Carl von Ossietzky
Universität Oldenburg

Zwei-Fächer Bachelor:
Sozialwissenschaften / Philosophie

Bachelorarbeit

Sicherheit und Freiheit im Informationszeitalter

Eine Politikfeldanalyse unter besonderer Berücksichtigung des Gesetzes zur Regelung von De-Mail-Diensten

vorgelegt von
Konrad Keck

Betreuender Gutachter
Dr. Klaus Finke

Zweite Gutachterin
Prof. Dr. Anabella Weismann

Oldenburg, 27. September 2011

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungen

1:1	„Eins zu Eins“
1:n	„Eins zu n“ bzw. „Eins zu Beliebig viele“
9/11	11. September 2011; Tag der islamistischen Terroranschläge gegen die USA
a.M.	am Main
Abb.	Abbildung
Abs.	Absatz
AG	Aktiengesellschaft
AK Zensur	Arbeitskreis gegen Internetsperren und Zensur
ANT	Actor-Network Theory (Akteur-Netzwerk Theorie)
(D)ARPA	(Defense) Advance Research Project Agency
Art.	Artikel
B'90/Grüne	Bündnis 90/Die Grünen (Grüne)
BDSG	Bundesdatenschutzgesetz
BEUC	Bureau Européen des Unions de Consommateurs
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BKA	Bundeskriminalamt
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMI	Bundesministerium des Inneren
BMWi	Bundesministerium für Wirtschaft und Technologie
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BRD	Bundesrepublik Deutschland
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTX	Telebox-System und Bildschirmtext
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CCC	Chaos Computer Club
CDU	Christlich Demokratische Union

CERN	Conseil Européen pour la Recherche Nucléaire (Europäische Organisation für Kernforschung)
Code	Source / Programmcode / Quelltext
CSU	Christlich Soziale Union
d.h.	das heißt
DBP	Deutsche Bundespost
(D)DoS	(distributed) denial of service ((verteilte) Verweigerung der Dienstleistung)
DDR	Deutsche Demokratischen Republik
DKIM	DomainKeys Identified Mail Signatures (Adressschlüssel identifizierende Mail Signaturen)
DMailG	Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften
DPI	Deep Package Inspektion (tiefe Pakete-Einsicht)
ebd.	Ebenda: genau, gerade dort (= wie vorgenannt)
EDV	Elektronischen Datenverarbeitung
ELENA	elektronische Entgeltnachweis-Verfahren
E-Mail	electronic mail (elektronische Briefpost)
EMO	European Music Office
. . . et al.	. . . und andere
EU	European Union (Europäische Union)
FDP	Freie Demokratische Partei
G10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz)
GeStaPo	Geheime Staatspolizei
GG	Grundgesetz für die Bundesrepublik Deutschland
GMail	Google-Mail
GUI	Graphical User Interface (grafische Benutzeroberfläche)
Herv. v. Vf	Hervorhebung vom Verfasser
I/O	An/Aus
IBM	International Business Machines Corporation
IMAP	Internet Message Access Protocol (Internet-Nachrichtenzugriffsprotokoll)
IP	Internet Protocol

ISO	Internationalen Organisation für Normung
ISP	Internet Service Provider (Internet Dienstanbieter; Provider)
IT	Informationstechnik
KGB	Komitet gossudarstwennoi besopasnosti pri Sowjete Ministrow SSSR (Komitee für Staatssicherheit beim Ministerrat der UdSSR)
LulzSec	Lulz Security
m.a.W.	mit anderen Worten
MS	Microsoft
Nr.	Nummer
OS	Operating System (Betriebssystem)
OSI	Open Systems Interconnection Reference Model
P2P	Peer-to-Peer (Anschluss zu Anschluss)
PC	Personal Computer
PEC	posta elettronica certificata (zertifizierte elektronische Post)
Piraten	die Piratenpartei
POP3	Post Office Protocol (Postübertragungsprotokoll Version 3)
RAF	Rote Armee Fraktion
REM	Registered E-Mail
RFC	Requests for Comments (Anfrage nach Kommentaren)
SMTP	Simple Mail Transfer Protocol (einfaches Nachrichtenversandprotokoll)
SNS	Sozial Network Sites (Soziale Netzwerk-Seiten)
SPD	Sozialdemokratische Partei Deutschlands
SWIFT	Society for Worldwide Interbank Financial Telecommunication (weltweite Gemeinschaft der Geldinstitute und Telekommunikation)
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.a.	unter anderem
URL	Uniform Resource Locator (einheitlicher Quellenanzeiger)
USA	United States of America (Vereinigte Staaten von Amerika)
VDS	Vorratsdatenspeicherung(-sgesetz)
vgl.	vergleiche
Win	Windows
WWW	World Wide Web (Weltweites Netzwerk) = Web (Netz)

1. Einleitung

Diese Arbeit thematisiert die verfassungsrechtlichen Grundwerte Sicherheit und Freiheit, deren Problematik im Informationszeitalter besondere Bedeutung erlangt hat. Politik und Wissenschaft sind durch das Aufkommen digitaler Kommunikationstechnologien dazu aufgerufen, sich mit neuen gesellschaftlichen Phänomenen auseinanderzusetzen. Innerhalb dieses noch jungen Themenkomplexes ist der alte Konflikt zwischen Sicherheit und Freiheit abermals zu betrachten. Debatten in diesem Feld fanden u.a. bereits über Datenschutz, „Cyberwar“, „Vorratsdatenspeicherung“, „Netzsperren“ und „Netzneutralität“ statt. Ob und wie der Staat regulierend eingreifen sollte, war dabei jeweils Gegenstand der Diskussion.

Repräsentatives Element in diesem Themenkomplex ist die bundesdeutsche Teilumsetzung der s.g. *Bolkestein-Richtlinie* des Europäischen Parlaments und des Rates durch das „Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“. Auf dieses wird hier speziell eingegangen. Inhaltlich handelt es sich um die Etablierung einer sicheren schriftlichen Onlinekommunikationsplattform unter staatlicher Aufsicht. Sie ist als Symbiose des klassischen Postwesens und der modernen E-Mail konzipiert und soll u.a. für hoheitliche Aufgaben verwendbar sein. Im Rahmen einer Politikfeldanalyse wird hier erörtert, welche Politik in Deutschland hinsichtlich dieser aktuellen Entwicklungen in den Kommunikationstechnologien betrieben wird. Der normativ antithetische Konflikt zwischen Sicherheit und Freiheit stellt hierbei einen besonderen Schwerpunkt dar.

In der Auseinandersetzung mit dem Thema geht der erste Teil auf die staatliche Pflicht zur Wahrung von Sicherheit und Freiheit in den digitalen Kommunikationsmedien ein (Nr. 4). Die gegensätzlichen Positionen und ihre Konfliktlinien sind hier Gegenstand der Untersuchung. Zur Analyse werden technologie- und wissenschaftssoziologische Theorien herangezogen, um den Bezug zwischen politischem Willen und Technik herzustellen (Nr. 2). Des Weiteren erfolgt eine kurze Einführung in Informationstechnologie, Internet und juristische Zusammenhänge (Nr. 3) sowie Motivation und Verhalten der wichtigsten Akteure (Nr. 5).

Im zweiten Teil wird das Fallbeispiel De-Mail behandelt. Die Eigenschaften von Versandwesen (Nr. 6.1) und elektronischer Post (Nr. 6.2) sind Maßgeblich zum Verständnis des Kontextes der Gesetzesinitiative (Nr. 7).

Teil I.

Das Politikfeld moderner Telekommunikation in Deutschland

2. Bedeutung technischer Artefakte für die Politologie

Bedingung für das Verständnis der hier dargestellten Zusammenhänge ist das Verständnis über den Zusammenhang zwischen Mensch und Technik. Verkürzt dargestellt, beschränkt sich der Wirkungskreis der Politikwissenschaft auf soziale Machtstrukturen. Technik hingegen ist kein soziales Wesen und zählt somit nicht zu den politischen Akteuren. Angesichts des Bedarfs eines Maßstabs zur Kategorisierung individueller Interessen (vgl. unten Nr. 4ff), stellt sich die Frage, ob und wie die Technik überhaupt das Politische tangiert. Vier Annahmen sind denkbar: Kein Zusammenhang zwischen Mensch und Technik, Abhängigkeit des Menschen von Technik, Abhängigkeit der Technik vom Menschen und beidseitige Abhängigkeit.

Laut Gehlen (2004, 189) ist der Mensch ein „Mängelwesen“, das auf die Nutzung (technischer) Artefakte[1] angewiesen ist. Ogburn (1969a, passim), einer der wichtigsten Mitbegründer der Technologiefolgenabschätzung (Technology Assessment, TA), interpretiert „Technik als Umwelt“. Sie verschmilzt mit der Umgebung menschlichen Verhaltens und bildet das eigentliche *natürliche* Habitat des Menschen; sie bildet ein „Technotop“ von dem unbewusst etwa die Existenz und Beschaffenheit von Gemeinschaften abhängt (vgl. Ogburn 1969b, 242f und Gaycken 2008, 36). Außerdem beschreibt Ogburn das Phänomen des „cultural lag“, demzufolge Kultur ausschließlich verzögert auf umweltliche Veränderungen reagieren kann. Dies gilt auch für das Politische in Bezug auf technische Neuerungen (vgl. Ogburn 1969b, 245ff und Degele 2002, 17).

Ohne menschliches Zutun kann allerdings keines dieser Artefakte existieren (vgl. Heidenreich et al. 2008, 193). Wenn also angesichts der gezeigten Umstände die Annahme keines Zusammenhangs als widerlegt gelten kann, bleiben drei Annahmen übrig. Ihnen entsprechend sind drei Denkrichtungen zu identifizieren, die den Umgang mit Technik

[1] Technik wird neben *stofflichen* Artefakten auch in *Wissen* und *Handeln* unterschieden. Diese Begriffe werden hier synonym verwendet. Zur Definition vgl. Degele 2002, 19f und Gaycken 2008, 28ff

in sozialen Kontexten thematisieren. Sie werden in der Disziplin der *Wissenschafts- und Techniksoziologie*, auch „science studies“ genannt, beschrieben (vgl. Latour 1995, 9). Eine der wichtigsten wissenschaftlichen Theorien ist die *Actor-Network Theory* (Akteur-Netzwerk Theorie, ANT). Sie geht davon aus, dass sich die Sphären des Menschlichen und des Technischen überschneiden (vgl. 2.2). Die beiden anderen Denkrichtungen unterstellen im Gegensatz dazu die Trennung der Sphären (vgl. 2.1). Ihnen ist gemeinsam, Technik als eine Dynamik zu interpretieren, die nach einer eigenen Logik handelt (vgl. Degele 2002, 32). Ihre Einschätzungen zur abhängigen Variable weichen jedoch grundlegend voneinander ab.

2.1. Einseitige Abhängigkeit in deterministischen Technologieskeptizismen

Aus der Anthropologie lassen sich mehrere unterschiedliche Technikverständnisse in Abgrenzung zum Menschen ableiten. Das Menschsein wird etwa bei Lindemann (2002, 84f; 2009a, 98 und 2009b, passim) durch vier „Grenzregime“ von seiner Umwelt abgegrenzt: Geburt und Sterben; Natur und Technik. Als Mängelwesen ist der Mensch jedoch auf Artefakte angewiesen, die bestimmte Körperfunktionen ersetzen, verstärken oder entlasten. Denn anders als bei anderen Spezien sind diese nicht bereits genetisch bspw. in der Physiognomie veranlagt (vgl. Herder 1981, 270f und Gehlen 2004, 189). Aus diesem anthropologischen Technikverständnis kann der s.g. „technological fix“ abgeleitet werden. Kritiker werfen diesem vor, Technik als schnelle Antworten auf komplexe Fragen zu betrachten. Anstatt die eigentlichen Problemursachen anzugehen, kommt Technik die Rolle der oberflächlichen Lösung für nicht-technische Probleme zu. Die Behandlung von Symptomen anstelle dauerhafter ganzheitlicher Erleichterung impliziert einen Fortschrittsoptimismus, der die Möglichkeit der zivilisatorischen Selbstzerstörung ignoriert (vgl. Volti 1995, 25f und Degele 2002, 25f).

Trotz dieser Bedenken bauen die von Degele (2002, 23–27) als „konservativ“ und „links“ bezeichneten skeptischen Sichtweisen auf dieser Annahme auf. Ihre konsequente Übersteigerung führt jedoch zu beunruhigenden Szenarien: Mensch und Technik streben demnach auf ein entweder technisch oder sozial determiniertes Ziel zu.

Konservative Interpretationen der gesellschaftlichen Bedeutung von Technik finden sich vor allem in religiös-normativen Wertvorstellungen sowie im Taylorismus und den darauf

aufbauenden Wirtschaftstheorien wieder. Dieser Technikdeterminismus problematisiert die Ohnmacht und Abhängigkeit, aber auch potentielle Vorteile bzw. Segnungen durch wissenschaftlich technischen Fortschritt. Sie ist außerdem grundlegend, um TA bspw. für die politische Entscheidungsfindung durchzuführen (vgl. Grunwald 2007, 63). Artefakten – seien sie etwas triviales wie ein Bett, etwas abstraktes wie Riten und Gebräuche, oder etwas hochkomplexes wie Bürokratien und Atomkraftwerke – werden dabei inhärente Fähigkeiten zugeschrieben. Diese Fähigkeiten machen sie vom Menschen unabhängig und ergeben sich nicht etwa aus einer Art *Persönlichkeit* heraus, sondern aus allen möglichen bzw. nicht eingeschränkten (Verwendungs-) Optionen. Zu dieser prädestinierten Verwendung gehört auch die Herstellung und Zerstörung anderer Artefakte. Die Annahme eines Eigenlebens, in dem Menschen nur mathematischer Faktoren sind, wird dadurch bestärkt (vgl. Siegert 2008, 21ff). Folglich strebt Technik in letzter Instanz einem vorbestimmten Zustand entgegen.

Um ein aktuelles Beispiel zu nennen, ist die Endlichkeit fossiler und nuklearer Ressourcen auf der Erde im Grunde bereits seit ihrer Entdeckung und Nutzbarmachung absehbar. In einer Zeit in der die modernen (zumeist westlichen) Zivilisationen hochgradig von ihnen abhängen, ist es deswegen zwangsläufig, dass es eine Art technische Revolution geben wird. Um nicht in einen vorindustriellen Zustand zurückzufallen, muss die Menschheit den Verlust dieser Ressourcen kompensieren. Seither – so gemäßigte konservative Argumentationslinien – habe die Möglichkeit bestanden, durch gezieltes Vorantreiben des Fortschritts diese Entwicklung in ihrer zeitlichen und technologischen Dimension zumindest geringfügig zu beeinflussen, um die Menschheit in der absehbaren Zukunftsrealitäten vorteilhaft zu positionieren (vgl. Degele 2002, 22, 25ff, 36f, 153ff). Allerdings sind nur wenige Probleme so klar zu skizzieren wie in diesem Beispiel. Aufgrund hoher Komplexität sind im Allgemeinen weder der Fortschrittsverlauf noch dessen Ziel ohne Weiteres absehbar. Deswegen wird Technik zuweilen unterstellt, einer sakralen Macht zu entspringen oder/und eine subversive Kraft zu sein. Animismus und Personalisierung bilden dies sprachlich ab, sind jedoch nicht zwangsläufig repräsentativ für einen Technikdeterminismus.

Ein typischer Vertreter der konservativen Sichtweise ist Schirrmacher. Er postuliert, dass es keinen Sinn macht die Produkte und Dienstleistungen beeinflussen zu wollen. Weder normative Werte noch gesetzliche Vorgaben können verhindern, dass alles was technisch möglich ist, früher oder später auch umgesetzt wird. Wichtiger ist es deswegen,

die Bevölkerung auf den fortschrittsbedingten Wandel vorzubereiten, bspw. indem Lehrpläne an sich verändernde Arbeitsmarktsituationen und Berufsbilder angepasst werden (vgl. Schirrmacher 2009, 51ff, 75ff, 209ff).

Im Gegensatz zu der eher makrosoziologisch fokussierten konservativen Sichtweise des Technikdeterminismus, ist die linke Sichtweise des Sozialdeterminismus konstruktivistisch und somit eher mikrosoziologisch orientiert (vgl. Degele 2002, 31). Sie begreift technische Artefakte als etwas, das Lebensbereiche kolonisiert. Sie schließt sich deswegen vor allem marxistischen und feministischen Theorien an. Linke reinterpretieren dabei die Metapher vom Mängelwesen derart, dass technische Artefakte Hilfsmittel seien, deren gesellschaftlicher Wert das Produkt menschlicher Schaffenskraft und Fantasie sei. Es sei schließlich nicht die Schusswaffe, die einen Menschen töte, sondern derjenige der sie bedient (vgl. Latour 1998, 31ff). Technik ist demzufolge keine autonome Dynamik, wie es Technikdeterminismus impliziert. Sowohl in ihrer Entwicklung und Herstellung als auch im Gebrauch ist die Technik vor allem vom Menschen bestimmt und abhängig. Dieser wiederum wird sie ausschließlich zum eigenen Vorteil nutzen. Dabei ist nicht ausgeschlossen, dass Einzelhandlungen oder die Summe aller individueller Handlungen schädliche Effekte für bestimmte Bevölkerungsanteile oder der Menschheit als Ganzes haben kann.

Technik, so folgert McInerney (2009, 207f) in seinen Theorien zur „social construction of technology“ (SCOT) aufbauend auf Bijker et al. (1987, 17ff), materialisiere den menschlichen Willen und entwickle sich somit zwangsläufig zu einem Politikum. Dies entspricht der Position von Weber (1958, 524). Dieser formuliert, dass Politiker mit „Zorn und Eingenommenheit“ kämpfen und auch das Asoziale politisch aufladen müssten, um ihren gesellschaftlichen Aufgaben gerecht zu werden. Mit Joschka Fischer (B'90/Grüne):

> „Alle großen Sozial- und Technik-Utopien haben [...] endgültig ihre Unschuld verloren [...]. Sie alle münden in der Vorstellung: Wir schaffen uns eine neue Welt ohne Gewalt und Klassenschranken, und um dieses große Glücksversprechen zu realisieren, sind wir legitimiert, das große Unglück zu produzieren.“ (in Luik et al. 2009, 14)

Aus der Sicht von Kurz und Rieger, vom *Chaos Computer Club* (CCC), sind es deswegen auch nicht Computer die auf kriminelle Weise handeln. Es sind vor allem menschliche Faktoren, die Gelegenheiten zum Missbrauch schaffen und ausnutzen. Personen, die sich der elektronischen Datenverarbeitung (EDV) aussetzen und ihre Daten preisgeben, verleihen den verarbeitenden Akteuren Macht. Umgesetzt werden, könnte diese Macht dann

sowohl finanziell als auch zur politischen Einflussnahme. Aus diesem Grund streben Kurz und Rieger (2011, 199ff, 202) ein ausgeprägtes öffentliches Bewusstsein über dementsprechende Zusammenhänge an, damit der Einzelne in der Lage ist, sich gegebenenfalls zu wehren.

Beide Denkrichtungen, sowohl Technik- wie auch Sozialdeterminismus, neigen zur Generalisierung mitunter verstörender gesellschaftlicher Effekte. Diese verorten sie in Globalisierung, Ökonomie und Technologie. Sie sind daher eher skeptisch im Umgang mit Technik (vgl. Ritzer 1996, 293, 304f; Grunwald 2007, 70). Die Gemeinsamkeit dieser deterministischen Denkrichtungen impliziert, dass die Menschheit sich durch ihr eigenes Handeln zunehmenden Gefahren aussetzt. Laut Beck (1986, 254-299), seien Wissenschaft und (Informations-) Technologie „*(Mit)Ursache*, *Definitionsmedium* und *Lösungsquelle*“ (Beck 1986, 254) in Einem, was ein dreifaches „wiederspruchsvolles“ (ebd.) Risiko darstelle. Ob die Technik also autonom oder abhängig ist, ändert nichts an der Tatsache, dass sich die Gesellschaft in einer Spirale aus Problemdiagnose, Lösungsansatz und Nebenwirkungs- bzw. Fehlerwahrscheinlichkeit einschließt (vgl. ebd.; Adorno 2007, 15f; Degele 2002, 25f; Heidegger 1962, 5–36; Turner 2001, passim und Taylor und Dürrenschmidt 2007, 95ff, Siegert 2008, 32ff, 51f).

2.2. Beidseitige Abhängigkeit und Actor-Network Theory

Als gänzlicher Gegenpart zu den deterministisch-skeptischen Sichtweisen gilt Latour, dessen Arbeiten die Symbiose von Mensch und Technik sowie unterschiedliche Hybridisierungsphenomäne aufzeigen. Zusammengefasst werden sie in der „actor-network theory“ (ANT), welche auf der Luhmannschen *Systemtheorie* basiert. Technik, so die Argumentation, generiert einerseits Komplexität, kann diese in ihrer Anwendung jedoch auch reduzieren (vgl. Luhmann 1984, 515ff). Demnach ist es weder die Waffe, die jemanden tötet, noch der Mensch, der sie nutzt (vgl oben Nr. 2.1). Es ist vielmehr die spezifische Kombination aus Akteur (Mensch) und Artefakt (Waffe), der als neuer Agent (Mensch mit Waffe) das Töten als eine von vielen Optionen möglich bzw. nicht vorbehalten ist (vgl. Latour 1998, 31ff). Folglich bemängelt Latour den Begriff des Fortschritts und die konsequente Zerteilung jeglicher Erkenntniszusammenhänge in unterschiedliche Disziplinen (bspw. innerhalb des Journalismus; vgl. Latour 1995, 7ff, 41, 53ff).

Der sich daraus ergebende Unterschied zu den vorangegangenen Theorien ist frappie-

rend: Nicht der eine beherrscht den anderen, sondern beide (Akteur und Artefakt) bedingen einander (vgl. Siegert 2008, 53ff). Nur mit der Weiterentwicklung der Technik, kann sich die Zivilisation weiterentwickeln. Umgekehrt kann nur eine gereifte Gesellschaft hoch komplexe und gefährliche Technologien beherrschen (bspw. die Atomtechnologie). Friebe und Lobo (2006, 39ff) beschreiben die „digitale Bohème“ als einen dementsprechenden Zustand. Es handelt sich dabei um ein soziales Milieu, das meist aus kreativen jungen Menschen besteht. Sie haben spezielle Ideen, Kompetenzen und Beziehungen, die größtenteils nur durch die modernen Kommunikationskanäle lose zusammengehalten werden. Dabei schafft sich die digitale Bohème ihren eigenen Wirtschaftskreislauf. Darin zirkulieren spezielle Produkte und Dienstleistungen durch die sie sich definieren und von anderen Milieus abgrenzen. Unter diesen Produkten befinden sich auch technische Artefakte, welche nicht nur konsumiert sondern auch produziert werden. Folglich hängen die Menschen nicht nur von ihren Artefakten ab, sondern die Nutzung, Existenz und Weiterentwicklung der Artefakte auch von den Menschen. Ohne ihr Zusammenspiel würde sich die digitale Bohème auflösen (vgl. Friebe und Lobo 2006, passim, insbesondere 42f)[2].

