis für die Verwirklichung des guten Lebens verste-

hen. In beiden Fällen ist die Zugriffsweise auf den Wert der Privatheit die gleiche: Privatheit wird wesensmäßig und in Hinsicht auf eine Ethik des guten Lebens hin perspektiviert.

5.1.3.5 Deliberativer Zugriff

Eine deliberative Zugriffsweise zielt schließlich auf eine notwendige Neuverhandlung des Wertes der Privatheit ab. Der semantische Gehalt des Begriffs bleibt offen, gleichwohl spielt der Wert eine handlungsleitende Rolle – allerdings nicht als fixierte Bedingung des guten Lebens, sondern als in ihrem normativen Gehalt erst noch zu bestimmende Größe. Anstatt den Wert als gegeben anzusehen und seine Bewahrung anzustreben, wird eine (mehr oder weniger reflexive, offene, gesamtgesellschaftliche) Neuaushandlung eingefordert. An die Stelle der Propagierung von Form und Funktion der Privatheit treten Vorschläge von Mechanismen, die dieses Ziel erreichen helfen sollen. Ein deliberativer Zugriff versucht also nicht den Status Quo unter den gewandelten Bedingungen der Digitalisierung zu erhalten, sondern Privatheit und deren Rolle neu zu erfinden. Betont werden kann, dass deliberative Zugriffe auf Privatheit im untersuchten Arena-Segment marginal bis abwesend sind – und hier gerade aufgrund dieser tendenziellen Abwesenheit bestimmt werden.

Die Zusammenführung der Forschungsresultate liefert uns bis an diesen Punkt eine Reihe von analytischen Ankerpunkten, die es bei der abschließenden Fallanalyse zu berücksichtigen gilt. Wir werden nun abschließend den Verlauf der Arena-Aushandlung als Trajektorie rekonstruieren, um den Umgang mit der Privatheit in diesem Arena-Segment zu analysieren. Aus den bisherigen Ausführungen dieses Kapitels ergibt sich dabei zum einen die Notwendigkeit, die im Arena-Segment dominante semantische Form der Privatheit zu bestimmen; zum anderen muss letztere immer in Beziehung zum jeweiligen Wertegefüge betrachtet werden, in dessen Rahmen Befürworter und Gegner ihre Vorstellungen vom soziotechnischen „worldmaking“ durchzuboxen versuchen. Zum Dritten muss zudem auch die Zugriffsweise der involvierten sozialen Welten dargestellt werden. Auf

diese Weise wird sich schließlich eine robuste These hinsichtlich der politischen Qualität des Lösungsvorschlags, und somit eine Charakterisierung der in diesem Segment dominanten techno-politischen Logik formulieren lassen.

5.2 Die Verlaufskurve des nationalen Routings und die Reproduktion der Container-Gesellschaft

An diesem Punkt der Analyse werden wir nun die Karriere des Lösungsvorschlags des nationalen Routings als Verlaufskurve rekonstruieren (vgl. Strauss 1993: 52-54), welche sich in drei Phasen gliedern lässt: *Aufstieg*, *Fall* und *Überleben.* In diesem Zuge werden wir zeigen, wie unterschiedlich Konzepte von und Zugriffsweisen auf Privatheit aktiviert werden, um schließlich in einem bestimmten Aushandlungsstil zu kristallisieren, der das untersuchte Arena-Segment dominiert.

5.2.1 Aufstieg

Das nationale Routing begann seine Karriere als teils attraktiver Lösungsvorschlag in einer Situation, in der Probleme der Digitalisierung durch die Geheimdienstenthüllungen neue Brisanz gewannen – darunter nicht zuletzt die Krise des Privaten. Attraktiv war der Vorschlag zunächst für die Deutsche Telekom als Vertreterin der sozialen Welt der Industrie, deren Praktiken auf Effizienz und zentralisierte Lösungen setzen (Boltanski/Thévenot 2007: 276-286). Die Routing-Idee passt als Strategie der Reterritorialisierung und Rezentralisierung gut zur Herangehensweise der Welt der Industrie (vgl. 3.2). Auch Teile der Welt des Staates konnten sich zeitweise auf das Konzept einlassen; im November 2013 sprach sich die damals neue Regierungskoalition für eine Berücksichtigung des nationalen Routings aus (CDU/CSU/SPD 2013: 103). Eine deutliche Befürwortung der Idee äußerte einige Monate später Alexander Dobrindt, Bundesminister für Verkehr und digitale Infrastruktur (Welt.de 2013). In diesem Sinne kann von einer Allianz zwischen den Welten der Industrie und des Staates gesprochen werden. Der Vorschlag des nationalen Routings diente als geteiltes Anliegen beider Welten, das Konzept des (trans-)nationalen Routings konnte sich als obligatorischer Passagepunkt etablieren (Callon

1986), d.h. als ein Lösungsvorschlag, der versprach, die Interessen zweier sozialer Welten in ein geteiltes Interesse zu übersetzen: Mit der Idee des Deutschland-Routings lässt sich das Interesse der Telekom an einem Wettbewerbsvorteil mit dem Interesse des BMVI am Infrastrukturausbau kombinieren. Sofern Privatheitsschutz als Argument für die Realisierung dieser Interessen herangezogen wurde, lässt sich die Zugriffsweise auf den Wert der Privatheit an diesem Punkt recht klar als instrumentell charakterisieren. Darüber hinaus passt der Routing-Ansatz aber auch zu den Logiken der beteiligten sozialen Welten und der bislang genannten Akteure: Als ehemaliger Staatsmonopolist unterhält die Telekom nicht nur notwendigerweise regen Kontakt zum BMVI; vielmehr hegen beide auch eine historisch bedingte Vorliebe für territoriale und nationalstaatliche Lösungen. Die semantische Form der Privatheit, um die es hier geht, ist offenkundig die informationelle; doch wird sie in den Wertekanon eines national-territorialen Schutzraums eingeordnet: Ein national verfasster Staat und seine Industrie versprechen den Bürgern, sie vor externen Organisationen zu schützen, ohne die eigene problematische Rolle als potentielle Angreifer zu thematisieren. Die territoriale, technologische, ökonomische und politische Stoßrichtung, der Industrie-Politik des nationalen Routings ist in diesem Sinne nicht nur mit den Praktiken sowohl der sozialen Welt der Industrie als auch mit der des Staates kompatibel; sie zielt auch darauf ab, die moderne Form national-territorialer Container-Gesellschaft mit den Mitteln soziotechnischer Infrastruktur zu reproduzieren – und dies alles unter der Rubrik des Privatheitsschutzes.

5.2.2 Fall

Doch der Lösungsvorschlag des nationalen Routings aktiviert nicht nur Befürworter, sondern auch Gegner. Am Ende der Verlaufskurve kann der Vorschlag keine umfassende Mobilisierungskraft als obligatorischer Passagenpunkt entfalten, und zwar deshalb, weil andere soziale Welten den Wert der Privatheit auf andere Werte beziehen und dabei auch folgerichtig auf andere Art und Weise auf Privatheit zugreifen. Denn mag der Routing-Ansatz den Praktiken der Welt der

Industrie auch entsprechen, so erzeugt er dennoch Widerstand innerhalb der Welt der Ökonomie insgesamt. Artikuliert wird dieser z.B. durch die DE-CIX Management GmbH (DE-CIX 2013), die als Repräsentantin der Welt des Marktes weniger an zentralistischen, sondern vielmehr an dezentralen und „nicht-regulierten" Wettbewerbsbedingungen interessiert ist (Boltanski/Thévenot 2007: 264-267). Während die in vielerlei Hinsicht dezentrale Struktur des Internets gut zur Logik des Marktes zu passen scheint, folgt die Welt der Industrie einem ökonomischen Modell, das an einem territorial definierten Staat und dessen Bürokratie, Rechtsordnung und politischem System ausgerichtet ist. Es ist also die Differenz innerhalb der ökonomischen Welt zwischen Industrie und Markt, die „inner-ökonomischen" Widerstand gegen den Routing-Vorschlag auf den Plan ruft. Das Schisma ist nicht zuletzt Ausdruck unterschiedlicher territorialer, technologischer, ökonomischer und politischer Logiken. Während die Routing-Strategie mit einer Reterritorialisierung von Daten durch technische Mittel und in diesem Sinne mit der national-ökonomischen Art des Wirtschaftens und Regierens verknüpft ist, stellen die Angehörigen der sozialen Welt des Marktes den Wert des Wettbewerbsprinzips und der globalen „freien" Märkte dagegen. Diese Differenz materialisierte sich auch im Zuge eines Konflikts, der im Branchenverband BITKOM ausbrach (Wirtschaftswoche 2014): Eine Reihe US-amerikanischer Unternehmen formte eine Allianz in Opposition zur Telekom, um eine öffentliche Befürwortung des Routing-Vorschlags durch den gemeinsamen Verband zu verhindern. Die Spaltung zwischen Industrie und Markt und ihren jeweiligen Werten kam hier also auch als Differenz zwischen US-amerikanischen und deutschen bzw. europäischen Interessen zum Tragen.

So wie die ökonomische Welt ist auch die des Staates kein homogener Block. Relativierende Zugriffe, die den Wert der Privatheit von vornherein anderen Werten, wie etwa Sicherheit oder ökonomischem Wachstum, unterordnen und daher jedwede Veränderungsnotwen-

digkeit herunterspielen, finden sich hier ohnehin immer wieder.[190] Bezogen auf den Fall des nationalen Routings lässt sich indes festhalten, dass im Gegensatz zum BMVI die beiden anderen Ministerien der Digitalen Agenda Zurückhaltung gegenüber dem nationalen Routing äußern. Insbesondere das Wirtschaftsministerium wendete sich ausdrücklich gegen eine gesetzliche Regelung, und zwar mit dem Argument, das offene und freie Internet nicht gefährden zu wollen (BMWi 2014). Das BMWi scheint hier für die Interessen der Welt des Marktes einzutreten, deren Praktiken von „freien" und „offenen" digitalen Netzwerken eher profitieren. Insbesondere die Formulierung aus dem BMWi, man wolle „das offene und freie Internet erhalten", und es brauche beim „nationale[n] Routing (…) keine gesetzlichen Regelungen. Wir begrüßen stattdessen ausdrücklich freiwillige Angebote von Unternehmen"[191] verdeutlicht, dass der per Routing erfolgte Privatheitsschutz eher als Parameter betrachtet wird, der je nach Bedarf (z.B. auf Konsumenten-Wunsch hin) marktgerecht in die Systeme eingebaut werden kann. Denkbar ist allerdings auch, dass sich hinter der Haltung pro Entwicklungsoffenheit des digitalen Raumes ein strategisches Motiv der standortorientierten Wirtschaftsförderung (diesmal auch von kleinen und mittelständischen Unternehmen) verbirgt. Einigermaßen unwahrscheinlich ergab sich dennoch eine Allianz zwischen Vertretern der Welt des Marktes und der der Netzgemeinde, sofern all diese sozialen Welten sich nicht nur gegen die Routing-Strategie wendeten, sondern den Widerstand auch an demselben Wert aufhängten. So votierte die Netzgemeinde gegen den Routing-

[190] Das Argument ist an dieser Stelle gewissermaßen generisch, aber deshalb nicht unzutreffend. Verwiesen werden kann auf die schon weiter oben erwähnten Einlassungen des Ex-Innenministers Friedrich zum „Supergrundrecht Sicherheit" (Friedrich, zit. in: Bewarder/Jungholt 2013); sowie auf die im Jahr 2015 erfolgte klare Positionierung Kanzlerin Merkels im Hinblick auf Datenschutz per se: „Wir müssen hohe Datensicherheit haben, aber wenn wir uns das Big Data Management, wenn wir uns die Möglichkeit der Verarbeitung großer Datenmengen durch einen falschen rechtlichen Rahmen zu sehr einengen, dann wird nicht mehr viel Wertschöpfung in Europa stattfinden." (Merkel im Rahmen ihrer Rede auf dem 9. IT-Gipfel am 19. November 2015 in Berlin, vgl. http://www.bundesregierung.de/Content/DE/Rede/2015/11/2015-11-19-merkel-it-gipfel.html).

[191] Vgl. die diesbezügliche Pressemitteilung auf der Website des BMWi vom 13. Juni 2014 unter http://www.bmwi.de/DE/Presse/pressemitteilungen,did=642114.html.

Vorschlag, weil ihre Praktiken auf „Offenheit" und „Zugänglichkeit" des Internets und anderer Technologien angewiesen sind. Obwohl denselben Wert gegen den Routing-Vorschlag vorbringend, war die Positionierung der Netzgemeinde doch von einem recht anderen Zugriff auf Privatheit gekennzeichnet, sofern sie ethisch argumentierte – schließlich wurde der Wert der „Offenheit" als fundamentaler Wert an sich in Stellung gebracht.

