forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

Arbeitspapier

Akteure, Interessenlagen und Regulierungspraxis im Datenschutz

Eine politikwissenschaftliche Perspektive

Arbeitspapier

Akteure, Interessenlagen und Regulierungspraxis im Datenschutz

Eine politikwissenschaftliche Perspektive

Autoren:
Philip Schütz[1], **Murat Karaboga**[1]

(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe

Herausgeber:
Peter Zoche, Regina Ammicht Quinn, Jessica Heesen, Thomas Hess, Jörn Lamla, Christian Matt, Alexander Roßnagel, Sabine Trepte, Michael Waidner

Inhalt

1 Einleitung 5

2 Entwicklung des heutigen Datenschutzes 7

3 Regulierungspraxis zentraler Akteure beim Datenschutz 12
3.1 Politische Exekutive 12
3.2 Legislative 14
3.3 Judikative 15
3.4 Parteien 17
3.5 Datenschutzbehörden 19

4 Einflussreiche Interessenlagen im Datenschutz 22
4.1 Ökonomische Interessen 22
4.1.1 Datenbasierte Geschäftsmodelle 22
4.1.2 Datenschutzgeschäftsmodelle 25
4.2 Sicherheitsinteressen 28
4.2.1 Fluggastdatenübermittlung 29
4.2.2 Banktransaktionsdatenübermittlung im Rahmen von SWIFT 30
4.2.3 Die Vorratsdatenspeicherung in Deutschland 32
4.2.4 Nachrichtendienstliche Überwachung 33
4.3 Bürgerrechtsinteressen 36
4.3.1 Geschichte des zivilgesellschaftlichen Datenschutzes 36
4.3.2 Zivilgesellschaftlich organisierte Datenschützer 37
4.3.3 Einfluss von Bürgerrechtsinteressen 38

5 Fazit und Ausblick 40

Literaturverzeichnis **42**

Abkürzungsverzeichnis **69**

Anhang **71**

1 Einleitung

Am 6. Juni 2013 veröffentlichte der Guardian und die Washington Post auf Grundlage von geleakten Dokumenten des Whistleblowers Edward Snowden die ersten beiden einer bis heute andauernden Reihe von Artikeln über weltweit stattfindende Ausspähaktionen durch die US-amerikanische *National Security Agency* (NSA) und kooperierende Nachrichtendienste (Gellman und Poitras 2013; Greenwald 2013a). Das bekannt gewordene Ausmaß globaler Überwachung verdeutlichte mehr als je zuvor, wie stark das strategische Interesse an Daten ist und wie sehr darauf basierendes Wissen und Machtstreben miteinander zusammenhängen. Weder die gesellschaftskritische Auseinandersetzung mit Überwachung (Foucault 1977) noch die generelle Debatte um das Verhältnis von Wissen und Macht, wie schon die Feststellung des englischen Philosophen Francis Bacon „Nam et ipsa scientia potestas est" („Denn auch Wissen(schaft) selbst ist Macht") (1597) vermuten lässt, sind jedoch neu. Ganz im Gegenteil reichen daran anknüpfende Fragen zu Legitimation von Herrschaft, Machtausübung und -beschränkung weit bis in die Antike zurück und stellen bis heute zentrale Aspekte bedeutender Werke der Politischen Theorie und Ideengeschichte dar. Allerdings entwickelte sich erst vor dem Hintergrund der Aufklärung und eines aufstrebenden Bürgertums, das Autonomie und politische Teilhabe einforderte, ein modernes Verständnis von Privatheit, der im Kontext einer damals durch Urbanisierung und Printmedien neu geschaffenen Öffentlichkeit insbesondere die Funktion eines Rückzugsraumes gegenüber Dritten (Sennett 1983: 29 ff.) sowie eines Abwehrrechtes gegenüber dem Staat zukam. Vor allem letztere Funktion sollte mit dem Aufkommen elektronischer Datenverarbeitung und staatlicher Großrechner in den 1960er Jahren auch der Datenschutz übernehmen. Demokratietheoretisch kann Privatheit und Datenschutz somit eine große und je nach Denktradition unterschiedliche Aspekte in den Vordergrund rückende Bedeutung zugeschrieben werden (vgl. Seubert 2012; Roberts 2015; Lever 2006).

Ein gesellschaftlich relevantes Thema sind Datenschutz und Privatheit damit schon lange vor der Entstehung des Internets gewesen (vgl. Abschnitt 2). Allerdings hat erst die massenhafte Verbreitung moderner Informations- und Kommunikationstechnologien (IKT) in Verbindung mit der Entstehung datengetriebener Märkte (vgl. Abschnitt 4.1.1) dazu geführt, dass es zu einem gewaltigen Anstieg personenbezogener bzw. -beziehbarer Daten und somit auch zu einem erhöhten Überwachungsrisiko gekommen ist. Diese Konvergenz privatwirtschaftlich gesammelter Daten und staatlich betriebener Überwachung haben insbesondere die Snowden-Enthüllungen zu PRISM – dem Programm, das die Kooperation von NSA und führenden US-amerikanischen IT Konzernen regelt und die wichtigste NSA-Rohdatenquelle darstellt (The Washington Post 2013) – deutlich gemacht (vgl. Abschnitt 4.2.4).

Den heutigen Datenschutz kennzeichnet eine vergleichsweise hohe Institutionalisierungs- und Verrechtlichungsdichte, der jedoch eine ungeklärte Ressortzuständigkeit auf Parlaments- und Regierungsebene gegenübersteht. Im Folgenden wird Datenschutz deswegen weniger als Politik-, sondern vielmehr als Themenfeld verstanden, das sich querschnittsartig zu klassischen Politikfeldern wie der Innen-, Außen- oder Wirtschaftspolitik verhält.

Dieser Aufsatz zielt darauf ab, einen ersten Überblick zum Thema Datenschutz aus politikwissenschaftlicher Perspektive zu geben. Eingangs führt ein kurzer Abriss zur Geschichte des Datenschutzes in das Thema ein. Anschließend wird die Regulierungspraxis anhand zentraler an der Regelsetzung und -auslegung des Datenschutzes beteiligter Akteure skizziert. Um Erklärungsansätze für die unterschiedliche Art und Weise, wie Datenschutzregulierung stattfindet, zu erforschen, wird der institutionelle Zugang im darauffolgenden Abschnitt um die Darstellung idealtypischer Interessenlagen beim Datenschutz ergänzt.

Dabei orientieren sich die Autoren an drei von Busch (2012a: 423 ff.) skizzierten analytischen Frames (Wirtschafts-, Sicherheits- und Bürgerrechtsinteressen), die die unterschiedlichen Sichtweisen und Diskussionen zum Thema Datenschutz nachhaltig prägen. Im Fazit wird neben einer Zusammentragung der Ergebnisse auf Zukunftsperspektiven des Datenschutzes eingegangen.

2
Entwicklung des heutigen Datenschutzes

Im Amerika des ausgehenden 19. Jahrhunderts und dem zeithistorischen Kontext aufkommender Massenmedien, die insbesondere durch einen ungezügelten Boulevardjournalismus in Verbindung mit der Einführung kleiner, handlicher und vor allem finanzierbarer Fotokameras gekennzeichnet waren, schrieben Warren und Brandeis (1890) ihren wegweisenden Aufsatz „The Right to Privacy". Das darin eingeforderte „right to be let alone" versteht sich in der Auslegungstradition des Artikels 4 der amerikanischen Verfassung, der die Freiheit eines jeden Bürgers von staatlicher Überwachung gewährleisten soll (Whitman 2004).[1] Mit der Entstehung elektronischer Datenverarbeitung Ende der 1960er Jahre in den USA wandelte sich – zumindest in der Rechtstheorie – auch das Verständnis von *Privacy* als negatives hin zu einem positiven Recht: dem Anspruch auf persönliche Kontrolle über private Informationen (Westin 1967).[2]

Angestoßen von Diskussionen über den regulatorischen Umgang mit elektronischen Großdatenbanken in den USA und Schweden kam man auch in Deutschland zu dem Schluss, dass es einer neuen Rechtsgrundlage bedürfe, um die Verarbeitung personenbezogener Daten zu regeln (Mayer-Schönberger 1998: 221 ff.).[3] Dies führte dazu, dass das Bundesland Hessen 1970 das weltweit erste Datenschutzgesetz verabschiedete, gefolgt von Schweden 1973, den USA 1975 und der BRD 1977 (vgl. Bennett 1992: 59). Während das Bundesdatenschutzgesetz (BDSG) seitdem vor allem die Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen (wie beispielsweise Unternehmen) sowie öffentliche Stellen des Bundes regelt,[4] gelten die unterschiedlichen Datenschutzgesetze der Bundesländer insbesondere für öffentliche Verwaltungen des jeweiligen Landes (z. B. Landesbehörden und Kommunalverwaltungen). Zentrale Kontrollstellen sind hier die Landesbeauftragten für den Datenschutz (LFDs) bzw. der Bun-

[1] Aus Gründen der Lesbarkeit wird im Folgenden auf das Gendern von Personengruppen verzichtet. Die Verwendung des generischen Maskulinums schließt ausdrücklich alle Geschlechterformen mit ein.

[2] In der amerikanischen Rechtsprechung dominiert allerdings bis heute die Wahrnehmung von *Privacy* als negatives Recht (Abwehrrecht) gegenüber dem Staat (vgl. z. B. das wegweisende Urteil zu Katz v. United States (U.S. Supreme Court 1967)) bzw. anderen großen Organisationen. War dies in der Entstehungszeit des deutschen Datenschutzrechts (beispielsweise in Hessen) ebenfalls der Fall, so hat spätestens die Entwicklung des Konzeptes der informationellen Selbstbestimmung einen Paradigmenwechsel in Deutschland und Europa eingeläutet. Dies zeigt auch die rechtliche Lage: Während in den USA ein weitgehend fragmentiertes, sektorales Datenschutzrecht mit erheblichen Regelungslücken insbesondere im privatwirtschaftlichen Bereich besteht, hat sich in Europa ein flächendeckendes Datenschutzrecht herausgebildet, das sogar Einzug in die Charta der Grundrechte der EU gehalten hat.

[3] Man nahm hier jedoch Abstand vom im Deutschen gängigen Begriff der Privatsphäre und kreierte den Terminus „Datenschutz". Ein für die Datenschutzgesetzgebung wegweisendes Gutachten erklärt dazu, dass die vom Bundesverfassungsgericht (BVerfG) ab 1957 entwickelte Sphärentheorie und das darin enthaltene rechtliche Konzept der Privatsphäre untauglich für die Anwendung von präzisen Regeln im Umgang mit personenbezogenen Daten sei (Steinmüller et al. 1971: 53). Dennoch ist die Entstehung des Begriffes Datenschutz unklar (Lewinski 2009: 197; 2014: 3 f.). Während Garstka (2008: 134) die Orientierung am Konzept des Maschinenschutzes, der in den sechziger Jahren zur Verbesserung der Sicherheit an Arbeitsmaschinen eingeführt wurde, für ursächlich hält, nimmt Simitis (2014: 83 f.) an, dass der Begriff der „Datensicherung" als Vorbild gedient habe.

[4] Öffentliche Stellen des Bundes schließen auch öffentlich-rechtliche Wettbewerbsunternehmen mit ein (Dammann 2014: 1145 f.). Während nach Telekommunikationsgesetz (TKG) und Postgesetz (PostG) der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zudem zuständig für die Datenschutzkontrolle von Telekommunikations- und Postdiensten ist, werden Rundfunkanstalten des Bundesrechts ausschließlich durch einen eigenen Rundfunkbeauftragten kontrolliert (ebd.).

Entwicklung des heutigen Datenschutzes

desbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (vgl. Abschnitt 3.5).