Allerdings sprechen viele Autoren nicht direkt von einer symbiotischen Verbindung, wie sie Latour formuliert. Es handelt sich bei ihnen eher um eine unstrittige Grundannahme, dass Mensch und Technik nicht ohne einander denkbar sind. Bedeutender für ihre Betrachtungen ist, dass die bisherigen Regeln (bspw. in der Marktwirtschaft) durch die Digitalisierung nicht verändert oder ausgehebelt wurden. Stattdessen hat sich die Umwelt gewandelt. Dieser Gedanken findet sich bei Gaycken (2010 und 2011a, 21f, 26f, vgl. unten Nr. 4.1), der das Aufkommen digitaler Waffen aufgrund eines neuen Schlachtfeldtyps begründet, sowie Schirrmacher (2009, passim, insbesondere 51ff, 75ff, 209ff; vgl. oben Nr. 2.1), Friebe und Lobo (2006, passim, insbesondere 42f; vgl. oben), die das Aufkommen neuer Lebensstile mit den veränderten Lebenswirklichkeiten als auch den daraus erwachsenden Bedürfnissen begründen. Ebenso postulieren Jarvis (2009, passim, insbesondere 24ff, 40ff, 48ff, vgl. unten Nr. 4.3 und 5), Kurz und Rieger (2011, passim, insbesondere 13ff, 51ff, 247ff, vgl. oben Nr. 2.1 und unten Nr. 5) die Entstehung neuer Wertschöpfungskettentypen aufgrund der Weltmarktsystemergänzungen durch das Internet. Die *alten* Regeln haben somit zwar nach wie vor Bestand, müssen jedoch aufgrund neuer Machtgleichgewichte und

[2]vgl. außerdem Kommunikation in der Systemtheorie bei Luhmann 1984, 193ff; mediierte Kommunikation, der Menschen als „Cyborg“ sowie die Verschmelzung von sozialen und technischen Raum bei Licklider 1990, 1ff, 21ff und Murdoch 1997, passim, insbesondere 733

Handlungsoptionen für die zukünftige Anwendung strategisch reevaluiert werden. Dabei ist es unerheblich ob es sich im Sinne skeptischer Determinismen um Akteure und Artefakte handelt oder im Sinne der ANT um Agenten. Zudem wird deutlich, dass die drei Sichtweisen nicht homogen sind. Tatsächlich gibt es trotz grundlegender Differenzen auch erhebliche Überschneidungen.

Es kann konstatiert werden, dass sich aus allen drei Ansätzen durchaus ein Zusammenhang zwischen dem Politischen und dem Technischen ergibt. Die Theorien gehen sogar soweit, den Menschen mit seinen technischen Artefakten eng zu verknüpfen und voneinander abhängig zu machen. Mit Winner (1986, 11f): „We do not *use* technologies as much as *live* them." Es bleibt allerdings offen, ob der Mensch Herrscher oder Beherrschter der Technik ist, oder vielleicht etwas Drittes zutrifft.

Für die Politik sind diese Erwägungen unerheblich. Sie ist dem Diktat der Realität unterworfen: Ihr geht es um Bedürfnisse und Wahlverhalten der Bürger, um Machtpositionen von Akteuren, äußere Einflüsse und systemische Gegebenheiten. Um jedoch unterschiedliche Diskussionsbeiträge in dieser Politikfeldanalyse einschätzen zu können, sind die drei gezeigten Ansätze unabdingbar. Sie ermöglichen in beliebigen politischen Szenarien zu bestimmen, welche Rolle politische Akteure einnehmen (vgl. Siegert 2008, 15ff).

3. Die Informationstechnik im sozial-historischen Kontext

3.1. Entstehungsprozess der Informationstechnik

Bereits in den 1930er Jahren griffen Militär und Industrie auf die Möglichkeiten erster spezialisierter Rechenanalagen zurück (bspw. die *Rotor-Chiffriermaschine* „Enigma", vgl. Harper 2001, 136ff). Der erste Universalrechner, der das Variieren seiner Programmierung erlaubte, wurde von Konrad Zuse 1936 patentiert. Dessen Realisierung erfolgte 1938 mit dem Z1 und feierte 1941 mit dem Z3 einen Durchbruch (vgl. Mainzer 2011, 178; Zuse 1970, 60ff). Computer wie diese erwiesen sich daraufhin für militärische Konflikte umso schneller als strategisch vorteilhaft. Aufgrund der seinerzeit begrenzten Verfügbarkeit von Rechenanlagen und -Kapazitäten, wurde, um die Zerstörung einzelner Anlagen kompensieren zu können, deren Vernetzung begonnen. Fester Bestandteil dieser, von der Pentagonunterabteilung *(Defense) Advance Research Project Agency* (ARPA bzw. DARPA) als „Arpanet" bezeichneten Urform des Internets (vgl. Clarke und Knake 2010, 283), war,

dass Daten sich ihre Wege entlang von s.g. Nodes[3] suchten. Hierdurch konnten im Falle eines Ausfalls automatisch neue Verbindungen ermittelt und genutzt werden, damit dennoch Datenübertragungen zustande kämen. Diese waren dann bspw. zur Datensicherung und Kommunikation nutzbar (vgl. Kleine-Voßbeck 2000, 7).

Maßgeblich zukunftsbestimmende Innovationen erfolgten in den 1980er Jahren. Nach Militär, Wissenschaft und Wirtschaft befähigte die wesentliche Vereinfachung der Handhabung nun auch Laien selbstständig informationstechnisch Tätig zu werden. Ausschlaggebend dafür waren nicht nur sinkende Preise für elektrotechnische Bauteile sondern vor allem die Durchsetzung bestimmter Normen und Standards. Dazu zählen u.a. der Personal Computer Standard (PC) der *International Business Machines Corporation* (IBM) von 1981 und das ab 1983 damit vertriebene *Operating System* (Betriebssystem, OS) Windows der Firma Microsoft. Dessen Ausnutzung eines „Graphical User Interface“ (grafische Benutzeroberfläche; GUI) wurde Marktweit übernommen. Zu den grundlegenden Funktionen der Informationstechnik (IT) und des weltumspannenden Netzwerks gehört bis heute, neben dem militärischen Unterbau, vor allem der 1989 von Tim Berners-Lee vom *Conseil Européen pour la Recherche Nucléaire* (Europäische Organisation für Kernforschung, CERN) stammende „World Wide Web“ Multimediastandard (WWW oder Web, vgl. Berners-Lee 1998). Um das Zitieren zu vereinfachen, wurde hierbei die Verweismethode der „Hyperlinks“[4] eingeführt, wodurch das Anlegen komplexer Datenstrukturen ermöglicht wurde. Die dafür benötigte Adressierung erfolgt durch *Internet Protocol* (IP) -Adressen (vgl. RFC: 791 und RFC: 1166 sowie zum Nachfolgestandard RFC: 2460[5]), die eindeutig und temporär allen Netzwerkgeräten zugeordnet werden. Eine Gewichtung bestimmter Daten, bspw. abhängig von Inhalt, Größe oder Herkunft, wurde nicht vorgesehen. Dies erhielt später in der Diskussion um *network neutrality* (auch *netneutrality* oder Netzneutraliät) besondere Relevanz, da alle Daten beim Versand ungesehen – d.h. vertraulich und gleich priorisiert – bearbeitet werden müssen. Es handelt sich folglich um ein technisch realisiertes und striktes Diskriminierungsverbot, aus dem ein Kommunikationsgeheimnis hervorgeht (vgl. Art. 4–6, 10, 12–14 GG, Kleine-Voßbeck 2000, 44ff und Cebulla 2010, 313).

In Deutschland wurde das Internet – und damit die E-Mail – als erstes 1982 an der

[3]Node: Knotenpunkt; Unterkategorie der Server
[4](hyper-) link = (besonderer) Verweis, vgl. RFC: 1738
[5]Die Standards des Arpanet (später Internet) sind chronologisch nummeriert und werden im *Requests for Comments* (RFC) zur Diskussion veröffentlicht.

Universität Dortmund eingerichtet (vgl. Kleine-Voßbeck 2000, 8). Privat genutzt werden, konnte die Technik jedoch erst durch „Telebox-System und Bildschirmtext“ (BTX) der von der Bundespost entwickelten „Datenfernkommunikationsdienstleistungen“. Sie blieben jedoch unpopulär und erwiesen sich als fehlerhaft (vgl. N.N. 2006 und Dornseif 2005, 224f). Erst als das Tochterunternehmen des ehemaligen Staatsunternehmens Telekom, die T-Online International AG (vgl. unten Nr. 6.1), neue Angebote auf den Markt brachte und sich der PC zunehmend durchsetzte, nahm die Verbreitung auch in Deutschland signifikant zu. 1996 bestand das weltweite Netzwerk „aus mehr als 90.000 Netzen in über 100 Staaten“ (Kleine-Voßbeck 2000, 7) und wird inzwischen als „Internet“ bezeichnet. Derzeit nutzen, laut dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) e. V., in Deutschland unabhängig von Geschlecht und Bildungsgrad etwa drei Viertel der Bevölkerung regelmäßig das Internet (vgl. Abb. 2 und 3; nach Arenz et al. 2011). Jedoch ist ein deutliches Gefälle der Nutzer hinsichtlich ihres Alters zu verzeichnen: Je älter die Befragten sind, desto mehr distanzieren sie sich von der IT. Gerade jene Generationen, die im Gegensatz zu den s.g. „digital natives“ (digitaler Ureinwohner) nicht im s.g. „Informationszeitalter“[6] aufgewachsen sind, neigen zur Verweigerung und Skepsis (vgl. Abb. 4, 5 und 1; nach Arenz et al. 2011). Gerade die über 65-Jährigen bevorzugen die Überwachung des Internets und Speicherung von Verbindungsdaten (vgl. ebd., 47ff). Entsprechend stimmen sie der staatlichen Überwachung zu (vgl. ebd., 49ff).

Peter Kruse, Unternehmensberater und Professor der Psychologie, stellt zudem fest, dass es auch altersunabhängig einen signifikanten Unterschied zwischen der Perspektive der „Digital Residents“ und der „Digital Visitors“ gibt. Zwar begeben sich die Gruppen mitunter in die Sphäre des jeweils anderen, deuten die komplexen sozialen Strukturveränderungen jedoch vollkommen unterschiedlich. Eine Kollision beider Weltbilder ist demnach zwangsläufig (vgl. Kruse 2010).

3.2. Paradigmenwechsel zum Web 2.0

Für die rapide Verbreitung des Webs innerhalb von drei Jahrzehnten (seit Erscheinen des PCs, vgl. oben Nr. 3.1), war neben Moores Gesetz (vgl. Moore 1965, 114ff) vor Allem eine starke Technikeuphorie verantwortlich. Sie erstreckte sich sowohl über Produktions-

[6] Das Informationszeitalter beschreibt Castells (2000, 5ff) als Zeitperiode der gesellschaftlichen Evolution von der ursprünglichen Agrarökonomie (primär), über die Industrialisierung (sekundär) hin zur dienstleistungs- oder auch postindustriellen Gesellschaft (tertiär); vgl. Hradil (2006, 31ff, 167ff), Geißler und Meyer (2002, 21ff, 163ff)

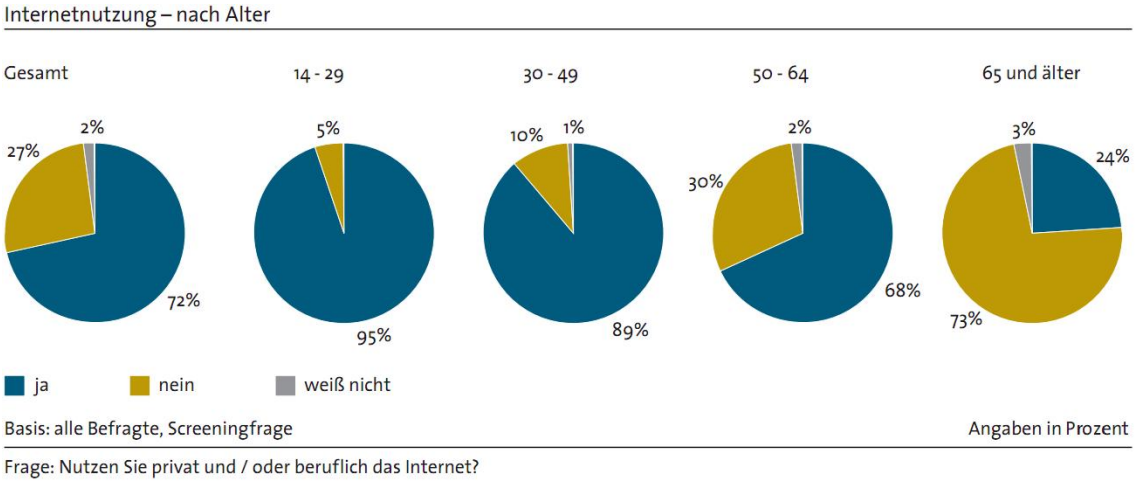

Abb. 1: Internetnutzung – in Deutschland nach Alter (Arenz et al. 2011, 7)

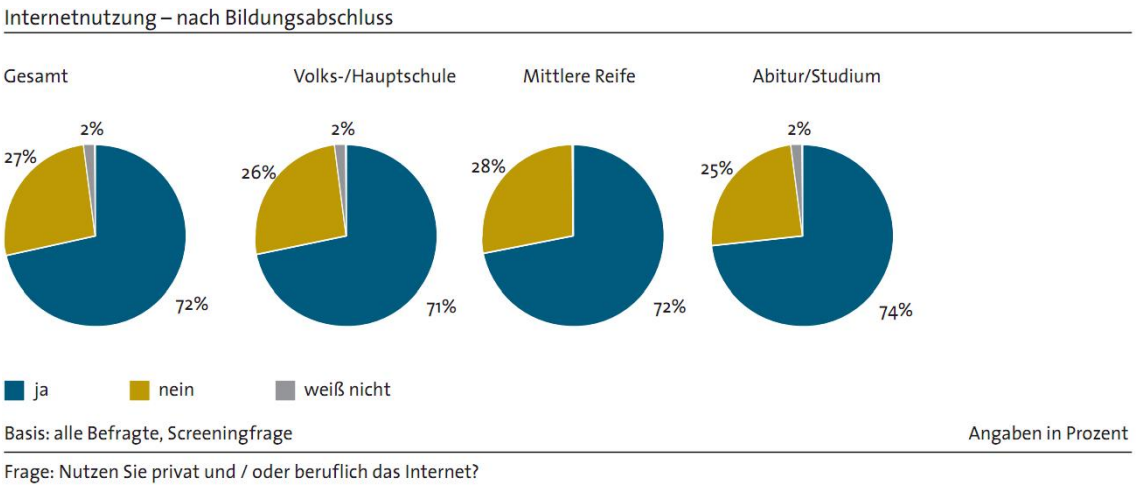

Abb. 2: Internetnutzung – in Deutschland nach Bildungsabschluss (Arenz et al. 2011, 7)

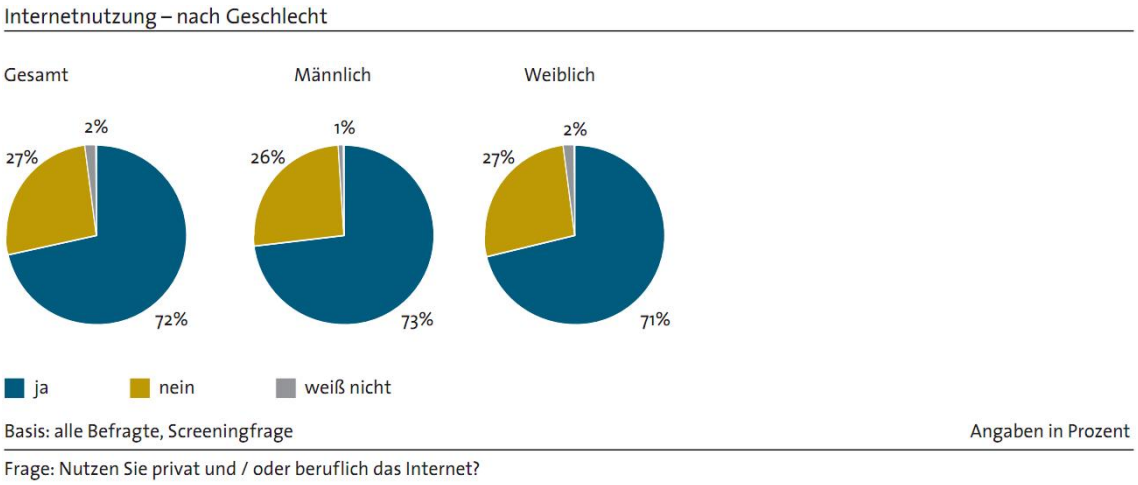

Abb. 3: Internetnutzung – in Deutschland nach Geschlecht (Arenz et al. 2011, 7)

und Dienstleistungsgewerbe als auch Finanzwesen und Kultur (vgl. Friebe und Lobo 2006, 165ff). Im Zuge dessen entwickelten sich neue Geschäftsideen, denen eine Börsengangswelle folgte. Große Investitionen ermöglichten und verstärkten diese Tendenzen und steigerten den Aktienhandel signifikant. Da jedoch noch keine einschlägigen Erfahrungen mit dieser s.g. „New Economy“ vorlagen, wurde der Markt überreizt. Das Platzen dieser s.g. „dot-com“-Blase im Jahre 2000 markiert einen Wendepunkt im Informationszeitalter: Durch die radikale Bereinigung des Marktes von nicht tragfähigen Finanzierungs- und Geschäftsmodellen, fand ein ökonomischer Selektionsprozess statt, dem ein wirtschaftlicher Evolutionssprung folgte (vgl. Jarvis 2009, 63ff). Das Internet, so eine der ersten Erkenntnisse nach dem Börsen-Crash, ist kein Medium einseitigen Sendens, wie etwa bei Rundfunk, Fernsehen oder Druckwaren. Das Internet erlaubt bidirektionalen Informationsaustausch, welcher sowohl asynchron als auch synchron gestaltet werden kann. Neben statischen Inhalten – u.a. Texten, Geräusche, Bilder und Videos – können nun auch dynamische Inhalte – u.a. interaktive Programme und soziale Netzwerke – multimedial genutzt werden.

Das Schlagwort „Web 2.0“ wurde 2004 durch die Internet-, IT- und EDV-Branche erdacht. Sie bezweckte damit die Selbstmotivation nach dem Börsencrash und eine Belebung des Marktes. Im Nachhinein wurde damit jedoch die Wende von Statisch zu Dynamisch und von einseitiger Massenkommunikation zur massenhaften bidirektionalen Individualkommunikation markiert. Das Web 2.0 gilt heute als (relativ) sozial, offen und transparent (vgl. Friebe und Lobo 2006, 15, 165ff). Jedoch prognostizierte Licklider (1990, 1ff, 21ff) dies bereits in den 1960er Jahren, als er schrieb: „ . . . men will be able to communicate more effectively through a machine than face to face.“ (ebd., 21)

3.3. Regulierung automatisierter Datenverarbeitung in Deutschland

In der neuen New Economy – d.h. im Web 2.0 – werden erfahrungsgemäß kostenlose und individualisierte Angebote vom Nutzer am besten akzeptiert. Zur Finanzierung dieser Angebote entstanden neue Geschäftsmodelle, wie etwa „Freemium“. Hier müssen kostenpflichtige Premiumangebote lediglich von einem Bruchteil der Nutzer bezogen werden, um ein kostenlos lockendes Basisportfolio zu amortisieren (bspw. bei Spielen oder Büroanwendungen; vgl. Anderson 2009, 245ff; Jarvis 2009, 59, 76ff und Wölbert 2011). Vorwiegend werden Gewinne jedoch noch immer mit Werbe- und Querfinanzierungsmodellen erzielt (bspw. bei Suchmaschinen und SNS), welche Datenschützern (bspw. bei

Kurz und Rieger 2011, 13ff, 247ff) als besonders *datengierig* und somit bedenklich gelten. Diese Eigenschaft teilen sie sich mit Staaten und ihren Geheim- und Sicherheitsdiensten (bspw. Vorratsdatenspeicherung, vgl. unten Nr. 4f; sowie Coy 2008, 47f).

In dieser Hinsicht gilt die Periode zwischen Mitte der 90er Jahre und Anfang des 20ten Jahrhunderts als das *verschlafene Jahrzehnt*: Von den Bundesregierungen Deutschlands[7] ging seit dem Fehlstart des BTX-Systems und den Postreformen (vgl. oben Nr. 3.1) keine signifikanten Impulse für den vielbeschworenen „Technologiestandort Deutschland“ aus. Der (Kommunikations-) Technologiesektor wurde infolgedessen weitestgehend sich selbst und der Selbstregulierung des Marktes überlassen. Der normative Imperativ zur Aktualisierung des Gesetzeskatalogs, ging aus dem regulativen Vakuum und der ungezügelten – oft als zu rasant empfundenen – Entwicklungen in Technologie und Gesellschaft hervor. Obwohl dies der Kompetenz des Gesetzgebers zufällt, war es vor allem deutsche Rechtsprechung, welche geltendes Recht in die Lebensrealität des Informationszeitalters überführte.

U.a. ist hier das vom Bundesverfassungsgericht (BVerfG) ergangene Urteil zum Volkszählungsgesetz von 1983 maßgeblich. Es stellt eine Reinterpretation des s.g. Persönlichkeitsrechts dar, welches sich aus Art. 1 I GG und Art. 2 I GG ergibt (vgl. BVerfGE 65, 1 und Kleine-Voßbeck 2000, 42ff). Inhaltlich wird damit die Abkehr der s.g. Sphärentheorie zur Theorie des Rechts auf *informationelle Selbstbestimmung* vollzogen. Der Bürger muss demnach stets in die Lage sein, zu wissen „wer wann was und bei welcher Gelegenheit“ (ebd., 43) über ihn wisse. Ohne dieses Recht, müsste der Bürger angesichts der Möglichkeiten automatisierter und massenhafter Datenverarbeitung davon ausgehen, permanent überwacht zu werden. Dies würde ihn in seiner Freiheit bedeutend einschränken und Missbrauch ermöglichen. Daraus ergibt sich für den Bürger nicht nur das Recht auf Kontrolle über die „Erhebung, Speicherung, Verwendung und Weitergabe“ (BVerfGE 65, 1) seiner Daten (vgl. Hornung 2008, 257ff), sondern theoretisch ebenso ein Recht auf Löschung selbiger (vgl. ebd., 55f; Mainusch und Burtchen 2010, 450). Das impliziert, dass Unternehmen nur dann Daten erheben, speichern, verwenden und weitergeben dürfen, wenn dies einen unmittelbaren Mehrwert für die betroffene(n) Person(en) hat. Dies wird im Bundesdatenschutzgesetz (BDSG) wieder aufgegriffen (§ 1), greift nach § 2 jedoch nur, wenn die Kompetenzen der Landesgesetze ausgeschöpft sind.

[7] Hier speziell unter Helmut Kohl (CDU/CSU und FDP; 1973–1998) und Gerhard Schröder (SPD und B'90/Grüne 1998–2005)

Zum Richtspruch zum Umgang mit personenbezogenen oder/und empfindlichen Daten – d.h. vertrauliche und geheime Daten u.a. zu Geburt, Standort, Finanzen, Biometrie und Gesundheit von natürlichen und juristischen Personen sowie des Staates – kamen 2004 das Telekommunikationsgesetz (TKG) und 2007 das Telemediengesetz (TMG) hinzu. Hiermit wurden die europäischen Richtlinien 98/48/EG, 98/34/EG, 2003/58/EG und die Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) umgesetzt als auch die Rahmen- (2002/21/EG), Genehmigungs- (2002/20/EG), Zugangs- (2002/19/EG), Universaldienst- (2002/22/EG) und Datenschutzrichtlinie (2002/58/EG). Sie sichern jedoch kein Recht auf Datenschutz und Datensicherheit (oder ähnliches) zu. Hierfür wäre eine Art Menschen- oder Bürgerrecht von Nöten, wie es Netzaktivisten fordern. Stattdessen regulieren, kontrollieren und sanktionieren TKG und TMG Angebote und Anbieter (vgl. Polenz und Thomsen 2010, 614f, 618). Sie behandeln also eher die Symptome, anstelle mittel- bis langfristige Strategien erkennen zu lassen. Eine grundsätzliche Auseinandersetzung mit den Verwerfungen im Technotop findet nicht statt (vgl. oben Nr. 2).