Allgemeiner lässt sich sagen, dass Praktiken der digitalen Vernetzung aktuell vielerorts an Bedeutung gewinnen, die quer liegen zu den oftmals territorialen Logiken moderner Staaten. „Offenheit" in diesem Sinne spielt eine wichtige Rolle für Prozesse der Digitalisierung und ist ein zentraler, teils integraler Wert für viele soziale Welten der Privacy-Arena. Dieser Umstand ist nun ein Grund dafür, dass sich Konzepte des nationalen Routings letztendlich nicht als obligatorischer Passagenpunkt etablieren können, jedenfalls solange sie als inkompatibel mit dem Wert der Offenheit empfunden werden. Nicht nur kann festgestellt werden, dass, während der Routing-Vorschlag darauf abzielt, national-territoriale Container-Gesellschaften zu reproduzieren, die informationellen Praktiken einer immens großen Zahl von Akteuren und sozialen Welten schon längst die Bedingungen zur Reproduktion eines solchen Gesellschaftstypus massiv, nachhaltig und gleichsam „unter der Hand" verschoben haben; es stellt sich auch die Frage, inwiefern ein Problematisierungs- und Lösungsansatz der, so wie der Routing-Ansatz, an historisch entstandenen Kompromisslinien anknüpft und auf die unhinterfragte Reproduktion institutioneller Routinen (hier: des territorial begrenzten Nationalstaates im digitalen Bereich) abzielt, überhaupt noch Aussicht auf Erfolg haben kann.

5.2.3 Überleben

Festhalten lässt sich also, dass mit der Karriere des nationalen Routings eine Strategie der Reterritorialisierung artikuliert wurde, die wiederum als Ausdruck einer bestimmten Form des Regierens verstanden werden kann, nämlich als Versuch, national-territoriale Logiken in ein Zeitalter der Digitalvernetzung zu retten. Die hier vorgeleg-

ten empirischen Analysen (vgl. Kap. 3) zeigen, wie der Lösungsvorschlag des nationalen Routings am Ende scheiterte. Heißt das, dass die Reterritorialisierungsstrategie damit zukünftig vom Tisch sein dürfte? Keineswegs: Zwar spricht einiges dagegen, dass technische Routing-Konzepte erfolgreich zurückkehren. Jedoch finden sich für die darunterliegende Strategie der Reterritorialisierung auch Fürsprecher z.B. in der Welt der Netzgemeinde, wenn sie Routing-Ansätze nicht gänzlich ablehnen, sondern als sinnvollen Baustein einer Dezentralisierung der globalen Netzinfrastruktur in Erwägung ziehen (z.B. Rieger 2014: 16, 20). Auch im Strategiepapier der Digitalen Agenda wird die „technologische Souveränität Deutschlands" (BMWi/BMI/BMVI 2014: 4) als eines der Ziele ausgewiesen. Darüber hinaus müssen Strategien der Reterritorialisierung nicht an technische Lösungen wie Routing gebunden sein und können auch mit anderen Mitteln wie Gesetzen oder freiwilliger Selbstverpflichtung der Unternehmen verfolgt werden. So können Strategien der Reterritorialisierung jenseits von Routing-Lösungen letztendlich überleben.

Im Sinne eines Fazits können wir nun zusammenfassend den im Routing-Segment vorfindlichen dominanten Charakter dieses Lösungsvorschlags und der Art und Weise seiner Verfolgung bestimmen: Es handelte sich um einen Vorschlag, der sich in das nationalökonomische Wertgefüge der Industrie-Politik national-territorialer Container-Gesellschaften einfügte, und in diesem Rahmen einen instrumentellen Zugriff auf den Wert der Privatheit aufwies. Unter der Maßgabe der Bewahrung einer informationellen Privatheit innerhalb eines territorial abgesteckten Schutzraumes wurden veränderte Rahmenbedingungen rekursiv kaum bis gar nicht in Rechnung gestellt. Vereinfachend formuliert könnte man sagen: Die Befürworter des nationalen Routings taten so, als ob sich nichts geändert habe und man in Hinblick auf den Bau aktueller Gesellschaft so weitermachen könne wie bisher. Ein rekursives In-Frage-stellen nicht nur der Privatheitssemantik, sondern auch der Praktiken, Werte und Institutionen (z.B. der staatlichen Institutionen selbst), in die Privatheiten immer verstrickt sind, blieb aus. Es stellt sich jedoch mit Dringlichkeit

die Frage, ob die in diesem Arena-Segment dominanten Formen der Artikulation von Privacy-Problemen der Krisensituation angemessen sein können: Wie erfolgversprechend sind Arenapolitiken, die primär auf technische und rechtliche Regulation setzen oder die Verteidigung und Bewahrung gewohnter Datenschutzstandards in den Mittelpunkt stellen? Inwieweit muss die Krise als fundamentale Herausforderung der gegebenen Verfasstheit oder als Symptom einer umfassenderen gesellschaftlichen Krise anerkannt werden?

5.2.4 Die Verfasstheit der digitalen Welt

Angesichts der hohen Dynamik und weitreichenden Interdependenzen des digitalen Wandels geht es in der Privacy-Arena auch um die Frage nach der Herausbildung und Stabilisierung einer problemangemessenen Vertrauensinfrastruktur für das digitale Zeitalter. Insofern fast alle Akteure der Arena in den Turbulenzen und Ungewissheiten, Krisen und Skandalen, Unbestimmtheiten und Gestaltungsmöglichkeiten, die mit dem digitalen Wandel einhergehen, nicht nur ein Problem für den Schutz der Privatheit, sondern zugleich eine Herausforderung für die Demokratie sehen, welche Garant für das Vertrauen der Bürger in die digitale Zukunft sein soll,[192] stellt sich die Frage, unter welchen Voraussetzungen welche Form von Demokratie diese Last zu schultern vermag. Hier wird deutlich, dass in den Verhandlun-

[192] Eine Auswahl: Die Spionageaktivitäten des US-Geheimdienstes sind laut dem Ex-Telekom-Vorstandschef René Obermann „demokratiegefährdend", weil sie „das Vertrauen in zwei Grundpfeiler unserer Gesellschaft, die freie Kommunikation und die Privatsphäre, erschüttert (haben)" (Handelsblatt 2013). Der Sprecher des Chaos Computer Club Frank Rieger fordert: „Wir müssen jetzt entscheiden, ob wir das weiter wollen. Oder ob wir sagen: Als demokratisch verfasste Gesellschaften wollen wir uns diese Art Geheimdienste, die die Geschäftsgrundlagen unserer Demokratie gefährden, so nicht mehr leisten" (Faz.net 2013). Für die Grünen ist die Überwachung ein „fundamentaler Angriff auf die Demokratie in Deutschland" (Fr-Online.de 2013). „Ein echtes Demokratieproblem" konstatiert auch Jean-Claude Juncker im Hinblick auf den Kontrollverlust der Regierungen über ihre Geheimdienste (Welt.de 2014). Und ver.di-Chef Bsirske ruft mit Blick auf die Anfälligkeit der IT-Infrastrukturen nach einer „demokratischen Raumordnung für die vernetzte Welt" (heise.de 2014). Snowden schließlich habe „mit Mut und Kompetenz das beispiellose Ausmaß staatlicher Überwachung enthüllt […], die grundlegende demokratische Prozesse und verfassungsmäßige Rechte verletzt" (Right Livelihood Award Stiftung 2014).

gen um Privatheit immer auch die Verfasstheit der digitalen Welt insgesamt auf dem Spiel steht. Die Strategie der Reterritorialisierung, die wir in Form von Routing-Ansätzen vorgefunden haben, zeigt sich dabei als ein Regierungsmodus, der einer „Neuversammlung des Kollektivs“ (Bruno Latour), wie sie die Digitalvernetzung erfordern könnte, entgegengesetzt zu sein scheint.

Wir bezeichnen den im untersuchten Arena-Segment vorgefundenen Modus als „demokratischen Protektionismus“, da seine Regierungspraktiken auf die Bewahrung eines Status quo politischer Routinen, ökonomischer Freiheiten und etablierter Institutionen abzielen. Krisen werden außerhalb dieser Institutionen verortet, die selbst nicht in Frage gestellt werden. Die institutionellen und politischen Mechanismen gelten als funktional und angemessen, Anlass zur Wiederbelebung oder Neuerfindung gibt es nicht. Die bestehende politische Ordnung gilt als geeignet, um passende Lösungen zu generieren. Als angemessen und stabil gilt etwa ein Gleichgewicht aus rechtsstaatlich garantierten, negativen Freiheiten und einem tolerierbaren und notwendigen Maß an staatlicher Überwachung. In der Logik des demokratischen Protektionismus wird diese Ordnung primär gefährdet durch äußere Einflüsse wie technologische Entwicklungen, ausländische Nachrichtendienste oder neue digitale Wirtschaftsformen. Entsprechend gilt dann auch Privatheit mehr als zu bewahrender Wert und weniger als wandelbares Konzept.

6 Schluss: Demokratische Alternativen der Reterritorialisierung

Jörn Lamla

Die vorliegende Studie hat Zwischenergebnisse aus der Analyse und Kartographie der Privacy-Arena zusammengetragen, die auf spezifische Bestrebungen der Reterritorialisierung des Digitalen hinweisen. Diese Bestrebungen sind nicht allein durch die Sorge um Privatheit getrieben, sondern durch ein komplexes Arrangement motiviert, das nicht zuletzt auf den Schutz etablierter institutioneller Routinen des Nationalstaats ausgerichtet ist. Nicht nur erhält der Begriff und Wert der Privatheit durch diesen Zugriff eine besondere Bedeutung. Vielmehr wird damit auch ein Möglichkeitsraum festgelegt, mit welchen Antworten auf die Krise der Privatheit im digitalen Zeitalter nach Snowden reagiert wird und werden kann.

Infrage steht dabei, ob diese Reaktionsweisen den Herausforderungen noch angemessen sind und ob sie das Digitale überhaupt in der gewünschten Weise zu reterritorialisieren vermögen.[193] Ist die identifizierte Reaktion nationaler Demokratie also der krisenhaften Ausgangssituation angemessen oder nicht? Welche problematischen Nebenfolgen und nicht intendierten, vielleicht sogar paradoxen Effek-

[193] Um diese Frage in ein Bild zu fassen: Geht es um eine Problembewältigung, die kurzfristig die Routinen aller Beteiligten und Betroffenen mittels kleiner Reparaturen stützt? Geht es womöglich darum, aufzupassen, dass wir mit unserem Wunsch nach Privatheit nicht von diesem Zug abgehängt werden und mit altbackenen Privatheitsvorstellungen als ausrangierte Waggons aufs Abstellgleis geschoben werden? Oder geht es um die Einbeziehung möglichst vieler Anliegen und Sichtweisen auf die Zukunft des digitalen Lebens, auch wenn das bedeutet, dass der Zug verlangsamt werden und an jedem noch so kleinen Bahnhof erneut anhalten muss, um zu schauen, ob jemand einsteigen oder aussteigen will und eine gültige Fahrkarte besitzt? Oder können wir uns darauf beschränken, zu überprüfen, ob das Personal und die Routinen in den elektronischen Stellwerken noch zuverlässig arbeiten?

te löst diese protektionistische Form der Reterritorialisierung aus? Werden die Verstrickungen dieser nationalen (in Teilen supranationalen) Konfiguration des Rechts, der Bürgerschaftlichkeit, der Privatheits- und Misstrauenskulturen, der Wirtschaftspolitik usw. reflektiert? Ist dieses Muster digitaler Territorialität nicht selbst konstitutiv oder mitverantwortlich für die Krisenerscheinungen einer überbordenden Überwachung, des Datenhungers, des Aufschaukelns von Konflikten und Kämpfen um Informationshoheit oder das Wettrüsten zwischen den Sicherheitsarchitekturen und Angriffsoptionen der Nationalstaaten, Unternehmen, Geheimdienste, Hacker und am Ende womöglich auch Privatanwender?

Diese Fragen sind Anschlussfragen, die an dieser Stelle nicht beantwortet werden können, aber doch soweit aufgeworfen und konturiert werden sollen, dass sie die weitere Forschung des Projekts anleiten können. Es sind Fragen, die nur dann beantwortet werden können, wenn die vorgefundenen Strategien mit *Alternativen der Reterritorialisierung* des Digitalen konfrontiert werden. Solche Alternativen lassen sich in einem ersten Schritt idealtypisch entwerfen, legen im zweiten Schritt aber sogleich die Frage nahe, ob sie in der Privacy-Arena empirisch eine Rolle spielen, historisch gespielt haben und/oder warum sie gegebenenfalls zum Schweigen verurteilt sind. Durchaus im Sinne auch von Deleuze und Guattari (1992) geht es bei der Frage nach diesen Alternativen immer auch um die Demokratie, d.h. um die Frage, wie alternative Reaktionen auf die Krise der Privatheit nach Snowden die faktischen Deterritorialisierungstendenzen der Digitalsphäre – nicht nur räumliche Entgrenzungen, auch Rechtsbrüche, Entzivilisierungen, Vertrauenskrisen usw. – so zu reterritorialisieren vermögen, dass Selbstbestimmung in einem umfassenden und mit Blick auf die *Issues*, also die Probleme, angemessenen Sinne gewahrt oder sogar gesteigert wird. Antworten und Kriterien lassen sich hier nicht einfach aus dem Begriff der Privatheit oder Freiheit ableiten oder aus einer Theorie der Demokratie deduzieren, sondern machen weitere Analysen erforderlich. Das Denken in Alternativen zu ermöglichen ist mit Blick auf diese weitere empirische Analyse aber außerordentlich hilf-

reich, auch wenn die im Folgenden unterschiedenen idealtypischen Reaktionsweisen der Demokratie nur heuristischen Charakter haben und noch keine abschließende Typologie und Deutungsfolie bereitstellen.