Mit dem Volkszählungsurteil (1983) und der Schaffung eines neuen Grundrechts – der informationellen Selbstbestimmung – setzte das Bundesverfassungsgericht (BVerfG) jedoch neue Maßstäbe, was die Novellierung eines Großteils der Datenschutzgesetze der Länder und des Bundes zur Folge hatte.[5]

Neben den zahlreichen nationalen Datenschutzgesetzgebungen spielten für deren Verbreitung auch internationale Regime eine wichtige Rolle. Während die *OECD Privacy Guidelines* (1980) noch unverbindlichen Charakter hatten, entfaltete die Datenschutzkonvention des Europarates (1981) für alle unterzeichnenden Mitglieder schon rechtsverbindliche Wirkung. Das erste internationale Gesetzesvorhaben ließ jedoch noch weitere 14 Jahre auf sich warten und mündete in der noch heute gültigen EU-Datenschutzrichtlinie (1995).

Bevor diese Richtlinie allerdings zum ersten Mal international verbindliche Regeln im Umgang mit personenbezogenen Daten aufstellte, war die EU von einem Flickenteppich nationaler Datenschutzgesetze gekennzeichnet. Die unterschiedlichen Rechtsstandards drohten enorme Handelshemmnisse für immer mehr auf den Austausch von personenbezogenen Daten angewiesene Unternehmen entstehen zu lassen (Bennett und Raab 2006: 93). Dies nahm die EU-Kommission trotz des teilweise heftigen Widerstands nationaler Regierungen und Wirtschaftvertreter zum Anlass, eine europäische Harmonisierung des Datenschutzrechtes anzustreben. Bei dieser Entscheidung spielte auch der Einfluss untereinander stark vernetzter und institutionell eingebetteter Datenschutzbehörden der EU-Mitgliedsstaaten eine wichtige Rolle (Newman 2008). Allerdings sah die EU-Kommission neben bürgerrechtlichen Erwägungen (Gonzalez-Fuster 2014: 125) vor allem aus ökonomischer Sicht heraus Handlungsbedarf (Gutwirth 2002: 91).[6]

In der Folge wurden auf Grundlage der Richtlinie, die den Mitgliedsstaaten in der rechtlichen Umsetzung einen gewissen Spielraum bot, europaweit nationale Datenschutzgesetze verabschiedet bzw. bestehende gesetzliche Grundlagen an die EU-Anforderungen angepasst. In Deutschland betraf dies vor allem das BDSG, das allerdings erst mit erheblichen Verzögerungen 2001 aktualisiert wurde (vgl. Schaar 2012: 97; Ramm 2007), sowie die Datenschutzgesetze der Länder. Da die EU-Richtlinie zudem grundsätzlich verbietet, personenbezogene Daten in Drittstaaten, die über keine vergleichbaren Datenschutzstandards verfügen (Art. 25 und 26), zu übertragen, mussten mit diversen Nicht-EU-Ländern in der Folge separate Abkommen ausgehandelt werden. Das wohl bekannteste ist das sogenannte *Safe-Harbor*-Abkommen mit den USA, dem mittlerweile ein Großteil der führenden US-amerikanischen (IT-) Konzerne beigetreten ist und das diese bei der Verarbeitung personenbezogener Daten von EU-Bürgern verpflichtet, im Abkommen festgelegte Datenschutzprinzipien zu achten sowie sich dabei der Kontrolle durch die US-amerikanische Handelsaufsicht *Federal Trade Commission* (FTC) zu unterwerfen.[7] Allerdings wurde das Abkommen regelmäßig von verschiedenster Seite für seinen Mangel an Wirkungskraft kritisiert (Düsseldorfer Kreis 2010; Seeger 2011; EU

[5] Zu den damaligen gesellschaftlichen Rahmenbedingungen, die das Volkszählungsurteil erst ermöglichten siehe Abschnitt 4.3.1 bzw. Busch und Jakobi (2011).

[6] Offiziell wurde somit die Ausarbeitung der Richtlinie mit der Notwendigkeit einer Harmonisierung des europäischen Binnenmarktes (Art. 100a EG-Vertrag) begründet und bei der Generaldirektion XV, zuständig für den Binnenmarkt, angesiedelt (Bennett und Raab 2006: 93). Der ausführliche Titel der Datenschutzrichtlinie macht schließlich deutlich, dass sich der „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten" auf der einen und der „freie Datenverkehr" auf der anderen Seite als gleichberechtigte Gewährleistungsziele gegenüberstehen.

[7] Zur Entstehungsgeschichte des *Safe-Harbor*-Abkommens siehe Busch (2005) und (2012a).

Commission 2013a). Zudem scheint insbesondere nach den Snowden-Enthüllungen zweifelhaft, ob bei einem Transfer von personenbezogenen Daten in die USA ein hinreichender Grundrechtsschutz für den Betroffenen nach europäischem Rechtsverständnis gewährleistet werden kann (ULD 2014). Aus diesem Grund erklärte der Europäische Gerichtshof (EuGH) (2015), einer vom Aktivisten Max Schrems initiierten Klage folgend, das *Safe-Harbor*-Abkommen in einer wegweisenden Entscheidung im Oktober 2015 für ungültig – mit weitreichenden Folgen für den transatlantischen Datenverkehr (vgl. Beuth 2015a).[8]

War die Datenschutzrichtlinie noch im technologischen Kontext einer stetig wachsenden Verbreitung von Personal Computern (PC) entstanden, so folgte 2002 ein erster Versuch der Datenschutzregulierung im Internetzeitalter. Die wenig beachtete EU-Datenschutzrichtlinie für elektronische Kommunikation („ePrivacy-Richtlinie") (2002) und deren Novellierung durch die sogenannte *Cookie-Richtlinie* (2009) widmen sich insbesondere dem Schutz personenbezogener bzw. -beziehbarer Daten (wie mittels Cookies erhobener Daten oder Verbindungsdaten) bei der Internetnutzung (vgl. Poullet 2010; Roßnagel et al. 2012: 296 ff.). Die Umsetzung in deutsches Recht verlief jedoch sehr holprig. Während erst ein Vertragsverletzungsverfahren gegenüber Deutschland die Umsetzung der ePrivacy-Richtlinie durch die Anpassung des Telekommunikationsgesetzes (TKG) 2004 erzwang, ist bis heute unter Experten strittig, ob die Cookie-Richtlinie adäquat umgesetzt wurde (Störing 2014).

Ein weiterer Meilenstein war die Verankerung des Datenschutzes als europäisches Grundrecht. Denn mit dem Vertrag von Lissabon erhielt die bereits zuvor ausgehandelte Charta der Grundrechte der Europäischen Union (2010) im Jahre 2009 trotz Scheiterns des Vertrags über eine Verfassung für Europa nun Rechtskraft, wodurch sowohl der *Achtung des Privat- und Familienlebens* (Art. 7) als auch dem *Schutz personenbezogener Daten* (Art. 8) Grundrechtsstatus verliehen wurde.

Reformprozess des europäischen Datenschutzrechts

Darüber hinaus wird seit 2012 das europäische Datenschutzrecht grundlegend reformiert. Das EU-Reformpaket, bestehend aus Datenschutz-Grundverordnung (DS-GVO) (EU-Kommission 2012a) und einer häufig außer Acht gelassenen neuen Datenschutzrichtlinie (EU-Kommission 2012b), soll neue rechtliche Maßstäbe auch in Deutschland setzen. Während Erstere als EU-Verordnung in unmittelbar geltendes Recht übergehen und auf jede datenverarbeitende öffentliche und nichtöffentliche Stelle in der EU ihre Anwendung finden wird (mit zahlreichen Ausnahmen für Polizeien und Nachrichtendienste), beinhaltet Letztere eine rechtliche Rahmensetzung für die Datenverarbeitung von Polizei- und Justizbehörden in den EU-Mitgliedsstaaten, deren Vorgaben allerdings noch in nationales Recht umzusetzen sind.[9]

Bereits 2009 – also weit vor den Snowden Enthüllungen – erkannte die EU-Kommission die Notwendigkeit, das europäische Datenschutzrecht, das Anfang der 1990er Jahre noch im technikhistorischen Kontext des PCs entwickelt wurde, grundlegend zu reformieren, um es den aktuellen digitalen Herausforderungen des Internetzeitalters anzupassen (EU Commission 2010).

[8] Davor hatte nicht nur das EU-Parlament (2014) eine Aussetzung des Abkommens gefordert, sondern auch die EU-Kommission sah Handlungsbedarf und startete bereits im Herbst 2013 Verhandlungen über ein neues *Safe-Harbor*-Abkommen mit den USA, die sich jedoch als äußerst zäh erwiesen und auch zwei Jahre später noch andauern (BfDI 2015).

[9] Sowohl der aktuelle Verhandlungsstand der DS-GVO als auch der neuen Datenschutzrichtlinie können online unter http://eur-lex.europa.eu/procedure/DE/201286 (14.08.2015) bzw. http://eur-lex.europa.eu/procedure/DE/201285 (23.08.2015) eingesehen werden.

Entwicklung des heutigen Datenschutzes

Schon im Vorfeld der offiziellen Vorstellung der Gesetzesinitiative durch die EU-Kommission 2012 zeichnete sich ab, dass das Reformvorhaben nicht nur ein gewaltiges, die Informationsgesellschaft nachhaltig veränderndes Regelwerk werden würde, sondern auch extrem starken Kräften aus Politik und Wirtschaft standhalten müsste. Denn die Möglichkeit mitzubestimmen, wie zukünftig mit der Ressource Information zu einem großen Teil umgegangen werden sollte, weckte Begehrlichkeiten von allen Seiten (Spiekermann 2012). Die damals für die Ausarbeitung der DS-GVO zuständige EU-Justizkommissarin Viviane Reding kritisierte, ein so aggressives Lobbying in ihrer zwanzigjährigen EU-Politikkarriere noch nie erlebt zu haben (Warman 2012). Und auch der Berichterstatter zur DS-GVO im zuständigen parlamentarischen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) Jan Philipp Albrecht monierte den unverhältnismäßig starken Einfluss wirtschaftlicher Interessenvertreter (Albrecht 2013). Insbesondere Lobbyisten der US-amerikanischen Wirtschaft hätten versucht all ihre Macht und Einfluss geltend zu machen (Cáceres 2013). Das massive Lobbying gipfelte in Enthüllungen darüber, dass zahlreiche EU-Parlamentarier des LIBE-Ausschusses offenbar ganze Seiten und Textpassagen aus Positionspapieren von Wirtschaftsvertretern wortwörtlich in ihren Änderungsanträgen zur DS-GVO übernommen hatten (Kuhn 2013).[10]

Obwohl sich die Verhandlungen u. a. aufgrund von über 4000 Änderungsvorschlägen als schwierig erwiesen (Albrecht 2014: 121 ff.), wurde im Herbst 2013 ein Kompromiss zur DS-GVO im zuständigen Ausschuss beschlossen und ein halbes Jahr später in 1. Lesung im EU-Parlament (2013a) mit überwältigender Mehrheit verabschiedet. Insbesondere das Bekanntwerden der NSA-Spähaffäre im Sommer 2013 in Verbindung mit dem Ziel vieler EU-Parlamentarier, vor der im Frühling 2014 stattfindenden Europawahl das für notwendig befundene Datenschutzreformvorhaben wenn nicht schon fertiggestellt, so doch zumindest auf den Weg gebracht zu haben, spielten einen nicht unerheblichen Einfluss auf die gegen Ende beschleunigte Konsensfindung im EU-Parlament.

Während die EU-Abgeordneten somit schon nach zwei Jahren einen im Parlament mehrheitsfähigen Kompromiss vorweisen konnten, kam der EU-Rat (2015) erst ein weiteres Jahr später zu einer endgültigen Einigung. Die zähen Verhandlungen im Ministerrat waren immer wieder durch Blockadehaltungen einzelner Regierungen – insbesondere der britischen und auch der deutschen – gekennzeichnet (Spiegel Online 2013). Die Gründe hierfür sind vor allem in der ablehnenden Haltung gegenüber einer stärkeren Regulierung sowohl des öffentlichen (Hecking 2013a) als auch privatwirtschaftlichen Sektors zu finden (ULD 2013; Fontanella-Khan 2013a; Ebbinghaus et al. 2014).[11] Aber auch die vielfältigen Möglichkeiten der EU-Kommission, durch sogenannte delegierte Rechtsakte die weitere datenschutzrechtliche Ausgestaltung und praktische Umsetzung der DS-GVO maßgeblich zu bestimmen, stießen vermehrt auf Kritik (vgl. Hornung 2012: 105).