In logischer Fortführung dessen, erging 2008 erneut ein Urteil gegen den Gesetzgeber. Das BVerfG (vgl. BVerfG, 1 BVG 370/07) stellt dabei zur s.g. „Online-Durchsuchung“ (unter Verwendung eines s.g. „Bundestrojaner“) fest, dass die „heimliche Infiltration eines informationstechnischen Systems“ (ebd.) nur dann verfassungsrechtlich zulässig sei, wenn die konkrete Gefahr für Leib, Leben und Freiheit von Personen oder Güter der Allgemeinheit vorliege. Um den „Kernbereich privater Lebensgestaltung zu schützen“ (ebd.), müsse grundsätzlich die richterliche Anordnung erforderlich sein und das Brief-, Post- und Fernmeldegeheimnis nach Art. 10 I GG beachtet werden. Da dies die Kenntnisnahme aller Kommunikationsteilnehmer über die Überwachung erfordert, gelten zukünftige Gesetzesvorhaben zur automatisierten Kontrollnahme als weitestgehend blockiert. Das Volkszählungsurteil wird folglich noch einmal bestärkt.

Nach 9/11 hatte es dennoch weltweit verstärkt Bemühungen gegeben aufzurüsten. Mit *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) und dem s.g. „Otto-Katalog“ (nach dem damaligen Innenminister Otto Schily) wurden Anti-Terrorgesetze und -abkommen in USA, EU und Deutschland verabschiedet, die den Terror mit Daten zu bekämpfen suchten.

Für die Zukunft versichert Obama (2009) jedoch mit Nachdruck *keine* Bürgerrechte zu beschneiden. Die europäische Politik lässt hingegen gegenteilige Tendenzen erkennen: Die EU-Kommissarin Anna Cecilia „Censilia“ Malmström innitiierte im März 2010 ein Zu-

gangserschwerungsgesetz gegen die sexuelle Ausbeutung von Minderjährigen im Internet (vgl. Freude 2010 und Bleich 2010). Gesetzesentwürfe sehen die Einschränkung der Netzneutralität vor und würden zur Grenzziehung innerhalb des europäischen Internets führen, wie es bereits in China („Great Firewall"), Großbritannien und den USA geschehen ist.

In Deutschland kippte das BVerfG bereits die Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung (VDS, vgl. Roßnagel 2010, 544f, 548; Petri und Schaar 2010, 206; Engling 2008, 67, 78; Gietl 2010, 403; Leicht 2010; Bundesverfassungsgericht – Pressestelle – 2010; 2006/24/EG; §§ 113a, 113b TKG und § 100g StPO) und die Online-Durchsuchung aufgrund Verfassungswidrigkeit (vgl. oben und § 20k BKA-Gesetzes). Damit erfolgte jedoch nicht die Unterbindung von Diskussion und Konzept: Nach wie vor existieren Bemühungen der verfassungskonformen Umsetzung. Vor allem, war es das *Bundesministerium für Familie, Senioren, Frauen und Jugend* (BMFSFJ) unter Ursula „Zensursula" von der Leyen, das 2008 versuchte, ein Gesetz für Netzsperren zu erlassen (vgl. Tinnefeld 2010, 19; Bleich 2010; Freude 2009 und 2010). Es musste jedoch aufgrund einer Petition durch den *Arbeitskreis gegen Internetsperren und Zensur* (AK Zensur) und einer heftigen öffentlichen Debatte letztendlich einlenken. Erklärtes Ziel ist nun Löschen statt Sperren. Die Gesetzesinitiative von Malmström setzt jedoch den in Deutschland gescheiterten Kurs fort.

4. Sicherheitbedürfnis und Freiheitsgrundsatz im Informationszeitalter

Für die Staatsadministration haben die antagonistischen Prinzipien Sicherheit und Freiheit eine traditionell herausgehobene Bedeutung. Zwischen ihnen herrscht stetig ein empfindliches Spannungsfeld. Sie angesichts veränderter Rahmenbedingungen (vgl. oben Nr. 2) erneut zu betrachten, erscheint daher trivial (vgl. Gaycken 2011a, 28f und Petri 2010, 25, 29). Aktuell stehen eine Vielzahl Normen zur Debatte, die u.a. Kommunikation, Privatsphäre und Eigentum betreffen. Ihre Wurzeln reichen mitunter Jahrhunderte zurück, ohne seitdem eine wesentliche Veränderung erfahren zu haben. Bei ihrer Verabschiedung konnten die, durch das Aufkommen der EDV bedingten, erheblichen sozio-ökonomischen Veränderungen der letzten Jahrzehnte unmöglich antizipiert werden. Dieser Wandel vom Industrie- zum Informationszeitaler, brachte Veränderungen, die im Rahmen offener und detaillierter Reevaluationen nun eine angemessene Berücksichtigung finden müssen.

Im Folgenden wird daher auf das Spannungsfeld zwischen Sicherheit und Freiheit eingegangen und dabei speziell der Bezug auf die IT und das Internet genommen, um in den folgenden Abschnitten die geltenden Regularien und Konfliktlinien in Kontext setzen zu können. Hierbei wird unter Sicherheit, prinzipiell das Bedürfnis nach würdevollem Leben, physischer und psychischer Unversehrtheit und stabilen Verhältnissen verstanden. Dies umfasst den Schutz materiellen und immateriellen Eigentums (vgl. Hobbes 1976, 94ff, 104f, 110f und Locke 1967, 201ff) und kann im Sinne der Staatsadministration in innere und äußere Sicherheit unterschieden werden.

4.1. Konflikte im virtuellen Raum

In den Debatten über die äußere Sicherheit hat sich in jüngsten Zeit der Begriff „Cyberwar“ etabliert. Der *virtuelle Raum* oder auch *Cyberspace* wird dabei als „das fünfte Schlachtfeld“ (nach Boden, Gewässer, Luftraum und Weltall) bezeichnet (vgl. Clarke und Knake 2010, 6; N.N. 2010 und Hersh 2010). Aufgrund der sehr unspezifischen Definition möglicher Aggressoren und ihrer Ziele, verwischen die Grenzen zwischen äußerer und innerer Sicherheitspolitik (vgl. Dornseif 2005, 409): Fälle multinational orchestrierter als auch innerstaatlicher Kriegshandlungen sind bereits jetzt verzeichnet worden (vgl. unten). In der Regel ist jedoch nicht einmal der Kontinent des Angriffs zurückverfolgbar, da die Angreifer verdeckt operieren. In den meisten Cyberwar-Scenarien können folglich Vergeltungsmaßnahmen, sowohl mit konventionellen als auch unkonventionellen Mitteln, als nicht sinnvoll geschweige denn zweckdienlich erachtet werden. Idealtypische (alte) Kriegsszenarien, in denen sich zwei Staaten feindlich gegenüberstehen und eine Eskalation oder Deeskalation herbeiführen (vgl. Clarke und Knake 2010, 285), geraten damit zunehmend ins Hintertreffen.[8]

Dessen ungeachtet findet bereits jetzt ein Wettrüsten in der IT statt. Aufgrund der technischen Möglichkeiten sind Akte direkter Tötung, Zerstörung oder Zersetzung vorerst eher nicht zu erwarten. Spionage und Sabotage gelten derzeit als das größere Bedrohungspotential. Der bisherige Fokus westlicher Nationen auf Defensivmaßnahmen stellt, angesichts immer raffinierter werdender Angriffsmethoden, jedoch keine dauerhafte Lösung dar. Anzeichen für aufkommende Kriegshandlungen im virtuellen Raum, wurden durch den Virus *StuxNet* (wahrscheinlich aktiv seit 2005), Skandale um *Wikileaks* (gegründet in 2006), die

[8] Vgl. zu „neuen Kriegen“, Bürgerkriegen und asymmetrischer Kriegsführung Münkler (2002, 7, 10ff) und deren Umsetzung in der IT Gaycken (2011a, 39)

Operation Shady RAT (wahrscheinlich aktiv seit 2006), die *distributed denial of service* (DDoS) -Attacken gegen Estland und Georgien (2007; auch „Web War 1“ genannt) sowie die Hackerattacken in 2011 u.a. auf das Pentagon, den deutschen Zoll und das italienische Cyber-Abwehr-Zentrum offensichtlich (vgl. Alperovitch 2011; Clarke und Knake 2010, passim, insbesondere 257ff, 282, 284; Dornseif 2005, 325ff, 268f und Gaycken 2011a, 169ff)[9].

4.2. Delinquenz und informationstechnische Systeme

Auch wenn die Bedrohungslage von außen derzeit als immanent einzuschätzen ist, ist sie für die Zivilbevölkerung eher abstrakt und zweitrangig. Als Partizipanten der technisierten Gesellschaft (vgl. oben Nr. 2) ist ihre Lebenswirklichkeit durch mehrere unterschiedliche Bedrohungspotentiale tangiert. In jüngster Zeit künden Meldungen über s.g. „Datenskandale“ in immer kürzeren Abständen von Kriminalität und Fahrlässigkeit im Umgang mit EDV und IT, wodurch das öffentliche Meinungsbildung nachhaltig geprägt wird. Einbrüche in drei der weltweit bedeutensten Medien- und Unterhaltungselektronikkonzernen (namentlich Sony, Nintendo, und Electronic Arts; vgl. Gieselmann 2011); das unberechtigte Speichern und Verarbeiten von Standortdaten durch drei der weltweit verbreitetsten Mobiltelefon-Betriebssysteme (namentlich Apples iOS, Microsofts Windows Phone und Googles Android; vgl. Wirtgen 2011) sowie die Massenerfassung von Mobiltelefondaten durch die Dresdener Polizei (vgl. Wrusch 2011; Krempl und Briegleb 2011), sind nur einige Beispiele. Sie verdeutlichen, dass Grund zur Achtsamkeit nicht nur vor kriminellem Verhalten und fragwürdigem Geschäftsgebahren besteht, sondern auch gegenüber öffentlichen und hoheitlichen Institutionen.

Jene Achtsamkeit findet jedoch ihre Grenzen angesichts der Vormachtstellung s.g. *Gatekeeper*: Derzeit werden bspw. über 90% aller Internetanfragen über Rechner mit einem Betriebssystem von Microsoft (Windows XP, Vista oder 7) getätigt; sind über 90% (in Deutschland über 95%) aller Suchanfragen an Googles Suchalgorithmen gerichtet und nutzen knapp die Hälfte der deutschen Internetnutzer Soziale Netzwerke (Sozial Network Sites, SNS). Facebook hält hier mit über einer halben Milliarde registrierten Nutzern einen Marktanteil von weltweit über 60% und deutschlandweit über 70% (vgl. Arenz et al. 2011, 18ff; Budde und Huth 2011, 4ff; 2011e, Carlson 2011 und N.N. 2011d). Multi-

[9] vgl. außerdem Pressemeldungen von Boie und Heckenberger (2010); Broad et al. (2011); Davis (2007); Elkenberg (2011); Gaycken (2010); Hamann (2011); Hegmann und Graf (2011); Hersh (2010); Klingst (2011) und Schuller (2010)

nationale Großkonzerne wie diese, sind *Oligarchen* des Internets. Sie zeichnen sich durch die Bereitstellung und Gestaltung systemrelevanter Soft- und Hardware aus, die u.a. die Mensch-Maschine-Interaktion erst ermöglichen. Ihr jeweiliges Leistungsportfolio verleiht ihnen monopolartige Positionen in bestimmten Marktsegmenten. Ihr Einfluss auf den Zugriff und die Bearbeitung von im Internet veröffentlichten Daten, ist folglich nicht zu unterschätzen (vgl. Simons 1948, 43). Autoren wie Schirrmacher (2009), Kurz und Rieger (2011, 195ff) kritisieren deshalb, dass moderne Technologien die Menschen nicht mehr nur entlasteten (bspw. im Finanzwesen, vgl. Schirrmacher 2009, 57ff): Da der Mensch bereits jetzt, die von ihm generierte Informationsflut nicht mehr ohne technische Hilfsmittel beherrschen kann, sind diese Hilfmittel inzwischen in der Lage Kontrolle über ihn auszuüben (vgl. ebd., 51ff, 75ff und N.N. 2011c).

Hierzu kommen die s.g. *Internet Service Provider* (Internet Dienstanbieter, ISP oder auch Provider) hinzu, deren Leistungsportfolio sowohl Kommunikationsdienste (bspw. E-Mail oder Webpräsenzen) als auch -Verbindungen (bspw. Internet oder Mobilfunk) enthalten können. Als Bereitsteller der dafür notwendigen Speicher-, Bearbeitungs-, Erhebungs- und Übermittlungstechnologien, fällt ihnen auch die zentrale Administration bedeutender Datenmengen zu. Nirgends finden sich mehr valide (personenbezogene) Datensätze, dieser hohen Quantität als auch Qualität. Angesichts des Gefahrenpotentials automatischer Datenverarbeitung (vgl. Dornseif 2005, 81; Gaycken 2011b, 347 und Schlüter 2011; sowie unten Nr. 3.3), stehen Gatekeeper folglich in besonderer gesellschaftlicher Verantwortung. Um das in sie gesetzte Vertrauen zu rechtfertigen, ist ein erhebliches Maß an Sorgfalt, Sicherheit und Vertraulichkeit zu erwarten (vgl. oben Nr. 3.2f). Allerdings rechnen Juristen, wie Ernst (2010, 475), angesichts der sich häufenden Fälle s.g. „Datenlecks“, in den nächsten Jahren mit erheblichen Klagewellen.

Das ursprünglich ausschließlich spielerische *Hacken*[10] hat sich im Laufe der Zeit zunehmend zur Gewinnmaximierung professionalisiert (vgl. Dornseif 2005, 400ff). Neben dezentralen Organisationen – wie *Anonymous* (auch *Anon*) und dessen kleinerer Ableger *Lulz Security* (LulzSec), welche als autoritätsfeindliche Protestbewegungen gelten und ausschließlich aus informell und *ad hoc* eingebundenen Personen bestehen (vgl. Ogg

[10]Unter Hacken werden alle denkbaren Handlungen zusammengefasst, die das Nutzen von Artefakten auf unkonventionelle Weise umfassen, um bis dahin unvorhergesehene Mehrwerte zu generieren. Dabei wird Wandalismus oder Selbstbereicherung von der Hacker-Szene geächtet, während erfolgreiches Hacken zum politischen Aktivismus (Hacktivismus) glorifizierend und der Schaden durch *böse* Hacker solidarisierend wirkt. Zu Definition und Auflistung der Untergruppen vgl. Dornseif (2005, 50f, 121ff) und CCC (1999)

und Mills 2011) – werden Hacker zunehmend in einen florierenden Schwarzmarkt eingebunden. In diesem wird gehandelt, paktiert und investiert, weswegen das Bundeskriminalamt (BKA) zuletzt erhebliche Verlagerungen in der Kriminalität verzeichnete: In regelmäßigen Abständen sinkt die generelle Kriminalität, während die Computerkriminalität (IT-Delinquenz) im zweistelligen Bereich ansteigt und dessen Aufklärungsquoten kontinuierlich sinken (vgl. Dornseif 2005, 97ff; Köppen 2010, passim und BKA 2010, 4, 8, 58). „Die sichere Kommunikation [...] ist auch ein ‚Hase und Igel'-Spiel" (in Scherer 2011), führte dazu der seinerzeit im Wechsel vom Innen- zum Verteidigungsministerium befindliche Bundesminister Thomas de Maizière in einem Fernsehinterview aus. Da das Internet in erster Linie ein Kommunikationsnetzwerk ist, sprach er damit indirekt ebenso über die Unverletzlichkeit der Privatsphäre, das Recht auf geistiges Eigentum und andere (Schutz-) Rechte. Weiter führte er aus, dass im virtuellen Raum ein System „sich gegenseitig übertreffender Intelligenz" entstünde (ebd.). Als Indiz dafür registrierten Hersteller von Sicherheitssoftware eine rasante Vermehrung s.g. Malware[11] und Spam[12] zu verzeichnen (vgl. Symantec 2010).

Ein ernst zu nehmendes Signal und Beispiel für *Cybercrime* ist der Fall Sony: Über 100 Millionen Datensätze zu stehlen, gilt als äußerst schwierig und riskant. Da die Verwertung jedoch andere Kompetenzen erfordert, ist es wahrscheinlich, dass die Daten anschließend über Hehler päckchenweise veräußert wurden. Ihre Käufer nutzten sie dann etwa um auf Bankkonten zuzugreifen, Phishing[13] zu betreiben oder bestehende Datensätze zu vervollständigen, um so deren Verkaufswert oder/und Verwertbarkeit zu steigern (vgl. Kurz und Rieger 2011, 195, 199ff, kakl 2011). Zu dieser Art organisierter Kriminalität kommen Akte des persönlichen Angriffs, wie bspw. (*Cyber-*) *Mobbing* oder *Stalking* (vgl. Dornseif 2005, 381f). Die IT und vor allem das Internet – auch wenn sie beliebt sind und flächendeckend genutzt werden (vgl. oben Nr. 3; Abb. 1–3) – gelten deshalb in der öffentlichen Auseinandersetzung zunehmend als riskant (vgl. Abb. 4 und 5; sowie Arenz et al. 2011, 6ff, 21ff). Hier mit politischen Mitteln einzugreifen – d.h. Strafen zu verhängen,

[11] Unter Malware werden hier Schadprogramme aller Art verstanden, wie bspw. Viren und Trojaner zur Spionage oder/und Manipulation des Rechners (vgl. Clarke und Knake 2010, 287). Autoren wie Dornseif (2005, 319) fassen den Begriff mitunter jedoch enger, etwa auf Schadprogramme, die die verdeckte Kommunikation ermöglichen.

[12] Unter Spam werden in der Regel unerwünschte und massenhaft auftretende Nachrichten verstanden, die meist zu Werbezwecken und in Form von E-Mails verbreitet werden. Sie treten oft in Verbindung mit Malware und Phishing auf; vgl. Dornseif (2005, 370)

[13] Unter Phishing werden alle Formen der Kommunikation verstanden, die betrügerisch den Erhalt sensitiver oder/und personenbezogener Daten anstrebt. Es tritt oft in Verbindung mit Spam auf; vgl. Dornseif 2005, 223f

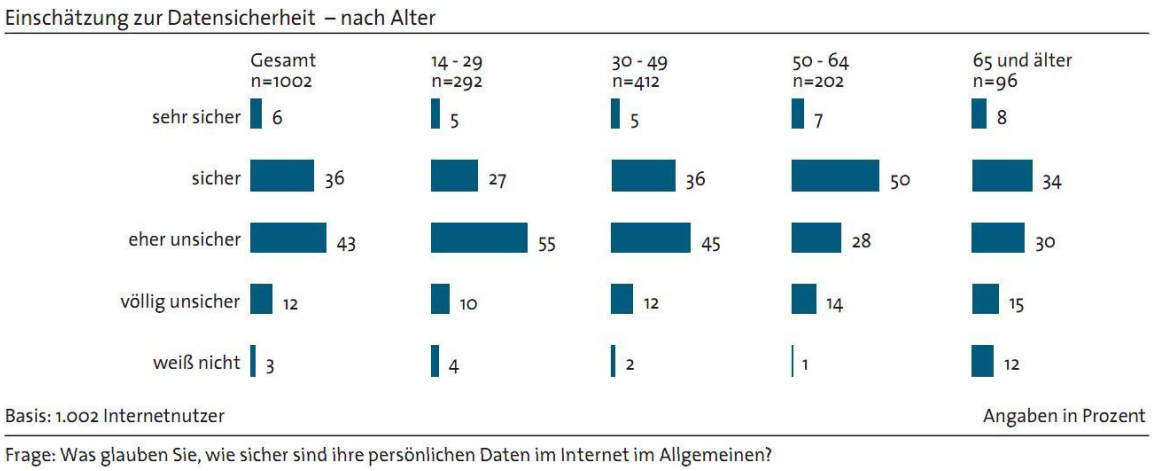

Abb. 4: Einschätzung zur Datensicherheit – in Deutschland nach Alter (Arenz et al. 2011, 22)

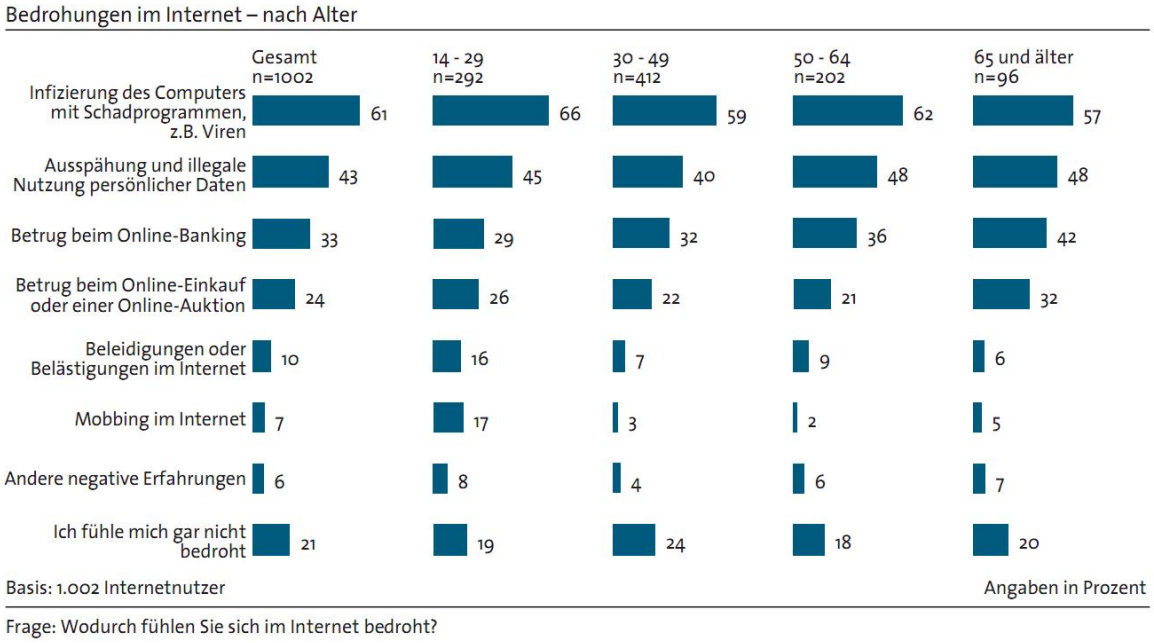

Abb. 5: Bedrohungen im Internet – in Deutschland nach Alter (Arenz et al. 2011, 29)

Gesetze zu verschärfen und das Internet zu regulieren – gehört zu den verbreiteten Forderungen der öffentlichen Auseinandersetzung (vgl. unten Nr. 5; sowie Arenz et al. 2011, 43ff; Seeger 2010, 478 und Schäfers 2010b). Dazu gehören u.a. Netzsperren gegen Kinderpornographie (vgl. oben Nr. 3.3), Vorratsdatenspeicherung gegen Terrorismus (vgl. oben Nr. 3.3; sowie EU Richtlinie 2006/24/EG und Engling 2008, 67, 78) und ein „Kill-Switch“ zur Notabschaltung des Internets (vgl. Kurz 2010).