Ausgangspunkt dieser Konstruktion von idealtypischen Alternativen der Reterritorialisierung bildet die Abstraktion und Steigerung jener Momente, die am Fall des nationalen Routings identifiziert worden sind. Rekonstruiert wurde ja ein Muster der Krisenreaktion auf die Erschütterungen durch den NSA-Skandal, das in Deutschland seit langem verankerte institutionelle Routinen in Anschlag bringt und zugleich schützen soll: Großunternehmen, Verbände und Regierung suchen in historisch eingeübter Abstimmung nach einer technischen Problemlösung, die im gemeinsamen Interesse dieser Welten liegt; zugleich sind es die tradierten Maßstäbe eines staatlicherseits zu gewährleistenden hohen Datenschutzniveaus, seiner rechtlichen Interpretation als informationelle Selbstbestimmung sowie eines Schutzes wirtschaftlicher Interessen vor Fremdspionage und Verdrängung im Standortwettbewerb, die das Verständnis von Privatheit bei den Befürwortern des Vorschlags prägen und den Lösungsweg für die Reterritorialisierung des Digitalen vorzeichnen. In idealtypischer Generalisierung und Überzeichnung lässt sich dieses Muster als *Demokratischer Protektionismus* bezeichnen. Alternativen hierzu werden dann sichtbar, wenn zwei typische Elemente dieses Reaktionsmusters variiert werden: zum einen der Grad an Transparenz von Verfahren, die hier als legitimationsrelevant für die Demokratie ins Spiel gebracht werden, und zum anderen die Richtung der Krisenreaktion, die eher ein Zurück zu alten Routinen der Demokratie anstreben oder aber die konsequente Einlassung auf das Unbekannte der deterritorialisierenden Problemdynamik vorschlagen kann. Mittels dieser zwei Unterscheidungsdimensionen lässt sich eine Kreuztabelle mit vier idealtypischen Reaktionsweisen der Demokratie gewinnen, mit der sich die Analyse und Kartographie der Privacy-Arena kontrastierend fortführen lässt und die hier abschließend im Uhrzeigersinn erläutert werden soll (Tab. 1):

	Intransparente Verfahren (besitzstandsorientiert)	Transparente Verfahren (legitimationsorientiert)
Institutionell gebunden (Routinemodus)	a.) Demokratischer Protektionismus	b.) Demokratischer Konstitutionalismus
Institutionell ungebunden (Krisenmodus)	d.) Postdemokratie	c.) Demokratischer Experimentalismus

Tab. 1: Vier Idealtypen demokratischer Reaktionsweisen auf die Krise der Privatheit

Ad a.) *Demokratischer Protektionismus* wird eine Reaktions- und Artikulationsweise genannt, die das Bestehende idealtypisch als demokratische Errungenschaft behandelt, das durch neue Entwicklungen bedroht wird und entsprechend gegen diese Entwicklungen zu verteidigen ist. Die Krise liegt folglich im Außenbereich der Demokratie, in Bedrohungen durch das Neue (die digitale Technologie) und äußere Feinde (die Geheimdienste anderer Staaten), wohingegen die politischen Routinen des eigenen Gemeinwesens, etwa dessen Rechtsauffassung, das liberale Freiheitsverständnis oder das Modell der Interessenrepräsentation und -artikulation als intakt und schützenswert hingestellt werden. Zugleich erlaubt diese eindeutige Außenadressierung der Krise eine abkürzende öffentliche Kommunikation über die eigenen Verstrickungen, Interessen, Profite usw. Solange die eigene Demokratie nicht unter Erklärungsdruck, sondern auf der Sonnenseite steht, kommt die Frage nicht auf, ob sie einseitige Vorteile gewährt, unsolidarische Verhältnisse abstützt, Potentiale zur Steigerung ihrer Rationalität nicht ausschöpft oder angesichts der globalen, grenzüberschreitenden digitalen Revolution einer Erneuerung bedarf. Ihre eingespielten Privacy-Praktiken und Standards des Datenschutzes, der Achtung von Persönlichkeitsrechten, der öffentlichen Meinungsbildung usw. erscheinen pauschal als anerkannt. Es besteht wenig Druck, solche *black boxes* zu öffnen und zu prüfen.

Ad b.) Als *demokratischen Konstitutionalismus* lässt sich demgegenüber eine Reaktions- und Artikulationsweise bezeichnen, die zwar ebenfalls an bestehende Institutionen und Routinen anschließt, damit jedoch ein Problem im Innern der eigenen Demokratie insofern anzeigt, als sie höhere, fundierende Prinzipien gegen andere Praktiken und Gewohnheiten des eigenen politischen Gemeinwesens zur Geltung bringt, etwa gegen Rechtsauslegungen seitens der Geheimdienste oder Regulierungsdefizite im Bereich des staatlichen Datenschutzes. Die Formen der Anrufung solcher höheren Instanzen der Demokratie reichen von Petitionen über Verfassungsbeschwerden bis hin zum zivilen Ungehorsam und zur Einrichtung von Untersuchungsausschüssen.[194] Auch in dieser Wahrnehmung der Problemsituation werden geltende Verfahrensordnungen und Rechtskonstruktionen nicht überschritten. Vielmehr werden die in demokratischen Verfassungen institutionell verankerten Lern- und Anpassungspotentiale in der Hoffnung aktiviert, damit den Problemen des Schutzes der Privatheit und der Wiederherstellung von Vertrauen in die digitale Entwicklung und Zukunft beikommen zu können.

Ad c.) Der Idealtyp des *demokratischen Experimentalismus* entlässt die Demokratie demgegenüber nicht in den Routinemodus, weil er annimmt, dass diese sich mit neu auftretenden gesellschaftlichen Problemen und Interdependenzen laufend neu entdecken muss. Theoretisch lässt sich dieser Ansatz ausgehend von John Dewey und Bruno Latour fruchtbar machen (vgl. Lamla 2013a, 2013b). Eine experimentalistische Reaktions- und Artikulationsweise würde den Zusammenhang von Demokratie und Privatheit angesichts der digitalen Heraus-

[194] Einen Modellfall hierfür gibt der „zivile Ungehorsam" Edward Snowdens selbst ab, der mit Berufung auf die amerikanische Verfassung und deren liberale Tradition eine Schieflage der Demokratie seines Heimatlandes anprangert. Sein Geheimnisverrat ist stark legitimationsorientiert und beruft sich insbesondere auf Prinzipien der Öffentlichkeit, die als höchste Instanz darüber zu wachen habe und wachen können muss, dass die verfassungsmäßig verbürgten Grund- und Menschenrechte gewahrt bleiben. Da diese aus seiner Sicht durch die NSA-Praktiken aber stark gefährdet sind, sieht er sich nicht nur berechtigt, sondern auch genötigt, der Wächterinstanz „Öffentlichkeit" durch bewussten Rechtsbruch die Ausübung ihrer Kontrollfunktion zu ermöglichen (vgl. Scheuerman 2014).

forderungen als „gesellschaftsweites Forschungsprojekt“ rahmen. Sie würde die Verunsicherung in den unterschiedlichen sozialen Welten anerkennen und ernst nehmen, um ihnen in der Hoffnung auf den Grund zu gehen, tragfähige Situationsdefinitionen und Problembeschreibungen zu finden und darauf aufbauend neue Lösungen zu erarbeiten. Mit der Orientierung an einer kooperativen Forschungslogik bindet auch dieser Idealtyp sich gleichwohl an Verfahrensnormen, die durch eine starke Öffentlichkeit sichergestellt werden müssten.

Ad d.) Das unterscheidet ihn vom blinden *trial-and-error*-Prinzip, bei dem das Zustandekommen und die Durchsetzung von Lösungsvorschlägen für die Krisen des digitalen Zeitalters öffentlich nicht mehr transparent und nachvollziehbar sind und sich dadurch einem Legitimationsdruck entziehen. Wenn unter der Hand laufend neue Fakten geschaffen werden und demokratische Beteiligung bloß simuliert wird (Blühdorn 2013), handelt es sich um eine *postdemokratische Krisenreaktion und Artikulationsweise* (Crouch 2008). Die digitalen Revolutionen vollziehen sich nach Gesetzen des Stärkeren oder Schnelleren, wenn IT-Konzerne mit ihren Geschäftsmodellen oder Geheimdienste die technologischen Möglichkeiten laufend weitertreiben und ausreizen und in der Folge unaufhörlich neue Ordnungen des Zusammenlebens, der Kommunikation und auch der Privatheit kreieren. Beteiligung nutzen sie dabei selbst noch als Element der sozialen Mobilisierung der Massen oder isolierten Subjekte. Die Öffentlichkeit mag protestieren und auch einzelne Erfolge erzielen, bleibt aber ein Machtfaktor, dem die nötigen Ressourcen fehlen, um den digitalen Wandel auf ein Verfahren kollektiver Lösungssuche zu verpflichten.

Idealtypen nennen wir diese demokratischen Prozessmuster deshalb, weil sich die politische Realität der Privacy-Arena nicht strikt an solche Differenzen hält. Vielmehr finden sich Spuren und Elemente aller vier Idealtypen in der Privacy-Arena. Die Frage ist aber, welche dieser Prozessformen die Verläufe von Aushandlungen und Lösungssuchen in der Privacy-Arena dominiert, ob sich ein synergetisches Zusammenspiel oder nur wechselseitige Irritation und Blockade zwischen diesen – teils implizit, teils explizit in der Arena verfolgten – Masterplänen zur

Wiedergewinnung von Vertrauen in die Gestaltung des digitalen Wandels abzeichnen.

Vor dem Hintergrund der vorliegenden Exploration lautet die Hypothese, deren Reichweite durch Untersuchungen weiterer Segmente der Privacy-Arena überprüft, d.h. falsifiziert bzw. verfeinert werden soll, dass protektionistische Motive und Demokratievorstellungen in der Privacy Arena sehr stark sind, wobei nicht immer deutlich wird, was genau geschützt werden soll (grundgesetzlich verbriefte Persönlichkeitsrechte und Freiheiten oder wirtschaftliche bzw. weltenspezifische Interessen, die sich hinter einer eher instrumentellen Anrufung von Werten der Privatheit oder Rechten und Pflichten des Privatheitsschutzes verbergen). Sofern dadurch zahlreiche *black boxes* der Privacy-Arena ungeöffnet bleiben – etwa die Praktiken der eigenen Geheimdienste, die formale Ausrichtung am individuellen Rechtssubjekt oder die Geschäftsmodelle der IT-Wirtschaft – weil der Schutz der Privatheit diesen als Parameter bloß hinzugefügt wird, sind postdemokratische Entwicklungen der demokratischen Vertrauensinfrastruktur wahrscheinlicher als deren konstitutionelle oder experimentelle Erneuerung. Wohl werden Verfassungsfragen diskutiert, Kontrollorgane mobilisiert und die Notwendigkeit einer offenen, gesellschaftsweiten und kooperativen Lösungssuche behauptet. Aber es zeichnet sich im bisher untersuchten Arenasegment kein systematischer Pfad für eine solche demokratische Erneuerung ab. Offenheit und Gesprächsbereitschaft bleiben leere Versprechen und die demokratischen Kontrollinstanzen blockieren sich nicht selten selbst, indem sie ihre prozeduralen Möglichkeiten für Machtkämpfe missbrauchen.

7 Literaturverzeichnis

87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2014): Gewährleistung der Menschenrechte bei der elektronischen Kommunikation, Entschließung v. 27.3.2014. In: datenschutz.de (2014). URL: https://www.datenschutz.de/dsb-konferenz/.

AK Vorrat (2012): zeichnemit.at: 100.000 Unterschriften gegen die Vorratsdatenspeicherung. 13.4.2012. URL: http://www.akvorrat.at/zeichnemit-100k.

Allen, Anita L./Mack, Erin (1989): How Privacy Got Its Gender. In: Northern Illinois Law Review 10, S. 441–478.

Altman, Irwin (1976): Privacy: A Conceptual Analysis. In: Environment and Behavior 8 (1), S. 7–29.

Altman, Irwin (1977): Privacy Regulation: Culturally Universal or Culturally Specific? In: Journal of Social Issues 33 (3), S. 66–84.

Amann, Melanie/Blome, Nicolaus/Gebauer, Matthias/Nelles, Roland/Repinski, Gordon/Schindler, Jörg/Weiland, Severin (2014): Handys bleiben draußen. In: Der Spiegel 30/2014: 24-26.

Amann, Melanie/Medick, Veit (2014): Vorerst nichts speichern. In: Der Spiegel 2/2014: S. 30-32.

Arnbak, Axel/Goldberg, Sharon (2014): Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad. Working Paper, 27.6.2014. URL: www.petsymposium.org, https://www.petsymposium.org/2014/ pa-pers/Arnbak.pdf.

Aust, Helmut P. (2014): Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, A-Drs. 56, MAT A SV-4/1.