Obwohl Vertreter von Kommission, Parlament und Rat sich im Rahmen der ersten Trilog-Sitzung gemeinsam für eine zügige Einigung bis zum Ende des Jahres 2015 ausgesprochen haben, ist nicht wirklich abzusehen, wie lange die Verhandlungen letztendlich noch andauern werden. Fraglich bleibt zudem auch, wie stark die von der Kommis-

[10] Die für den Grimme Online Award nominierte Plattform LobbyPlag.eu hat detailreich jene kopierten Textabschnitte dokumentiert, graphisch aufgearbeitet und anhand ihres Einflusses auf eine Erhöhung bzw. Verringerung des Datenschutzniveaus analysiert (vgl. http://lobbyplag.eu/lp (23.08.2015)).

[11] Im März 2015 wurden mehr als 11.000 interne Dokumentenseiten über Verhandlungen des EU-Ministerrates zur DS-GVO im Internet veröffentlicht (vgl. http://lobbyplag.eu/governments/ (14.08.2015); Beuth 2015b). Aus diesen geht hervor, dass insbesondere die deutsche Bundesregierung bzw. Vertreter des Bundesinnenministeriums vermehrt Änderungsvorschläge eingebracht haben, die eine Absenkung des Datenschutzniveaus zugunsten von Wirtschaftsinteressen zur Folge hätten (ebd.).

sion und dem Parlament eingebrachten Entwürfe durch Kompromisse mit Regierungsvertretern der Mitgliedsstaaten im Rat abgeschwächt werden (Levy-Abegnoli 2015).[12]

[12] Während relativ viel über den Stand der Verhandlungen zur DS-GVO in den Medien zu lesen war, bleiben Neuigkeiten und Interna zum Aushandlungsprozess der zu Anfang beschriebenen neuen Datenschutzrichtlinie, die einen harmonisierten Rechtsrahmen für Regeln zur Datenverarbeitung von Polizei- und Justizbehörden in EU-Mitgliedsstaaten vorsieht, größtenteils aus. Nachdem sich das EU-Parlament (2013b) auch hier über einen Kompromissvorschlag im Frühjahr 2014 verständigen konnte, steht im Gegensatz zur DS-GVO eine Einigung im EU-Ministerrat seitdem noch aus.

3 Regulierungspraxis zentraler Akteure beim Datenschutz

Die Entwicklungen auf EU-Ebene sind, wie durch den geschilderten Ablauf der Verhandlungen zum europäischen Datenschutzreformpaket deutlich wurde, auch für den Datenschutzdiskurs in Deutschland höchst relevant. Deswegen wird im Folgenden immer wieder versucht, europäische Akteure in die Analyse mit einzubeziehen. Konzentriert wird sich jedoch in erster Linie auf Akteure der deutschen Datenschutzpolitik wie die Bundesregierung (politische Exekutive), den Bundestag (Legislative), das Bundverfassungsgericht (Judikative), die politischen Parteien und die Datenschutzbehörden.

3.1 Politische Exekutive

Daten bedeuten Informationen, Wissen, Kontrolle und Macht. Generell unterliegt die politische Exekutive deswegen beim Datenschutz einem Interessenkonflikt: Einerseits geht es ihr in Machterhalt und -ausübung um einen gewissen, immer stärker auch auf Daten basierten Kontrollanspruch, andererseits ist sie dem Grundrechtsschutz und der Erhaltung demokratischer Werte verpflichtet.[13]

Die bekannt gewordene Massenüberwachung elektronischer Kommunikation auch durch deutsche Nachrichtendienste, die Vorratsdatenspeicherung in Verbindung mit immer wieder aufflammenden Diskussionen um ihre Wiedereinführung, die häufig in rechtlichen Grauzonen stattfindenden Online-Durchsuchungen, all dies sind Beispiele, die darauf hindeuten, dass der politischen Exekutive in Deutschland insgesamt eine Tendenz zur Priorisierung von sicherheitspolitischen Zielen gegenüber einer Stärkung von Bürgerrechten attestiert werden kann (Baumann 2013; Fritz 2013; Busch 2013). Doch muss innerhalb der Bundes- und Landesregierung(en) durchaus zwischen unterschiedlichen, teils konträren Positionen der einzelnen Ministerien differenziert werden.[14] Fast schon legendär sind hierbei die politischen Auseinandersetzungen zwischen dem Bundesinnen- und Bundesjustizministerium.[15] In den Justiz-, Wirtschafts- und In-

[13] Zudem kommen hier staatlich-strukturell bedingte Aspekte zum Tragen, denen Datenschutz in einem Spannungsverhältnis gegenübersteht. So sehen Busch und Jakobi (2011: 312) hinter den Auseinandersetzungen zur Volkszählung 1983 einen generellen gesellschaftlichen Konflikt, der bereits Teil der in den 1960er Jahren geführten Diskussion um staatlichen Planungs- und Kontrollanspruch gewesen sei. Nach Giddens (1995: 180, 238) steht dieser Konflikt zwischen Sicherheits- bzw. Verwaltungs- und Bürgerrechtsinteressen sogar in einem strukturellen Spannungsverhältnis, da der moderne Staat seine Existenz nicht zuletzt dem Einsatz differenzierter Überwachungstechniken verdankt, durch die der administrative Zugriff auf und die Verwaltung von großen Populationen erst möglich gemacht wird.

[14] Zusätzlich wird die ministerielle Durchsetzungskraft bzw. Vetospielerposition im Policy-Making Prozess durch den im Grundgesetz verankerten Regierungsgrundsatz des Ressortprinzips, das den einzelnen Ministerien eine relativ starke Autonomie in ihrem Handeln ermöglicht, verstärkt.

[15] Die wohl bekannteste und am vehementesten für den Datenschutz eintretende Justizministerin war Sabine Leutheusser-Schnarrenberger. Im Jahr 1995 stoppte die damalige FDP-Bundesjustizministerin die Einführung der akustischen Wohnraumüberwachung (Großer Lauschangriff). Eine deswegen anberaumte Urabstimmung, in der sich über 63,6% der FDP-Mitglieder für den Großen Lauschangriff aussprachen, nahm sie daraufhin konsequenterweise zum Anlass zurückzutreten (Böhm 2011: 153 ff.). Und auch in ihrer zweiten Amtszeit als Bundesjustizministerin machte sie mit der später erfolgreichen Verfassungsbeschwerde gegen die Vorratsdatenspeicherung und der Weigerung einer erneuten Umsetzung derselben von sich reden (Betz 2010). Darüber hinaus sind die Differenzen über geeignete Anti-Terrormaßnahmen zwischen Bundesinnenminister Schäuble (CDU) und Bundesjustizministerin Zypries (SPD) (ebd.) sowie die nach den Anschlägen von Paris im Januar 2015 wiederbelebte Diskussion zur abermaligen Einführung der Vorratsda-

nenministerien spiegeln sich somit auch die in Abschnitt 4 angesprochenen bürgerrechtlichen, wirtschafts- und sicherheitspolitischen Positionen wider (Fritz 2013: 102; Karaboga et al. 2014: 10).[16]

Dementsprechend agiert die gegenwärtige Bundesregierung beim Thema Datenschutz ambivalent. Auf der einen Seite werden u. a. als Reaktion auf die Snowden-Enthüllungen regelmäßig Forderungen nach einer Verbesserung von IT-Sicherheit und der Stärkung des Datenschutzes laut.[17] Auf der anderen Seite sind deutsche Regierungsvertreter innerhalb des EU-Rats immer wieder als Bremser im Reformprozess des europäischen Datenschutzrechts aufgefallen (vgl. Abschnitt 2). Bei der Aufarbeitung der Massenüberwachung durch ausländische Nachrichtendienste im NSA-Untersuchungsausschuss wird der politischen Exekutive ebenfalls eine Blockadehaltung zugeschrieben (vgl. Abschnitt 3.2),[18] und schließlich zeigt sich die Bundesregierung selbst hinsichtlich einer Stärkung der Unabhängigkeit und Durchsetzungskraft des BfDI nur wenig bemüht (vgl. Abschnitt 3.5).

Es drängt sich zudem die Vermutung auf, dass es insbesondere in Legislaturperioden der Großen Koalition auf Bundesebene zu einer Häufung von für den Datenschutz problematischen Sicherheitsgesetzen kommt.[19] Denn sowohl CDU/CSU als auch die

tenspeicherung zwischen Bundesinnenminister de Maizière (CDU) und Bundesjustizminister Maas (SPD) (Jungholt 2015) zu nennen, wobei allerdings Letzterer mit seinem Vorstoß einer „grundrechtsverträglichen Form der Vorratsdatenspeicherung" (Rath 2015) einen überraschenden Richtungswechsel vollzog (vgl. Fn. 31).

[16] Diese Beobachtung kann auch auf EU-Ebene bestätigt werden. Insbesondere seit der Aufspaltung des EU-Ressorts *Justiz, Freiheit und Sicherheit* (von 1995 bis 2010) in die Ressorts *Justiz und Grundrechte* sowie *Inneres* tritt der Konflikt zwischen bürgerrechtlichen und sicherheitspolitischen Interessen deutlicher zutage. So kann das durch Vivian Reding (damalige Kommissarin für Justiz und Grundrechte) initiierte Datenschutzreformvorhaben und das Dagegenhalten ihrer Amtskollegin Cecilia Malström (damalige Kommissarin für Inneres), die sich darüber hinaus auch vehement für eine Beibehaltung der EU-Richtlinie zur Vorratsdatenspeicherung einsetzte (FAZ 2012), als ein zentrales Beispiel für diesen Konflikt angeführt werden (Bersing 2014; Hecking et al. 2014). Allerdings findet auf oberster Ebene der EU-Kommission sowie im EU-Ministerrat, in dem sich nationale Regierungsvertreter aus Innen- und Justizministerien auf eine gemeinsame Linie einigen müssen, häufig eine Priorisierung von sicherheitspolitischen Zielsetzungen statt. So initiierten bzw. priorisierten die Führungsspitze der EU-Kommission sowie der EU-Ministerrat (Rat für Justiz und Inneres (JI-Rat)) des Öfteren sicherheitspolitische Vorhaben wie die Einführung der EU-Richtlinie zur Vorratsdatenspeicherung (Fritz 2013: 139 ff.), das PNR- oder SWIFT-Abkommen und setzten sich so gegenüber bürgerrechtlichen Positionen anderer Regierungsmitglieder wie der Justizminister durch (vgl. Abschnitte 4.2.1 und 4.2.2). Und auch hinsichtlich der bekannt gewordenen Massenüberwachung von europäischen Bürgern durch die *Five Eyes* blieben Reaktionen dieser Institutionen der EU-Exekutive weitestgehend aus.

[17] Exemplarisch sei an dieser Stelle auf die Arbeiten der Bundesregierung am ersten IT-Sicherheitsgesetz (De Maizière 2014), auf die neu entstandenen Forschungsschwerpunkte IT-Sicherheit und Privacy (BMBF 2015) sowie auf die Digitale Agenda verwiesen (BMWi et al. 2014).