Neben liberalen Argumenten (vgl. unten Nr. 5), steht der gesetzlichen Regulierung jedoch vor allem die Netzneutralität entgegen: Die Bewegungen, der im Netz verteilten Daten, hängen weder von Ort und Jurisdiktion ab noch von sozialen, wirtschaftlichen oder sonstigen Bedingungen. Mit Clinton (2011): „[T]here's just the internet.“ Lediglich

die IP-Adressen von Endgeräten[14] und Servern lassen sich territorial bestimmen. Erst dadurch können sie jeweils einer Jurisdiktion zugeordnet und ihre Nutzer gegebenenfalls belangt werden. Für weiter reichende Initiativen müsste demnach die Netzneutralität – und damit ein basisdemokratisches Grundelement des Netzes – eingeschränkt werden. Derartige Bemühungen werden von einigen Datenschützern als Versuch gewertet, Macht gewinnen und ausüben zu können (vgl. Rammert 2008, 189ff. Beispiele reichten von der Volkszählung durch Kaiser Augustus (vgl. Lukas 2, 1–3) über die Machenschaften von KGB und GeStaPo bis zum Bundestrojaner (vgl. Coy 2008, 47f, sowie oben Nr. 3.3). Andere appellieren, dass der Staat sich bei der eigenen Datenverarbeitung zurückhalten müsse. Statt dessen solle er für den Schutz vor exzessiver Datenerfassung und Profilbildung durch nicht-öffentliche Stellen einstehen (vgl. Barnitzke 2010, 485; Petri und Schaar 2010, 206). Allerdings verweisen Datenschützer angesichts der rasanten sozialen und technischen Entwicklung auch auf die Frage der Beherrschbarkeit:

> „Wie viel können, sollen und müssen sie [die Bürger] selbst verstehen und entscheiden? [...] Inwieweit werden sie dabei Hilfestellung durch Infrastrukturen, Tools oder andere Beteiligte erhalten?“ (Hansen und Thomsen 2010, 288)

Keulartz et al. (2004, 25) merken jedoch an, dass normative Ansätze zur Kontrolle und Regulierung grundsätzlich zum Scheitern verurteilt sind. Stattdessen schlagen sie einen pragmatischen Dreiklang aus „Antifoundationalism“ (Anti-Fundamentalismus), „Antidualism“ (Anti-Dualismus) und „Antiskepticism“ (Anti-Skeptizismus) vor, um einen offenen, aber nicht naiven Umgang mit den neuen Technologien zu ermöglichen (vgl. ebd., 14ff). US-Präsident Barack Obama geht es deswegen nicht um Kontrolle sondern um Ausnutzung der IT: Auch er betont die Gefahren des Internets, als „one of the most serious economic and national security challenges we [the USA] face as a nation“ (Obama 2009). Die „economic revolution“ (Obama 2011) habe innerhalb einer einzigen Generation eine Transformation „[of] the way we live, work and do business“ (ebd.) hervorgebracht, die die Menschen verstöre. Jedoch sei der effektivste Weg, sowohl den Gefahren als auch der ökonomisch fiskalen Krise (nach 2008) zu begegnen, das „greater potential“ (Obama 2009) der IT im (liberalen) Wettbewerb für sich auszunutzen: „We need to out educate, out innovate and out build the rest of the world.“ (Obama 2011)

[14] Als „Endgerät“ kommen neben PCs auch internetfähige Mobiltelefone, eBook-Reader, Tablet-PCs und Notebooks in Frage; zukünftig kommen Alltagsgegenstände hinzu, wie etwa Küchengeräte und Kraftfahrzeuge, vgl. Bertsch et al. (2011, 8f, 10ff, 23ff)

4.3. Die Bedeutung des Freiheitsgrundsatzes für die IT

Dem Liberalismus folgend, ist es hingegen erstrebenswert größtmögliche Gestaltungsfreiräume zu lassen, damit die Menschen sich entfalten und produktiv sein können. Zur Herstellung von Sicherheit Regularien zu induzieren – d.h. Rechte und Pflichten, sowie Kontrollinstanzen und Sanktionsmechanismen einzurichten – beschränkt diese Freiheit. Intrusive Sicherheitspolitik, so die Argumentation, kann Gefühle des *Beobachtetseins*, der Maßregelung und Bevormundung erzeugen (vgl. Arenz et al. 2011, 49; BVerfG, 1 BVG 370/07 und unten Nr. 3.3). Es existieren zwar auch subtil indirekte Ansätze, die nur sacht und unmerklich in die Lebenswirklichkeit eindringen, diese bedürfen jedoch einem langfristigen Engagement und einer ausführlichen Planung. Sie erregen wenig Aufmerksamkeit, werden dann jedoch meist negativ und nur selten positiv aufgefasst. Der Staat muss immer befürchten, eher zum *Sündenbock* als zum *Heilsbringer* erklärt zu werden. Für liberale Staatsphilosophien ist hingegen die Fähigkeit der Gesellschaft zur Selbstregulierung das ultimative Mittel zur basisdemokratischen Behandlung normativer Gesellschaftsprobleme. Institutionelle Deregulierung, so die Argumentation, kann durch Abbau und Vermeidung formeller Regularien, die zur Selbstregulierung benötigte Freiheit fördern. Der *Störfaktor* Staat dürfe deswegen seine hervorgehobene Rolle ausschließlich für das übergeordnete Wohl der Gemeinschaft nutzen. In Erscheinung treten sollte er nur, bei dringendem Bedarf, bspw. zur Bereitstellung und Aufrechterhaltung einer gemeinschaftlich zu nutzenden Infrastruktur oder im Ausnehmezustand (vgl. Plickert 2010, passim, insbesondere 62f). Allerdings ist es in den unterschiedlichen Schulen liberaler Staatsphilosophie strittig, wann diese Bedingung als erfüllt gilt. Fundamentalisten streben den vollständigen Verzicht auf staatliche Institutionen und den Staat an sich an (vgl. Viner 1960, 221). Dem gegenüber heben gemäßigte Liberale die essentielle Bedeutung bestimmter gesellschaftlicher Einrichtungen hervor, deren Werdegang nicht den unberechenbar schwankenden Stimmungen der Gesellschaft unterworfen werden sollte (vgl. Rüstow 1963, passim).

Ungeachtet der Risiken von Cyberwar, Cyberterror und Cybercrime, liegt der Grund für den Erfolg der IT und speziell des Internets – d.h. für dessen Beliebtheit, Verbreitung und rasante Evolution (vgl. oben Nr. 3) – für Autoren wie Jarvis (2009, 49ff), Friebe und Lobo (2006, 165ff), sowie für einen Großteil der s.g. Netzgemeinde (auch *net community*; Netzgemeinde oder *digital natives*, vgl. unten Nr. 5) vor allem in seiner Eigenschaft Menschen miteinander zu verbinden (vgl. Kruse 2010). Der Erfolg sozialer Netzwerke

(bspw. Facebook, StudiVZ, Xing, Google+), von Kommunikationskanälen (bspw. E-Mail, Instant Massaging, Voice-over-IP) sowie verschiedenen Kollaborations- und Publikationsplattformen (bspw. Flickr, Wikipedia, Wikileaks, Vroniplag) heben dabei einen besonderen Gemeinschaftscharakter hervor und werden durch Cloud-Dienste in Zukunft sogar noch erweitert werden (vgl. Schlüter 2011; sowie oben Nr. 3.2). Um von den gesellschaftlichen Entwicklungen nicht überholt zu werden, schlägt Jarvis (2009, passim, insbesondere 101ff, 123ff) Unternehmen, Regierungen und Privatpersonen vor, sich an den Erfolgsmodellen dieser Unternehmen (vor allem Google) zu orientieren. Sie seien „. . . platforms that help us to organize ourselves“ (Jarvis 2009, 50) – Das gilt zumindest dann, wenn Nutzer in der Lage sind, sie ohne künstliche Beschränkungen mitzugestalten (vgl. ebd., 116ff).

Liberalismus, im Sinne der freien Entfaltung im Netz, ist folglich essentiell für den Bestand dieses neuen Mediums, in dem jeder Nutzer ein potentieller Journalist ist. In diesem Sinne – wie Journalismus nach Exekutive, Judikative und Legislative als vierte Staatsgewalt gilt und hierfür besondere Rechte beansprucht – so beanspruchen Aktivisten für ein digitales Bürgerrecht die uneingeschränkte Nutzung des weltweiten und grenzenlosen Netzwerks. Erst die Freiheit macht es zu einem Vehikel der Kommunikation, Globalisierung, Liberalisierung und Demokratisierung. Ihm wird eine maßgebliche Rolle am arabischen Frühling und in der Enttarnung falscher Doktoranden zugeschrieben (vgl. Pham 2011; Mattausch 2011; Motadel und Stockrahm 2011). Um diese und weitere Funktionen zu gewährleisten, müsste prinzipiell völlige Transparenz vorherrschen. D.h. jeder müsste alles von überall, jedem und jederzeit erheben, speichern, verwerten und weitergeben dürfen, wie es ihm oder ihr beliebt. Löschung, Geheimhaltung, Besitzstandsansprüche (bspw. Urheberrechte) und Schutzräume (bspw. Privatsphäre) sind folglich Einschränkungen die Vertrauen, Verständigung und das soziale Miteinander negativ beeinträchtigen. Sie sind, so eine radikale Lesart, veraltete Konzepte, die, mit der sich ankündigen s.g. *post-privacy* Ära, nicht mehr zu vereinen sind.

Ein unfreies Netz ist demnach intransparent, zensiert und verkappt; es erlaubt Propaganda, Verschleierung, Unrecht, Diskriminierung und Unterdrückung auch jenseits des virtuellen Raums (vgl. oben Nr. 4.3 und unten Nr. 5). Regulierungen würden *das Gute* am Internet maßgeblich beschneiden und unterminieren. Schließlich würde das Phänomen Internet in seiner ursprünglich wilden, unzähmbaren Form verloren gehen. Seine heilsame Wirkungskraft wäre damit unwiderruflich zerstört (vgl. Schäfers 2010b).

Zusammengefasst geht es darum, entweder über öffentliches Teilen die Welt demokra-

tisch zu sozialisieren und die Daten zum gesellschaftlichen Nutzen zu liberalisieren *oder* über Zugriffslimitationen Diskretion zu errichten und Sicherheit zu gewährleisten. Der Antagonismus zwischen Sicherheitsbedürfnis und Freiheitsgrundsatz im Informationszeitalter lässt sich somit auf den Cleavage zwischen Kontrollnahme (Macht) und Kontrollverzicht (Post-Privacy) reduzieren.

5. Netzpolitik, politischer Aktivismus und Hacker

Um im Rahmen der Netzpolitik produktiv gestaltend tätig zu werden, beginnen derzeit die deutschen Parteien eigene Diskussionsgruppen zu gründen (bspw. „SPD Netzpolitik“ oder der CSU Netzrat). Sie begegnen damit vor allem dem Vorwurf der eigenen Desinformation, Ignoranz, oppresiven Sicherheitspolitk und des blinden Aktionismus (vgl. oben Nr. 3 und 4). Als parteiübergreifende Arbeitsgruppe zum Thema „Internet und digitale Gesellschaft“ wurde 2010 außerdem die 26. Enquete-Kommission des Bundestags einberufen. Bestehend aus Vertretern der Parteien und von ihnen berufenen Sachverständigen, ist die Kommission beauftragt bis 2012 einen Empfehlungsbericht für die Herausforderungen des Informationszeitalters zu erstellen. Die Auswahl der Sachverständigen umfasst dabei einige der wichtigsten netzpolitischen Akteure Deutschlands.

Auffällig ist, dass mit Verlauf vom linken ins rechte Parteienspektrum, die Nähe zur Ökonomie zunimmt, während sich der Abstand zur Netzgemeinde vergrößert. Gerade für die Unionsparteien sind mit Dr. Bernhard Rohleder (BITKOM e.V.), Harald Lemke (Deutsche Post AG; McKinsey & Co.; BKA und IBM) und Prof. Dieter Gorny (EMO) vor allem Vertreter der etablierten Medien, proprietärer Technologien und Gatekeeper in die Kommission berufen worden. Angesichts der Entwicklungen im Web 2.0 werfen Netzaktivisten ihnen Protectionismus sozial und technologisch überholter Lebensrealitäten vor (vgl. oben Nr. 3.2f). Gleiches gilt für Dr. Wolf Osthaus (1&1 Internet AG), der für die FDP berufen wurde. Mit Cornelia Tausch (BEUC) und Dr. Wolfgang Schulz (Hans-Bredow-Institut) für die SPD wurden jedoch auch relativ unparteiische Personen berufen.

Die Netzgemeinde hingegen, ist zum einen sozial-liberal (bspw. Digitale Gesellschaft e.V.; vgl. oben Nr. 2.1 und 4.3) und zum anderen marktliberal deregulierend (wie etwa bei Jarvis) geprägt. Sie ist grundlegend skeptisch gegenüber proprietärer Systeme und zentralistischer Organisationsstrukturen; bringt kulturelle Güter hervor und findet ihr Weltbild umgekehrt, etwa in Kulturgattungen wie dem *Cyberpunk*, wieder (vgl. McCarron 1995,

262, 263f, 271ff). Ihr Aktivismus weist sowohl extreme (wie bspw. bei den Hackerorganisationen LulzSec und Anonymous) als auch formelle (wie bspw. dem Journalismus von netzpolitik.org oder der Petition des AK Zensur) Tendenzen auf und ist am besten mit der digitalen Bohéme (vgl. oben Nr. 2.2, sowie Friebe und Lobo 2006, 39ff) zu vergleichen. Ihre einzelnen Gruppierungen unterscheiden sich durch ihren rechtlichen Status, Organisations- und Mitgliederstruktur, öffentliche (Selbst-) Darstellung, territoriale Verbreitung und Aggressionspotential. So kritisieren fast alle Gruppen bspw. „Datenkraken" wie Facebook, publizieren ihre Kritik jedoch nicht nur im Netz oder der Realität, sondern starten u.U. auch Kampagnen unterschiedlicher Größe. Darüber hinaus rufen Gruppen wie Anonymous öffentlich zum Sturm gegen das SNS auf (Stichwort #opfacebook, vgl. AnonymousAnonV 2011).

Die Netzgemeinde ist folglich keinesfalls als homogene Bewegung zu betrachten. Gemein ist ihnen jedoch ein reger, gruppenübergreifender Ideen- und Meinungsaustausch. Diese hohe geistige Vernetzung erfolgt meist über Internet, aber auch über öffentliche Veranstaltungen, wie der *re:publica* (deutsche Konferenz für „Blogs, soziale Medien und die digitale Gesellschaft") oder dem *Chaos Communication Congress* (Kongress des CCC). Dabei wird sie in der Enquete-Kommission vor allem durch Constanze Kurz (CCC)[15] für die Linke; Markus Beckedahl (netzpolitik.org, Digitale Gesellschaft e.V.) für B'90/Grüne; Alvar C. H. Freude (AK Zensur) für die SPD und „padeluun" (Künstler und Netzaktivist) für die FDP vertreten. Ihre Argumentationslinien zusammenfassend, gäbe es in Bezug auf die Verfügungsmacht über Daten keinen Konflikt zwischen Freiheit und Sicherheit: Es gäbe lediglich die *Wahl* zwischen „Freiheit und Kontrolle" (Kurz und Rieger 2011, 187).

Dennoch bemängelt die Netzgemeinde, an der Politik der etablierten Parteien nicht ausreichend gehört zu werden. Vor allem die FDP, als staatsphilosophisch nächstliegende Partei, erweckt, aufgrund ihrer programmatischen Nähe zur Ökonomie, den Eindruck, entgegengesetzt der netz-liberalen Logiken zu agieren (vgl. oben Nr. 4.3; sowie Rieger 2011). Mit Ursprung in Schweden gründete sich aus diesem Grund die *Piratenpartei* (auch Piraten, ursprünglich „Piratpartiet"). Unter erheblicher Zuhilfenahme von EDV (vgl. Altenbockum 2011) konzentriert sich in ihr der sozial-liberale Willen der Netzgemeinde. Beschrieben als eine Mischung aus FDP, Links-Partei und Chaos Computer Club (vgl.

[15] Zu den bekanntesten Persönlichkeiten des CCC gehören u.a. Wikileaks-Gründungsmitglied Daniel Domscheit-Berg (inzwischen vom CCC ausgeschlossenen, vgl. N.N. 2011a), Sicherheitsforscher Sandro Gaycken, sowie Constanze Kurz und Frank Rieger (u.a. Sachverständige vorm BVerfG, vgl. presse 2009 und Kurz und Rieger 2009, passim)

Wagner 2011) breitete sie sich schnell weltweit aus (vgl. Bundeszentrale für Politische Bildung 2009). Bereits 2009 erlangte sie, in ihren jeweils ersten Wahlen für das Europaparlament mit annähernd 1% und den deutschen Bundestag mit 2%, die besten Ergebnisse unter den sonstigen Parteien. In der Wahl vom 18.09.2011 zogen sie schließlich mit 8,9% vor der FDP (1,8%) in das Berliner Abgeordnetenhaus ein (vgl. Steffen 2011 und B.U. 2011). Dies stellt eine „schallende Ohrfeige für etablierte Parteien“ (Brüggmann 2011) dar und erinnert stark an den Werdegang von Bündnis'90/Die Grünen (vgl. Goffart 2011).

Obgleich diese Analyse nicht vorbehaltlos auf den Bundestag verallgemeinerbar ist, ist keine programmatischer Schieflage feststellbar. Allerdings ist angesichts der wenigen Aktivisten bzw. netz-liberalen Vertreter in der Kommission, eine personelle Schieflage deutlich zu erkennen.

Teil II.

Fallbeispiel: Sichere Massenkorrespondenz in Deutschland

6. Ausgangssituation

Nach der bekannten Formel von Watzlawick et al. (1967, 51) „one cannot *not* communicate“ (Herv. v. Vf), finden weltweit eine Vielzahl von Kommunikationsmethoden Anwendung. Deren Beschaffenheit, Regulierung und Nutzung variieren historisch und sozial bedingt mitunter stark.

Aufgezeigt wird hier zuerst die historisch gewachsene Ausgangssituation in den schriftlichen Kommunikationstechnologien. Hier ist zum einen das Postwesen (Nr. 6.1) und zum anderen die E-Mail (Nr. 6.2) relevant. Es werden ihre Stärken und Schwächen erläutert als auch ihre gesellschaftliche Bedeutung, um für den darauf folgenden Abschnitt 7 die Notwendigkeit einer Novellierung herzuleiten.

6.1. Stoffliches Versandwesen in Deutschland

Eine der ersten standardisierten Methoden zur Kommunikation über weite Distanzen ist die Übermittlung von Nachrichten und Gütern auf dem Postweg. Zwar versahen bereits seit Jahrtausenden Boten und reisende Händler Versanddienstleistungen wie diese, jedoch erlaubte erst die Einrichtung von Postenstrecken eine vergleichsweise regelmäßige und zuverlässige Korrespondenz. Ihre Nutzung erwies sich dabei gleichzeitig als relativ günstig und unkompliziert. Die Einrichtung der dafür benötigten Infrastruktur wurde in Deutschland maßgeblich durch Kaiser Max I und Kaiser Karl V ab Anfang des 15. Jahrhunderts nach französischem Vorbild vorangetrieben.

Vor allem zur Koordination geschäftlicher Kontakte und staatlicher Dienststellen mit- und untereinander wurde das Verfahren schnell unersetzlich. Der dadurch stetig steigende soziale Stand der Familie Thurn und Taxis, welcher die Administration übertragen wurde, spiegelt dabei Erfolg und Bedeutung der „Kaiserlichen Reichspost“ im Wandel der Zeit wieder (vgl. Dietz 1806, 5ff). Durch die Post entstand außerdem ein Verbreitungskanal

für s.g. *Avisen* und *Relationen*, wodurch der moderne Journalismus maßgeblich beeinflusst bzw. zusammen mit dem Buchdruck erst ermöglicht wurde (vgl. Stöber 2005, 61ff, 99ff). Das heute (zumindest deutschlandweit) flächendeckende Versanddienstwesen bildete sich allerdings erst heraus, als die einzelnen Strecken im Laufe der Zeit immer weiter ausgebaut wurden. Für den Großteil der Bevölkerung verhinderten jedoch mangelnder Wohlstand und schlechte Alphabetisierung die aktive Partizipation. Erst mit Aufkommen allgemeiner Schulpflicht im 18. Jahrhundert und dem ökonomischen Aufstieg des Landes, konnte eine breite Öffentlichkeit diese Einstiegshürden überwinden und sich das Medium erschließen.

Der gesellschaftliche Stellenwert wuchs daraufhin derart an, dass 1831 Hessen erstmalig in der Deutschen Geschichte ein Briefgeheimnis in seine Verfassung aufnahm (vgl. Sterzel 1968a, 24). Diese juristische Garantie wurde dringend benötigt, um das Vertrauen der Bürger in ihren Souverän und dessen Kommunikations- und Sicherheitspolitik wieder herzustellen (vgl. oben Nr. 4). Mit dem Gesetz wurde Behörden untersagt, ihre hoheitlichen Kompetenzen durch Spionage am eigenen Volk zu missbrauchen. Dieser Kerngedanke floss in darauf folgenden deutschen Verfassungen immer wieder mit ein. 1949 findet er in Artikel 10 I mit den Worten „Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich“ (Art. 10 I GG) Einzug in das Grundgesetz für die Bundesrepublik Deutschland (GG). Die Allierierten Siegermächte forcierten es, um ein erneutes Erstarken des Faschismus in Deutschland zu unterbinden. In seiner Kürze schreibt es fest, dass der Transport ununterbrochen stattfinden soll und alle nachrichtenbezogenen Informationen vertraulich sind. Unabhängig von Umständen und Inhalten der Kommunikation garantiert das „Brief-, Post- und Fernmeldegeheimnis“ somit eine sichere Kommunikationsplatform für jedermann (im Gegensatz zu Art. 4–6, 12–14 GG; vgl. Hornung 2008, 256f) und Kleine-Voßbeck 2000, 49f.

Das gesamte Kommunikationswesen der BRD wurde bei Wiederaufbau zur „Deutsche Bundespost“ (DBP) zusammengefasst und folglich staatlich betrieben. Darin enthalten war sowohl die Hoheit über Versand- als auch Fernmeldewesen (heute „Telekommunikation“, vgl. Scherer 1995, 73). Unter Vorbereitung einer Koalition aus Unionsparteien und FDP unter Ludwig Erhard sowie Finalisierung in Großer Koalition unter Kurt Georg Kiesinger erfuhr Art.10 I GG bald eine Einschränkung: Als Eingriff in die Grundrechte wurde 1968 das *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* (Artikel 10-Gesetz bzw. *G10*, vgl. Art.10 II GG; sowie Brenner 1990, 71f, 74; Kleine-Voßbeck 2000, 133; Sterzel 1968b, passim, insbesondere 18f und 1968a, 24ff, 40ff) verabschiedet.