Australian Law Reform Commission (2007): Review of Australian Privacy Law. Discussion Paper 72, Vol.1, September 2007. URL: http://www.alrc.gov.au/sites/default/files/pdfs/publications/DP72_full.pdf.

Baban, Constance Pary (2012): Der innenpolitische Sicherheitsdiskurs in Deutschland. Zur diskursiven Konstruktion des sicherheitspolitischen Wandels 2001-2009. Wiesbaden: Springer VS.

Bäcker, Matthias (2014): Strategische Telekommunikationsüberwachung auf dem Prüfstand. In: K&R 2014, S. 556-561.

Bäcker, Matthias (2014a): Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, A-Drs. 54, MAT A SV-2/3.

Bager, Jo (2014): Das Ende der Privatsphäre. In: c't 20/2014, S. 76-79.

Baumgärtner, Maik (2014): Geheimdienste – Das Wetter in New York. In: Der Spiegel 28/2014, S. 22-26.

Beckedahl, Markus (2013): Stimmen zum Deutschlandnetz. In: Netzpolitik.org, 11.11.2013. URL: https://netzpolitik.org/2013/stimmen-zum-deutschlandnetz/.

Becker, Sven/Gude, Hubert/Horchert, Judith/Müller-Maguhn, Andy/Poitras, Laura/Reißmann, Ole/ Rosenbach, Marcel/Schindler, Jörg/Schmid, Fidelius/Sontheimer, Michael/Stark, Holger (2014): Snowdens Deutschland-Alte. In: Der Spiegel 25/2014: 18.

Beetz, Michael/Corsten, Michael/Rosa, Hartmut/Winkler, Torsten (2014): Was bewegt Deutschland? Sozialmoralische Landkarten engagierter und distanzierter Bürger in Ost und Westdeutschland, Kapitel 4. Weinheim/ Basel: Beltz Juventa.

Bendiek, Annegret (2014): Die deutsche Antwort auf die NSA-Reform heißt Europa. In: Stiftung Wissenschaft und Politik, 20.1.2014. URL: http://www.swp-berlin.org/de/nc/publikationen/kurz-gesagt/die-deutsche-antwort-auf-die-nsa-reform-heisst-europa/print/1.html.

Bergmann, Jens (2010): Ökonomisierung des Privaten. Aspekte von Autonomie und Wandel der häuslichen Privatheit. Bielefeld: VS.

Bergmann, Jörg (1987): Klatsch. Zur Sozialform der diskreten Indiskretion. Berlin, New York: Walter de Gruyter.

Berke, Jürgen (2014): Deutsche Telecom und der Abhörskandal. In: Wirtschaftswoche, 17.2.2014. URL: http://www.wiwo.de/unternehmen/it/deutsche-telekom-und-der-abhoerskandal-allein-gegen-die-amerikaner-/9481452.html.

Berke, Jürgen (2014a): Regierung bremst Telekom bei Spionageabwehr aus. In: Wirtschaftswoche, 17.5.2014. URL: http://www.wiwo.de/politik/deutschland/national-routing-abgelehnt-regierung-bremst-telekom-bei-spionageabwehr-aus/9903108.html.

Bewarder, Manuel (2014): Ins Netz gegangen. In: Die Welt. Veröfft. 08.05.2014. URL: http://www.welt.de/print/die_welt/politik/article127747868/Ins-Netz-gegangen.html.

Bewarder, Manuel/Jungholt, Thorsten (2013): Friedrich erklärt Sicherheit zum „Supergrundrecht". In: Die Welt v. 16.07.2013.

Bielefeldt, Heiner (2004): Freiheit und Sicherheit im demokratischen Rechtsstaat. Berlin: Institut für Menschenrechte.

Bild.de (2014): Legt euer Geheimdienste an die Kandare. In: Bild.de, 07.07.2014, URL: http://www.bild.de/politik/inland/bnd/von-der-leyen-geht-auf-clinton-los-merkel-spricht-von-vertrauensbruch-36707264.bild.html.

Birk, Volker (2014): pretty Easy Privacy – Whatsapp verschlüsseln. Und Facebook-Nachrichten. Auch mit Outlook. In: Netzpolitik.org. Veröfft: 15.09.2014. URL: https://netzpolitik.org/2014/pretty-easy-privacy-whatsapp-verschluesseln-und-facebook-nachrichten-auch-mit-outlook/.

Birnbacher, Dieter (2003): Analytische Einführung in die Ethik. Berlin: de Gruyter.

Birnbaum, Robert/Müller, Ingrid/Tretbar, Christian (2013): Das Handygate und die Folgen. In: Cicero Online v. 29.10.2013. URL: http://www.cicero.de/berliner-republik/nsa-affaere-das-handygate-und-die-folgen/56243.

BITKOM (2013): BITKOM Positionspapier zu Abhörmaßnahmen der Geheimdienste und Sicherheitsbehörden, Datenschutz und Datensicherheit. In: BITKOM, 31.10.2013, URL: http://www.bitkom.org/files/documents/BITKOM-Positionspapier_zu_Abhoermassnahmen_2013.pdf.

Blank, Philipp (2013): Deutschland-Routing: Mehr Vertrauen ins Netz. URL: http://blog.telekom.com/2013/10/15/deutschland-routing/#more-7006.

Bleich, H. (2013): Das DE-CIX und das „Schland-Netz": Betreiber empört über Telekom-Pläne zum „Schengen-Routing". URL: http://www.heise.de/netze/meldung/Das-DE-CIX-und-das-Schland-Netz-Betreiber-empoert-ueber-Telekom-Plaene-zum-Schengen-Routing-2044731.html.

Blome, Nicolaus/Gude, Hubert/Röbel, Sven/Schindler, Jörg/Schmidt, Fidelius (2014): Beifang im Netz. In: Der Spiegel 34/2014: S. 22-24.

Blühdorn, Ingolfur (2013): Simulative Demokratie: Neue Politik nach der Postdemokratischen Wende. Berlin: Suhrkamp.

BMWI (2014): Staatssekretär Kapferer: Offenes und freies Internet erhalten. URL: http://www.bmwi.de/DE/Presse/pressemitteilungen,did=642114.html.

BMWi/BMI/BMVI (2014): Bundesministerium für Wirtschaft und Energie/ Bundesministerium des Innern/ Bundesministerium für Verkehr und digitale Infrastruktur – Digitale Agenda 2014-2017, vom 20.08.2014. URL: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.

Boltanski, Luc/Thévenot, Laurent (2007): Über die Rechtfertigung Eine Soziologie der kritischen Urteilskraft. Hamburg: Hamburger Edition.

Bourdieu, Pierre (1987): Die feinen Unterschiede: Kritik der gesellschaftlichen Urteilskraft. Frankfurt a.M: Suhrkamp.

Bowie, Norman E. (2013): Privacy and the Internet. In: Hugh LaFollette (Hg.): The International Encyclopedia of Ethics. Hoboken, New Jersey: Wiley-Blackwell, S. 4110–4114.

Boyd, Danah (2011): Dear Voyeur, meet Flâneur… Sincerely, Social Media. In: Surveillance & Society 8(4): S. 505-507.

Boyd, Danah (2012): Networked Privacy. In: Surveillance & Society 10(3/4): 348-350.

Braun, Herbert (2014): Kommentar: Wie die USA ihre IT-Wirtschaft zerstört. In: heise.de, 5.8.2014. URL: http://heise.de/-2283109.

Brin, David (1998): The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? New York: Perseus Books.

Bröcker, Michael (2013): Friedrich: „Stolz auf unsere Geheimdienste“. In: Rheinische Post v. 16.08.2013.

Brüne, Klaus (2009): Lexikon E-Business. Frankfurt a./M.: Deutscher Fachverlag.

Brunst, Phillip W. (2011): Staatlicher Zugang zur digitalen Identität. In: Datenschutz und Da-tensicherheit-DuD 35 (9), S. 618–623.

Bundesministerium des Innern (2014) (Hg.): Verfassungsschutzbericht 2013. Berlin: Bundesministerium des Innern.

Bundesregierung (2014): Pressekonferenz zur Digitalen Agenda 2014 – 2017, Nr. 67, vom 08.03.2014. URL: http://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2014/03/2014-03-08-pk-digitale-agenda.html.

Bundesverband IT-Mittelstand e.V. (2013): Koalitionsvertrag verpasst den digitalen Auf-bruch. In: bitmi.de, 28.11.2013. URL: http://www.bitmi.de/php/evewa2.php?menu=019901&newsid=1870.

Butterwegge, Christoph (2002): Rechtsextremismus. Freiburg i. Br./Zürich/Wien: Herder.

Callon, Michel (1986): Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fisherman of St. Brieuc Bay. In: Law, John (Hg.): Power, Action, and Belief. A New Sociology of Knowledge? London/Boston/Henley.

Campact (2013): Starker europäischer Datenschutz jetzt. URL: https://www.campact.de/eu-datenschutz/appell/teilnehmen/.

Cancik, Hubert/Schneider, Helmuth (Hg.) (2014): Der Neue Pauly. Stuttgart: Metzler.

Cauley, Leslie (2006): NSA has massive database of Americans‘ phone calls. In: USA Today, 11.5.2007. URL: http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

CDU/CSU/SPD (2013): Deutschlands Zukunft gestalten, Koalitionsvertrag zwischen CDU, CSU und SPD, 18 Legislaturperiode. Berlin: Union Betriebs-

GmbH. URL:
http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=6D554BC1411A57B8961E32868D3EF374.s4t1?__blob=publicationFile&v=2.

Chambers, John T. (2014): Letter To Barack Obama. Veröfft. 15.05.2014.

Clarke, Adele (1991): Social Worlds Theory as Organizational Theory. In: Maines, D. (Hg.): Social Organization and Social Process: Essays in Honour of Anselm Strauss. Hawthorne, NY: Aldine de Gruyter, S. 17-42.

Clarke, Adele (2012): Situationsanalyse. Grounded Theory nach dem Postmodern Turn. Wiesbaden: Springer VS.

Clarke, Adele/Keller, Reiner (2011): „Für mich ist die Darstellung der Komplexität der ent-scheidende Punkt." Zur Begründung der Situationsanalyse. Adele Clarke im Gespräch mit Reiner Keller. In: Mey, Günter/Mruck, Katja (Hrsg.) (2011): Grounded Theory Reader, 2. aktualisierte und erweiterte Auflage. Wiesbaden: Springer VS, S. 109-131.

Clarke, Richard A./Morell, Michael J./Stone, Goffrey R./Sunstein, Cass R./Swire, Peter (2013): The NSA Report: Liberty and Security in a Changing World. Princeton: Princeton University Press.

Coke, Edward (1669): The Third Part of the Institutes of the Laws of England, Concerning High Treason, and Other Pleas of the Crown and Criminal Issues, 4. Aufl. London.

Cole, David (2014): We Kill People Based on Metadata. In: The New York Review of Books, 10.05.2014. URL:
http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/.

Computerwoche.de (2014): http://www.computerwoche.de/a/jede-initiative-fuer-mehr-datensicherheit-hat-meine-unterstuetzung,2555720

Cooley, Thomas M. (1906): A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract. Chicago: Callaghan & Company.

Cornevin, Christophe (2013): Squarcini: Nous aussi nous espionnons les Américains. In: Le Figaro, 23.10.2013. URL: http://www.lefigaro.fr/actualite-

france/2013/10/23/01016-20131023ARTFIG00546-squarcini-nous-aussi-nous-espionnons-les-americains.php.

Crouch, Colin (2008): Postdemokratie. Frankfurt a. M.: Suhrkamp.

cybererrorism (2013): Privacy-Handbuch. In: linksunten.indymedia.org. Veröfft. 07.06.2013. URL https://linksunten.indymedia.org/en/node/88268.

Das, S., & Kramer, A. (2013, June). Self-Censorship on Facebook. In *ICWSM*.

de Maizière, Thomas (2014): „Unser Datenschutzrecht hat ausgedient". In: FAZ v. 18.08.2014.

de Maizière, Thomas (2014a): „Schutz – Sicherheit – Vertrauen". In: Konferenz für Datenschutz und Datensicherheit, 23.06.2014. URL: http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/06/dud-fachkonferenz.html.

DE-CIX (2013): Nationales Routing: DE-CIX lädt Deutsche Telekom an den Verhandlungs-tisch. Pressenmitteilung, 13.11.2013. URL: http://presse.de-cix.net/uploads/media/PM_DE-CIX-NationalesRouting_vfinal.pdf.

Degele, Nina/ Dries, Christian (2005): Modernisierungstheorie. München: Wilhelm Fink.

Deleuze, Gilles/Guattari, Félix (1992): Tausend Plateaus. Kapitalismus und Schizophrenie II. Berlin: Merve.

Deleuze, Gilles/Guattari, Félix (1994): What Is Philosophy? New York: Columbia University Press.

Der Spiegel (1983): Muß das Recht kontingentiert werden? In: Der Spiegel 29/1981: S. 20.

Der Spiegel (2012): Eindringliche Bitte. In: Der Spiegel 21/2012: S. 15.

Der Spiegel (2013): Aufschub gefordert. In: Der Spiegel 51/2013: S. 17.

Der Spiegel (2014): ,,Schlandnet? Furchtbar!". In: Der Spiegel 28/2014: S. 74 f.