[18] Auch die strafrechtliche Aufarbeitung des NSA-Spähskandals durch den damaligen Generalbundesanwalt Harald Range wies einen teilweise merkwürdig anmutenden Schlingerkurs auf. Während die Anfang August 2013 begonnenen Vorermittlungen zur Massenüberwachung von deutschen Staatsbürgern und Politikern durch die NSA Mitte 2014 zunächst in deren Einstellung mündeten, wurde bald darauf in Folge massiver öffentlicher Kritik verkündet, dass zumindest im Falle des abgehörten „Kanzlerinnen-Handys" weiter ermittelt werde, das Abhören deutscher Staatsbürger durch ausländische Geheimdienste jedoch mit den Mitteln des deutschen Strafrechts nicht verfolgbar sei (Leyendecker und Mascolo 2014; Prantl 2014). Im Sommer 2015 wurden schließlich auch die Ermittlungen zum NSA-Lauschangriff auf das Handy der Bundeskanzlerin mit der Begründung Ranges, der Vorwurf ließe sich nicht gerichtsfest beweisen, eingestellt (Rosenbach und Schindler 2015).

[19] Schon die erste Große Koalition von 1966 bis 1969 sorgte mit der Einführung der Notstandsgesetze und der darin enthaltenen Einschränkung des Telekommunikationsgeheimnisses (vgl. Fn. 71) für einen Paradigmenwechsel hinsichtlich der von da an verfassungsrechtlich abgesicherten Telekommunikationsüberwachung deutscher Staatsbürger. Die zweite Große Koalition von 2005 bis 2009 sorgte gleich in mehrfa-

SPD räumen bürgerrechtlich-liberalen Fragestellungen üblicherweise wenig Patz in ihren Wahlprogrammen und der praktischen Regierungspolitik ein, während die FDP (insbesondere mit Leutheusser-Schnarrenberger als Bundesjustizministerin (vgl. Fn. 15)) und auch die Grünen von ihrer parteipolitischen Ausrichtung bzw. Tradition bürgerrechtlichen Themen sehr viel aufgeschlossener gegenüberstehen (vgl. Abschnitt 3.4).[20] Obwohl Grünen und FDP das Hochhalten bürgerrechtlicher Positionen vor dem Hintergrund der Regierungsbeteiligung regelmäßig schwergefallen ist (vgl. Busch 2007; 2012b: 869), so kommt ihnen als *kleinen* Koalitionspartnern jedoch häufig eine gewisse Korrektivfunktion in für den Datenschutz problematischen Gesetzesvorhaben zu, die in der Großen Koalition gänzlich abhanden gekommen zu sein scheint.

3.2 Legislative

Generell kann beobachtet werden, dass im Gegensatz zu einem Großteil der politischen Exekutive sowohl die Länderparlamente als auch der Deutsche Bundestag und das EU-Parlament Datenschutzfragen sehr viel offener und unterstützender gegenüberstehen.[21] Datenschutz als Instrument zur Machtkontrolle wird so zu einem zentralen Bestandteil der parlamentarischen Kontrollfunktion gegenüber der Exekutive.[22]

Im Bundestag wurden Datenschutzthemen vor allem im Rahmen der Enquete-Kommission „Internet und digitale Gesellschaft", des NSA-Untersuchungsausschusses sowie in zahlreichen Großen und Kleinen Anfragen der Opposition diskutiert.[23]

Besagte Enquete-Kommission untersuchte von 2010 bis 2013 die Auswirkungen der Digitalisierung auf die Gesellschaft. Mit dem Thema Datenschutz setzte sich die Kommission innerhalb der Projektgruppe „Datenschutz, Persönlichkeitsrechte" auseinander und formulierte neben der Bestandsaufnahme bestehender Datenschutzregeln eine

---

cher Hinsicht für Aufsehen, da zahlreiche von ihr initiierte Gesetze zur Antiterrordatei (von 2006) sowie zur Vorratsdatenspeicherung und Bestandsdatenauskunft (beide 2007) entweder als verfassungswidrig zurückgewiesen wurden oder immer noch als Verfassungsbeschwerden beim BVerfG anhängig sind, wie dies bei der umstrittenen BKA-Gesetzreform (von 2008), die die bereits als verfassungswidrig eingestufte Online-Durchsuchung für das BKA legalisiert hat, der Fall ist. Schließlich fällt die dritte Große Koalition seit 2013 bis auf die Wiedereinführung der Vorratsdatenspeicherung weniger durch verfassungsrechtlich problematische Gesetzesinitiativen als vielmehr durch ihre Untätigkeit nach den Snowden-Enthüllungen bzgl. einer notwendigen Aufklärung und Reform nachrichtendienstlicher Strukturen und Praktiken auf (Prantl 2013; Sauerbrey 2013).

[20] Die Thesen der Großen Koalition als Katalysator für eine Ausweitung des Überwachungsstaates sowie der *kleineren* Koalitionspartner als Korrektive bedürfen jedoch weiterer empirischer Forschung und beziehen sich ausdrücklich auf die Bundesebene. Regierungszusammensetzungen auf Landesebene und deren Einfluss auf den Datenschutz wurden hier weitestgehend vernachlässigt. Schon der Umstand, dass beispielsweise das 2006 durch die FDP geführte nordrhein-westfälische Innenministerium federführend war für das zwei Jahre später vom BVerfG kassierte Landesverfassungsschutzgesetz, das Online-Durchsuchungen gesetzlich erlauben sollte, zeigt, wie stark sich Politiken von ein und derselben Partei auf Bundes- und Landesebene unterscheiden können.

[21] So zeigt z. B. Baumann (2013), dass die Bereitschaft zur Stärkung des Datenschutzes insbesondere mit der Entfernung zu politischer Verantwortung in der Reihenfolge a) Bundesregierung, b) Landesregierungen, c) Bundesopposition, d) Landesoppositionen wächst.

[22] Da in Deutschland die politische Exekutive sowohl auf Landes- als auch auf Bundesebene aus der Legislative hervorgeht, sie also stark miteinander verschränkte Gewalten darstellen, sind offen ausgetragene Auseinandersetzungen häufig auf Regierung und Opposition begrenzt. Auf EU-Ebene verhält sich dies aufgrund der stark getrennten Sphären von gesetzgebender und ausführender Gewalt anders. Dementsprechend tritt hier der Konflikt zwischen EU-Kommission (z. T. EU-Rat) und gesetzgebender (EU-Parlament und z. T. EU-Rat) Gewalt sehr viel stärker und öfter gerade auch in Bezug auf Datenschutzthemen in Erscheinung.

[23] Der Bundestag ernennt zudem auf Vorschlagsrecht der Bundesregierung den BfDI (vgl. Abschnitt 3.5).

Reihe von Handlungsempfehlungen (Deutscher Bundestag 2012: 51 ff.). Darüber hinaus wurde Vertretern von Wirtschaft, Wissenschaft, Datenschutzbehörden und Bürgerrechtsorganisationen die Möglichkeit geboten, ihre Positionen in die politische Debatte mit einfließen zu lassen. Gleichzeitig bemängelten eben jene Sachverständige jedoch immer wieder den faktisch sehr geringen Einfluss der Enquete-Kommission auf die Bundespolitik (vgl. Deutscher Bundestag 2013a: 19 ff.).

Der NSA-Untersuchungsausschuss konstituierte sich im März 2014 auf Antrag aller Fraktionen mit dem Ziel, das Ausmaß und die Hintergründe der Internet- und Telekommunikationsüberwachung durch ausländische Nachrichtendienste seit 2001 aufzuklären und hieraus Handlungsempfehlungen für die Zukunft abzuleiten (Deutscher Bundestag 2014a). In den bisherigen Anhörungen wurden u. a. die Verträglichkeit der Auslandsüberwachung des Bundesnachrichtendienstes (BND) und der Überwachung durch die NSA mit deutschem, europäischem und internationalem Recht, technische Schutzmöglichkeiten vor Massenüberwachung sowie die Zusammenarbeit von BND und NSA behandelt.[24] Hitzige Debatten entbrannten vor allem darüber, ob Edward Snowden als Zeuge vernommen werden sollte (Bannas 2014). Auch seien die von der Bundesregierung und den jeweiligen Behörden zur Verfügung gestellten Akten dermaßen stark geschwärzt worden, dass teils lediglich banale Inhalte wie etwa eine Anrede übrigblieben, und in weitere potentiell wichtige Akten werde der Einblick gar komplett verwehrt (Biermann 2014). Die Auseinandersetzungen zwischen Bundeskanzleramt und Untersuchungsausschuss erreichten ihren vorläufigen Höhepunkt, als eine Reihe von als geheim klassifizierten Dokumenten des Ausschusses an die Öffentlichkeit geriet und das Kanzleramt den Ausschussmitgliedern mit einer Strafanzeige drohte (Gude und Meiritz 2014).

3.3 Judikative

Der Judikative kommt beim Thema Datenschutz eine Schlüsselfunktion zu. Zum einen fällen die obersten deutschen Gerichtshöfe immer häufiger Urteile mit direktem Bezug zum Datenschutz.[25] Zum anderen wirkt die Verfassungsgerichtsbarkeit regelmäßig als Korrektiv vor allem gegenüber sicherheitspolitischen Bestrebungen der Exekutive, indem in Persönlichkeitsrechte eingreifende Gesetze auf Verfassungsverträglichkeit und Verhältnismäßigkeit, d. h. den legitimen Zweck, die Geeignetheit, Erforderlichkeit und Angemessenheit, hin überprüft werden.

Die verfassungsrechtlichen Prüfungen von für den Datenschutz problematischen Gesetzen haben insbesondere seit den Anschlägen vom 11. September 2001 und dem daran anschließenden sicherheitspolitischen Paradigmenwechsel signifikant zugenommen (Roßnagel 2011: 37). Nicht nur haben hier die Bedrohungslage durch den international

[24] Die Stellungnahmen und Gutachten der geladenen Sachverständigen können auf der Webseite des Deutschen Bundestages (2015) abgerufen werden.

[25] So gab z. B. der Bundesgerichtshof (BGH) erst kürzlich einem Bewertungsportal Recht, das sich auch nach einem Urteil des Oberlandesgerichts Stuttgart weigerte, Nutzerdaten an einen Arzt herauszugeben, der sich zu Unrecht von einem Nutzer bewertet gefühlt hatte (BGH 2014; FAZ 2014a). Und auch das Bundesverwaltungsgericht entschied vor Kurzem, dass die Polizei in Bayern weiterhin massenhaft Kfz-Kennzeichen auf Autobahnen im Freistaat erfassen und diese mit polizeilichen Datenbanken abgleichen dürfe (BVerwG 2014; Spiegel Online 2014a). Während das Bundesarbeitsgericht zudem in regelmäßigen Abständen wichtige Entscheidungen im Bereich des Beschäftigtendatenschutz trifft (z. B. BAG 2013), wies das Bundessozialgericht erst im letzten Jahr eine Klage aufgrund von Datenschutzbedenken gegenüber der elektronischen Gesundheitskarte ab (BSG 2014; Handelsblatt 2014). Schließlich sorgt auch der Bundesfinanzhof in Urteilen wie jenes über die festgestellte Rechtmäßigkeit eines Abgleichs von Beschäftigtendaten mit den sogenannten Anti-Terror-Listen für Rechtsklarheit im Datenschutzrecht (BFH 2012).

vernetzten Terrorismus, sondern ebenfalls neue Formen und Möglichkeiten der Kommunikation über das Internet einen reflexartigen Kontrollanspruch staatlicher Akteure ausgelöst,26 der häufig in Form von ausschweifenden Sicherheitsgesetzen zutage tritt.

In regelmäßigen Abständen, aber keineswegs immer hat das BVerfG solche Gesetze beanstandet (vgl. Tabelle 1, S. 71). Im Folgenden soll beispielhaft vor allem das Urteil zur Online-Durchsuchung diskutiert werden, das ähnlich zukunftsrelevanten und wegweisenden Charakter haben könnte wie das Volkszählungsurteil von 1983.