Sinn war es zu verhindern, dass kriminelle, gemeingefährliche oder/und systemfeindliche Organisationen – seinerzeit vor allem die RAF und die *Bewegung 2. Juni* – bestimmte freiheitliche Grundrechte West-Deutschlands missbrauchen, um bspw. den Systemumsturz mit Gewalt herbeizuführen. Wesentlicher Bestandteil des G10 waren die Befugnisse zur befristeten Überwachung und Protokollierung der Kommunikation per Post und Telefon einzelner Personen. Im Fall unmittelbarer Gefahr sollte damit die Gefahrenquelle ermittelt werden können – bspw. eine Terrorzelle, deren Motivation und Ziele – um sie rechtzeitig unschädlich machen zu können. Es ermöglichte außerdem die gleichzeitige Beweismittelsicherung, um in späteren Gerichtsverfahren die Beweisführung zu gewährleisten.

1989 wurde durch die Bundespostreform (I) die DBP in mehrere öffentliche Unternehmen untergliedert. Diese wurden wiederum 1994 zusammen mit der „Deutsche Post“ – das Pendant der DBP in der DDR – im Zuge der Bundespostreform II privatisiert. Es entstanden dadurch drei eigenständige Aktiengesellschaften: Deutsche Post AG (Versandwesen), Deutsche Postbank AG (Finanzdienstleistung) und Deutsche Telekom AG (Telekommunikation).

Seit 2005 ist die zuständige Aufsichtsbehörde auf Bundesebene sowohl für Post als auch Telekommunikation die *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (BNetzA), welche dem Bundesministerium des Innern (BMI) untersteht. Speziell für die Belange der Kommunikations- und Informationstechnologie existieren zudem weitere Ämter, wozu der bzw. die *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI; derzeit Peter Schaar) sowie das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) zählen. Zu ihren Aufgaben gehört u.a. den Kommunikationsmarkt zu überwachen, Datenschutz und -sicherheit einzufordern, Fürsprecher der Bürger bzw. Verbraucher zu sein und in diesem Sinne auf die Umsetzung geltender Gesetze zu achten.

Das Monopol, welches die DBP (mit Ausnahme der Finanzsparte) einst inne hatte, ist mit den Postreformen *de jure* aufgelöst. *De facto* existieren jedoch nach wie vor Strukturen, die einem freien Wettbewerb entgegenstehen. Dies gilt etwa für Festnetzanschlüsse u.a. zur Nutzung von Telefon und Internet. Derzeit sind die hierfür benötigten Leitungen noch größtenteils im Besitz der Telekom. Allerdings ist gerade in diesem Bereich durch die neuen Mobilfunkstandards und der kontinuierlichen Weiterentwicklung der Telekommunikationstechnologie ein Aufbrechen des Monopols zu beobachten. Gerade junge Menschen verzichten zunehmend auf Festanschlüsse und schwächen somit die Marktposition

des ehemalige Staatsunternehmens. Weitestgehend liberalisiert ist ebenfalls der Paketversand. Der Großteil von Abholung, Logistik und Auslieferung des Briefversands sind jedoch weiterhin in Kontrolle der Deutschen Post. Grund hierfür ist, dass Konkurrenten bisher nur räumlich begrenzt, das Bereitstellen der Infrastruktur gelang.

Seit dem *Internetboom* sinkt zudem der Briefverkehr kontinuierlich ab. Zwar erfreuen sich Paketsendungen durch Onlinekaufhäuser wie eBay und Amazon großer Beliebtheit, die Einbußen der Deutsche Post AG werden jedoch weiterhin durch die unterschiedlichen Kommunikationskanäle des Internets unterminiert. Bereits ab den 1960er Jahren bestanden deswegen Bemühungen (etwa in den USA), diesem Trend entgegen zu wirken (vgl. Siegert 2008, 259ff). Deren Erfolge fielen jedoch eher mäßig aus und ein beherztes Investition in die elektronische Kommunikation wurde abgelehnt. Derzeit berichtet das Statistisches Bundesamt (2010) vom Fallen des Briefaufkommens um bis zu zwei Prozent jährlich. In voneinander unabhängigen Presse-Interviews erklärten Appel und Bégéle, Chefs der Deutschen und Schweizerischen Post, diese Entwicklung, mit der stark unterschätzten internetbedingten Marktentwicklung. Bis 2015 rechnen die Unternehmen nun mit einem Rückgang des Briefaufkommens von insgesamt 30%. Dieses Marktvolumen sei nicht wiederherstellbar. Aufgrund divergierender Interpretationen, kündigten die Unternehmer jedoch unterschiedliche Marktstrategien an, um die absehbaren Verluste zu kompensieren. Béglé verneint dabei den Einstieg in die elektronische Post, da er sich nicht slebst „kannibalisieren“ wolle. Er lehnt folglich Appels Kurs, in Richtig E-Postbrief bzw. De-Mail, ab (vgl. Appel et al. 2009 und Béglé et al. 2009).

6.2. Elektronische Briefpost

Da über das Arpanet Datenströme jeglicher Art koordiniert werden konnten, wurde mit der *electronic mail*[16] eine schnelle und günstige Alternative für hausinterne und postalische Kommunikation geschaffen. Der Dienst ist vordergründig zur direkten Kommunikation zweier (1:1) oder mehr (1:n) Personen vorgesehen. Er kann aber auch über s.g. Mailverteiler zur Massenverbreitung von Inhalten (bspw. Spam und Newsletter) oder mit Hilfsprogrammen zu einer automatisierten *Mensch-Maschine-Kommunikation* (bspw. zum Ab- oder Bestellen von Newsletter per E-Mail) genutzt werden.

„Die Vorteile der E-Mail-Anwendung sind sehr klar zu erkennen: Jeder kann

[16]electronic mail (E-Mail) = elektronische Briefpost: Erstmalig Definiert durch RFC: 822; Grundlegende Reformen erfolgten mit RFC: 2822 und RFC: 5322

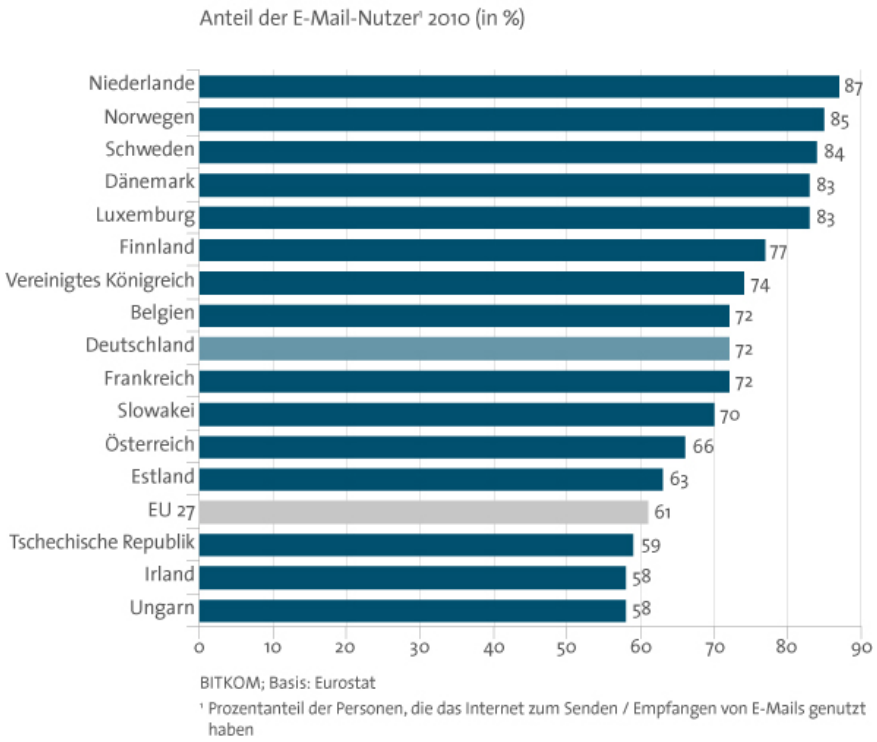

Abb. 6: E-Mail-Nutzung im europäischen Vergleich (BITKOM 2011)

damit umgehen, weil die Handhabung sehr einfach ist. Die E-Mails werden innerhalb weniger Sekunden weltweit übertragen und jeder kann immer mit Hilfe von Mail-Boxen erreicht werden. Die Inhalte und Anhänge der E-Mails können sofort weiter verwendet werden, es tritt kein Medienbruch auf. Die E-Mail Anwendung ist sehr kostengünstig, da i.d.R. keine extra Gebühren für den Austausch der E-Mail bezahlt werden müssen.

Der E-Mail Dienst ist für die vernetzte Informations- und Wissensgesellschaft inzwischen eine nicht mehr wegzudenkende Anwendung.“ (Pohlmann 2010a, 609)

Warenversand ist zwar aufgrund der Beschränkung auf Programmcode – d.h. Textnachrichten, Multimediainhalte oder Programme – ausgeschlossen, dies änderte jedoch nichts an der großen Beliebtheit des Dienstes (vgl. Mantovani 1994, 57f und Kleine-Voßbeck 2000, 7ff, sowie Abb. 6 nach BITKOM 2011). Seit seiner Einführung breitet sich der Dienst stets parallel zur Nutzung des Internets aus. Heute ist die E-Mail-Kommunikation aufgrund von flächendeckender Alphabetisierung, gesellschaftlicher Vertrautheit mit vergleichbaren Medien (bspw. Post) sowie der anhaltenden Computerisierung praktisch allgegenwärtig. Technischen Messungen zufolge, werden zu dessen Bereitstellung weltweit etwa 2,4 Millionen Mail-Server betrieben (vgl. Pohlmann 2010a, 608).

Im Vergleich zur Entstehungsphase haben sich die Verwendungsformen und Ansprüche jedoch stark verändert. Bei den meisten Anbietern von zugriffskontengestützten Webin-

halten (u.a. SNS, Cloud Computing, Foren und Blogs) sind E-Mail-Konten zur Authentifizierung[17] der Nutzer unverzichtbar geworden. Die E-Mail wird infolgedessen sowohl zur schnellen und einfachen (bspw. zum *Chat*, vgl. Flaherty und Seipp-Williams 2005, 201ff) als auch zur formellen und vertraulichen Korrespondenz verwendet (bspw. bei Online-Berufsbewerbungsverfahren, vgl. Mantovani 1994, 57f und Krueger 2006, 760).

Um automatisiert bearbeitet werden zu können, müssen E-Mails in Programmcode einer bestimmten Konvention entsprechen. Um dies dem Endanwender zu erleichtern, werden GUIs eingesetzt, die ein Formular mit Pflichtfeldern und optionalen Eingaben vorgeben. Die dort erfolgten Eingaben werden dann automatisiert in entsprechenden Code konvertiert. Eingegeben werden muss die E-Mail-Adresse des Empfängers. Alles andere – u.a. Betreff, Inhalt, Anhang, Grußformeln und eine beliebige Anzahl weiterer Empfänger – ist nicht verpflichtend. Der sehr offen gehaltene E-Mail-Standard erlaubt außerdem, dass Zusatzfunktionen beim Editieren der Nachricht helfen oder seine Funktionen, bspw. durch Verschlüsselung oder digitaler Signatur, erweitern. Ist die Nachricht fertig, wird sie erst im Postausgang des Nutzerkontos vom Absender abgelegt. Dies entspricht dem real existierenden Postkasten, ist jedoch individuell zugeordnet statt öffentlich exponiert. Dabei ist unerheblich, ob der Dienst am Internet oder einem anderen Netzwerk angeschlossen ist. Lediglich die Infrastruktur aus Benutzerkonten, Nodes sowie Postein- und -ausgängen[18] muss vorhanden sein. Dies erlaubt auch geschlossene Korrespondenz, wie bspw. in unternehmens- oder haushaltsinternen Netzwerken (s.g. Intranets oder „Binnen-Informationsnetze“, vgl. Kleine-Voßbeck 2000, 12).

Um übertragen werden zu können, wird der Code dann, im für Datenübertragungen allgemeingültige *Open Systems Interconnection Reference Model* (OSI oder auch ISO OSI-Schichtenmodell, vgl. Abb. 7 nach Stoll und der_Fahrer 2010), in sieben Schritten bis zum I/O-Signal abstrahiert. Damit nach der Übertragung dieser Prozess wieder umgekehrt werden kann, werden, wie bei einer Matrjoschka-Puppe, schichtweise neue, automatisch erstellte Daten der Nachricht beigefügt. Hierzu gehört neben der E-Mail-Adresse des Absenders auch Informationen über alle involvierten Programme, Server, IP-Adressen sowie Datum und Uhrzeit des Versands. Um das Gespräch nachvollziehbar zu halten, wird,

[17] Unter Authentifizierung wird die Feststellung der Zugriffsberechtigung verstanden; vgl. Clarke und Knake 2010, 281

[18] Post*ein*gangsserver sind derzeit entweder mit *Post Office Protocol* (POP3, vgl. RFC: 1939) oder *Internet Message Access Protocol* (IMAP, vgl. RFC: 3501) betrieben. Post*aus*gangsserver verwenden das *Simple Mail Transfer Protocol* (SMTP, vgl. RFC: 2821)

sofern nicht anders gewünscht, bei Konversationen in denen über Antwort- und Weiterleitfunktion sich mehrere Nachrichten verketten, die vorangegangenen Korrespondenzen protokolliert und der Nachricht angehängt. Protokolliert werden ebenfalls sämtliche Nodes, über die die Nachricht vom Sender zum Empfänger gelangte, um die automatische Pfadsuche des Webs ausnutzen und die Nachricht zuverlässig zustellen zu können (vgl. Kleine-Voßbeck 2000, 8ff, 11ff, 15ff, 31, 95ff).

Die E-Mail ist jedoch nicht rechtssicher, denn die „Zuverlässigkeit“ in der Zustellung ist nicht mit *Sicherheit bei der Zustellung* oder *Zuverlässigkeit der Nachricht* gleichzusetzen. Dafür war sie bei Inbetriebnahme nicht konzipiert und darauf kann sie heute auch nicht umdefiniert werden. Der Aufwand wäre zu groß (vgl. Pohlmann 2010a, 608).

Wie oben beschrieben (Nr. 3.2f und 4), tragen Gatekeeper in Punkto Sicherheit und Zuverlässigkeit der Kommunikation eine hervorgehobene Rolle. Daneben kündigte bspw. der Kommandeur des U.S. Cyber Command und Leiter der NSA, Army General Keith Alexander, bereits 2008 an, ebenfalls auf E-Mail-Daten zurückgreifen zu wollen, um für die nationale Sicherheit eintreten zu können (vgl. Hersh 2010). Die Erhebung der Daten wird bspw. mit „Deep Package Inspektion“ (DPI) -Software ermöglicht. An einem beliebigen Punkt im Netz sieht sie unbemerkt den Inhalt des durchgeleiteten Datenverkehrs ein (vgl. Clarke und Knake 2010, 283f). Gleichzeitig kann es Protokolle oder Kopien anfertigen; Datentransfairs kontextsensitiv unterbinden (m.a.W. Zensur) und Inhalte verfälscht weiterleiten (m.a.W. Herbeiführung von Desinformation). Unabhängig von Akteur und Motivation werden bei solchen Verletzungen informationeller Selbstbestimmung, neben den Rechten des Dateninhabers auch jene seiner Korrespondenten und mit den Nachrichten assoziierbaren Personen verletzt: Wenn sich also bspw. Person A mit Person B über Person C austauscht, werden beim Auslesen der Daten von Person A auch Daten der Personen B und C erhoben.

Bei ausreichend hoher Datendichte und -Menge wird es also möglich weitere Daten zu generieren. Bspw. kann über die IP-Adressen der Nodes und der jeweiligen Endgeräte ein detailliertes Bewegungsprofil der Nutzer erstellt werden. Noch raffiniertere Algorithmen, wie sie mitunter Cataphora, Iqbal et al. (2010, 8f) und Googles E-Mail-Dienst *GMail* verwenden, sind hingegen in der Lage den Programmcode der Nachrichten zu individualisierter Werbung, sozial-psychologischen Profilen und zuverlässigen Identifikationen zu verwerten (vgl. Dworschak 2011, 122f, Kurz und Rieger 2011, 182).

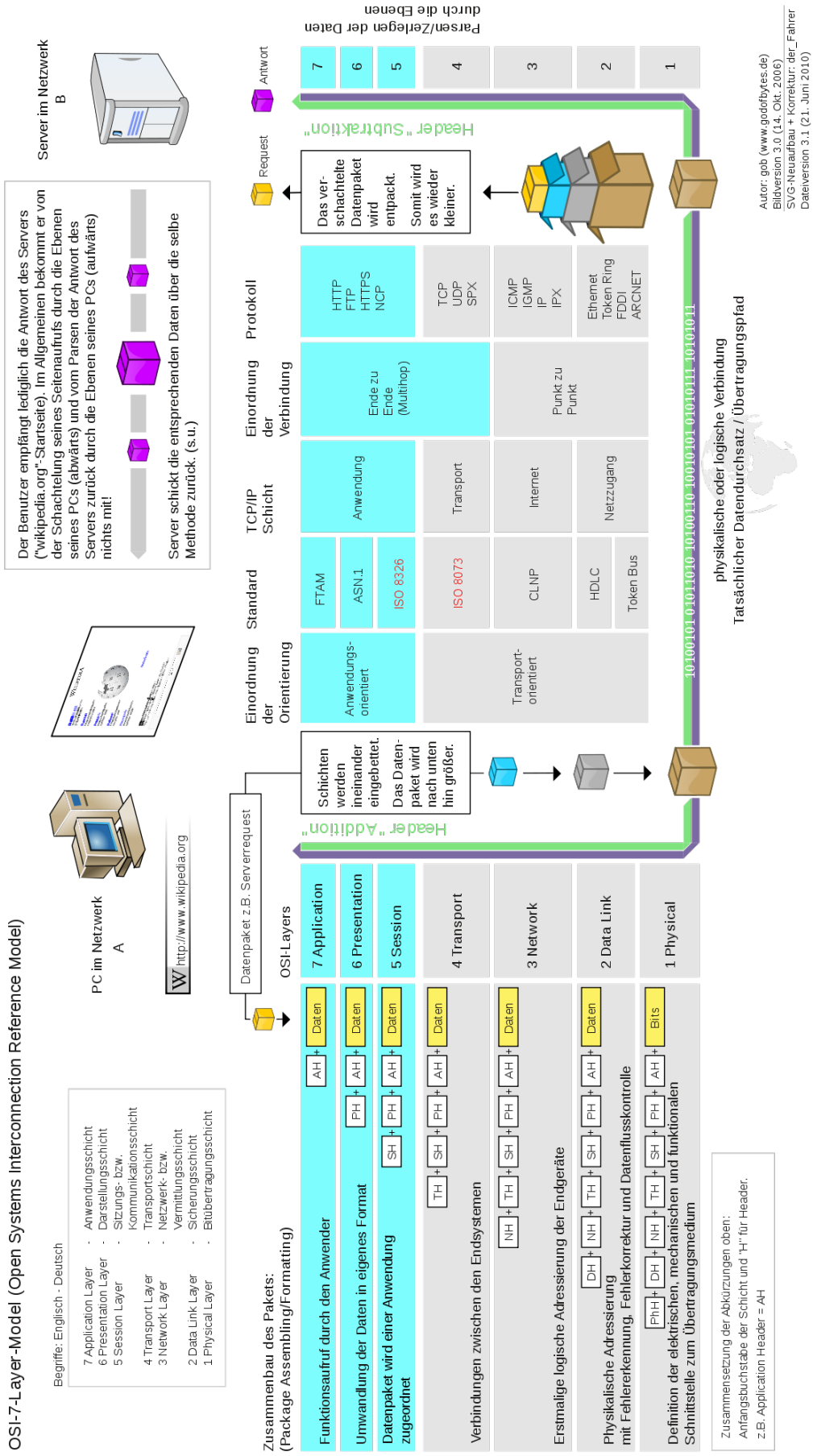

Abb. 7: Kommunikation im OSI-7-Schichten-Modell (Stoll und der_Fahrer 2010)

Bei aller Verwertbarkeit von E-Mail-Daten, ist eine ihrer größte Schwächen die (für Laien) schlechte Identifizierbarkeit der Benutzer. Abgesehen von Möglichkeiten der Fremdmanipulation, fällt gerade das Phishing mit plausibel gestalteten Mail-Adressen und verschleierter (nicht prüfbaren) Kontoinhaberidentitäten besonders leicht (vgl. Symantec 2010). Mertes (2010) stellt jedoch nach diversen Gerichtsentscheidungen fest, dass die Bedeutung des Dienstes, trotz Rechtsunsicherheit, nicht zu unterschätzen sei (ebd., 633). Die E-Mail ist demnach eine anerkannte Kommunikationsmethode, dessen Eintreffen beim Empfänger rechtlich mit dem Erhalt eines Briefes gleichgesetzt ist (ebd., 634). Da jedoch Unverfälschtheit und Vertraulichkeit nicht garantiert (vgl. oben) als auch Eingangs- und Empfangsbestätigungsanforderungen vom Empfänger abgelehnt werden können, ist die s.g. *E-Complience* für Unternehmen im Umgang mit E-Mail ein rechtliches *Minenfeld* (ebd. 637).

Eine nach Art.10 GG vertrauliche, zuverlässige und rechtssichere Korrespondenz, über die etwa verbindliche und rechtsgültige Verträge geschlossen werden könnten, ist demnach nur durch entsprechende Zusatzsoftware möglich. Diese müsste die Eindeutigkeit der Identität verifizieren, eine fälschungssichere Signatur ermöglichen und den Zwang zur Eingangs- und Empfangsbestätigung enthalten. Zwar gibt es hierfür bereits eine große Auswahl unterschiedlicher Lösungen, die seit langem zur Verfügung stehen; sie werden jedoch nicht genutzt (vgl. Hemker 2010, 629). Hinzu kommt, dass, wenn jeder Nutzer sein eigenes Programm mit seinen eigenen Einstellungen verwendete, ein sehr unübersichtlicher Pluralismus zu befürchten ist, dessen Folge eine Sprachverwirrung babylonisch-biblischen Ausmaßes wäre (vgl. Gen 11,1–9).

„Die Sicherheitsrisiken des E-Mail-Dienstes im Internet sind zurzeit zu hoch“, folgert deswegen Pohlmann (2010a, 613). Die Forderungen sind daher klar: Entweder ziehen einheitliche technische Richtlinien, elektronische Signatur und Revisionssicherheit (Archivierung, Identifizierung und Rechtssicherheit) als Mindestanforderungen weltweit in die E-Mail-Kommunikation ein oder jedermann sollte seine Kommunikation intensiv reevaluieren (vgl. Kleine-Voßbeck 2000, 211; Reiners 2010, 632 und Pohlmann 2010b).

Als Alternativen zu Versand- und E-Mail-Diensten stehen neben der De-Mail (vgl. unten Nr. 7) sowie diversen Speziallösungen (bspw. für unternehmensinterne Kommunikation) eine weite Palette öffentlicher Kommunikationsmethoden zu Verfügung. Fuchs (2010, 458) hebt allerdings erneut die großen Risiken hervor und stellt gleichzeitig fest, dass angesichts der Vorteile des Webs 2.0 und SNS – vor allem in Bezug auf Benutzerfreundlichkeit und

Verbreitung (vgl. Bertsch et al. 2011, 33ff, 46ff) – Verzicht unrealistisch sei. Eine neue Netzpolitik, so Fuchs weiter, sei hier dringend erforderlich.