Der Spiegel (2014): Ärger über Maas. In: Der Spiegel 3/2014: S. 15.

Der Spiegel (2014): Cyberkriminalität – „Was gedacht werden kann, wird auch gemacht". In: Spiegel 32/2014: 32-34.

Der Spiegel (2014): Das große Speichern. In: Der Spiegel 37/2014: S. 16.

Der Spiegel (2015): Die Legende von Hilden. In: Der Spiegel 37/2015: S. 40.

Desoi, Monika/Knierim, Antonie (2011): Intimsphäre und Kernbereichsschutz – Ein unantastbarer Bereich privater Lebensgestaltung in der Rechtsprechung des Bundesverfassungsgerichts. In: DÖV (2011): S. 398-405.

Detjen, Stephan (1999): In bester Verfassung?!. Köln: Verlag Dr. Otto Schmidt.

Deutsche Wirtschaftsnachrichten (2014): Wegen NSA-Affäre: Brasilien plant direkte Internetverbindung nach Europa. In: deutsche-wirtschafts-nachrichten.de, 24.02.2014. URL: http://deutsche-wirtschafts-nachrichten.de/2014/02/24/wegen-nsa-affaere-brasilien-plant-direkte-internetverbindung-nach-europa/.

Dierichs, Stefan/Pohlmann, Norbert (2008): So funktioniert Internet-Routing. In: heise.de, 15.9.2008. URL: http://heise.de/-221495.

Diersch, Verena (2014): Ein Bericht über Cyber Security Summit 2013 der Münchener Sicherheitskonferenz und der Deutschen Telecom in Bonn. In: Zeitschrift für Außen- und Sicherheitspolitik (2014): S. 67-73.

Digitale Gesellschaft e.V. (Hg.) (2014): Internationale Bürgerrechtsorganisationen: Unternehmen gefährden unsere Grundrechte auf Privatsphäre und Datenschutz. URL: https://digitalegesellschaft.de/wp-content/uploads/2013/04/EUDATAP_REPORT_DE1-0.pdf Veröfft. 25.04.2013.

DIVSI/dimap (2014): Untersuchung zur Wahrnehmung des „Snowden/NSA-Skandals“ in Deutschland. Bonn 08.05.2014.

Dohmen, Frank/Traufetter, Gerald (2013): Traum vom Internetz. In: Der Spiegel 46/2013: S. 46.

Dreier, Horst (2013): Grundgesetz, Kommentar. Tübingen: Mohr Siebeck.

Duden, Konrad (2007): Deutsches Universalwörterbuch. Mannheim: Bibliographisches Institut.

DW (2014): NSA wollte Yahoo Millionenstrafe aufdrücken. In: DW, 11.09.2014. URL: http://www.dw.de/nsa-wollte-yahoo-millionenstrafe-aufdr%C3%BCcken/a-17917251.

Ehrenberg, Alain (2004): Das erschöpfte Selbst. Depression und Gesellschaft in der Gegenwart. Frankfurt a.M.: Campus.

Endert, Julius (2014): re:publica: Netzaktivisten fordern Asyl für Snowden. In: Hyperland. Veröfft. 06.05.2014. URL. http://blog.zdf.de/hyperland/2014/05/republica-netzaktivisten-fordert-asyl-fuer-snowden/.

Esch, Franz-Rudolf (2011): Strategie und Technik der Markenführung. 7. Aufl. München: Vahlen.

Ess, Charles (2005): "Lost in Translation"?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia). Ethics and Information Technology 7(1), 1–6.

Etzioni, Amitai (1999): The Limits of Privacy. New York: Basic Books.

EU-Kommission (2000): Mitteilung der Kommission zum Status der Grundrechtscharta der europäischen Union, Dok. CHARTE 4487/00 (CONVENT 50).

Europäisches Parlament (2001): Bericht über die Existenz eines globalen Abhörssystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), 11.7.2001 (A5-0264/2001).

Europäisches Parlament (2014): Bericht über das Überwachungsprogramm der Nationalen Sicherheitsagenturen der Vereinigten Staate, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres, 21.2.2014 (A7-0139/2014, 2013/2188(INI)).

Evans, M.D.R./Kelley, Jonathan (2002): National Pride in the Developed World. Survey Data From 24 Nations. In: International Journal Of Public Opinion Research 14 (3), S. 303-338.

Faz.net (2013): Im Gespräch: René Obermann und Frank Rieger. Snowdens Enthüllungen sind ein Erdbeben, erschienen am 29.11.2013. URL: http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/im-gespraech-rene-obermann-und-frank-rieger-snowdens-enthuellungen-sind-ein-erdbeben-12685829.html.

Felipe, Nancy Jo/Sommer, Robert (1966): Invasions of Personal Space. In: Social Problems 14 (2), S. 206–214.

Foschepoth, Josef (2012): Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik. Göttingen: Vandenhoeck & Ruprecht.

Foucault, Michel (2006): Die Geburt der Biopolitik. Geschichte der Gouvernementalität II. Frankfurt a.M.: Suhrkamp.

Frevert, Ute (2013): Vertrauensfragen. Eine Obsession der Moderne. München: C. H. Beck.

Frings, Cornelia (2010): Soziales Vertrauen. Eine Integration der soziologischen und der öko-nomischen Vertrauenstheorie. Wiesbaden: VS.

Fr-Online.de (2013): Grüne wenden sich an Menschenrechtsausschuss, erschienen am 12.09.2013, unter http://www.fr-online.de/politik/nsa-spionage-gruene-wenden-sich-an-menschenrechtsausschuss,1472596,24297468.html.

Frotscher, Werner/Pieroth, Bodo (2012): Verfassungsgeschichte. München: C. H. Beck.

Fujimura, Joan H. (1992): Crafting Science: Standardized Packages, Boundary Objects and 'Translation.' In: Pickering, Andrew (1992): Science as Practice and Culture. Chicago.

fukami (2014): Die fünf B und die IT-Sicherheit. In: Netzpolitik.org, 25.08.2014. URL: https://netzpolitik.org/2014/die-fuenf-b-und-die-it-sicherheit/.

Gabriel, Sigmar (2013): Die offene Gesellschaft und ihre digitalen Feinde. In: FAZ v. 02.07.2013.

Gabriel, Sigmar (2014): Die Demokratie im digitalen Zeitalter. In: FAZ v. 16.05.2014.

Gärditz, Klaus Ferdinand (2014): Anmerkung zum Urteil des BVerwG vom 28.05.2014 (6 A 1/13, JZ 2014, 994) - Zur Rechtmäßigkeit strategischer Telekommunikationsüberwachungsmaßnahmen durch den Bundesnachrichtendienst und Ausschluss von Popularklagen. In: JZ (2014): S. 998-1002.

Garrett, Roland (1974): „The Nature of Privacy“. In: Philosophy Today 18 (4) , S. 263-284.

Gaugele, Jochen/Kade, Claudia/Malzahn, Claus Christian/Vitzthum, Thomas (2014): Dobrindt will mit „Netzallianz" an die Weltspitze. In: Die Welt v. 12.01.2014.

Gavison, Ruth (1980): Privacy and the Limits of Law. In: The Yale Law Journal 89 (3), S. 421–471.

Gavison, Ruth (1992): Feminism and the Private-Public Distinction. In: Stanford Law Review 45, S. 1–45.

Gaycken, Sandro (2014): Sachverständigengutachten „IT-Infrastruktur“, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, A-Drs. 53, MAT A SV-1/1.

Gellman, Barton/Tate, Julie (2014): In NSA-intercepted data, those not targeted far outnumber the foreigners who are. In: Washington Post Online, 5.7.2014. URL: http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?tid=pm_pop.

Geminn, Christian L. (2014): Rechtsverträglicher Einsatz von Sicherheitsmaßnahmen im öffentlichen Verkehr. Wiesbaden: Springer.

Geminn, Christian L. (2015): Die Debatte um nationales Routing – Eine Scheindebatte? Eine kritische Analyse der Argumentationslinien. In: MMR (2015): S. 98-103.

Geminn, Christian L./Roßnagel, Alexander (2015): „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts – ein Überblick. In: JZ (2015): S. 703-708.

Generalbundesanwalt (2014): Pressemitteilung des Generalbundesanwalts 17/2014, 4.6.2014.

Gerber, Tim (2014): Mitleser. In: c’t 14/2014: S. 36.

Gerling, Rainer W. (2014): De-Mail und E-Mail made in Germany sind ein konsequenter Schritt. In: DuD (2014), S. 109-111.

Geuss, Raymond (2013): Privatheit. Eine Genealogie. Frankfurt a.M.: Suhrkamp.

Giddens, Anthony (1990): The Consequences of Modernity. Stanford, Kalifornien: Stanford University Press.

Glaeßner, Gert-Joachim/Lorenz, Astrid (2005b): Europäisierung der Politik innerer Sicherheit – Konzept und Begrifflichkeiten. In: Glaeßner, Gert-

Joachim/Lorenz, Astrid (Hrsg.) (2005a): Europäisierung der inneren Sicherheit. Eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus. Wiesbaden: VS, S. 7-41.

Glaeßner, Gert-Joachim/Lorenz, Astrid (Hg.) (2005a): Europäisierung der inneren Sicherheit. Eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus. Wiesbaden: VS.

Goetz, John/Leyendecker, Hans/Obermaier, Frederik (2014): BND will soziale Netzwerke live ausforschen. In: SZ v. 30.05.2014.

Greenwald, Glenn (2014): Die globale Überwachung. München: Droemer.

Greger, Reinhard (2000): Justizreform? Ja, aber…. In: JZ (2000): S. 842-851.

Gude, Hubert/ Schindler, Jörg (2015): Bundesregierung. Ein Gesetz für den Weltraum. In: Der Spiegel 16/2015: S. 13.

Habermas, Jürgen (1987): Theorie des kommunikativen Handelns. Bd. 1. Frankfurt a.M.: Suhrkamp.

Habermas, Jürgen (1987): Theorie des kommunikativen Handelns. Bd. 2. Frankfurt a.M.: Suhrkamp.

Habermas, Jürgen (1990): Strukturwandel der Öffentlichkeit. Frankfurt a.M.: Suhrkamp.

Habermas, Jürgen (1996): Der europäische Nationalstaat – Zu Vergangenheit und Zukunft von Souveränität und Staatsbürgerschaft, in: ders. (1996): S. 128-153.

Habermas, Jürgen (1996): Die Einbeziehung des Anderen. Studien zur politischen Theorie. Frankfurt a.M.: Suhrkamp.

Haffke, Bernd (2005): Vom Rechtsstaat zum Sicherheitsstaat? In: Kritische Justiz 38 (1), S. 17-35.

Hahn, Kornelia/Koppetsch, Cornelia (2011): Zur Soziologie des Privaten. Einleitung. In: Kornelia Hahn und Cornelia Koppetsch (Hg.): Soziologie des Privaten. Wiesbaden: VS, S. 7–16.

Hahn, Sebastian (2014): Tor-Fragen. Veröfft. 04.07.2014. URL: https://wwwcip.cs.fau.de/~snsehahn/Tor-Fragen.

Hall, Edward T. (1969): The Hidden Dimension. New York: Anchor Books.

Han, Byung-Chul (2012): Transparenzgesellschaft. Berlin: Matthes & Seitz.

Handelsblatt (2013): Politik muss in der NSA-Affäre endlich handeln, erschienen am 09.12.2013. URL: http://www.handelsblatt.com/unternehmen/it-medien/telekom-chef-obermann-politik-muss-in-der-nsa-affaere-endlich-handeln/9190358.html.

Handelsblatt (2014): Regierung hält Überwachung sozialer Netzwerke für rechtens. In: Handelsblatt, 25.07.2014.

Handelsblatt (2014a): Apple will besser über Datenschutz informieren. In: Handelsblatt. Veröfft. 18.09.2014. URL: http://www.handelsblatt.com/unternehmen/it-medien/absicherung-der-privatsphaere-apple-will-besser-ueber-datenschutz-informieren/10717918.html.

Hannan, Michael T./John Freeman (1977): The Population Ecology of Organizations. In: American Journal of Sociology 82 (5): S. 929-964.

Hansen, Marit (2014): Datenschutz nach dem Summer of Snowden. In: DuD 2014: S. 439-444.

Harth, Annette/Scheller, Gitta (2012): Das Wohnerlebnis in Deutschland. Eine Wiederholungsstudie nach 20 Jahren. Wiesbaden: Springer VS.

Heesen, Jessica (2013): Sicherheit, Macht und Ethik. In: Ammicht Quinn, Regina (Hg.): Sicherheitsethik. Wiesbaden: Springer VS, S. 75-90.

heise.de (2014): Bund sichert überraschend Mailtransporte per DANE ab. In: heise.de, 23.5.2014. URL: http://heise.de/-2196565.

heise.de (2014a): „NSA keine Gefahr“: Regierung wart vor Wirtschaftsspionage. In heise.de, 8.5.2014. URL: http://heise.de/-2185450.

heise.de (2014b): NSA-Skandal: Auch Bundestag beendet Kooperation mit Verizon. In: heise.de, 27.6.2014. URL: http://heise.de/-2241967.

heise.de (2014c): Gewerkschafts-Chef umreißt Gesellschaftsvertrag fürs digitale Zeitalter, erschienen am 10.09.2014. URL: http://www.heise.de/newsticker/meldung/Gewerkschafts-Chef-umreisst-Gesellschaftsvertrag-fuers-digitale-Zeitalter-2389285.html.

heise.de (2015): Auch de Maizère wendet sich gegen Verschlüsselung. In: heise.de, 21.1.2015. URL: http://heise.de/-2523297.