Das Urteil zur Online-Durchsuchung (BVerfG 2008) nahm seinen Anfang mit einer Verfassungsbeschwerde gegen eine 2006 verabschiedete Änderung des nordrhein-westfälischen Landesverfassungsschutzgesetzes, das der gleichnamigen Behörde die heimliche Überwachung von Computern ermöglichen sollte (Heise Online 2007a).[27] Daraufhin entbrannte eine öffentliche Debatte über die rechtmäßige Nutzung von Spionagesoftware durch Nachrichtendienst- und Polizeibehörden (Tomik 2007; Spiegel Online 2007),[28] an deren Ende das besagte Urteil stand. Obwohl die Bundesverfassungsrichter die Online-Durchsuchung nicht per se verboten, so schränkten sie deren Anwendung in der Praxis doch erheblich ein.[29] Weit bedeutender in diesem Urteil war jedoch die nach 1983 abermalige Formulierung eines neuen Grundrechts, des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[30] Dieses sogenannte Computer- oder IT-Grundrecht erweitert nicht nur den Schutz des allgemeinen Persönlichkeitsrechts auf Bewahrung der Integrität informationstechnischer Systeme, sondern stellt zugleich einen „Schutzauftrag an den Gesetzgeber, aktiv auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Privatrechtsverkehr hinzuwirken" (Petri 2008: 448).

Erstaunlicherweise fand dieses neue Grundrecht in der Verfassungspraxis bisher kaum Anwendung (Baum et al. 2013), und das, obwohl ein eklatanter Unterschied zwischen der durch das Urteil vorgegebenen Verfassungsnorm und der durch Polizei und Nachrichtendienste gelebten Verfassungspraxis zu bestehen scheint (Buermeyer und Bäcker 2009; Prantl 2011). So führten immer wieder neue die Online-Durchsuchung legitimierende Gesetze wie die Neufassung des BKA-Gesetzes von 2008 zu Kritik (Hansen und Pfitzmann 2008) und zahlreichen noch immer anhängigen Verfassungsbeschwerden (Naumann 2009; Prantl 2010). Zudem wirft der *de facto* Einsatz von Spionagesoftware zum Zwecke der Online-Durchsuchung in Verbindung mit einem ausschweifenden Funktionsumfang dieser Technologien regelmäßig Fragen nach deren Rechtmäßigkeit auf. Insbesondere die durch den *Chaos Computer Club* (CCC) vorgenommene Analyse des sogenannten *Staatstrojaners* (später als *Bayerntrojaner* identifiziert (Biermann 2011)

---

[26] Vergleiche hierzu beispielsweise das öffentliche Werben des damaligen BKA-Präsidenten Jörg Ziercke für die Online-Durchsuchung (Ziercke 2008).

[27] Obwohl Nachrichtendienstbehörden wie der Bundesnachrichtendienst (BND) auch ohne spezifizierte Gesetzesgrundlage bereits zuvor Online-Durchsuchungen vorgenommen hatten (Heise Online 2007b; Pohl 2007: 684), war eine solche nun explizit notwendig geworden, da der BGH das Vorgehen einer seiner Ermittlungsrichter, der mit dem Argument einer fehlenden Ermächtigungsgrundlage eine vom Generalbundesanwalt beantragte Online-Durchsuchung abgelehnt hatte, in einem Beschluss auch gerichtlich bestätigte (BGH 2007; Hornung 2007: 575).

[28] Zur technischen Funktionsweise der Online-Durchsuchung siehe Hansen und Pfitzmann (2007) sowie Pohl (2007).

[29] So bedarf eine Online-Durchsuchung nicht nur einer klaren Gesetzesgrundlage, sondern sie ist nur dann zulässig, wenn „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut" vorliegen (BVerfG 2008). Zudem unterliegt die Online-Durchsuchung dem Richtervorbehalt (ebd.).

[30] Es dient als sogenanntes Auffanggrundrecht, d. h. es ist subsidiär und kommt somit erst zur Anwendung, wenn Grundrechte wie das Telekommunikationsgeheimnis (Art. 10 (1) GG), die Unverletzlichkeit der Wohnung (Art. 13 (1) GG) oder das Recht auf informationelle Selbstbestimmung nicht greifen (BVerfG 2008).

machte den tiefgreifenden und verfassungswidrigen Eingriff solcher Programme in die Privatheit des Betroffenen deutlich (Rieger 2011). Und auch die kürzlich erfolgte Fertigstellung des *Bundestrojaners* lässt Zweifel an der ernsthaften Würdigung des BVerfG-Urteils durch deutsche Nachrichtendienst- und Strafermittlungsbehörden erkennen (Monroy 2014; Schulzki-Haddouti 2015a).

Neben dem BVerfG als einem zentralen Akteur wechselseitiger politischer Kontrolle in Deutschland spielen in den letzten Jahren verstärkt auch höchstrichterliche Entscheidungen auf EU-Ebene eine wichtige Rolle für den Datenschutz (Streinz 2011). Insbesondere die durch den Vertag von Lissabon entstandene Rechtsverbindlichkeit der EU-Grundrechte-Charta und dem darin enthaltenen Datenschutzgrundrecht verleiht dem EuGH hier mehr Gewicht in seinen Entscheidungen. Wegweisende Urteile zum Datenschutz in den letzten Jahren waren z. B. die Bestätigung der „völligen Unabhängigkeit" von Datenschutzbehörden (vgl. Abschnitt 3.5), das Aufheben der EU-Richtlinie über die Vorratsspeicherung von Daten (EuGH 2014a), die Formulierung des „Rechts auf Vergessenwerden" in einer Klage gegen Google (EuGH 2014b) sowie die Annullierung des *Safe-Harbor*-Abkommens (EuGH 2015).

Mit Blick auf die Zukunft ist anzunehmen, dass der EuGH gerade auch im Kontext der sich abzeichnenden europaweiten DS-GVO weiter an Bedeutung gewinnen wird.

3.4 Parteien

Lange fristete das Thema Datenschutz in den politischen Parteien ein Nischendasein. Eine Wandlungstendenz ist in Deutschland vor allem seit den Protesten gegen die Vorratsdatenspeicherung und das Zugangserschwerungsgesetz sowie dem überraschend guten Abschneiden der Piratenpartei bei der Bundestagswahl 2009 (zwei Prozent) und der Wahl zum Abgeordnetenhaus von Berlin 2011 (8,9 Prozent) zu beobachten. Seither setzen sich die etablierten Parteien stärker mit Fragen des Datenschutzes und der Netzpolitik auseinander und versuchen ihre Expertise in diesem Bereich auszubauen, was sich nicht zuletzt in der Gründung parteinaher netzpolitischer Lobbyorganisationen wie CNetz und D64 äußert (Biermann 2012; Rosenbach und Schmundt 2009).

Laut ihren Wahlprogrammen zur Bundestagswahl 2013 stellt ein starker Datenschutz für alle im Bundestag vertretenen Parteien ein erstrebenswertes Ziel dar. Unterschiede offenbaren sich bei der Abwägung von Datenschutz gegenüber anderen Gütern wie wirtschaftlichem Wohlergehen oder Sicherheit. Im Spannungsfeld von Datenschutz und Wirtschaftsinteressen plädieren CDU/CSU und FDP für eine Selbstregulierung der Wirtschaft, Eigenverantwortung sowie Selbstdatenschutz durch den Bürger und stellen insbesondere die ökonomischen Chancen der Digitalisierung heraus (CDU/CSU 2013: 34 f., 61 ff.; FDP 2013: 53 ff.). SPD sowie insbesondere Grüne und Linkspartei treten dagegen für stärkere gesetzliche Regelungen bzw. Schutzmaßnahmen ein und benennen dabei vor allem auch die Risiken einer zunehmenden Digitalisierung in der Gesellschaft wie den sukzessiven Verlust von Privatheit (SPD 2013: 62; Bündnis 90/Die Grünen 2013: 188 f., 194 ff.; Die Linke 2013: 82 ff.; vgl. Baumann 2013).

Hinsichtlich des Konflikts zwischen Datenschutz und sicherheitspolitischen Interessen verschieben sich die Fronten: Obwohl im Nachgang der Snowden-Enthüllungen sowohl CDU/CSU (2013: 71) als auch SPD (2013: 100) den Begriff der Vorratsdatenspeicherung in ihren Wahlprogrammen meiden, halten beide Parteien die Speicherung von Verbindungsdaten zum Zweck der Verfolgung schwerer Straftaten nach Strafprozess-

ordnung (§ 100a StPO) generell für notwendig.[31] [32] Grüne, FDP und die Linke lehnen diese dagegen dezidiert ab (Bender et al. 2015: 177 ff.).

Diese parteipolitisch spezifischen Ausrichtungen zum Thema Datenschutz spiegeln sich ebenfalls auf EU-Ebene wider, wie das Abstimmungsverhalten der Parteien im EU-Parlament zu SWIFT (VoteWatch 2010), PNR (VoteWatch 2011; 2012; 2014a), dem Datenschutzreformpaket und dem Umgang mit dem NSA-Überwachungsskandal (VoteWatch 2013; 2014b; 2014c) zeigt:

Denn ihrem Abstimmungsverhalten nach zu urteilen, treten insbesondere die EU-Parlamentsfraktionen der Grünen (Grüne/EFA) und der Linken (GUE-NGL) für eine allgemeine Stärkung des Datenschutzes ein, während sich die europäischen Sozialdemokraten (S&D) (vor allem in Sicherheitsfragen) und die Allianz der europäischen Liberalen (ALDE) (vor allem im Hinblick auf wirtschaftspolitische Ziele) weniger stark für den Datenschutz engagieren.[33] Die christdemokratisch-konservative (EVP) sowie die konservative und EU-kritische Fraktion (EKR) haben schließlich – bis auf die Zustimmung zum Parlamentsentwurf der DS-GVO – sicherheitspolitischen stets den Vorzug gegenüber bürgerrechtlichen Erwägungen gegeben. Die Fraktion der euroskeptischen und rechtspopulistischen Parteien (EFDD) sowie Vertreter der extremen Rechten[34] zeigen hingegen ein abweichendes Abstimmungsverhalten, das sich in erster Linie gegen europäische Regulierungen im Allgemeinen richtet. So werden gesetzliche Vorhaben zur Ausweitung von Sicherheitsmaßnahmen zwar abgelehnt, doch Gesetze zur Stärkung des Datenschutzes mehrheitlich ebenso.

Die Fronten der unterschiedlichen Priorisierung von Datenschutz verlaufen jedoch auch innerhalb der Parteien selbst: Je nachdem von welchem Politikfeld auf das Thema Datenschutz geblickt wird, kommen unterschiedliche Positionierungen und auch ein abweichendes Abstimmungsverhalten bei einzelnen Abgeordneten zustande.

---

[31] Allerdings ist insbesondere die SPD beim Thema Vorratsdatenspeicherung parteiintern tief gespalten. Während sich vor allem die Parteispitze (wie auch schon zuvor in der Großen Koalition 2005-2009) nahezu geschlossen für eine gesetzliche Neuregelung ausspricht, stimmte nur eine sehr knappe Mehrheit von 58 Prozent der Delegierten auf dem SPD-Parteikonvent im Sommer 2015 für das von Bundesjustizminister Maas eingebrachte Vorhaben (Schulte 2015). Zudem regt sich insbesondere vonseiten der Parteibasis wiederholt Widerstand. So soll eine zweite Auflage eines Mitgliederbegehrens gegen die Vorratsdatenspeicherung (ein solches war bereits im Herbst 2012 wegen mangelnder Beteiligung gescheitert) deren Wiedereinführung doch noch verhindern (Der Tagesspiegel 2015).