In Ergänzung dazu, diskutieren Mislove et al. (2005, 171f, 183) die Kommunikationsplatform „ePOST“ auf Basis von „Peer-to-Peer“ (P2P) -Netzwerken. Diese Netzwerke hätten sich bereits in der Verwendung durch Kriminelle und Hacker als besonders robust ausgezeichnet. Vor als auch Nachteil der P2P-Technologie ist jedoch, dass die Daten nicht über Gatekeeper, sondern über die Rechner sämtlicher Nutzer geleitet werden. Eben hier könnten die Nachrichten potentiell abgefangen werden (vgl. BMWi 2008, 7). Ebenfalls werden *DomainKeys Identified Mail Signatures* (Adressschlüssel identifizierende Mail Signaturen, DKIM) diskutiert, die vom E-Mail-Provider allen E-Mails angehängt werden würden, um diese dann allseits eindeutig zuordnen zu können (vgl. Grimm und Pähler 2010, 89).

Den genannten Mindestanforderungen entsprechend, konnte sich bisher jedoch noch keine Lösung durchsetzen. Die Gründe reichen von mangelnden technischen Vorraussetzungen, divergierenden Interessen bis zu Mangel an Durchsetzungskraft und öffentlichem Vertrauen. Angesichts anhaltender Computerisierung der deutschen Lebensrealität, ist eine schleunige Erneuerung des Kommunikationswesens zur adäquaten Überführung geltenden Rechts ins Informationszeitalter immer dringender erforderlich.

7. Überführung der Korrespondenz ins Informationszeitalter

Infolge der Lissabon-Strategie ab März 2000 wurde 2006 die Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates (Bolkestein-Richtlinie) verabschiedet. Beabsichtigt wurde damit Dienstleistungen im europäischen Binnenmarkt zu vereinheitlichen, grenzüberschreitenden Handel zu erleichtern und einen europaweiten Wachstumsschub zu initiieren. Teil dieser Richtlinie sind die Vereinheitlichung, Vereinfachung und Digitalisierung von Verwaltungsverfahren innerhalb der Europäischen Union (Kap. II 2006/123/EG, insbesondere Art. 8). Um dies zu gewährleisten musste eine sichere, rechtsverbindliche und zuverlässige elektronische Kommunikationsplattform gefunden werden, die auch den hohen Ansprüchen hoheitlicher Aufgaben gerecht wird und unkompliziert anzuwenden ist. Da dieses klassische Spannungsdreieck „zwischen Benutzerfreundlichkeit (Usability), Administrierbarkeit (Operability) und Sicherheit (Security)“ (Völker 2010,

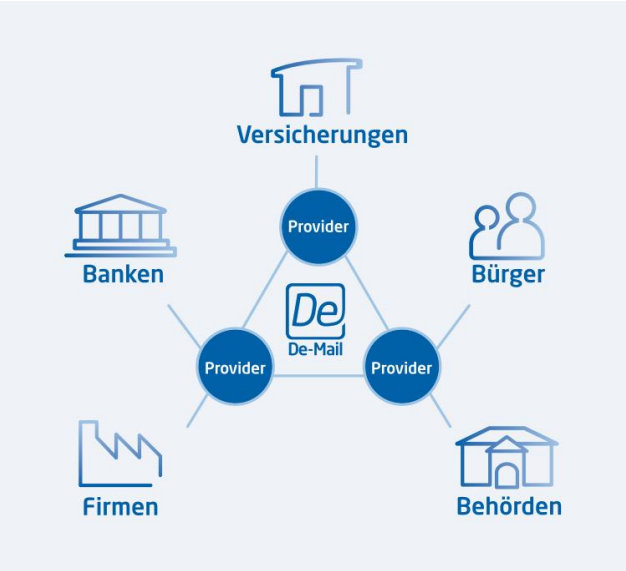

Abb. 8: Diagramm: „De-Mail ist keine ‚Behörden-Mail'." (BMI 2011, 13)

491) noch von keiner Plattform flächendeckend abgedeckt wird (vgl. oben Nr. 6.2), sind die europäischen Mitgliedsstaaten nun gezwungen eine solche zu implementieren. Resultat deutscher Bemühungen, dieser Richtlinie Folge zu leisten, war das *Projekt Bürgerportal* (später De-Mail), wofür eine Kooperation von Wirtschaft und Politik im November 2008 verkündet wurde:

> „Die Nutzung des Internets könnte bequemer und sicherer sein, wenn man zumindest bei der Kommunikation mit Behörden, Gerichten oder bei finanziellen Transaktionen Gewissheit hätte, dass die Person ‚am anderen Ende der Leitung' tatsächlich die Person ist, die sie vorgibt zu sein und dass die Daten auf dem Übertragungsweg nicht kopiert werden können." (BMWi 2008, 7)

Ein entsprechender Gesetzesentwurf wurde am 04.02.2009 von der deutschen Bundesregierung beschlossen (vgl. Deutscher Bundesrat 2009, passim). Gewonnen werden konnten die beiden ehemaligen deutschen Staatsbetriebe Deutsche Post AG und Deutsche Telekom AG sowie die United Internet AG[19]. Gemeinsam decken sie den Großteil des analogen als auch digitalen Kommunikationssektors in Deutschland ab, haben erhebliche technische Kompetenzen und ökonomische Erfahrung. Ihre Portfolien enthalten neben Festnetz- und mobiler Telekommunikation auch Internetanbindung, Versand-Dienste (E-Mail und Post), Onlinepublikation und diverse Buisness- und Premiumangebote (vgl. Borchers 2011). Die Politik ist hierbei nicht nur Moderator, sondern in ihrer Funktion als Gesetzgeber vor allem für zusätzliche Sicherheit und Kontingenz zuständig. Zukünftigen Anbietern und Nutzern ermöglicht sie die Berufung auf Rechte bzw. Pflichten.

[19]Mutterkonzern der 1&1 Internet AG und dessen Tochterunternehmen GMX und WEB.DE

7.1. Gesetz zur Regelung von De-Mail-Diensten [...] (DMailG)

Mit Wirkung vom 03.05.2011 soll das *Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften* (DMailG) einen „sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen“ (§ 1 I DMailG). Es berücksichtigt außerdem die europäischen Verfahren zu Normen und technischen Vorschriften (vgl. 98/34/EG) sowie der EU-Erweiterungen von 2007 (vgl. 2006/96/EG).

Um die Echtheit der Identität zu gewährleisten, müssen Nutzer sich bei Erstellung eines Nutzerkontos einmalig ausweisen. Zugriff und Nutzung erfolgt dann wie bei E-Mail-Nutzerkonten (vgl. §§ 4 und 5 DMailG), können jedoch in zwei unterschiedlich starken Authentifizierungsniveaus vor Fremdzugriff geschützt werden. Zudem wird dem *De-Mail-Dienstanbieter* (Provider) offen gelassen, Identitätsbestätigungsdienst (De-Ident) und Ablagefunktion (De-Safe) in sein Angebot zu integrieren (vgl. §§ 6–8 DMailG).

Angeboten werden, dürfen De-Mail-Dienstleistungen ausschließlich von zertifizierten und akkreditierten Providern. Die Akkreditierung kann jederzeit erteilt und ebenso wieder entzogen werden. Dabei muss eine Reihe einzelner Zertifikate vorliegen – darunter finanzielle Absicherung, Fachkunde (vgl. § 18 DMailG) und interkompatible Verschlüsselungtechnologie (vgl. § 5 Abs. 3 DMailG) – bevor die Akkreditierung erteilt werden kann (vgl. §§ 17–19 DMailG). Anstelle des Bundestages, werden die Zertifikatsstandards vom gemeinsamen „Ausschuss De-Mail-Standardisierung“ (vgl. § 22 DMailG) der akkreditierten Dienstanbieter beschlossen, um „ein angemessenes Sicherheitsniveau zu erreichen, gleichzeitig aber genügend Spielraum für die individuelle Gestaltung der Einsatzumgebung zu lassen“ (Schumacher 2010, 302, sowie vgl. 302f, 304ff; Abb. 9 und § 22 DMailG).

Die behördliche Zuständigkeit für De-Mail-Dienste – darunter Aufsicht und Erhebung von Gebühren (vgl. §§ 23 und 24 DMailG) – liegt beim BSI (vgl. §§ 2 und 20 DMailG). Eine Einsicht in die Kommunikation findet gemäß des Brief-, Post- und Fernmeldegeheimnisses (Art.10 I GG) nicht statt (vgl. § 20 Abs. 5 S. 3 DMailG). Zudem wird mit Art. 2 und 3 DMailG die De-Mail als gültige Kommunikationsmethode mit Behörden definiert.

7.2. Kritik an De-Mail

Laut Gelzhäuser (2010, passim) sei das Pilotprojekt von Oktober 2009 bis März 2010 in Friedrichshafen ein voller Erfolg gewesen: Mehr als 60% der Internetnutzer hätten angegeben das Angebot nutzen zu wollen, obwohl es noch keine Werbung gegeben habe.

Abb. 9: Akkreditierung & Aufsicht von De-Mail-Diensten (Schumacher 2010, 303)

Von denjenigen, die den Dienst bereits erprobt hätten, würden 90% ihn empfehlen. Zudem hätten Versicherungen bereits berechnet, dass es ein erhebliches Einsparpotential im Vergleich zur Briefpost gäbe.

> „Je mehr Unternehmen, Behörden und Privatpersonen De-Mail nutzen, desto schneller steigt die Zahl der Anwendungsmöglichkeiten – und damit auch der Mehrwert für die Nutzer." (ebd. 2010, 648)

Wie es Jarvis (2009, 49ff) ausdrücken würde, ist es jedoch nicht zu leugnen, dass beim Erfolg dieser Plattform zwischen bloßer Verwendung und umfangreicher Nutzung qualitative Unterschiede bestehen. Auch wenn De-Mail-Dienste also bereits jetzt für jedermann zur Vorab-Registratur offen stehen, wird der Dienst sich schätzungsweise erst in Behörden, dann in Unternehmen und erst zum Schluss bei Privatanwendern ausbreiten. Abzuwarten bleibt daher, ob dieser Verbreitungsgrad tatsächlich erreicht wird oder die De-Mail eher als eine „Behörden-Mail" endet (vgl. Abb. 8 sowie BMI 2011, 13 und Siegert 2008, 259f) Angesichts der Konkurrenz unter den Anbietern, ist es zudem möglich, dass sich der Dienst binnen kürzester Zeit bis zur Unkenntlich wandelt.

Nichts desto trotz – oder gerade deswegen – hat sich die Deutsche Post AG bereits während der Entwurfsphase im September 2009 aus dem Projekt zurückgezogen (vgl. Borchers 2010). Mit der wesentlich früheren Veröffentlichung des konzeptgleichen *E-Postbrief*s (E-Post) versprach sich das Versandunternehmen einen Vermarktungsvorteil gegenüber seinen Mitbewerbern in der sicheren schriftlichen und elektonischen Kommunikation. Sollte sie Erfolg haben, kann sie darauf hoffen, ihre aus dem Rückgang des Briefaufkommens

Abb. 10: Cover einer Werbebroschüre für den E-Postbrief (vgl. Deutsche Post AG 02/2011)

resultierenden Verluste kompensieren zu können (vgl. oben Nr. 6.1). Ihre Werbebotschaften, der E-Postbrief sei „so sicher und verbindlich wie der Brief“ und bringe „die Vorteile des klassischen Briefes ins Internet“, musste die Post jedoch nach einem Rechtsstreit mit der 1&1 Internet AG wegen Unwahrheit zurücknehmen (vgl. N.N. 2011f). Seither wirbt die Post etwa mit ihrer Erfahrung als auch mit „Verbindlichkeit“; „Vertraulichkeit“ und „Verlässlichkeit“ ihres Angebots (vgl. Abb. 10, sowie zu weiteren Rechtsauseinandersetzungen Braun 2010 und Klostermeier 2011). Da allerdings De-Mail und E-Postbrief einander nicht ausschließen, könnte sich die Deutsche Post dem Vorwurf mangelnder Rechtsverbindlichkeit entziehen, indem sie sich als De-Mail-Dienstanbieter akkreditieren ließe. Sie müsste dafür lediglich geringfügige Anpassungungen an ihrem E-Postbrief-Angebot vornehmen.

Es ist allerdings bezeichnend, dass neben den Internet-affinen Gruppen und den Verbraucherschutzorganisationen, auch BITKOM und Bundesrat sich negativ zu beiden Diensten aussprechen: Sowohl E-Postbrief (vgl. N.N. 2011f) als auch De-Mail (vgl. vzbv 2010) hielten oft nicht ihre Versprechen in Bezug auf (Rechts-) Sicherheit, Verbraucherfreundlichkeit und Kostenfaktor. Speziell der Hybridbrief (auch ePOST CLASSIC, nicht mit ePOST per P2P zu verwechseln, vgl. oben Nr. 6.2), als Zusatzangebot des E-Postbriefs, gilt im Ganzen als unsicher, da die Überführung der Nachricht von Elektronisch zu Stofflich durch den Art.10 GG nicht abgedeckt ist (vgl. Cebulla 2010, 311, 313 und Schulz 2011, 263ff). Außerdem lassen die Dienste, laut Schumacher (2010, 303) und Pohlmann (2010a, 611), trotz sicherer und nachvollziehbarer Kommunikation, nach wie vor die di-

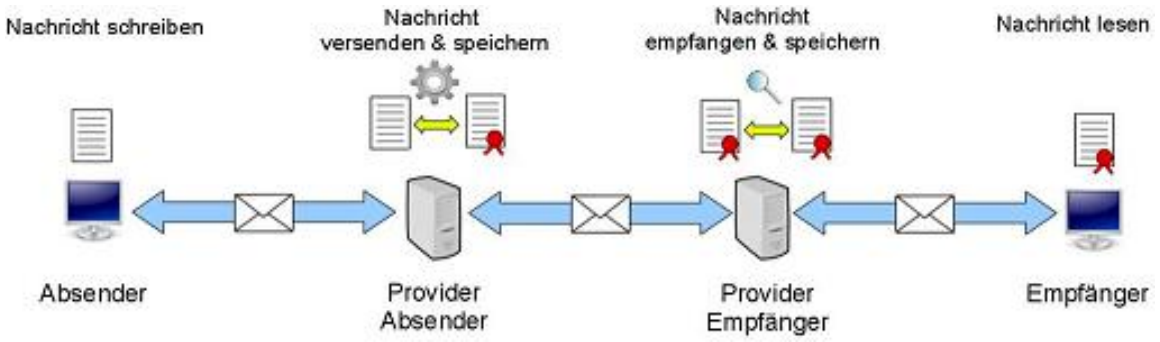

Abb. 11: Sicherheitsvorkehrung in De-Mail (vgl. BfDI 2011)

gitale Signatur vermissen, welche als einzig valide Ersatz eigenhändiger Signaturen gilt (vgl. Schäfers 2010d).

Unsicherheit verursacht außerdem die – zusätzlich zur Rechtssicherheit vorgesehene – Inhaltssicherheit (vgl. Borchers 2010). Das De-Mail-Konzept sieht hier eine „Punkt-zu-Punkt"-Verschlüsselung sämtlicher Teilverbindungen vor (vgl. Abb. 11 und BSI 2010). Dabei wird jeweils auf den Ein- und Ausgangsservern eine Sicherheitsprüfung anhand einer kurzfristig entschlüsselten Nachrichtenkopie durchgeführt. Hierbei sollen Malware und Spam erkannt, aussortiert und verfolgbar gemacht werden. Am Ende der Überprüfung wird die Kopie dann wieder gelöscht und die Originalnachricht entsprechend der Auswertungsergebnisse weiterverarbeitet. Trotz guten Willens, stellt dies einerseits einen Verstoß gegen die Netzneutralität sowie gegen Art.10 I GG dar. Außerdem bietet es Hackern eine Schwachstelle an, die ausgenutzt werden könnte.

Da De-Mails eng mit empfindlichen Daten assoziiert sind, verlangen Bundesrat (2010, e4), CCC (2011) und Lechtenbörger (2011, 269) eine durchgängige „Ende-zu-Ende"-Verschlüsselung. Die Urheber der Plattform wiegeln dies jedoch ab: Die kurzfristige Entschlüsselung sei technisch notwendig und ausreichend gesichert. In der Tat behindere eine dermaßen robuste Verschlüsselung den Dienst (vgl. hib et al. 2010) und die Nutzung von Zusatzdiensten, wie dem Hybridbrief. Der offene Standard erlaube es allerdings, dass der Nutzer dennoch eine eigene Ende-zu-Ende-Verschlüsselung implementiert (vgl. § 5 Abs. 3 DMailG), welche dann nicht entschlüsselt werden würde. Dies würde jedoch wiederum die von der Bolkestein-Richtlinie angestrebte Vereinfachung *ad absurdum* führen, wonach der Nutzer ent- statt belastet werden sollte (vgl. N.N. 2011b). Dass diese Zusatzsoftware außerdem schon bei E-Mail nicht genutzt wurde – was bekanntlich zur Einführung der De-Mail führte – wird ausgeblendet. Scharfe Kritiker unterstellen der De-Mail deshalb die logische Fortsetzung einer Sicherheitspolitik im Sinne von Otto-Katalog und G10: Indem

absichtlich eine Lücke für verdeckte Abhörmaßnahmen geschaffen wird, werde mit der angeblich sicheren Kommunikationsplattform der Öffentlichkeit ein informationstechnischer Spion untergeschoben (vgl. Schäfers 2010a und 2010c). Im Gegensatz zur dezentral organisierten E-Mail, bei der jedermann mir geringem Aufwand Konten eröffnen und ganze Mail-Server bereitstellen konnte, würden Daten nun wieder zentral bei einigen wenigen Gatekeepern zusammengetragen werden. Das erfolgreiche Eindringen in die Datenbanken bereits eines dieser Anbieter – sei es von staatlicher oder krimineller Seite – würde somit erneut einen Großteil der deutschen Bevölkerung bedrohen.

Hinzu kommt, dass aufgrund der Bolkestein-Richtlinie die De-Mail derzeit einer von vielen Alleingängen sicherer Kommunikation in Europa[20] darstellt. Zwar dürfen auch ausländische Unternehmen De-Mail anbieten, jedoch nur mit Sitz in Deutschland (vgl. BITKOM 2010, 5f). Aufgrund fehlender Interoperationalität und einer drohenden Überspezifizierung (vgl. ebd., 3f) wurde das ursprüngliche Ziel damit weit verfehlt (vgl. Lechtenbörger 2011, 268f).

Dabei wird jedoch verkannt, dass De-Mail eine dezentrale Organisationsstruktur mit konkurierenden Erfolgsmodellen aufweist. Die Aufteilung der Daten auf unterschiedliche Provider, ihr marktwirtschaftlicher Wettstreit und staatlich koordinierte Selbstkontrolle, mindern die Anfälligkeit erheblich und fördern Mehrwerte zu Tage. Durch die gesteigerte Freiheit von Nutzer und Unternehmen, wird somit die Sicherheit des Kommunikationswesens in Deutschland potentiell gesteigert.

Mit dem DMailG wurde außerdem der deutsche Kurs freier Marktwirtschaft in den Telekommunikationsdiensten konsequent fortgesetzt. Dies ist insofern klug, als dass das Risiko des Misserfolgs nun zum Großteil im Verantwortungsbereich der Privatwirtschaft liegt, während die Politik selbst lediglich den Handlungsrahmen vorgibt und sich ansonsten weitestmöglich distanziert. Eine Alternative wäre gewesen eine öffentliche Struktur einzurichten, welche erfahrungsgemäß für die technischen und gesellschaftlichen Anforderungen der Gegenwart zu träge gewesen wäre, und hierfür das volle Risiko zu tragen. Auch wäre es möglich gewesen, den Bürger zur Verwendung eines bestimmten Dienstes zu zwingen, aber auch dies ist – zumindest bis jetzt – unterblieben. Statt dessen versuchen die jeweiligen Ministerien ein analoges System nach dem anderen ins Informationszeitalter zu

[20] Eine weitere sichere Kommunikationsplattformen ist bspw. die italienische *posta elettronica certificata* (PEC, vgl. Arne und Tauber 2011). Diese wird zudem von Ruggieri (2010) als besonders kompatibel zum *Registered E-Mail* (REM) -System beschrieben, welches sich seiner Meinung nach, gut als weltweiter Standard anbieten würde

überführen. Die eID-Funktion des neuen Personalausweises ist ein Beispiel dieser Simplifizierungsbemühungen. Projekte wie dieses bedürfen des öffentlichen Vertrauens, welches versucht wird mit zunehmender Komplexität der zugrundeliegenden Infrastruktur einzuwerben (vgl. Wegener 2010, 334). Dabei versprechen der neue Personalausweis und die De-Mail durchaus Positivbeispiele staatlicher Bemühungen zu werden. Das *elektronische Entgeltnachweis-Verfahren* (ELENA) und BTX sind hingegen bereits jetzt Beispiele gescheiterter Bemühungen.

De-Mail, so BSI (2010), biete folglich eine Infrastruktur für sichere Kommunikation. Durch Sicherheitstechnik, Akkreditierungsverfahren, Konten-Benennungsnorm und Ausweisungspflicht, seien Authentizität und Integrität bei De-Mail-Diensten hergestellt worden. Sie sind dadurch besonders zuverlässig und betrugssicher; eine richtungweisende Innovation, die eine signifikante Verbesserung im Bereich der elektronischen Kommunikation darstellt (vgl. BITKOM 2010, 2). DMailG und die bisherige Umsetzung sind demnach ein voller Erfolg.

> „Das Rad in Sachen Sicherheit durch Verschlüsselung und die Verwendung von elektronischen Signaturen wurde [...] nicht neu erfunden, sondern neu – und vor allem für alle Projektteilnehmer einheitlich – zusammengesetzt.“ (Gelzhäuser 2010, 647)

8. Fazit

Final lässt sich feststellen, dass die deutsche Politik mit dem DMailG mächtig in das Informationszeitalter drängt und sich im Erfolgsfall erhebliche Administrationsverantwortung aufbürdet. Wie gezeigt werden konnte, bricht sie damit aus dem Kurs deregulierender Politik aus und zeigt sich dabei keineswegs als technikdeterministisch. Tatsächlich verknüpft sie sich ungewöhnlich eng – wie sonst mit nur sehr wenigen Fällen (bspw. Atomtechnologie) – bewahrt aber gleichzeitig jene Distanz die die Marktwirtschaft zur Selbstregulierung bedarf. Sie begegnet damit den hier dargestellten umfangreichen Sicherheitsbedürfnissen in der Telekommunikation, ohne dabei die liberalen Grundprinzipien außer acht zu lassen. Es wird jedoch erst die Praxis zeigen, ob damit der richtige Kurs verfolgt wurde.

Neben dem DMailG, sind Gesetze, wie VDS, TMG und TKG, im größeren Kontext jedoch Ideen, die ihren Weg über Brüssel in den Berliner Reichstag fanden. Hacker bezeichnen solchermaßen ferngesteuerte Rechenanlagen als „Zombies“ (vgl. Dornseif 2005, 327). Ist die „Wirtschaftslokomotive“ Deutschland also ein Zombie der EU? Die Antwort

ist *Nein*: Deutschland überlässt der EU lediglich Verbraucherschutz und Koordination grenzüberschreitender Problemstellungen. Diese Arbeit hob deswegen´, anhand ihrer Historie und aktuellen Verwendung, die Grenzenlosigkeit des Web 2.0 und deren Abhängigkeit vom Nutzer als besonders wichtig hervor. Die Verantwortung für Sicherheit und Freiheit im Informationszeitalter ist demnach auch nicht aus der Hand gelegt worden. Da nationale Alleingänge widersinnig erscheinen, können sich deutsche Bundesregierungen erlauben, in der IT einen Führungstil á la Laissez-faire zu verfolgen. Es handelt sich derzeit also keineswegs um ein weiteres verschlafenes Jahrzehnt. Vielmehr ist damit gezeigt, dass das Politikfeld „Netzpolitik“ lebendig und von breitem Interesse ist.