Heumann, Stefan/Scott, Ben (2013): Rechtsrahmen für geheimdienstliche Überwachung im Internet. USA, Großbritannien und Deutschland im Vergleich. In: Markus Beckedahl und Andre Meister (Hg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications, S. 149–171.

Heumann, Stefan/Wetzling, Torsten (2014): POLICY BRIEF Strategische Auslandsüberwachung: Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle. Stiftung Neue Verantwortung: Berlin.

Heuzeroth, Thomas (2014): „Es nützt nichts, Angst zu haben". In: Welt am Sonntag v. 2.11.2014, Ausg. 44: 5. URL: http://www.welt.de/print/wams/wirtschaft/article133893133/Es-nuetzt-nichts-Angst-zu-haben.html.

Hill, Hermann (1981): Rechtsschutz des Bürgers und Überlastung der Gerichte. In: JZ (1981): S. 805-815.

Hintz, Arne (2013): Ein Blick durch PRISMa. Whistleblowing, Informationsmacht und mediale Kurzsichtigkeit. In: Markus Beckedahl und Andre Meister (Hg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications, S. 91-100.

Hobbes, Thomas (1996 [1651]): Leviathan. Hamburg: Meiner.

Hoffmann-Riem, Wolfgang (2014): Freiheitsschutz in den globalen Kommunikationsinfrastrukturen. In: JZ (2014): S. 53-63.

Hoffmann-Riem, Wolfgang (2014a): Sachverständigengutachten, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, A-Drs. 54, MAT A SV-2/1 neu.

Hoffmann-Riem, Wolfgang (2014b): Globaler Auftrag. In: FAZ, 25.06.2014.

Holland-Cunz, Barbara (1998): Feministische Demokratietheorie. Thesen zu einem Projekt. Opladen: Leske und Budrich.

Hoppe, Till/Jakobs, Hans-Jürgen/Sigmund, Thomas (2014): „Wir arbeiten an einem Völkerrecht des Internets" In: Handelsblatt, 16.05.2014.

Hornung, Gerit (2012): Datenschutz – nur solange der Vorrat reicht?. In: PVS-Sonderheft 46/2012: S. 377-408.

House of Commons (2014): Counter-terrorism, Seventeenth Report of Session 2013-14, Home Affairs Committee. London.

Hufen, Friedhelm (2014): Staatsrecht II. München: C.H. Beck.

Huster, Stefan/Rudolph, Karsten (Hrsg.) (2008a): Vom Rechtsstaat zum Präventionsstaat. Frankfurt a.M.: Suhrkamp.

Illouz, Eva (2009): Die Errettung der modernen Seele. Gefühle und die Kultur der Selbsthilfe. Frankfurt a.M.: Suhrkamp.

Information Commissioner's Office (2007): Privacy Impact Assessment Handbook 2.0. URL: http://www.rogerclarke.com/DV/ICO-2007-V2.pdf.

Inness, Julie C. (1992): Privacy, Intimacy and Isolation. New York: Oxford University Press.

Internet & Gesellschaft Co:llaboratory. (2011): Gleichgewicht und Spannung zwischen digitaler Privatheit und Öffentlichkeit: Phänomene, Szenarien und Denkanstöße. Retrieved from http://dl.collaboratory.de/reports/Ini4_Privacy.pdf.

Internet Society German Chapter (2003): Balkanisierung des Internet kein geeignetes Konzept für mehr Datenschutz und Datensicherheit. 31.10.2003. URL: https://www.isoc.de/2013/10/balkanisierung-des-internet-kein-geeignetes-konzept-fur-mehr-datenschutz-und-datensicherheit/.

Isensee, Josef (1983): Das Grundrecht auf Sicherheit: Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Berlin: De Gruyter.

Isensee, Josef (2012 [1983]): Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Berlin: de Gruyter.

Ixquick (ohne Datum): 10 Wege, wie Sie mit Ixquick Ihre Privatsphäre zurückerobern. URL: https://www.ixquick.com/deu/top-ten-ways-ixquick.html.

Jarass, Hans/Pieroth, Bode (2012): Grundgesetz für die Bundesrepublik Deutschland. München: C. H. Beck.

Jarren Otfried/Röttger, Ulrike (2009): Steuerung, Reflexierung und Interpenetration: Kern-elemente einer strukturationstheoretisch begründeten PR-

Theorie. In: Röttger, Ulrike (Hg.): Theorien der Public Relations. Grundlagen und Perspektiven der PR-Forschung. 2 Auflage. Wiesbaden: VS, S. 29-50.

Jernigan, Carter/Mistree, Behram F. T. (2009): Gaydar: Facebook friendships expose sexual orientation. In: First Monday 14 (10).

Jeschke, Axel/Lamprecht, Werner (1981): Wir machen da keine gute Figur. In: Der Spiegel 32/1981: 35-45.

Joost, Gesche (2014): Schlandnet? Furchtbar!. In: Der Spiegel 28/2014: S. 74-76.

Kahn, Jonathan (2003): Privacy as a Legal Principle of Identity Maintenance. In: Seton Hall Law Review 33 (2), S. 371–410.

Kahn, Jonathan (2003): Privacy as a Legal Principle of Identity Maintenance. In: Seton Hall Law Review 33 (2), S. 371–410.

Karg, Moritz (2013): Die Renaissance des Verbotsprinzips im Datenschutz. In: Datenschutz und Datensicherheit-DuD 37 (2), S. 75–79.

Keiler, Hans/Kristoferitsch, Stephan (2006): Passagierdaten auf dem Flug in die USA. In: ZVR (2006): 484-489.

Keller, Reiner (2011): Diskursforschung. Wiesbaden: Springer VS.

Kleinz, Torsten/Krempl, Stefan (2015): Hacker mit Blick auf die Morgenröte. In: c't 3/2015: S. 16-19.

Klett, Detlef/Ammann, Torsten (2014): Gesetzliche Initiativen zur Cybersicherheit. In: CR (2014): S. 93-99.

Kling, Bernd (2013): PRISM: MIT-Tool erstellt Kommunikationsprofil aus Metadaten. In: ZDNet. Veröfft. 09.07.2013. URL: http://www.zdnet.de/88161487/prism-mit-tool-zeigt-kommunikationsprofil/.

Klumpp, Dieter/Kubicek, Herbert/Roßnagel, Alexander/Schulz, Wolfgang (2008): Informationelles Vertrauen für die Informationsgesellschaft. In: Dieter Klumpp, Herbert Kubicek, Alexander Roßnagel und Wolfgang Schulz (Hg.): Informationelles Vertrauen für die Informationsgesellschaft. Berlin: Springer, S. 1–16.

Koenzen, Ralf (2014): Schengen-Routing: Mit Verlaub, Mr. President, wir sind ein souveräner Staat. In: lancom-systems.de, 25.4.2014. URL: http://www.lancom-systems.de/blog/schengen-routing/.

Korff, Douwe (2014): Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the „5EYES" global surveillance systems revealed by Edward Snowden, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, A-Drs. 56, MAT A SV-4/3.

Krempl, Stefan (2008): 34.443 Klageschriften gegen die Vorratsdatenspeicherung. In: heise.de, 29.2.2008. URL: http://heise.de/-185285.

Krempl, Stefan (2014): Innenminister: „Vertrauen ist die neue Währung im Internet". URL: http://www.heise.de/newsticker/meldung/Innenminister-Vertrauen-ist-die-neue-Waehrung-im-Internet-2215318.html.

Kröger, Michael (2014): 200 US-Geheimdienstler spionieren offiziell in Deutschland. In: Spiegel Online, 15.06.2014. URL: http://www.spiegel.de/politik/deutschland/mehr-als-200-us-geheimdienstler-spionieren-offiziell-in-deutschland-a-975285.html.

Kubicek, Herbert (2008): Vertrauen durch Sicherheit - Vertrauen in Sicherheit. Annäherung an ein schwieriges Verhältnis. In: Dieter Klumpp, Herbert Kubicek, Alexander Roßnagel und Wolfgang Schulz (Hg.): Informationelles Vertrauen für die Informationsgesellschaft. Berlin: Springer, S. 17–36.

Kuhlen, Rainer (2008): Vertrauen in elektronischen Räumen. In: Dieter Klumpp, Herbert Kubicek, Alexander Roßnagel und Wolfgang Schulz (Hg.): Informationelles Vertrauen für die Informationsgesellschaft. Berlin: Springer, S. 37–52.

Kumbruck, Christel (2012): Vertrauen in virtuellen Gemeinschaften und Kooperationen. In: Heidi Möller (Hg.): Vertrauen in Organisationen. Riskante Vorleistung oder hoffnungsvolle Erwartung? Wiesbaden: VS, S. 169–198.

Lamla, Jörn (2013a): Arenen des Demokratischen Experimentalismus. Zur Konvergenz von nordamerikanischem und französischem Pragmatismus. Berliner Journal für Soziologie 23 (3-4), S. 345-365.

Lamla, Jörn (2013b): Verbraucherdemokratie. Politische Soziologie der Konsumgesellschaft. Berlin: Suhrkamp.

Lange, Hans-Jürgen (2008): Der Wandel des föderalen Sicherheitsverbundes. In: Huster, Stefan/Rudolph, Karsten (Hrsg.): Vom Rechtsstaat zum Präventionsstaat. S. 64-81.

Latour, Bruno (2005): Reassembling the Social. An Introduction to Actor-Network-Theory. New York et al.: Oxford University Press.

Latour, Bruno (2010): Das Parlament der Dinge. Für eine politische Ökologie. Frankfurt a.M.: Suhrkamp.

Lau, Mariam (2013): Mit Spaß dabei. In: Zeit Online. Veröfft. 01.08.2013. URL: http://www.zeit.de/2013/32/bnd-gerhard-schindler.html.

Levy, Steven (2014): How the NSA almost killed the internet. In: Wired.com, 7.1.2014. URL: http://www.wired.com/threatlevel/2014/01/how-the-us-almost-killed-the-internet/all/.

Lobo, Sascha (2014): Dämonisierte Digitalkonzerne. In: Spiegel Online. Veröfft. 27.08.2014. URL: http://www.spiegel.de/netzwelt/web/sascha-lobo-ueber-die-daemonisierung-der-netzkonzerne-a-988308.html.

Lobo, Sascha (2014a): Die Macht der Metadaten. In: Spiegel Online. Veröfft. 14.05.2014. URL: http://www.spiegel.de/netzwelt/netzpolitik/google-urteil-eugh-entscheidung-zu-suchmaschinen-a-969302.html.

Lossau, Julia (2002): Die Politik der Verortung. Eine postkoloniale Reise zu einer anderen Geographie der Welt. Bielefeld: transcript.

Luhmann, Niklas (1973): Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. Stuttgart: Ferdinand Enke Verlag.

Luhmann, Niklas (1993): Das Recht der Gesellschaft. Frankfurt a.M.: Suhrkamp.

Maas, Heiko (2014): Rede zum Safer Internet Day 2014. Konferenz „Mailen, Surfen, Chatten – Wie ist die Privatsphäre noch zu retten?“, 11.02.2014. URL: http://www.bmj.de/SharedDocs/Reden/DE/2014/20140211_Rede_Safer_Internet_Day.html?nn=2708420.

MacKinnon, Catharine (1989): Toward a Feminist Theory of the State. Cambridge, Massa-chusetts: Harvard University Press.

MACOSPOL Project (ohne Datum): Lippmannian Device. URL: http://www.mappingcontroversies.net/Home/PlatformLippmannianDevice.

Mallmann, Otto (1977): Zielfunktionen des Datenschutzes – Schutz der Privatsphäre. Frankfurt a.M.: Luchterhand Verlag.

Mangoldt, Hermann/Klein, Friedrich/Starck, Christian (2010): Grundgesetz, Kommentar. München: Vahlen.

Margalit, Avishai (2012): Politik der Würde. Über Achtung und Verachtung. Frankfurt a.M.: Suhrkamp.

Markoff, John (2008): Internet Traffic Begins to Bypass the U.S. In: nytimes.com, 30.8.2008. URL: http://www.nytimes.com/2008/08/30/business/30pipes.html.

Marres, Noortje; Moats, David (2015): Mapping Controversies with Social Media: The Case for Symmetry. In: Social Media + Society 1 (2), S. 1–17. DOI: 10.1177/2056305115604176.

Mascolo, Georg; Baars, Christian (2016): BND spioniert wieder mit der NSA. In: tagesschau.de, 08.01.2016. URL: https://www.tagesschau.de/inland/bnd-nsa-113.html

Maunz, Theodor/Dürig, Günther (2015): Grundgesetz, Kommentar. München: C. H. Beck.