[32] Bei der Erklärung des auffällig geringen Stellenwerts von Datenschutz für CDU/CSU und SPD spielt neben der traditionell bedingten, parteipolitischen Ausrichtung (mit einem Fokus auf Wirtschafts- und Sicherheitsthemen) vermutlich auch das innerparteiliche Selbstverständnis, als (ehemalige) Volkspartei führen und politische Verantwortung übernehmen zu wollen und sich dabei zwangsläufig stärker Themen im Kernbereich staatlichen Handelns (sogenannter *high politics* (vgl. Fn. 62)) – also vor allem sicherheitspolitischen Fragestellungen – zu widmen, eine entscheidende Rolle. Dieser politische Führungs- und Regierungsanspruch, der auch immer mit einem gesteigerten Interesse an Macht (u. a. im Sinne der Durchsetzungsfähigkeit auf nationaler und internationaler Ebene) und Machterhalt einhergeht und bei CDU/CSU und SPD besonders stark ausgeprägt zu sein scheint, steht häufig in scharfem Kontrast zur Bereitschaft einer Stärkung von politischen Freiheiten, Bürgerrechten und Datenschutz (vgl. Baumann 2013). Allerdings sind diese Thesen bisher empirisch kaum erforscht, so dass hier insbesondere im Hinblick auf die politikwissenschaftliche Parteienforschung Forschungsbedarf besteht.

[33] Diese Befunde decken sich weitestgehend auch (außer bei S&D und ALDE) mit den Ergebnissen der Analyse parlamentarischer Änderungsanträge zur DS-GVO, kategorisiert nach Fraktionszugehörigkeit und Auswirkungen (Schwächung bzw. Stärkung) auf den Datenschutz (vgl. http://lobbyplag.eu/map/groups (23.08.2015)).

[34] Der französische Front National, Geert Wilders PVV, der belgische Vlaams Belang oder die österreichische FPÖ hatten es bis zum Zeitpunkt der hier diskutierten Abstimmungen nicht geschafft eine eigene Fraktion zu bilden (FAZ 2014b).

3.5 Datenschutzbehörden

Die Datenschutzbeauftragten der Länder und des Bundes sind qua Datenschutzgesetze die zentralen Regulierungsakteure im Datenschutzbereich.[35] Ihnen unterstellt sind sogenannte Datenschutzbehörden. Der BfDI ist dabei ausschließlich für die Kontrolle von öffentlichen Stellen des Bundes (inklusive öffentlich-rechtlicher Wettbewerbsunternehmen) sowie Telekommunikations- und Postdiensteanbietern zuständig, während die LfDs die Verarbeitung personenbezogener Daten jeweiliger öffentlicher (z. B. Landesbehörden) und nichtöffentlicher Stellen (z. B. im Bundesland ansässige Unternehmen) überwachen.[36]

Datenschutzbehörden können verschiedenste Funktionen erfüllen: Sie dienen als Beschwerde- und Kontrollstelle, sind als Gutachter, (Politik-) Berater oder Vermittler tätig und zudem häufig mit einem Bildungsauftrag sowie Mitteln zur Rechtsdurchsetzung ausgestattet (Bennett und Raab 2006: 134; Weichert 2012: 113 ff.). Da sie die Art und Weise, wie mit (personenbezogenen) Daten umgegangen wird, regulieren, kommt ihnen eine in der heutigen Informationsgesellschaft immer wichtiger werdende Aufgabe zu. Aus diesem Grund ist neben einer adäquaten Finanzierung und Ausstattung mit effektiven Regulierungsinstrumenten ihre Unabhängigkeit von zentraler Bedeutung (Roßnagel et al. 2001: 19 f.).

[35] Eine Ausnahme stellt hier insbesondere die nachrichtendienstliche Kontrolle dar, die auf Landesebene von Kontrollgremien der Länderparlamente (mit Ausnahme von Baden-Württemberg) und auf Bundesebene vom Parlamentarischen Kontrollgremium (PKGr) sowie der von ihr ernannten G-10-Kommission ausgeübt wird. Das PKGr setzt sich aus Bundestagsabgeordneten zusammen, die am Anfang jeder Legislaturperiode vom Bundestag gewählt und deren Anzahl vom Bundestag (meist ausgerichtet nach dem Stimmenverhältnis im Bundestag) bestimmt werden. Gemäß Kontrollgremiumgesetz (PKGrG) überwacht das PKGr die Nachrichtendienste des Bundes und verfügt über eine Reihe von Kontrollbefugnissen wie die Möglichkeit der Akteneinsicht, der Befragung von Personen und des Zutritts zu sämtlichen Dienststellen, die allerdings allesamt an die Zustimmung einer Mehrheit der Gremiumsmitglieder gebunden sind. Im Hinblick darauf, dass die Regierungsfraktionen über eine Mehrheit an Mitgliedern im Gremium verfügen und deren Bedürfnis, die eigene Regierung zu schädigen, naturgemäß gering ausgeprägt sein dürfte, bewirkt diese Regelung eine „gesetzlich institutionalisierte Antriebsarmut" des Gremiums (Neskovic 2013). Zudem soll das PKGr durch die Bundesregierung zwar regelmäßig über nachrichtendienstliche Aktivitäten unterrichtet werden, in der Vergangenheit wurden jedoch immer wieder Fälle bekannt, in denen das Kontrollgremium nicht ausreichend informiert wurde oder gar keine Kenntnisse über die später in der Tagespresse zu lesenden nachrichtendienstlichen Aktivitäten hatte (Oswald 2010; Fürstenau 2014). Die G-10-Kommission ist gemäß Artikel-10-Gesetz für die Überprüfung der Zulässigkeit und Notwendigkeit jeglicher nachrichtendienstlicher Überwachungsmaßnahmen im Post- und Fernmeldeverkehr (inklusive Telefon- und Internetüberwachung) zuständig. Die Kommission tagt mindestens einmal pro Monat und wird in gleichem Zeitabstand vom Bundesinnenministerium über nachrichtendienstliche Abhörmaßnahmen unterrichtet. Im Allgemeinen wird immer wieder kritisiert, dass sowohl das PKGr als auch die G-10-Kommission unter chronischer Unterfinanzierung und Personalmangel, unzureichendem Zugang zu relevanten Informationen sowie übertriebenen Geheimhaltungspflichten litten, die einer effektiven demokratischen Kontrolle nachrichtendienstlicher Aktivitäten im Wege ständen (Leisegang 2013a: 133 ff.). Für einen weitergehenden Ländervergleich (USA, Großbritannien und Deutschland) zur demokratischen Kontrolle von Nachrichtendiensten siehe Heumann und Scott (2013).

[36] Nicht zu verwechseln sind BfDI und LfDs mit behördlichen und betrieblichen Datenschutzbeauftragten, die beispielsweise in einer öffentlichen Institution oder einem Unternehmen für die Datenschutzaufsicht zuständig sind und in enger Kooperation und regem Austausch mit der zuständigen Bundes- bzw. Landesdatenschutzbehörde stehen.

Zum einen ist deswegen – ähnlich wie bei Kartellämtern oder staatlichen Zulassungsbehörden – der Einfluss von privatwirtschaftlichen Akteuren zu begrenzen, d. h. das sogenannte *regulatory capture* (Laffont und Tirole 1991; Bó 2006) zu vermeiden. Zum anderen – und dies ist neu aus regulierungstheoretischer Perspektive – muss ebenfalls eine starke Unabhängigkeit von politischen Akteuren garantiert sein (Schütz 2012a; Thomé 2015). Denn BfDI und LfDs üben ihre Datenschutzaufsicht auch gegenüber den politischen Gewalten der Exekutive, Legislative und Judikative aus.[37]

Der EuGH hat in zwei wegweisenden Urteilen (2010, 2012) dieses Erfordernis der „völligen Unabhängigkeit" von Datenschutzbeauftragten und ihren Behörden auf Rechtsgrundlage der EU-Datenschutzrichtlinie Art. 28 (2) bestätigt und konkretisiert (Kamp und Thomé 2012: 301). Allerdings gibt es auch hier einen eklatanten Unterschied zwischen Verfassungsnorm bzw. Rechtsprechung und Verfassungspraxis. So ist zu beobachten, dass es zwar meistens zu keiner formalen Einmischung von politischer Seite in Entscheidungsprozesse der Datenschutzbehörden kommt, sich der politische Einfluss jedoch indirekt z. B. bei der Wahl des Datenschutzbeauftragten (Kandidatenauswahl durch die Bundes- bzw. Landesregierung), Finanzierung und personeller Ausstattung der Datenschutzbehörden sowie rechtlichen Rahmensetzungen, die es Datenschutzbehörden bisher kaum erlaubt haben, mit scharfen Sanktionen gegen (systematische) Datenschutzrechtsverletzungen vorzugehen, manifestiert (Schütz 2012a und 2012c).

Auch der momentane Gesetzentwurf der Bundesregierung zur „Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund durch Errichtung einer obersten Bundesbehörde" wird trotz der administrativen Loslösung des BfDI vom Innenministerium nichts an den vermehrt durch die politische Exekutive vorgenommenen Auswahlverfahren,[38] der chronischen Unterfinanzierung[39] und den fehlenden Sanktionsinstrumenten (auch vieler LfDs) ändern (vgl. Schulzki-Haddouti 2015b).[40] [41]

Trotz dieser durchaus als problematisch zu bezeichnenden Rahmenbedingungen haben sich Datenschutzbehörden in Deutschland auf verschiedenste Art und Weise als wichtige Regulierungsakteure etabliert. Je nach gesetzlich formulierten Befugnissen der Behörden können (unangekündigte) Kontrollen durchgeführt, Verbote der weiteren Datenverarbeitung erwirkt oder Strafzahlungen bei Verstößen veranlasst werden. Neben

[37] Die Unabhängigkeit der Datenschutzbeauftragten von politischer Seite steht in einem Spannungsverhältnis zu Rechenschaftspflichten und Verantwortlichkeiten gegenüber demokratisch legitimierten Institutionen wie dem Parlament (vgl. Schütz 2012b). So muss der BfDI gegenüber dem Bundestag und ein Großteil der LfDs gegenüber dem jeweiligen Länderparlament in Form eines jährlich erscheinenden, öffentlich zugänglichen Tätigkeitsberichtes Rechenschaft ablegen. Zudem wird der BfDI seit 1990 auf Vorschlag der Bundesregierung vom Bundestag gewählt.

[38] Der ehemalige Berliner Datenschutzbeauftragte Hansjürgen Garstka kritisiert dazu, dass so auch weiterhin „die zu kontrollierende Institution – die Bundesexekutive – sich ihren Kontrolleur selbst aussucht", anstelle den BfDI-Kandidaten aus der Mitte des Bundestages benennen zu lassen (Deutscher Bundestag 2014b).

[39] Während beispielsweise im Rahmen des geplanten IT-Sicherheitsgesetzes das Bundesamt für Verfassungsschutz (BfV) mit 55, das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit 133 und das Bundeskriminalamt (BKA) mit 79 neuen Stellen ausgebaut werden sollen (Heise Online 2014), sind trotz massiv gewachsener Herausforderungen in der Post-Snowden Ära lediglich vier zusätzliche Personalstellen für die Bundesdatenschutzbehörde vorgesehen (Denkler 2014; Weichert 2014a).

[40] Zudem wurde vielfach die im Gesetzentwurf vorgesehene Verpflichtung des BfDI, vor dem Tätigen einer Zeugenaussage mit Bezug zum „Kernbereich des Regierungshandelns" (z. B. im NSA-Untersuchungsausschuss) eine Genehmigung der Bundesregierung einholen zu müssen, als höchst problematisch kritisiert (Denkler 2014).