Die *Zensursula*-Debatte und deren Ausweitung auf den europäischen Raum stimmen allerdings bedenklich: Politische Stilblüten wie diese, stellen den *Technologiestandort Deutschland* – das *Land der Dichter und Denker* – nach 1945 und 1989 in ein ungutes Licht und stimmen pessimistisch. Ebenso bedenklich ist die mangelnde Kommunikation und Information zwischen Politik und Bürger. Bereits jetzt schlägt sich dies in Desinteresse, Desinformation und extremen Nutzerverhalten nieder (vgl. Arenz et al. 2011, passim). Wie gezeigt werden konnte, fürchten Aktivisten mit sozialdeterministischen Tendenzen einen aufkommenden Monopolismus und Seilschaften zu lasten öffentlicher Sicherheit und Freiheit. Angesichts der Koexistenz von Mensch und Maschine, kann ein solcher Mangel langfristig nicht gesund sein.

Die vergleichsweise großen Erfolge von Netzgemeinde und Piratenpartei, konnten außerdem, als anhaltende Symptome einer um sich greifenden Krankheit in der (Netz-) Politik der etablierten deutschen Parteien, identifiziert werden. Hypothetisch könnte es also nicht die Abwälzung politischer Verantwortung an die EU sein, welche die deutsche Politik lähmt, sondern tatsächlich Inkompetenz. Bestärkt wird diese Vermutung angesichts erfolgreicher Umsetzungen von EU-Richtlinien im europäischen Ausland, die in Deutschland kläglich scheiterten (vgl. Schafer 2010, 538). Folglich liegt es nun an den etablierten Parteien, zukünftig ihre *Medien-Kompetenz* zu beweisen und das Vertrauen in sie wieder zu bestärken.

Literaturverzeichnis

Adorno, T. W. (2007): *Vorlesung über Negative Dialektik. Fragmente zur Vorlesung 1965/66*. Frankfurt a.M.: Suhrkamp.

Alperovitch, D. (2011): Revealed: Operation Shady RAT. In: *McAfee Blog Central : McAfee Labs*.
URL http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

Altenbockum, J. v. (2011): Die Linux-Demokratie. Nicht nur die Piratenpartei will aus einer Kathedrale einen Basar machen. In: *Frankfurter Allgemeine Zeitung*, 38 D 1, 218, 10–10.

Anderson, C. (2009): *Free: The future of a radical price*. New York: Hyperion Books.

AnonymousAnonV (2011): Anonymous:Opfacebook. In: *YouTube*. Aufruf am 18.09.2011.
URL http://youtu.be/LsbNabK5FDE

Appel, P./ Bünder, H. und Steltzner, H. (2009): „Die Leute sehen nur den leeren Briefkasten". In: *Frankfurter Allgemeine Sonntagszeitung / FAZ.net*. Vom 01.09.2009. Aufgerufen am 19.01.2011.
URL http://www.faz.net/-00mtc7

Arenz, R./ Huth, N. und Thylmann, M. (2011): Datenschutz im Internet. Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM). Aufruf am 28.06.2011.
URL http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf

Arne und Tauber (2011): A survey of certified mail systems provided on the internet. In: *Computers & Security*, 30, 6-7, 464 – 485.

Barnitzke, B. (2010): Herausgabe von IP-Adressen. In: *Datenschutz und Datensicherheit – DuD*, 34, 7, 482–485.

Beck, U. (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt a.M.: Suhrkamp.

Berners-Lee, T. (1998): *Information Management: A Proposal*. Bern: Conseil Européen pour la Recherche Nucléaire. „A hand conversion to HTML of the original MacWord [...] document written in March 1989 and later redistributed unchanged apart from the date added in May 1990. [...]" – Aufruf am 19.07.2011.
URL http://www.w3.org/History/1989/proposal.html

Berners-Lee, T./ Masinter, L. und McCahill, M. (1994): Uniform Resource Locators (URL). In: *Request for Comments*. RFC: 1738. Aufruf am 16.09.2011.
URL http://tools.ietf.org/html/rfc1738

Bertsch, M./ Huth, N. und Arenz, R. (2011): Netzgesellschaft. Eine repräsentative Untersuchung zur Mediennutzung und dem Informationsverhalten der Gesellschaft in Deutschland. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM). Aufruf am 20.09.2011.

URL http://www.bitkom.org/files/documents/BITKOM_Publikation_Netzgesellschaft.pdf

Béglé, C./ Weiss di Spirito, G. und Puntas Bernet, D. (2009): „Die Briefpost wird bis 2015 um einen Drittel abnehmen“. In: *NZZ am Sonntag / NZZ Online*. Vom 20.12.2009. Aufgerufen am 19.01.2011.
URL http://www.nzz.ch/nachrichten/wirtschaft/aktuell/die_briefpost_wird_bis_2015_um_einen_drittel_abnehmen_1.4273844.html

Bijker, W. E./ Hughes, T. P. und Pinch, T. J. (Hrsg.) (1987): *The social construction of technological systems: New directions in the sociology and history of technology*. London and Cambridge: MIT Press.

Bleich, H. (2010): Déjà vu. EU-Kommission fordert Websperren gegen Kinderpornografie. In: *c't*, 10, 9, 53–55.

Boie, J. und Heckenberger, F. (2010): Men in Black. Die Internetseite Wikileaks setzt auf Transparenz und veröffentlicht geheime Papiere und Dokumente. Wer aber sind ihre Betreiber? In: *Süddeutsche Zeitung*, 98, 17–17.

Borchers, D. (2010): Elektronische Einschreiben Deutschland führt rechtsverbindliche E-Mail ein. In: *c't*, 10, 17, 74–75.

Borchers, D. (2011): Mail offiziell. Die Anbieter von De-Mail stehen in den Startlöchern. In: *c't*, 11, 78–80.

Braun, H. (2010): De-Mail verklagt E-Post. In: *Heise Online*. Aufruf am 27.01.2011.
URL http://heise.de/-1151657

Brenner, M. (1990): *Bundesnachrichtendienst im Rechtsstaat. Zwischen geheimdienstlicher Effizienz und rechtsstaatlicher Kontrolle*, *Recht*, Bd. 34. Baden-Baden: Nomos.

Brüggmann, M. (2011): Piraten-Partei: Klar zum Entern – aber ihr Programm ist diffus. In: *Handelsblatt*, G O 2531, 181, 12–13.

Broad, W. J./ Markoff, J. und Sanger, D. E. (2011): Israel tests on worm called crucial in iran nuclear delay.
URL http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

B.U. (2011): Arrr, mein hearties! In: *The Economist online*. Aufruf am 26.09.2011.
URL http://www.economist.com/node/21529260

Budde, L. und Huth, N. (2011): Soziale Netzwerke. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM). Aufruf am 20.09.2011.
URL http://www.bitkom.org/files/documents/BITKOM_Publikation_Soziale_Netzwerke.pdf

Bundesamt für Sicherheit in der Informationstechnik (2010): De-Mail. Eine Infrastruktur für sichere Kommunikation. Aufruf am 25.10.2010.
URL https://www.bsi.bund.de/cln_174/DE/Themen/EGovernment/DeMail/DeMail_node.html

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2011): Welche Sicherheitsvorkehrungen sind in De-Mail integriert? In: *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – Internetredaktion –*. Aufruf am 06.09.2011. URL `http://www.bfdi.bund.de/DE/Schwerpunkte/DEMail/InformationenNutzer/Artikel/FAQ/Artikel/Sicherheitsvorkehrungen.html`

Bundeskriminalamt (2010): Die Kriminalität in der Bundesrepublik Deutschland. Polizeiliche Kriminalstatistik für das Jahr 2010. Berlin: Bundesministerium des Innern. Aufruf am 28.07.2011.
URL `http://www.bka.de/pks/pks2010/download/pks2010_imk_kurzbericht.pdf`

Bundesministerium des Innern (2011): *De-Mail Broschüre Stand: März 2011.* Berlin. [PDF] Aufruf am 15.09.2011.
URL `http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Projekte/de_mail_informationsbroschuere_maerz2011_download.pdf`

Bundesministerium für Wirtschaft und Technologie (2008): Darmstädter Erklärung vom 20. November 2008. Dritter Nationaler IT-Gipfel: In Deutschland die digitale Zukunft gestalten. Aufruf am 24.07.2011.
URL `http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/it-gipfel-darmstaedter-erklaerung`

Bundesrat (2010): Stellungnahme des Bundesrates: Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften. In: , 645/10.

Bundesrepublik Deutschland (1950): *Strafprozeßordnung (StPO).* Bundesministeriums der Justiz / juris GmbH. Aufruf am 19.09.2011.
URL `http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf`

Bundesrepublik Deutschland (1990): *Bundesdatenschutzgesetz (BDSG).* Bundesministeriums der Justiz / juris GmbH. Aufruf 16.09.2011.
URL `http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf`

Bundesrepublik Deutschland (2004): *Telekommunikationsgesetz (TKG).* Baden-Baden: Bundesministeriums der Justiz / juris GmbH. Aufruf 30.08.2011.
URL `http://bundesrecht.juris.de/bundesrecht/tkg_2004/gesamt.pdf`

Bundesrepublik Deutschland (2007): *Telemediengesetz (TMG).* Baden-Baden: Bundesministeriums der Justiz / juris GmbH. Aufruf 15.09.2011.
URL `http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf`

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2010): Stellungnahme. Gesetzesentwurf der Bundesregierung zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften – De-Mail-Gesetz. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM). Aufruf am 20.09.2011.
URL `http://www.bitkom.org/files/documents/BITKOM_StN_De_Mail-Gesetz_2010_fin.pdf`

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2011): E-Mail-Nutzung. In: *Konsum- und Nutzungsverhalten.* Aufruf am 20.09.2011.
URL `http://www.bitkom.org/de/markt_statistik/64026_65223.aspx`

Bundesverfassungsgericht – Pressestelle – (2010): Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß. In: *Pressemitteilungen*, 11. Urteil vom 2. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 – Aufruf am 19.09.2011.
URL `http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011`

Bundeszentrale für Politische Bildung (2009): Piratenpartei Deutschland (PIRATEN). In: *Wer steht zu Wahl?* Aufruf am 18.09.2011.
URL `http://www.bpb.de/methodik/XO54ZW,0,Piratenpartei_Deutschland_(PIRATEN).html#footer`

Bundeverfassungsgericht (15.12.1983): *BVerfGE 65, 1 - Volkszählung. Urteil.* Karlsruhe.

Bundeverfassungsgericht (27.02.2008): *BVerfG 1 BvR 370/07.* Karlsruhe.
URL `http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html`

Carlson, N. (2011): Goldman to clients: Facebook has 600 million users. In: *msnbc.com — Tech & science.* Aufruf am 12.05.2011.
URL `http://www.msnbc.msn.com/id/40929239/ns/technology_and_science-tech_and_gadgets/`

Castells, M. (2000): *The rise of the network society, Information Age. Economy, Society and Culture*, Bd. 1. Malden, Oxford, Carlton: Blackwell Publishers.

Cebulla, M. (2010): Daten- und Geheimnisschutz beim Hybridbrief. In: *Datenschutz und Datensicherheit – DuD*, 34, 308–313.

Chaos Computer Club (1999): CCC — hackerethics. Aufruf am 29.06.2011.
URL `http://www.ccc.de/hackerethics`

Clarke, R. und Knake, R. (2010): *Cyber war: the next threat to national security and what to do about it.* Ecco.

Clinton, H. R. (2011): Internet Rights and Wrongs: Choices & Challenges in a Networked World. George Washington University; Washington, DC: U.S. Department of State. Aufruf am 25.07.2011.
URL `http://www.state.gov/secretary/rm/2011/02/156619.htm`

Coy, W. (2008): Ich habe nichts zu verbergen. Technische Überwachung in Zeiten des Internet. In: Gaycken, S. und Kurz, C. (Hrsg.), *1985.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien.* Bielefeld: Transcript, 47 – 52.

Crispin, M. R. (2003): Internet Message Access Protocol - Version 4rev1. In: *Request for Comments.* RFC: 3501. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc3501`

Crocker, D. H. (1982): Standard for the Format of ARPA Internet Text Messages. In: *Request for Comments.* RFC: 822. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc822`

Davis, J. (2007): Hackers Take Down the Most Wired Country in Europe. In: *Wired Magazine*, 15, 09.
URL `http://www.wired.com/politics/security/magazine/15-09/ff_estonia`

Deering, S. E. und Hinden, R. M. (1998): Internet Protocol, Version 6 (IPv6) Specification. In: *Request for Comments*. RFC: 2460. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc2460`

Degele, N. (2002): *Einführung in die Techniksoziologie*. München: Fink.

Deutsche Post AG (02/2011): „In diesem Brief stecken über 500 Jahre Erfahrung. Der E-Postbrief". Werbebroschüre.

Deutscher Bundesrat (2009): Entwurf eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften. Berlin: Bundesverwaltungsamt. Aufruf am 24.07.2011.
URL `http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2009/0101-200/174-09`

Deutscher Bundestag (2011): Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften (DMailG). In: Bundesministerium der Justiz (Hg.), *Bundesgesetzblatt*. 19, Bonn: Bundesanzeiger Verlag, 666–675.

Dietz, J. (1806): *Ältere und neuere Epoche des fürstlichen Thurn und Taxischen Reichs-Postwesen*. Regensburg: Google Books. Original aus der Bayerischen Staatsbibliothek. Digitalisiert am 25.07.2008. Aufruf am 08.11.2010.
URL `http://books.google.com/books?id=ej0AAAAAcAAJ`

Dornseif, M. (2005): *Phänomenologie der IT-Delinquenz: Computerkriminalität, Datennetzkriminalität, Cybercrime, Cyberterror und Cyberwar in der Praxis*. Bonn.

Dworschak, M. (2011): Im Netz der Späher. In: *Der Spiegel*, 2011, 2, 114 – 124.

Elkenberg, R. (2011): FBI will Bots von Rechnern löschen. In: *c't*, 11, 56.

Engling, D. (2008): Vorratsdatenspeicherung. In: Gaycken, S. und Kurz, C. (Hrsg.), *1985.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien*. Bielefeld: Transcript, 67 – 78.

erdgeist (2011): Chaos Computer Club erneuert Kritik am Gesetzentwurf zur De-Mail. In: *CCC Updates*. Aufruf am 14.09.2011.
URL `https://www.ccc.de/de/updates/2011/stellungnahme-gesetzentwurf-demail`

Ernst, S. (2010): Datenverlust und die Pflicht zur Öffentlichkeit. In: *Datenschutz und Datensicherheit – DuD*, 34, 7, 472–475.

European Parliament und Council (1968): *First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community*. Member States: European Commission / EUR-Lex. Multilingual. Aufruf am 15.09.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31968L0151:EN:NOT`

European Parliament und Council (1998a): *98/48/EC: Commission Decision of 28 November 1997 approving the programme for the eradication of scrapie for 1998 presented by France and fixing the level of the Community's financial contribution (Only the French text is authentic).* Member States: European Commission / EUR-Lex. Multilingual. Aufruf am 15.09.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998D0048:en:NOT`

European Parliament und Council (1998b): *Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations.* Member States: European Commission / EUR-Lex. Multilingual. Aufruf am 15.09.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0034:en:NOT`

European Parliament und Council (2000): *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').* Member States: European Commission / EUR-Lex. Multilingual. Aufruf am 15.09.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:NOT`

European Parliament und Council (2002a): *Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).* Member States: EUR-Lex. Multilingual. Aufruf am 30.08.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:NOT`

European Parliament und Council (2002b): *Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive).* Member States: EUR-Lex. Multilingual. Aufruf am 30.08.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:EN:NOT`

European Parliament und Council (2002c): *Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).* Member States: EUR-Lex. Multilingual. Aufruf am 30.08.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:NOT`

European Parliament und Council (2002d): *Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).* Member States: EUR-Lex. Multilingual. Aufruf am 30.08.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:DE:NOT`

European Parliament und Council (2003): *Directive 2003/58/EC of the European Parliament and of the Council of 15 July 2003 amending Council Directive 68/151/EEC, as regards disclosure requirements in respect of certain types of companies*. Member States: European Commission / EUR-Lex. Multilingual. Aufruf am 15.09.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0058:EN:NOT`

European Parliament und Council (2006a): *Council Directive 2006/96/EC of 20 November 2006 adapting certain Directives in the field of free movement of goods, by reason of the accession of Bulgaria and Romania*. Member States: European Commission / EUR-Lex. Multilingual. Aufruf am 20.09.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT`

European Parliament und Council (2006b): *Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market*. Member States: European Commission. COD 2004/0001. Multilingual. Aufruf am 09.06.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:NOT`

European Parliament und Council (2006c): *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*. Member States: European Commission / EUR-Lex. Multilingual. Aufruf am 15.09.2011.
URL `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT`

Europäisches Parlament und Rat (2010): Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). In: *Wettbewerbsrecht (WettbR), Markenrecht (MarkenR) / Kartellrecht (KartellR)*. dtv; Beck Juristischer Verlag, 69 – 78.

Flaherty, M. und Seipp-Williams, L. (2005): Sociotemporal rhythms in e-mail – A case study. In: *Time & Society*, 14, 1, 39–49.

Freude, A. C. (2009): Kategorie Politik. In: *BigBrotherAwards*. Preisträger: Dr. Ursula von der Leyen, Bundesministerin für Familie, Senioren, Frauen und Jugend.
URL `http://www.bigbrotherawards.de/2009/.pol`

Freude, A. C. H. (2010): „Internet-Sperren sind Unfug im Kampf gegen Kindesmissbrauch". Pressemeldung des Arbeitskreises gegen Internet-Sperren und Zensur zum Vorschlag von EU-Kommissarin von Cecilia Malmström zu Access-Blocking. In: *Arbeitskreis gegen Internet-Sperren und Zensur*. Aufruf am 12.09.2011.
URL `http://ak-zensur.de/2010/03/malmstroem-unfug.html`

Friebe, H. und Lobo, S. (2006): *Wir nennen es Arbeit. Die digitale Bohéme oder: intelligentes Leben jenseits der Festanstellung*. aktualisierte Aufl. München: Heyne.

Fuchs, C. (2010): Facebook, Web 2.0 und ökonomische Überwachung. In: *Datenschutz und Datensicherheit – DuD*, 34, 7, 453–458.

Gaycken, S. (2008): Die Vergeistigung des Technotops. Neue Naturgefahren in einer neuen technischen Situation. In: Gaycken, S. und Kurz, C. (Hrsg.), *1985.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien.* Bielefeld: Transcript, 25 – 46.

Gaycken, S. (2010): Wer war's? und wozu? In: *Die Zeit*, 48, 31–31.

Gaycken, S. (2011a): *Cyberwar: das Internet als Kriegsschauplatz.* München: Open Source Press.

Gaycken, S. (2011b): Informationelle selbstbestimmung und narrativistische rezeption. In: *Datenschutz und Datensicherheit - DuD*, 35, 346–350. 10.1007/s11623-011-0084-0. URL `http://dx.doi.org/10.1007/s11623-011-0084-0`

Gehlen, A. (2004): Die Seele im technischen Zeitalter und andere soziologische Schriften und Kulturanalysen. In: Rehberg, K.-S. (Hg.), *Arnold Gehlen. Gesamtausgabe*, Bd. 6. Frankfurt a.M.: Klostermann.

Geißler, R. und Meyer, T. (2002): *Die Sozialstruktur Deutschlands – Zur gesellschaftlichen Entwicklung mit einer Bilanz zur Vereinigung.* 4. auflage (überarbeitet & aktualisiert) Aufl. Westdt. Verl.

Gelzhäuser, S. (2010): Erfolgreiches De-Mail Pilotprojekt: Teilnehmer ziehen Bilanz. In: *Datenschutz und Datensicherheit – DuD*, 34, 9, 646–648.

Gieselmann, H. (2011): Der Millionen Hack. Datendiebe brechen in Sonys Netzwerk ein. In: *c't*, 11, 22.

Gietl, A. (2010): Die Zukunft der Vorratsdatenspeicherung. In: *Datenschutz und Datensicherheit – DuD*, 34, 398–403.

Goffart, D. (2011): Neue Schlappe für Merkel und Rösler. In: *Handelsblatt*, G O 2531, 181, 8–8.

Grimm, R. und Pähler, D. (2010): E-Mail-Forensik. In: *Datenschutz und Datensicherheit – DuD*, 34, 2, 86–89.

Grunwald, A. (2007): Technikdeterminismus oder Sozialdeterminismus. Zeitbezüge und Kausalverhältnisse aus der Sicht des „Technology Assessment". In: Dolata, U. und Werle, R. (Hrsg.), *Gesellschaft und die Macht der Technik. Sozioökonomischer und institutioneller Wandel durch Technisierung.* Frankfurt / New York: Campus, 63 – 82.

Hamann, G. (2011): Sie nennen es Krieg. Die Polizei nimmt Dutzende Hacker fest. Ihre Freunde stellen im Gegenzug weitere Konzerne und Behörden bloß. Der Cyberkonflikt eskaliert. In: *Die Zeit*, 31, 22.

Hansen, M. und Thomsen, S. (2010): Lebenslanger Datenschutz: Anforderungen an vertrauenswürdige Infrastrukturen. In: *Datenschutz und Datensicherheit – DuD*, 34, 283–288.

Harper, S. (2001): *Kampf um Enigma: die Jagd auf U-559.* Mittler.

Hegmann, G. und Graf, A. (2011): EADS rüstet im Cyberkrieg auf. In: *Financial Times Deutschland*, 2011, 1.

Heidegger, M. (1962): Die technik und die kehre. *Opuscula aus Wissenschaft und Dichtung*, Bd. 1. Pfullingen: Günther Neske Verlag. 2. Aufl.

Heidenreich, M./ Kirch, B. und Mattes, J. (2008): Die organisatorische einbettung von informationstechnologien in einem globalen entwicklungsprojekt. In: Funken, C. und Schulz-Schaeffer, I. (Hrsg.), *Digitalisierung der Arbeitswelt*. VS Verlag für Sozialwissenschaften, 193–219.

Hemker, T. (2010): Kann das jeder? – Ja, eigentlich schon! In: *Datenschutz und Datensicherheit – DuD*, 34, 9, 626–629.

Herder, J. G. (1981): Grundprobleme der großen Philosophen. In: Speck, J. (Hg.), *Philosophie der Gegenwart II*, Bd. 2. Göttingen: Vandenhoeck & Ruprecht.

Hersh, S. M. (2010): The online threat – should we be worried about a cyber war? In: *the New Yorker*. Aufgerufen: 01.01.2011 19:55 Uhr.
URL `http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh`

hib/ STO und AH (2010): Bundesrat fordert „Ende-zu-Ende-Verschlüsselung“ bei De-Mail. In: *Deutscher Bundestag – Presse –*. Aufruf am 24.09.2010.
URL `http://www.bundestag.de/presse/hib/2010_12/2010_418/04.html`

Hömig, D./ Seifert, K.-H. und Antoni, M. (Hrsg.) (2010): *Das Grundgesetz für die Bundesrepublik Deutschland (GG)*. 9. Aufl. Baden-Baden: Nomos-Verl.-Ges.