Mayer, Roger C./Davis, James H./Schoorman, F. David (1995): An integrative model of organizational trust. In: Academy of management review 20 (3), S. 709–734.McAdam, Doug/John D. McCarthy/ Mayer N. Zald (1996): Comparative Perspectives on Social Movements. Political Opportunities, Mobilizing Structures, and Cultural Framings. Cambridge: Cambridge University Press.

Meffert, Heribert/Burmann, Christoph/Koers, Martin (2012): Marketing. Grundlagen marktorientierter Unternehmensführung. 11. Aufl. Wiesbaden: Gabler.

Merkel, Angela (2013): Pressekonferenz vor dem EU-Gipfel, 24.10.2013.

Merkel, Angela (2014): „Wir gestalten Deutschlands Zukunft". Regierungserklärung, 11.06.2014.

Merkel, Angela (2014a): Video-Podcast der Bundeskanzlerin #02/2014, 15.02.2014.

Merkel, Angela (2014b): Video-Podcast der Bundeskanzlerin #05/2014, 08.03.2014.

Meyer, Jürgen (2014): Charta der Grundrechte der Europäischen Union. Baden-Baden: Nomos.

Meyer-Ladewig, Jens (2011): Europäische Menschenrechtskonvention. Baden-Baden: Nomos.

Microsoft (ohne Datum): Your Privacy Is Our Priority. In: Microsoft.com. Ohne Datum. URL: http://www.microsoft.com/en-GB/security/online-privacy/overview.aspx.

Miller, Russell/Poscher, Ralf (2013): Kampf der Kulturen. In: FAZ.net, 28.11.2013. URL: http://www.faz.net/aktuell/politik/staat-und-recht/praeventiver-datenschutz-kampf-der-kulturen-12685796.html.

Mitteldeutsche Zeitung (2013): Ex-BND-Präsident hält Überwachungsprogramme für legitim. In: Mitteldeutsche Zeitung, 26.06.2013.

Möller, Heidi (2012): Vertrauens- und Misstrauenskulturen in Organisationen. In: Heidi Möller (Hg.): Vertrauen in Organisationen. Riskante Vorleistung oder hoffnungsvolle Erwartung? Wiesbaden: VS, S. 13–28.

Moore, Adam (2008): Defining Privacy. In: Journal of Social Philosophy 39 (3), S. 411–428.

Moser-Knierim, Antonie (2014): Vorratsdatenspeicherung. Wiesbaden: Springer Vieweg.

Mühlberg, Annette (2013): Der Ausspähskandal - Weckruf für die Demokratie. In: Markus Beckedahl und Andre Meister (Hg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications, S. 37–46.

Münchner Projektgruppe für Sozialforschung e. V./Wissenschaftszentrum Umwelt Universität Augsburg (ohne Datum): Nanotechnology Risk Cartography. URL: http://riskcart.wzu.uni-augsburg.de/StartseiteVis.php?studie=NANO.

Nagenborg, Michael (2010): Vertrauen und Datenschutz. In: Maring, Matthias (Hg.): Vertrauen – zwischen sozialem Kitt und der Senkung von Transaktionskosten. Karlsruhe: Karlsruher Institut für Technologie, S. 153-167.

Nakashima, Ellen (2014): Judge orders Microsoft to turn over data held overseas. In: Washington Post, 31.7.2014. URL:

http://www.washingtonpost.com/world/national-security/judge-orders-microsoft-to-turn-over-data-held-overseas/2014/07/31/b07c4952-18d4-11e4-9e3b-7f2f110c6265_story.html.

NDR.de (2014): Snowden: NSA spioniert Wirtschaft aus. In: NDR.de, 25.1.2014. URL: http://www.ndr.de/nachrichten/netzwelt/Snowden-NSA-spioniert-Wirtschaft-aus,snowden235.html.

Neocleus, Mark (2007): Security, Liberty and the Myth of Balance. Towards a Critique of Security Politics. In: Contemporary Political Theory (2007) 6, S. 131–149.

Netzpolitik.org (2013): Stimmen zum Deutschlandnetz. Netzpolitik.org, 11.11.2013. URL: https://netzpolitik.org/2013/stimmen-zum-deutschlandnetz/.

Neumann, Linus (2013): Bullshit made in Germany. So hosten Sie Ihre De-Mail, Email und Cloud direkt beim BND! Vortrag auf dem 30c3. Veröff. 29.12.2013. URL: https://www.youtube.com/watch?v=V_SMsAA7wcg.

Nissenbaum, Helen (2010): Privacy in Context. Technology, Policy, and the Integrity of Social Life: Stanford University Press.

Obar, Jonathan/Clement, Andrew (2013): Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty, 1.7.2013. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311792.

Ochs, Carsten (2013): Digitale Glokalisierung. Das Paradox von weltweiter Sozialität und lokaler Kultur. Frankfurt/M.: Campus.

Ochs, Carsten (2014): Privat(heit) im Netz(werk). Internet Privacy zwischen kollektiver Normierung und individueller Kalkulation. In: Garnett, Simon/Halft, Stefan/Herz, Matthias/Mönig, Julia Maria (Hg.): Medien und Privatheit. Passau: Verlag Karl Stutz, S. 189-208.

Ochs, Carsten (im ersch.): Die Kontrolle ist tot – lang lebe die Kontrolle! Plädoyer für ein nach-bürgerliches Privatheitsverständnis. In: Mediale Kontrolle unter Beobachtung (4/1).

Olsen, Frances E. (1993): The Family and the Market. A Study of Ideology and Legal Re-form. In: Patricia Smith (Hg.): Feminist Jurisprudence. New York: Oxford University Press, S. 65-93.

Oppernhäuser, Holger (2011): Das Extremismus-Konzept und die Produktion von politischer Normalität. In: Forum für kritische Rechtsextremismusforschung (Hg.): Ordnung. Macht. Extremismus. Effekte und Alternativen des Extremismus-Modells. Wiesbaden: Springer VS, S. 35-58.

Palandt, Otto (2014): Bürgerliches Gesetzbuch. 73. Aufl. München: C.H. Beck.

Parent, William A. (1983): Privacy, Morality, and the Law. In: Philosophy & Public Affairs 12 (4), S. 269-288.

Patterson, Miles L./Mullens, Sherry/Romano, Jeanne (1971): Compensatory Reactions to Spatial Intrusion. In: Sociometry 34 (1), S. 114–121.

Pech, Sebastian (2014): Lizenzmodell der Cloud. In: ZUM (2014): S. 22-25.

Pfeffer, Jeffrey/Gerald R. Salancik (1978): The External Control of Organizations: A Resource Dependence Perspective. New York: Harper and Row.

Pfeiffer, Gerd (1981): Knappe Ressource Recht. In: ZRP (1981): S. 121-125.

Pohlmann, Norbert/Siromaschenko, Illya/Sparenberg, Michael (2014): Direktvermittlung, Das „Schengen-Routing" zu Ende gedacht: In: iX 2/2014: S. 112-118.

Pörksen, Bernhard/Detel, Hanne (2012): Der entfesselte Skandal: Das Ende der Kontrolle im digitalen Zeitalter. Köln: Herbert von Halem Verlag.

Privacy International (ohne Datum): What Is Privacy? URL: https://www.privacyinternational.org/?q=node/54.

Prosser, William L. (1960): Privacy. In California Law Review (1960), Volume 48, Issue 3: S. 383-423.

Rauscher, Thomas/Krüger, Wolfgang (2013): Münchener Kommentar zur Zivilprozessordnung, 4. Aufl. München: C. H. Beck.

re:publica (2014): INTO THE WILD – re:publica 2014. URL: https://republica.de/wild-republica-2014.

Reckwitz, Andreas (2006): Das hybride Subjekt. Eine Theorie der Subjektkulturen von der bürgerlichen Moderne zur Postmoderne. 1. Aufl. Weilerswist: Velbrück Wiss., S. 33-72.

Reda, Julia (2014): Europa Grenzenlos. In Piratenpartei. Veröff. 21.01.2014 URL: https://www.piratenpartei.de/2014/01/21/europa-grenzenlos/.

Regan, Priscilla M. (1995): Legislating Privacy. Technology, Scoial Values, and Public Policy. Chapel Hill, NC: Norh Carolina University Press.

Rieger, Frank (2013): Stimmen zum Deutschlandnetz. In: Netzpolitik.Org, 11.11.2013. URL: https://netzpolitik.org/2013/stimmen-zum-deutschlandnetz/.

Rieger, Frank (2013a): In: Schirrmacher, Frank: Snowdens Enthüllungen sind ein Erdbeben. In: FAZ, 29.11.2013.

Rieger, Frank (2014): NSA-Untersuchungsausschuss, Stenografisches Protokoll der 9. Sitzung, 26. Juni 2014, https://www.bundestag.de/blob/372418/97c666605f875474927dfcf5b42c4fcb/09-waidner_gaycken_rieger_endgueltig-data.pdf.

Rieger, Frank (2014a): Unser Jahr mit Edward Snowden. In: FAZ. Verööfft. 07.06.2014. URL: http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/frank-rieger-ueber-unser-jahr-mit-edward-snowden-12976923.html.

Ries, Uli (2014): SSL-Gau lässt Server bluten. In: c't Heft 10 (2014): S. 16-18.

Right Livelihood Award Stiftung (2014): Stockholmer Right Livelihood Award Stiftung belohnt Einsatz für Menschenrechte, Pressefreiheit, bürgerliche Freiheiten und Kampf gegen den Klimawandel, Pressemitteilung vom 24.09.2014. URL: http://www.rightlivelihood.org/fileadmin/Files/PDF/Press_releases/2014/German/20140924_announcement_DE.pdf.

Ripperger, Tanja (2003): Ökonomik des Vertrauens. 2. Aufl. Tübingen: Mohr-Siebeck.

Risebrodt, Martin (2000): Die Rückkehr der Religionen. Fundamentalismus und der ‚Kampf der Kulturen'. München: C.H. Beck.

Rogers, Mike/Ruppersberger, Dutch (2012): Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. U.S. Washington D.C.: House of Representatives.

Roggan, Frederik (2012), Nomos Kommentar zum G-10-Gesetz. Baden-Baden: Nomos.

Rolofs, Oliver (2014): Digitale Grundrechte Die Konsequenzen des NSA-Skandals sollte ein Cybersicherheitsabkommen. In: Internationale Politik (2014): S. 28-31.

Rosa, Hartmut (1998): Identität und kulturelle Praxis. Politische Philosophie nach Charles Taylor. Frankfurt a. M./New York: Campus.

Rosa, Hartmut (2005): Beschleunigung. Die Veränderung der Zeitstrukturen in der Moderne. Frankfurt a.M.: Suhrkamp.

Rosenbach, Marcel/Stark, Holger (2014): Der NSA-Komplex. München: Deutsche Verlags-Anstalt.

Rössler, Beate (2001): Der Wert des Privaten. Orig.-Ausg. Frankfurt a.M.: Suhrkamp (Suhrkamp Taschenbuch Wissenschaft, 1530).

Rubenfeld, Jed (2014): We need a new jurisprudence of anonymity. In: Washington Post, 13.1.2014. URL: http://www.washingtonpost.com/opinions/we-need-a-new-jurisprudence-of-anonymity/.

Ruhmann, Ingo (2014): NSA, IT-Sicherheit und die Folgen. In: DuD (2014): S. 40-46.

Sachs, Michael (2014): Grundgesetz, Kommentar. München: C.H. Beck.

Sassen, Saskia (2006): Territory – Authority – Rights. From Medieval to Global Assemblages. Updated Edition. Princeton/Oxford: Princeton University Press.

Schaar, Peter (2013): Welche Konsequenzen haben PRISM und Tempora für den Datenschutz in Deutschland und Europa? In: Markus Beckedahl und Andre Meister (Hg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications, S. 118–127.

Schaar, Peter (2013): Zwischen Big Data und Big Brother. In: RDV (2013): S. 223-227.

Schaar, Peter (2013a): Lässt sich die globale Internetüberwachung noch bändigen?. In: ZRP (2013): S. 214-216.

Schaar, Peter (2014): Parlamente müssen unsere Grundrechte verteidigen. In: Handelsblatt, 13.02.2014.

Schafer, Burkhard (2011): All changed, changed utterly?. In: DuD (2011): S. 634-638.

Schäfer, Hans-Bernd/Ott, Claus (2012): Lehrbuch der ökonomischen Analyse des Zivilrechts. Berlin/Heidelberg: Springer Gabler.

Schallaböck, Jan (2011): Grundfunktionen des Datenschutzes. In: Heinrich-Böll-Stiftung (Hg.): #public_life. Digitale Intimität, die Privatsphäre und das Netz, S. 69–73.

Scherer, Klaus (2014): Spionage unter Freunden – so what?. In: tagesschau.de, 6.5.2014. URL: http://www.tagesschau.de/ausland/nsa404.html.

Schetsche, Michael (2008): Empirische Analyse sozialer Probleme. Wiesbaden: VS.

Scheuerman, William E. (2014): Edward Snowden. Ziviler Ungehorsam im Zeitalter der totalen Überwachung. In: Mittelweg 36, 23 (2), S. 4-31.