[41] Allerdings sollen Datenschutzbehörden in Zukunft gemäß DS-GVO (Artikel 79 bzw. 79a) bei schwerwiegenden Datenschutzrechtsverstößen drastische Strafzahlungen verhängen können, deren Höchstmaß je nach Verordnungsentwurf von 1.000.000 Euro bzw. zwei Prozent bis 100.000.000 Euro bzw. fünf Prozent des weltweiten Jahresumsatzes eines Unternehmens reichen könnte.

diesen „harten“ Formen der Regulierung kommen verstärkt Beratungen und institutionell eingebettete Konsultationen zum Zuge. Zudem prägen die Datenschutzbeauftragten den öffentlichen Diskurs zum Thema Datenschutz nachhaltig, indem sie regelmäßig in den Medien Stellung zu Vorhaben aus Politik und Wirtschaft beziehen, Aufsätze und Bücher publizieren sowie an öffentlichen Veranstaltungen teilnehmen. Das Selbstverständnis der Beauftragten in der Wahrnehmung ihres Regulierungsauftrages reicht dabei vom rigorosen Verfechter und Hüter eines Grundrechtes bis hin zum pragmatischen Mittler und Kompromissgestalter unterschiedlicher Interessen. Als besonders aktiv und profiliert sind hier das Unabhängige Landeszentrum für Datenschutz (ULD) in Schleswig Holstein, der Berliner und Hamburger Datenschutzbeauftragte sowie der ehemalige BfDI Peter Schaar zu nennen.[42]

Allerdings zeigt sich am Beispiel der umstrittenen Neubesetzung des BfDI im Dezember 2013, wie stark die Qualität der Regulierungs- und Öffentlichkeitsarbeit von einer einzelnen fachkundigen und charismatischen Person an der Spitze einer Datenschutzbehörde abhängen kann.[43] Dieser Umstand unterstreicht ein weiteres Mal die große Relevanz der angesprochenen Auswahlverfahren.

[42] Eine besondere Rolle spielen darüber hinaus die zahlreichen Netzwerke auf regionaler, nationaler (Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Düsseldorfer Kreis, etc.) und internationaler (Article 29 Working Party, Berlin Group, etc.) Ebene. Der rege Wissens- und Erfahrungsaustausch innerhalb dieser Netzwerke stärkt nicht nur die dringend notwendige Fachkompetenz der Mitarbeiter einer Datenschutzbehörde, sondern erhöht ebenfalls den Organisationsgrad und die damit in Verbindung stehende Durchsetzungskraft von Datenschutzpositionen im politischen Prozess. Diese häufig institutionell eingebetteten Netzwerke spielen insbesondere bei datenschutzrelevanten Entscheidungsprozessen auf EU-Ebene eine herausragende Rolle (vgl. Newman 2008).

[43] Die Wahl von Andrea Voßhoff zur BfDI sorgte für einen Aufschrei in der (netz-) politischen Öffentlichkeit, da der ehemaligen CDU-Bundestagsabgeordneten neben fehlender Fachkenntnis auch eine problematische Einstellung zum Thema Datenschutz – abgeleitet durch ihre Zustimmung in den vorangegangenen Legislaturperioden zu Internetsperren, zur Vorratsdatenspeicherung und Online-Durchsuchung – vorgeworfen wurde (Kerkmann 2013; Biermann und Jacobsen 2013). Seit der anfänglichen Kritik scheinen sich die Befürchtungen, sie würde den hohen Erwartungen an das Amt des BfDI nicht gerecht werden, zudem zu bestätigen (Kurz 2014).

4 Einflussreiche Interessenlagen im Datenschutz

Der vorangegangene Überblick zu den zentralen Regulierungsakteuren im Datenschutzbereich hat bereits deutlich gemacht, dass Datenschutzpolitik durchzogen ist von immer wiederkehrenden, teilweise stark konfligierenden Interessen, Positionen, Wahrnehmungen und darauf aufbauenden Handlungsmaximen. In der Praxis verschwimmen zwischen den unterschiedlichen Überzeugungen und Ausrichtungen der Akteure häufig die Grenzen. Allerdings lassen sich idealtypisch drei einflussreiche Interessenlagen (Wirtschafts-, Sicherheits- und Bürgerrechtsinteressen) im Datenschutz voneinander abgrenzen (Busch 2012a: 423 ff.). Im Folgenden sollen diese Interessenbereiche näher beleuchtet werden, um die Regulierungspraxis beim Datenschutz besser nachvollziehen und schließlich einen Beitrag zur Erklärung des unterschiedlichen Akteursverhaltens leisten zu können.

4.1 Ökonomische Interessen

Auf der einen Seite ist davon auszugehen, dass marktnahe Akteure aus Politik und Wirtschaft, die entweder als Unternehmen ein kommerzielles Interesse oder wie im Fall von Wirtschaftsministerien daran anknüpfend wirtschaftspolitische Ziele (wie die häufig damit in Verbindung gebrachte Schaffung von Arbeitsplätzen) verfolgen, für klassisch marktliberale Positionen im Internet, z. B. eine Reduzierung von Transaktionskosten und ein geringes Maß an staatlicher Regulierung, eintreten werden.[44]

Auf der anderen Seite erfüllen Datenschutz und Datensicherheit den Zweck einer vertrauensbildenden Maßnahme zwischen Kunden und Anbietern. Dieses Vertrauensverhältnis ist besonders in der virtuellen Welt, in der es keinen physischen Kontakt mit Verkäufern oder Produkten gibt, zentral für den nachhaltigen Erfolg eines Unternehmens. Allerdings stehen vor allem die im Folgenden skizzierten datenbasierten Geschäftsmodelle in einem starken Spannungsverhältnis zum Datenschutz, da sie häufig im Kern grundlegenden Datenschutzprinzipien sowie dem Konzept der informationellen Selbstbestimmung zuwiderlaufen.

4.1.1 Datenbasierte Geschäftsmodelle

Obwohl Angeboten im Internet eine große Bandbreite von teilweise untereinander komplex verflochtenen Finanzierungsmodellen zugrunde liegt (Schlie et al. 2011), vereint die meisten Dienste- und Produktanbieter das Ziel, die bei der Internetnutzung anfallenden (personenbezogenen) Daten kommerziell für sich nutzbar zu machen (Hess und Schreiner 2012). Der Konsument eines Produktes oder Services und dessen Daten werden somit selbst zum gehandelten Produkt (Callas 2011). Dies kann ein äußerst

[44] Das Internet hat jedoch bereits zu einer enormen Erhöhung der Effizienz von Transaktionen geführt (Zerdick et al. 2001: 155). Einerseits hat eine Minimierung von Transaktionskosten durch das Vorhandensein einer global verfügbaren und preiswerten Infrastruktur stattgefunden, andererseits können Transaktionen sehr schnell, simultan, vollständig automatisiert und zu jeder Zeit abgeschlossen werden. Dies gilt nicht nur für Unternehmen, sondern auch generell für Internetnutzer. So haben sich beispielsweise die Kosten bei einem Wechsel des Diensteanbieters (sogenannte *switching costs*) im Internet um ein Vielfaches reduziert, obwohl Unternehmen durch sogenannte Lock-in-Strategien alles versuchen, die Kunden an ihre Produkte und Services zu gewöhnen bzw. zu binden, um so die Wechselkosten zu erhöhen (ebd.: 162). Vertrauen und der damit in Verbindung stehende Datenschutz sind Faktoren, die solche Wechselkosten zusätzlich erhöhen können (Culnan und Bies 2003: 327).

lukratives Geschäft sein und nimmt in seiner Ausgestaltung verschiedenste Formen an.[45] Während beispielsweise klassische Produkthersteller wie Apple und Microsoft sowie E-Commerce-Unternehmen wie Amazon darauf abzielen, eigene Produkte und Dienste auf Grundlage von personenbezogenen Daten maßgeschneidert für den Kunden anbieten und verbessern zu können, sind werbefinanzierte Diensteanbieter wie Google und Facebook daran interessiert, in Zusammenarbeit mit Online Marketing Agenturen möglichst effektiv – und das heißt vor allem personalisiert – Werbung zu platzieren.[46]

Die Ursprünge werbefinanzierter Online-Inhalte gehen zurück auf das Jahr 1994, als das Online Magazin *HotWired* erstmalig Werbebanner auf seiner Homepage platzierte, die zuvor an AT&T und andere Unternehmen verkauft worden waren (Becker 2002: 63). Online Werbung ist seitdem zu einem stetig wachsenden Markt geworden (BITKOM 2014). Neben dem Umstand, dass diese Werbung heute häufig sehr subtil eingesetzt wird, d. h. sich beispielsweise in Ergebnissen einer Suchabfrage bei Google (Sponsorenlink) oder in News Feeds bei Facebook (Sponsored Stories) versteckt, werden den Nutzern mit Hilfe von Cookies und anderen Profildatenbanken in Echtzeit personalisierte Werbeangebote unterbreitet.[47] Besonders gut funktioniert personalisierte Werbung dann, wenn ein möglichst allumfassendes Bild vom Nutzer gezeichnet werden kann.

Die Nutzungsszenarien großer Datenmengen (Big Data) gehen jedoch noch weit über das Schalten von Werbung hinaus. Mit einer der weltweit größten Bilddatensammlungen von menschlichen Gesichtern in Verbindung mit der massenhaften Unterstützung durch seine Nutzer, den Gesichtern reale Personen zuzuordnen, ist Facebook dazu in der Lage, einen höchst effektiven, selbst lernenden und sich ständig verbessernden Algorithmus zur Gesichtserkennung anbieten zu können (Wolter 2011). Und auch Google hat in der Vergangenheit bereits erfolgreich auf diesem Gebiet gearbeitet (Garfinkel und Rosenberg 2009). Praktische Verwertungsmöglichkeiten ergaben sich jedoch erst Jahre später, als die Videobrille *Google Glass* entwickelt wurde und anfänglich mit einer in der Öffentlichkeit möglichst gut funktionierenden App zur Gesichtserkennung ausgestattet werden sollte.[48]

Big Data ist jedoch weit mehr als nur eine schier unglaubliche Menge an Datensätzen. Zentrales Merkmal von Big Data ist die Kopplung dieser in unterschiedlichen Kontexten erhobenen Datensätze, die einer komplexen Analyse auf statistische Zusammenhänge unterzogen werden (Deutscher Bundestag 2013b; Mayer-Schönberger und Cukier 2013). Mit der Entwicklung darauf aufbauender mathematischer Modelle sollen dann möglichst genaue Aussagen und Prognosen über komplexe Sachverhalte wie menschliche Verhaltensweisen, Börsenkurse oder das Wetter gemacht werden können. Google hat hier bereits vor Jahren unter Beweis gestellt, dass präzise Vorhersagen zum Auftreten von Grippewellen auf Grundlage von quantitativen Analysen bestimmter Suchbe-

[45] Im Folgenden wird vor allem auf US-amerikanische IT-Unternehmen eingegangen, da diese in weiten Teilen die Internetwirtschaft dominieren. Dies sollte allerdings nicht darüber hinwegtäuschen, dass auch ein Großteil der deutschen und europäischen IT-Industrie das Ziel verfolgt, mehr Marktmacht und größere Profite durch massenhaftes Sammeln von personenbezogenen Daten zu generieren.

[46] Obwohl hier in der Praxis die Grenzen verschwimmen, d. h. Google und Facebook vermehrt auch in Geschäftsbereiche von klassisch bezahlten Hard- und Softwarekonzernen (z. B. durch die Übernahme von Motorola, Nest, Oculus Rift oder WhatsApp) vordringen, haben bestimmte durch Pfadabhängigkeit bedingte Kerngeschäftsmodelle der Unternehmen weiterhin Bestand.

[47] Für einen breiten Überblick zum Online-Marketing vgl. Sigler (2010: 159 ff.).

[48] Dass das Thema Gesichtserkennung in Deutschland jedoch ein sensibles ist, zeigt die auf Druck des Hamburger Datenschutzbeauftragten erwirkte vorläufige Einstellung von Facebooks automatischer Gesichtserkennung bei Fotomarkierungsaktionen (Zeit Online 2013) sowie Googles vorläufiger Verzicht auf eine eigene in *Google Glass* standardmäßig integrierte App zur Gesichtserkennung (Schulz 2014).

griffe prinzipiell möglich sind (Ginsberg et al. 2009; Budras 2014), auch wenn sich in einigen Fällen verschiedene Prognosen als falsch erwiesen haben (Butler 2013; Lazer et al. 2014).