Hobbes, T. (1976): Der Staat als Instrument eines aufgeklärten Egoismus. In: *Leviathan*. Frankfurt, Berlin, Wien: Luchterhand, 94–264.

Hornung, G. (2008): Datenschutz im Gefüge der Grundrechte und ihren gesellschaftlichen Wandel. In: Gaycken, S. und Kurz, C. (Hrsg.), *1985.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien*. Bielefeld: Transcript, 249–264.

Hradil, S. (2006): *Die Sozialstruktur Deutschlands im internationalen Vergleich*. 2 Aufl. VS Verlag.

Information Sciences Institute (1981): Internet Protocol (IP). In: *Request for Comments*. RFC: 791. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc791`

Iqbal, F./ Binsalleeh, H./ Fung, B. C. und Debbabi, M. (2010): Mining writeprints from anonymous e-mails for forensic investigation. In: *Digital Investigation*, 7, 1-2, 56 – 64.
URL `http://www.sciencedirect.com/science/article/B7CW4-4YW37G3-1/2/ebde8e474f23d7c78fa0c2536bb67ad9`

Jarvis, J. (2009): *What Would Google Do?* Intern. Aufl. New York: HarperCollins.

kakl (2011): Der Feind im Netz. In: *Frankfurter Allgemeine Zeitung*, , 165, 15.

Keulartz, J./ Schermer, M./ Korthals, M. und Swierstra, T. (2004): Ethics in technological culture: A programmatic proposal for a pragmatist approach. In: *Science Technology & Human Values*, 29, 1, 3–29.

Kirkpatrick, S./ Stahl, M. und Recker, M. (1990): Internet Numbers (IP-Adresses). In: *Request for Comments*. RFC: 1166. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc1166`

Kleine-Voßbeck, B. (2000): *Electronic Mail und Verfassungsrecht*. Marburg: N.G. Elwert Verlag.

Klensin, J. (2001): Simple Mail Transfer Protocol. In: *Request for Comments*. RFC: 2821. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc2821`

Klingst, M. (2011): Der Staatsfeind. In: *Die Zeit*, 18, 5.

Klostermeier, J. (2011): Post verliert gegen GMX und Web.de. In: *CIO*. Aufruf am 20.09.2011.
URL `http://www.cio.de/public-ict/communication/2270338/`

Köppen, H. (2010): Entwicklung der Computer-, IuK- und Internetkriminalität im Jahr 2009. In: *Datenschutz und Datensicherheit – DuD*, 34, 11, 771–772.

Krempl, S. und Briegleb, V. (2011): Bundesregierung sieht keinen Korrekturbedarf nach Dresdner Handy-Affäre. In: *taz.de*. Aufruf am 27.07.2011.
URL `http://heise.de/-1285335`

Krueger, B. S. (2006): A comparison of conventional and Internet political mobilization. In: *American Politics Research*, 34, 6, 759–776.

Kruse, P. (2010): Vortrag: What's Next – Wie die Netzwerke Wirtschaft und Gesellschaft revolutionieren. In: *re:publica*.
URL `http://youtu.be/ryiuuUKQJy0`

Kurz, C. (2010): Sicherheit im Netz? Nur durch Vernetzung! In: *Frankfurter Allgemeine Zeitung / FAZ.net*. Vom 06.08.2010. Aufruf am 27.05.2011.
URL `http://www.faz.net/-01ez1y`

Kurz, C. und Rieger, F. (2009): *Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung*. (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) Aufruf am 18.09.2011.
URL `http://213.73.89.124/vds/VDSfinal18.pdf`

Kurz, C. und Rieger, F. (2011): *Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen*. Frankfurt a.M.: S.Fischer.

Latour, B. (1995): *Wir sind nie modern gewesen. Versuch einer symmetrischen Anthropologie*. Berlin: Oldenbourg Akademieverlag.

Latour, B. (1998): Über technische Vermittlung. Philosophie, Soziologie, Genealogie. In: Rammert, W. (Hg.), *Technik und Sozialtheorie*. Frankfurt a.M. / New York: Campus Verlag, 29–81.

Lechtenbörger, J. (2011): Zur Sicherheit von De-Mail. In: *Datenschutz und Datensicherheit – DuD*, 35, 4, 268–269.

Leicht, R. (2010): Daten gegen Terror. Der Rechtsstaat erlaubt es, Informationen auf Vorrat zu speichern. Aber nur, um Leib und Leben zu schützen. In: *Die Zeit*, C 7451 C, 48, 1–1.

Licklider, J. C. R. (1990): *In Memoriam: J. C. R. Licklider. 1915–1990.* Palo Alto: Systems Research Center / Digital Equipment Corporation. Aufruf am 19.07.2011. URL `http://memex.org/licklider.pdf`

Lindemann, G. (2002): Können Maschinen handeln? Soziologische Beiträge zum Verhältnis von Mensch und Technik. Frankfurt a. M.: Campus Verlag, 79–100.

Lindemann, G. (2009a): *Das Soziale von seinen Grenzen her denken*, Kap. 2. Weilerswist: Velbrück.

Lindemann, G. (2009b): Gesellschaftliche Grenzregime und soziale Differenzierung. In: *Zeitschrift für Soziologie*, 38, 2, 92–110.

Locke, J. (1967): Der Staat als Zusammenschluß zur Sicherung natürlicher Grundrechte. In: *Zwei Abhandlungen über die Regierung*, Bd. II. Frankfurt a.M.: Europäische Verlagsanstalt, 200–302.

Luhmann, N. (1984): *Soziale Systeme. Grundriss einer allgemeinen Theorie.* Frankfurt a.M.: Suhrkamp.

Luik, A./ Fischer, J./ Graf Lambsdorff Freiherr von der Wenge, O. F. W./ Rommel, M./ Merkel, A./ Müntefering, F./ Lafontaine, O./ Becker, B./ Witt, K./ Kuczynski, J./ Steinkühler, F./ Klink, V./ Rogowski, M./ Hengsbach, F./ Werner, G./ Thews, G./ Kolle, O./ Walser, M./ Unseld, J./ Todenhöfen, J./ Hein, C./ Hammerstingl, H./ Buergenthal, T./ Jens, I./ Jens, W./ Schrobsdorff, A. und Walser, M. (2009): *„Wer zum Teufel sind Sie nun?“ Sechzig Jahre Bundesrepublik. Gespräche über uns.* München: Verlag Antje Kunstmann — Stern.

Luther, M. (1985): *Die Bibel nach der Übersetzung Martin Luthers.* revidierte Aufl. Standardausgabe mit Apokryphen.

Mainusch, J. und Burtchen, C. (2010): Kontrolle über eigene Daten in sozialen Netzwerken. In: *Datenschutz und Datensicherheit – DuD*, 34, 7, 448–452.

Mainzer, K. (2011): Computer als neue Technologie. Vom Rechner zu integrierten IuK-Systemen. In: Kehrt, C./ Schüßler, P. und Weitze, M.-D. (Hrsg.), *Neue Technologien in der Gesellschaft. Akteure, Erwartungen, Kontroversen und Konjunkturen.* Bielefeld: Transcript, 177 – 190.

Mantovani, G. (1994): Is Computer-Mediated Communication Intrinsically apt to enhance Democracy in Organizations. In: *Human Relations*, 47, 1, 45–62.

Mattausch, B. (2011): Die Macht der Sozialen Medien. In: *Zeit Online – Leserartikel.* Aufruf am 26.09.2011.
URL `http://www.zeit.de/digital/2011-04/leserartikel-social-media-revolutionen`

McCarron, K. (1995): Corpses, Animals, Machines and Mannequins: The Body and Cyberpunk. In: Featherstone, M. und Burrows, R. (Hrsg.), *Cyberspace/cyberbodies/cyberpunk: cultures of technological embodiment.* Theory, culture & society, Sage, 261–274.

McInerney, P.-B. (2009): Technology Movements and the Politics of Free/Open Source Software. In: *Science Technology & Human Values*, 34, 2, 206–233.

Mertes, P. (2010): E-Mails im Rechtsverkehr: keine Lappalie. In: *Datenschutz und Datensicherheit – DuD*, 34, 9, 633–637.

Mislove, A./ Haeberlen, A./ Post, A. und Druschel, P. (2005): ePOST. In: *Peer-to-peer Systems and Applications*, *Lecture Notes in Computer Science*, Bd. 3485. BERLIN: Springer-Verlag Berlin, 171–192.

Münkler, H. (2002): *Die Neuen Kriege*. 5. Aufl. Reinbek: Rowohlt Verlag.

Moore, G. E. (1965): Cramming more components onto integrated circuits. In: *Electronics*, 38, 8, 114–117.

Motadel, D. und Stockrahm, S. (2011): Revolutionen kommen selten allein. Diktatoren fürchten heute Facebook und Twitter. In: *Zeit Online*. Aufruf am 26.09.2011.
URL `http://www.zeit.de/wissen/geschichte/2011-04/revolution-geschichte/seite-2`

Murdoch, J. (1997): Inhuman/nonhuman/human: actor-network theory and the prospects for a nondualistic and symmetrical perspective on nature and society. In: *Environment and Planning D – Society & Space*, 15, 6, 731–756.

Myers, J. G. und Rose, M. T. (1996): Post Office Protocol – Version 3. In: *Request for Comments*. RFC: 1939. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc1939`

N.N. (2006): Der legendäre BTX-Hack des Chaos Computer Clubs. In: *Google Videos*. Aufzeichnung ZDF heute journal vom 19.11.1984. Moderation Hans Scheicher. Aufruf am 22.08.2011.
URL `http://video.google.com/googleplayer.swf?docid=-8396178892678063881`

N.N. (2010): War in the fifth domain. Are the mouse and keyboard the new weapons of conflict? In: *the Economist*, 396, 8689, 22 – 24.

N.N. (2011a): Chaos Computer Club wirft Domscheit-Berg raus. In: *FAZ.net / dpa*. Preisträger: Dr. Ursula von der Leyen, Bundesministerin für Familie, Senioren, Frauen und Jugend. Aufruf am 18.09.2011.
URL `http://www.faz.net/-022ahz`

N.N. (2011b): Geplante Regelung zu De-Mail-Diensten umstritten. In: *Deutscher Bundestag – Dokumente –*. Aufruf am 24.09.2010.
URL `http://www.bundestag.de/dokumente/textarchiv/2011/33281422_kw05_pa_inneres/index.html`

N.N. (2011c): Google Panda erreicht Deutschland. In: *Suchmaschinen- & SEO-Blog*. Aufruf am 22.08.2011.
URL `http://www.sistrix.de/news/996-google-panda-erreicht-deutschland.html`

N.N. (2011d): StatCounter Global Stats. Online. (Interaktive Statistik) Aufruf am 22.08.2011.
URL `http://gs.statcounter.com/`

N.N. (2011e): Statistics. In: Facebook (Hg.), *Press room*. Palo Alto. Aufruf am 12.05.2011. URL `http://www.facebook.com/press/info.php?statistics`

N.N. (2011f): „Werbung der Post ist unwahr“. In: *Steuern + Recht – Meldungen*. Aufruf am 20.09.2011.
URL `http://www.test.de/themen/steuern-recht/meldung/Urteil-zu-E-Postbrief-Werbung-der-Post-ist-unwahr-4267219-4267221/`

Obama, B. H. (2009): Remarks by the President on Securing our Nation's Cyber Infrastructure. Washington, D.C.: The White House – Office of the Press Secretary. Aufruf am 25.01.2011.
URL `http://www.whitehouse.gov/video/President-Obama-on-Cybersecurity`

Obama, B. H. (2011): The 2011 State of the Union Address: Enhanced Version. Washington, D.C.: The White House – Office of the Press Secretary. Aufruf am 25.01.2011.
URL `http://www.whitehouse.gov/photos-and-video/video/2011/01/25/2011-state-union-address-enhanced-version`

Ogburn, W. F. (1969a): Die Technik als Umwelt. In: Ogburn, W. F. und Duncan, O. D. (Hrsg.), *Kultur und sozialer Wandel : ausgewählte Schriften*, *Soziologische Texte*, Bd. 56. Neuwied and Berlin: Luchternand, 125–133.

Ogburn, W. F. (1969b): Die Ursachen für die Veränderung der Familie. In: Ogburn, W. F. und Duncan, O. D. (Hrsg.), *Kultur und sozialer Wandel : ausgewählte Schriften*, *Soziologische Texte*, Bd. 56. Neuwied and Berlin: Luchternand, 238–252.

Ogg, E. und Mills, E. (2011): Hackers steal more customer info from Sony servers. In: *CNET News*. Aufruf am 18.09.2011.
URL `http://news.cnet.com/8301-31021_3-20068414-260/hackers-steal-more-customer-info-from-sony-servers/`

Petri, T. (2010): Wertewandel im Datenschutz und die Grundrechte. In: *Datenschutz und Datensicherheit – DuD*, 34, 1, 25–29.

Petri, T. und Schaar, P. (2010): Aus Den Datenschutzbehörden. In: *Datenschutz und Datensicherheit – DuD*, 34, 4, 206–206.

Pham, K. (2011): Goalgetter und Dr. Klicken. Wie Internetplattform Vroniplag Dokterarbeien von Politikern durchleuchtet. Begegnung mit zwei Plagiatsjägern. In: *Die Zeit*, 29, 4.

Plickert, P. (2010): Der missverstandene Neoliberalismus. In: *Politische Studien*, 61, 431, 55 – 63. Aufruf am 13.07.2011.

Pohlmann, N. (2010a): Bedrohungen und Herausforderungen des E-Mail-Dienstes. In: *Datenschutz und Datensicherheit – DuD*, 34, 9, 607–613.

Pohlmann, N. (2010b): Wie zuverlässig ist die E-Mail-Anwendung? In: *Datenschutz und Datensicherheit – DuD*, 34, 9, 656–656.

Polenz, S. und Thomsen, S. (2010): Internet- und E-Mail-Nutzung. In: *Datenschutz und Datensicherheit – DuD*, 34, 9, 614–618.

presse (2009): Chaos Computer Club veröffentlicht Stellungnahme zur Vorratsdatenspeicherung. In: *CCC Updates*. Aufruf am 18.09.2011.
URL `http://www.ccc.de/updates/2009/vds-gutachten`

Rammert, W. (2008): Die Macht der Datenmacher in der fragmentierten Wissensgesellschaft. In: Gaycken, S. und Kurz, C. (Hrsg.), *1985.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien*. Bielefeld: Transcript, 181–194.

Reiners, W. (2010): E-Mail Compliance fordert E-Mail Richtlinie. In: *Datenschutz und Datensicherheit – DuD*, 34, 9, 630–632.

Resnick, P. W. (2001): Internet Message Format. In: *Request for Comments*. RFC: 2822. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc2822`

Resnick, P. W. (2008): Internet Message Format. In: *Request for Comments*. RFC: 5322. Aufruf am 16.09.2011.
URL `http://tools.ietf.org/html/rfc5322`

Rieger, F. (2011): Das kommende Vorratsdatenschutzdrama. In: *Frankfurter Allgemeine Zeitung*, 16, 29–29.

Ritzer, G. (1996): The McDonaldization Thesis: Is Expansion Inevitable? In: *International Soziology*, 11, 3, 291–308.

Roßnagel, A. (2010): Das Bundesverfassungsgericht und die Vorratsdatenspeicherung in Europa. In: *Datenschutz und Datensicherheit – DuD*, 34, 8, 544–548.

Rüstow, A. (1963): Die staatspolitischen Voraussetzungen des wirtschaftspolitischen Liberalismus. In: *Rede und Antwort*, 249–258.

Ruggieri, F. (2010): Registered e-mail (REM) — Reliable e-mail for everybody. In: *Datenschutz und Datensicherheit – DuD*, 34, 314–317.

Schafer, B. (2010): The UK Cleanfeed system — Lessons for the German debate? In: *Datenschutz und Datensicherheit – DuD*, 34, 8, 535–538.

Scherer, J. (1995): Postreform II. Privatisierung ohne Liberalisierung. In: Hoffmann-Riem, W. und Vesting, T. (Hrsg.), *Perspektiven der Gesellschaft, Synopsien des Hans-Bredow-Instituts*, Bd. 16. Baden-Baden/Hamburg: Nomos Verlagsgesellschaft, 72 – 89.

Scherer, K. (2011): Angriff aus dem Internet. In: Norddeutscher Rundfunk (Hg.), *45Min*. Hamburg: NDR Fernsehen. Erstausstrahlung am 29.03.2011 um 22:30 Uhr.
URL `http://www.ndr.de/fernsehen/sendungen/45_min/videos/minuten273.html`

Schäfers, J.-O. (2010a): Always on dank E-Postbrief! Aufgerufen: 26.10.2010 00:05 Uhr.
URL `http://www.netzpolitik.org/2010/always-on-dank-e-postbrief/`

Schäfers, J.-O. (2010b): BKA, Bitkom, BDK, Stadlmaier: Lauter Missverständnisse! Aufgerufen: 25.10.2010 23:58 Uhr.
URL `http://www.netzpolitik.org/2010/bka-bitkom-bdk-stadlmaier-lauter-missverstandnisse/`

Schäfers, J.-O. (2010c): De-Mail: Freund liest mit. Aufgerufen: 25.10.2010 23:59 Uhr.
URL `http://www.netzpolitik.org/2010/bka-bitkom-bdk-stadlmaier-lauter-missverstandnisse/`

Schäfers, J.-O. (2010d): E-Post vs. De-Mail: Es lebe das Chaos! [Update]. Aufgerufen: 26.10.2010 00:07 Uhr.
URL `http://www.netzpolitik.org/2010/e-post-vs-de-mail-es-lebe-das-chaos/`

Schirrmacher, F. (2009): *Payback: Warum wir im Informationszeitalter gezwungen sind zu tun, was wir nicht tun wollen, und wie wir die Kontrolle über unser Denken zurückgewinnen.* München: Blessing.

Schlüter, N. (2011): Verschollen in der Wolke. In: *Financial Times Deutschland*, 16, 1–1.

Schuller, K. (2010): Der Spion der aus dem Cyberspace kam. In: *Frankfurter Allgemeine Sonntagszeitung*, 51, 6–6.

Schulz, S. (2011): Datenschutz beim E-Postbrief. In: *Datenschutz und Datensicherheit – DuD*, 35, 4, 263–267.

Schumacher, A. (2010): Akkreditierung und Zertifizierung von De-Mail-Diensteanbietern. In: *Datenschutz und Datensicherheit – DuD*, 34, 302–307.

Seeger, M. (2010): Three years hacker paragraph. In: *Datenschutz und Datensicherheit – DuD*, 34, 7, 476–478.

Siegert, P. F. (2008): *Die Geschichte der E-Mail: Erfolg und Krise eines Massenmediums*, *Technik - Körper - Gesellschaft*, Bd. 1. Bielefeld: Transcript Verlag.

Simons, H. (1948): A Positive Program for Laissez Faire. In: Simons, H. (Hg.), *Economic Policy for a Free Society.* Chicago.

Statistisches Bundesamt (2010): *Erzeugerpreisindizes für private Post- und Kurierdienste. Veränderungsraten zum Vorjahresquartal in %.* Wiesbaden. Vom 29.04.2011. Aufruf am 08.06.2011.
URL `http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/Zeitreihen/WirtschaftAktuell/Basisdaten/Content75/dlpr043j.psml`

Stöber, R. (2005): *Deutsche Pressegeschichte.* Konstanz: UVK Verlagsgesellschaft.

Steffen, T. (2011): Piraten zwischen Öko und Liberalismus. In: *Zeit Online.* Aufruf am 26.09.2011.
URL `http://www.zeit.de/politik/deutschland/2011-09/piraten-gruene-liberale`

Sterzel, D. (1968a): Beschränkung des Brief-, Post und Fernmeldegeheimnisses; Ausschluss des Rechtsweges. In: Sterzel, D. (Hg.), *Kritik der Notstandsgesetze.* Frankfurt a.M.: Suhrkamp, 24–42.

Sterzel, D. (1968b): Zur Entstehung der Notstandsgesetze. In: Sterzel, D. (Hg.), *Kritik der Notstandsgesetze.* Frankfurt a.M.: Suhrkamp, 7–23.

Stoll, J. und der_Fahrer (2010): Kommunikation im OSI-7-Schichten-Modell. Aufruf am 16.04.2011.
URL `http://de.wikipedia.org/w/index.php?title=Datei:OSI7Layer_model_3.1.svg`

Symantec (2010): Norton cybercrime report: Deutsche sind ganz groß im schwindeln. In: . Aufruf am 08.07.2011.
URL `http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20100908_01`

Taylor, G. und Dürrenschmidt, J. (2007): *Globalization, Modernity & Social Change. Hotspots of Transition*. London: Palgrave MacMillan.

Tinnefeld, M.-T. (2010): Stopp-Schilder im Internet. In: *Datenschutz und Datensicherheit – DuD*, 34, 1, 15–19.

Turner, B. S. (2001): Risks, rights and regulation: an overview. In: *Health Risk & Society*, 3, 1, 9–18.

Viner, J. (1960): The intellectual history of laissez faire. In: *Journal of Law and Economics*, 3, 45–69.

Völker, J. (2010): iPhone Security. In: *Datenschutz und Datensicherheit – DuD*, 34, 7, 486–491.

Volti, R. (1995): *Society and technological change*. 3. Aufl. New York: St Martin's Press.

vzbv (2010): De-Mail-Dienste und De-Mail-Gesetz: Stellungnahme zum Referentenentwurf. In: *Verbraucherzentrale Bundesverband e.V.* Aufruf am 20.09.2011.
URL `http://www.vzbv.de/go/dokumente/944/8/36/`

Wagner, M. K. (2011): Aufstieg, Fall und Triumph einer Blogpartei. In: *Frankfurter Allgemeine Zeitung*, 38 D 1, 218, 2–2.

Watzlawick, P./ Bavelas, J. B. und Jackson, D. D. (1967): *Pragmatics of human communication: a study of interactional patterns, pathologies, and paradoxes*. Norton.

Weber, M. (1958): Politik als Beruf (Okt. 1919). In: Winckelmann, J. (Hg.), *Gesammelte politische Schriften*. Tübingen: J.C.B. Mohr, 505–560.

Wegener, C. (2010): Was schafft eigentlich Vertrauenswürdigkeit? In: *Datenschutz und Datensicherheit – DuD*, 34, 334–334.

Winner, L. (1986): Do artefacts have politics. In: *The Whale and the Reactor. A Search for Limits in the Age of High Technology*. Chicago/London: UCP, 19–39.

Wirtgen, J. (2011): Wirbel um Bewegungsprofile im iPhone und iPad. Programmierfehler in Apples iOS führen zu ungeschützten Ortsdaten. In: *c't*, 11, 18–20.

Wölbert, C. (2011): Die Kostenlos-Maschine. Gratis-Geschäftsmodelle im Netz. In: *c't*, 11, 76–77.

Wrusch, P. (2011): Demo-Überwachung per Mobilfunk. In: *taz.de*. Aufruf am 27.07.2011.
URL `http://taz.de/!72708/`

Zuse, K. (1970): *Der Computer: mein Lebenswerk*. Verlag moderne Industrie.

Abschlusserklärung

Hiermit versichere ich, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Außerdem versichere ich, dass ich die allgemeinen Prinzipien wissenschaftlicher Arbeit und Veröffentlichung, wie sie in den Leitlinien guter wissenschaftlicher Praxis der Carl von Ossietzky Universität Oldenburg festgelegt sind, befolgt habe.

_____