Schindler, Gerhard (2013): Rede des BND-Präsidenten Gerhard Schindler anlässlich der 1. Nachrichtendienst-Konferenz am 13.9.2013. URL: http://www.bnd.bund.de/DE/Themen/Reden_der_Leitung/Redetexte/ Rede-Nachrichten-dienstKonferenz2013.html.

Schindler, Gerhard (2014): Rede des BND-Präsidenten Gerhard Schindler anlässlich der Eröffnung der Ausstellung „Die BND-Zentrale in Pullach" am 23. Juni 2014. URL: http://www.bnd.bund.de/DE/Themen/Reden_der_Leitung/Ausstellungseroeffnung/Rede_Ausstellungseroeffnung_node.Schmundt, Hilmar/Traufetter, Gerald (2014): Digitale Souveränität. In: Der Spiegel 6/2014: S. 78-80.

Schneier, Bruce (2012): Liars & Outliers. Enabling the Trust That Society Needs to Thrive. Indianapolis, Indiana: John Wiley & Sons.

Schneier, Bruce (2013): Die US-Regierung hat das Internet verraten. Wir müssen es uns zurückholen. In: Markus Beckedahl und Andre Meister (Hrsg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications, S. 217–219.

Schneier, Bruce (2013a): Die NSA-Spionage macht uns weniger sicher. In: heise.de, 29.10.2013. URL: http://www.heise.de/tr/artikel/Die-NSA-Spionage-macht-uns-weniger-sicher-1982369.html.

Schönleben, Dominik (2013): In Zukunft wird nichts mehr privat sein. In: Motherboard. Veröfft. 22.07.2013. URL: http://motherboard.vice.com/de/blog/in-zukunft-wird-nichts-mehr-privat-sein.

Schütze, Fritz (2002): Das Konzept der sozialen Welt im symbolischen Interaktionismus und die Wissensorganisation in modernen Komplexgesellschaften. In: Inken Keim und Werner Kallmeyer (Hg.): Soziale Welten und kommunikative Stile. Festschrift für Werner Kallmeyer zum 60. Geburtstag. Tübingen: Narr, S. 57–83.

Schuler, Ralf/Solms-Laubach, Franz (2013): BND weitet Internet-Überwachung aus. In: Bild, 16.06.2013.

Seemann, Michael (2014): Das Neue Spiel: Strategien für die Welt nach dem digitalen Kontrollverlust. Freiburg: orange-press.

Sendler, Horst (1979): Normenflut und Richter. In: ZRP (1979): S. 227-232.

Sennett, Richard (1978): The Fall of Public Man. New York: Penguin Books.

Simitis, Spiros (2014): Bundesdatenschutzgesetz. Wiesbaden: Nomos.

Sloterdijk, Peter (1998): Sphären. Bd. 1: Blasen. Frankfurt a.M.: Suhrkamp.

Solms-Lausbach, Franz (2014): De Maizière will Geheimdienst gegen USA einsetzen. In: Bild.de, 7.7.2014. URL: http://www.bild.de/politik/inland/cia/bnd-agent-spitzelte-fuer-cia-de-maiziere-fordert-schnelle-aufklaerung-36696936.bild.html.

Spiegel Online (2013): BND leitet massenhaft Metadaten an die NSA weiter. In: Spiegel Online, 04.08.2013. URL: http://www.spiegel.de/politik/deutschland/bnd-leitet-massenhaft-metadaten-an-die-nsa-weiter-a-914649.html.

Spiegel Online (2014): Friedrich fordert Deutsche zu mehr Datenschutz auf. In: Spiegel Online. Veröff. 16.07.2014. URL: http://www.spiegel.de/politik/deutschland/friedrich-fordert-deutsche-zu-mehr-datenschutz-auf-a-911445.html (Letzter Zugriff: 01.03.15).

Spinello, Richard A. (1997): The End of Privacy. In: America 176 (1), S. 9–13.

Stalder, Felix (2011): Autonomy beyond privacy: A rejoinder to Bennett. Surveillance & Society 8(4): 508-512.

Steeves, Valerie (2009): „Data Protection Versus Privacy: Lessons from Facebook's Beacon." In The contours of privacy, edited by David Matheson. Newcastle: Cambridge Scholars Publishing, 2009.

Strauss, Anselm L. & Corbin, Juliet (1996): Grounded Theory: Grundlagen Qualitativer Sozialforschung. Weinheim: Beltz.

Strauss, Anselm L. (1978): A Social World Perspective. In: Studies in Symbolic Interaction, Jg. 1, S. 119–128.

Strauss, Anselm L. (1982): Social Worlds and Legitimation Processes. In: Studies in Symbolic Interaction, Jg. 4, S. 171-190.

Strauss, Anselm L. (1993): Continual Permutations of Action. Hawthorne, NY: de Gruyter.

Strübing, Jörg (2007): Anselm Strauss. Konstanz: UVK.

Stuhr, Mathias (2010): Mythos New Economy. Die Arbeit an der Geschichte der Informationsgesellschaft. Bielefeld: transcript.

Süddeutsche.de (2014): Codewort Eikonal - der Albtraum der Bundesregierung, erschienen am 4.10.2014. URL: http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432.

Süddeutsche.de (2014a): BND leitet Date von Deutschen an NSA weiter. In: su-eddeutsche.de, 3.10.2014. URL: http://www.sueddeutsche.de/politik/spaeh-affaere-bnd-leitete-daten-vondeutschen-an-nsa-weiter-1.2157406.

Süßbauer, Alfons (1991): Sind Unternehmen moralisch verantwortlich? In: Kriterion 1991 (2), S. 33-48.

tagesschau.de (2014): Schnüffeln, bellen und beißen. In: tagesschau.de, 1.7.2014. URL: http://www.tagesschau.de/inland/geheimdienste-100.html.

tagesschau.de (2014a): Von der NSA als Extremist gebrandmarkt. In: tagesschau.de, 3.7.2014. URL: http://www.tagesschau.de/inland/nsa-xkeyscore-100.html.

tagesschau.de (2014c): Spionage unter Freunden – so what?. In. tagesschau.de, 6.5.2014. URL: https://www.tagesschau.de/ausland/nsa404.html.

tagesschau.de (2015): Großer NSA-Lauschangriff auf Bundesregierung. In: tagesschau.de, 1.7.2015. URL: https://www.tagesschau.de/inland/nsa-wikileaks-101.html.

tagessschau.de (2014b): „No Spy" soll Pflicht werden. In: tagesschau.de, 29.8.2014. URL: http://www.tagesschau.de/inland/nsa-skandal-bundeslaender-100.html.

Talbot, David (2013): Die NSA-Spionage macht uns weniger sicher. In: heise.de, 29.10.2013. URL: http://www.heise.de/tr/artikel/Die-NSA-Spionage-macht-uns-weniger-sicher-1982369.html.

Talmon, Stefan (2014): Der Begriff der „Hoheitsgewalt" in Zeiten der Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste. In: JZ (2014): S. 783-787.

Talmon, Stefan (2014a): Sachverständigengutachten gemäß Beweisbeschluss SV-4 des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, A-Drs. 56, MAT A SV-4/2.

Tamblyn, Thomas (2015): David Cameron Want To Ban Snapchat. In: huffingtonpost.co.uk, 12.1.2015. URL: http://www.huffingtonpost.co.uk/2015/01/12/david-cameron-wants-to-ban-snapchat_n_6456326.html.

Tanenbaum, Andrew S./Wetherall, David J. (2011): Computer Networks. Washington: University of Washington.

Teubner, Gunther (1987): Episodenverknüpfung. Zur Steigerung von Selbstreferenz im Recht. In: Dirk Baecker, Jürgen Markowitz und Rudolf Stichweh (Hg.): Theorie als Passion. Niklas Luhmann zum 60. Geburtstag. Frankfurt a.M: Suhrkamp, S. 423–446.

Teubner, Gunther (1989): Recht als autopoietisches System. Frankfurt a.M: Suhrkamp.

Thevesen, Elmar (2013): Ex-NSA-Chef spottet über deutsche Politiker. In heute.de. Veröfft. 20.07.2013. URL: http://www.heute.de/ex-nsa-chef-michael-hayden-im-interview-mit-terror-experte-elmar-thevessen-28928066.html.

United States Trade Representative (2014): 2014 Section 1377 Review v. 4.4.2014. URL: http://www.ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf.

Venturini, Tommaso (2010): Diving in magma: How to explore controversies with actor-network theory. In: Public Understanding of Science, Jg. 19, Nr. 3, S. 258-273.

Venturini, Tommaso (2012): Building on faults: how to present controversies with digital methods. In: Public Understanding of Science, Jg. 21, Nr. 7, S. 796-812.

Voigt, Rüdiger (1989): Recht als strategische Ressource. In: Luthardt/Söllner (1989): Verfassungsstaat, Souveränität, Pluralismus. Opladen: Westdeutscher Verlag.

Waidner, Michael (2014): Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode, A-Drs. 53, MAT A SV-1/2.

Warren, Samuel D./Brandeis, Louis D. (1890): The Right to Privacy. In: Harvard law review 4 (5), S. 193–220.

Warren, Samuel D./Brandeis, Louis D. (2012 [1890]): Das Recht auf Privatheit – The Right to Privacy. In: DuD 2012 (10), S. 755-766.

Weichert, Thilo (2012): Datenschutzverstoß als Geschäftsmodell - der Fall Facebook. In: DuD 36 (10), S. 716–721.

Welt am Sonntag (2014): Das Viertelfinale ist Pflicht, Interview mit Bundesinnenminister Dr. Thomas de Maizière, erschienen am: 18.05.2014. URL: http://www.bmi.bund.de/SharedDocs/Interviews/DE/2014/05/bm-welt-am-sonntag.html.

Welt.de (2014): Angeblich mehr US-Spione in deutschen Ministerien, erschienen am 13.07.2014. URL: http://www.welt.de/politik/deutschland/article130092561/Angeblich-mehr-US-Spione-in-deutschen-Ministerien.html.

Werhane, Patricia H. (1992): Rechte und Verantwortung von Korporationen. In: Lenk, Hans/Maring Matthias (Hg.): Wirtschaft und Ethik. Stuttgart: Reclam, S. 329–336.

Westin, Alan F. (1967): Privacy and Freedom. New York: Atheneum.

WirtschaftsWoche (2014): Echte Zerreißprobe, erschienen am 17.02.2014, Ausgabe 8/2014, S. 52-54.

Wohlrab-Sahr, Monika (2011): Schwellenanalyse - Plädoyer für eine Soziologie der Grenz-ziehungen. In: Kornelia Hahn und Cornelia Koppetsch (Hg.): Soziologie des Privaten. Wiesbaden: VS, S. 33–52.

Wohlrab-Sahr, Monika (2011): Schwellenanalyse - Plädoyer für eine Soziologie der Grenz-ziehungen. In: Kornelia Hahn und Cornelia Koppetsch (Hg.): Soziologie des Privaten. Wiesbaden: VS, S. 33–52.

Wohlwill, Joachim F. (1974): Human Adaptation to Levels of Environmental Stimulation. In: Human Ecology 2 (2), S. 127–147.

zeit.de (2014): Guillaume war nicht mal Mittelkasse. In: zeit.de, 2.11.2014. URL: http://www.zeit.de/2014/43/stasi-geheimdienst-spionage.

zeit.de (2014a): NSA soll Heartbleed-Lücke ausgenutzt haben. In: zeit.de, 11.4.2014. URL: http://www.zeit.de/digital/datenschutz/2014-04/heartbleed-nsa-internet-sicherheit.

Zuckerberg, Mark (2010): In: Johnson, Bobbie: Privacy no longer a social norm, says Facebook founder. In: The Guardian, 11.01.10.

Zuckerberg, Mark (2014): In: Pohl, Elisabeth: Facebook legt plötzlich Wert auf Privatsphäre. In: Netzpolitik.org, 28.07.2014. URL: https://netzpolitik.org/2014/facebook-legt-ploetzlich-wert-auf-privatsphaere/.

In Reaktion auf die Enthüllungen Edward Snowdens und die dadurch aktualisierte Krise der Privatheit tritt die Reterritorialisierung des Digitalen als Reaktionsweise zeitgenössischer Demokratien auf den Plan. Verwerfungen im Zuge zunehmend globalisierter Datenströme sollen nach altbekanntem Muster der territorialen und nationalen Containergesellschaften gekittet werden. Reterritorialisierung adressiert dabei einen digital induzierten Wandel und versucht, Antworten zu geben auf Fragen der gegenwärtigen Neukonfiguration des Verhältnisses von Demokratie und Gesellschaft. Die Kartografie der dynamischen Arena um das umstrittene Konzept Privatheit liefert empirische Erkenntnisse zu einem der meistdiskutierten sozialen Ordnungsmechanismen und zeigt, wie die politische Suche nach Lösungen angesichts der tektonischen Verschiebungen der Digitalisierung mit bestehenden Institutionen, Routinen und Ressourcen verbunden bleibt. Die Publikation präsentiert Ergebnisse des BMBF-Projektes "Kartografie und Analyse der Privacy-Arena", an dem die Disziplinen Soziologie, Rechtswissenschaft und Philosophie/Ethik beteiligt sind.

UNIKASSEL VERSITÄT

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

ISBN 978-3-86219-106-2