Daten- und werbebasierte Geschäftsmodelle sind in den letzten zehn Jahren aber auch deswegen auf dem Vormarsch, weil Konsumenten zum einen immer weniger dazu bereit sind, für bestimmte Online-Services und Produkte wie z. B. Nachrichteninhalte zu zahlen (vgl. Reuters Institute 2014: 55 ff.), und zum anderen erfolgreich mit vermeintlich kostenlosen Angeboten gelockt werden. Dieser Logik folgend finanziert sich beispielsweise ein Großteil der kostenlos angebotenen Apps auf mobilen Endgeräten über das Sammeln, Verarbeiten und Weiterverkaufen von Kontaktdaten aus dem Telefonbuch, Bild-, Audio- und Videodaten, Kalender- und Notizeinträgen, usw. (Stiftung Warentest 2012; GPEN 2014; Barczok 2014).[49] Der Handel mit personenbezogenen Daten hat mit der Einführung von Tablets und Smartphones, die technisch durch eine Vielzahl von neuartigen Sensoren in Verbindung mit fehlenden Kontrollmöglichkeiten der Nutzer über ihre Daten gekennzeichnet sind, zudem eine neue Dimension erreicht (Biermann und Polke-Majewski 2014).

Allerdings steht der steigenden Relevanz datenbasierter Geschäftsmodelle ein in seinen Grundzügen vergleichsweise restriktiv konzipiertes europäisches und deutsches Datenschutzrecht gegenüber. Denn generell gilt rechtlich zunächst einmal, dass jedwede Erhebung und Verarbeitung personenbezogener Daten nur auf Grundlage eines Gesetzes oder der Einwilligung durch die Person, deren Daten erhoben werden sollen, stattfinden darf (BDSG Art. 4 (1)).[50] Und auch dann müssen zentrale Prinzipien wie Zweckbindung und Datensparsamkeit erfüllt sein (Tinnefeld et al 2012: 237 ff.). Zudem besteht EU-weit das bereits erwähnte generelle Verbot eines Transfers von personenbezogenen Daten in Drittstaaten, die keine vergleichbaren Datenschutzstandards haben. Davon sind insbesondere US-amerikanische Anbieter betroffen, denen der Datenaustausch jedoch über das umstrittene *Safe-Harbor*-Abkommen bis vor kurzem gestattet war (vgl. Abschnitt 2).

Einige dieser Datenschutzprinzipien widersprechen allerdings auf fundamentale Art und Weise der Geschäftslogik der aufstrebenden *data-driven economy*. Im Fall von Big Data wird beispielsweise das Konzept der Zweckbindung systematisch untergraben, da die zentrale Idee hinter dem Anhäufen und Analysieren riesiger Datenmengen genau darin besteht, „Daten nicht nur viele Male für denselben […], sondern auch für viele unterschiedliche Zwecke [zu nutzen]" (Mayer-Schönberger und Cukier 2013: 129). Dabei sind es oftmals erst Big Data-Analysen selbst, die neue Nutzungsmöglichkeiten personenbezogener Daten vor allem aufgrund statistischer Zusammenhänge entstehen lassen.[51] Aber auch andere Unternehmen, die ihre Angebote – sei es Werbung, E-Commerce oder der Verkauf konventioneller Waren und Dienstleistungen – auf Grundlage von personenbezogenen Daten optimieren wollen oder sogar langfristig andere

[49] Mittlerweile gibt es jedoch auch Möglichkeiten, die Zugriffsberechtigungen von Apps auf mobilen Endgeräten (beispielsweise bei iOS) einzuschränken, was jedoch keinen Effekt auf die Zugriffsrechte der Betriebssystemhersteller hat.

[50] Diese datenschutzrechtliche Grundregel wird auch als *Verbot mit Erlaubnisvorbehalt* bezeichnet (vgl. Tinnefeld et al 2012: 235 und kritisch zur Terminologie Sokol und Scholz 2014: 450 f.).

[51] In der Vergangenheit waren es in Deutschland vor allem Statistikämter, die umfangreiche personenbezogene Daten erhoben und verarbeitet haben, dies jedoch im Gegensatz zu heutigen Big Data-Unternehmen immer auf gesetzlicher Grundlage, einem der zentralen Ausnahmetatbestände im Datenschutzrecht. Die statistische Erhebung von Daten in Verbindung mit daraus ableitbaren Erkenntnissen über einzelne Personen kann jedoch grundsätzlich zu Recht als „blinder Fleck" des deutschen und europäischen Datenschutzrechtes bezeichnet werden (Lewinski 2014: 59).

Verwertungsideen für die gesammelten Daten haben, stoßen immer wieder an datenschutzrechtliche Grenzen.

Auf der einen Seite werden die gesetzlichen Regeln zum Datenschutz deswegen aus ökonomischer Sicht und insbesondere von Seiten der auf Daten angewiesenen Wirtschaft kritisch und mittlerweile sogar als Handelshemmnis betrachtet (Hughes 2014).[52] Diese Wahrnehmung und die mit aller Macht gewollte Durchsetzung darauf beruhender Interessen trat wie nie zuvor im Kontext der in Abschnitt 2 geschilderten Verhandlungen zur DS-GVO zutage.[53]

Auf der anderen Seite sind die IT-Branche und insbesondere service-orientierte Internetunternehmen wie Facebook und Google, die ihren Nutzern keinen materiellen Gegenwert, sondern ausschließlich immaterielle Güter zur Verfügung stellen, stark vom Vertrauen ihrer Konsumenten abhängig. Dieses Vertrauen, das ohnehin schon durch etliche Datenskandale und Privatheitseingriffe in den letzten Jahren in Mitleidenschaft gezogen wurde, ist mit dem Bekanntwerden der aktuellen NSA-Spähaffäre auf einem Tiefpunkt angelangt.[54] Und so werden verstärkt Fragen nach alternativen IT Produkten und Diensten, die auf *Privacy by Design*, also der standardmäßigen Integration datenschutzfreundlicher Technologien, setzen (vgl. Rost und Bock 2011, Cavoukian 2012), lauter. Diese Technologien (sogenannte *Privacy-Enhancing Technologies* (PETs)) (vgl. Borking et al. 1995; London Economics 2010) verzichten nicht nur – wenn möglich – auf die Erhebung, Speicherung und Auswertung personenbezogener Daten, sondern es kommen vermehrt auch Verschlüsselungs- und Anonymisierungstechniken zum Einsatz, die den Nutzer vor Privatheitseingriffen Dritter (z. B. Hackern), aber auch rechtlich legitimierter Akteure (wie kommerzieller Anbieter oder staatlicher Sicherheitsorgane) schützen sollen.

4.1.2 Datenschutzgeschäftsmodelle

Im Gegensatz zum florierenden Geschäft mit personenbezogenen Daten im Internet fristen Anbieter von PETs und Datenschutztechnologien häufig ein Nischendasein. Schlecht funktionierende Geschäftsmodelle, fehlende Monetarisierung (und somit die Abhängigkeit von Spenden oder ehrenamtlichem Engagement), geringer Bekanntheitsgrad und/oder komplizierte Handhabung der Dienste/Produkte sind einige der vielschichtigen Gründe hierfür. Fehlende Nachfrage oder das Desinteresse der Internetnutzer an einem effektiven Schutz ihrer Daten gehören jedenfalls nicht zu diesen Ursachen, wie bereits zahlreiche empirische Forschungsarbeiten aus der Verhaltensökonomik (z. B. Spiekermann et al. 2001 sowie Acquisti und Grossklags 2007) belegen. Aller-

[52] Juristisch von einem (nichttarifären) Handelshemmnis in Bezug auf Datenschutz zu sprechen, ist jedoch höchst problematisch (vgl. Dix 2013: 8 f.; Weichert 2014b: 850) und wird in der Diskussion um das momentan in Verhandlungen stehende transatlantische Freihandelsabkommen *Transatlantic Trade and Investment Partnership* (TTIP) politisch instrumentalisiert.

[53] Nach Bekanntwerden von PRISM und Tempora kam es jedoch zu teils gewaltigen Zerwürfnissen zwischen den in Deutschland vertretenen IT-Konzernen. Insbesondere der IKT-Branchenverband BITKOM war geprägt durch einen hinter den Kulissen tobenden Richtungs- und Machtkampf, der tiefe Gräben zwischen deutschen und ebenfalls im BITKOM repräsentierten US-amerikanischen Unternehmen entstehen ließ (Berke 2014). Die Deutsche Telekom und andere deutsche IT Konzerne strebten einen Strategiewechsel an, indem sie versuchten, aus den Snowden-Enthüllungen Profit zu schlagen. So wurden beispielsweise Möglichkeiten des sogenannten *Schengen-Routing*, d. h. Datenpakete werden nur noch über innereuropäische Server gesendet, diskutiert (Clauß 2014) oder die Initiative *E-mail made in Germany* ins Leben gerufen (Zivadinovic 2014; Kiometzis 2014).

[54] Während beispielsweise die Forschungsgruppe *Information Technology & Innovation Foundation* allein für die amerikanische Cloud Computing Industrie einen durch den NSA-Spähskandal hervorgerufenen Schaden von 22 bis 35 Milliarden US-Dollar berechnete (Castro 2013), kommt eine Studie von *Forrester Research* sogar auf eine Summe von 180 Milliarden US-Dollar (Staten 2013).

dings steht der häufig geäußerten Sorge um den Verlust von Privatsphäre ein oft widersprüchliches Verhalten in der alltäglichen Nutzung von datenbasierten Diensten gegenüber (ebd.). Dieses Phänomen ist auch als *Privacy Paradox* bekannt geworden (vgl. Barnes 2006; Acquisti 2010: 6). Obwohl anzunehmen ist, dass das *Privacy Paradox* auch nach einschneidenden Ereignissen wie den Snowden-Enthüllungen in weiten Teilen der Gesellschaft relativ stabil bleiben wird, könnte der NSA-Skandal und die damit verstärkte tiefe Vertrauenskrise in Politik und Wirtschaft langfristig zu einem Paradigmenwechsel im IKT-Sektor führen. Denn in Deutschland hat sich nicht nur eine Bereitschaft, für die Gewährleistung von Datenschutz zu zahlen, entwickelt (DIVSI 2014: 14), es sind auch erste Erfolgsgeschichten von auf Datenschutz als zentrales Verkaufsargument setzenden Unternehmen, die sich am Markt behaupten können, entstanden.

Als beispielsweise WhatsApp von Facebook im Februar 2013 für 19 Milliarden US-Dollar übernommen wurde, führte das in Deutschland zu einer Welle von Anbieterwechseln (Hänßler 2014). So verdoppelte der auf Ende-zu-Ende-Verschlüsselung zurückgreifende und somit als sicher geltende Schweizer Instant Messaging Dienst Threema innerhalb von 24 Stunden seine Nutzerzahlen auf 400.000 Nutzer (Tanriverdi 2014) und konnte diese bis Sommer 2015 auf 3,5 Millionen Nutzer ausbauen (Iseli 2015).[55] Der ebenfalls auf Verschlüsselung setzende deutsche Emailanbieter Posteo konnte seine Nutzerzahlen innerhalb kürzester Zeit nach dem NSA-Spähskandal sogar verdreifachen (Buess 2014) – obwohl hier die Gesamtzahl von 100.000 Nutzern deutlich geringer ausfällt als bei Threema – und einem Hamburger Start-up namens Protonet, das einen sicheren, durch den Nutzer vollständig selbst kontrollierten Mini-Server für Zuhause anbietet, gelang es im Sommer 2014 mit einer mittels Crowdfunding eingeworbenen Summe von 1,5 Millionen Euro in nur 10 Stunden einen neuen Weltrekord aufzustellen (Welt Online 2014).[56]

Es scheint, als ob hier nach und nach ein Markt für „bewusste" Internetnutzer entsteht (vgl. Simonite 2014), der in Zukunft ähnlich erfolgreich sein könnte wie die heutige Bio-, Öko- oder erneuerbare Energien-Branche. Anerkannte Prüfverfahren und Datenschutzsiegel wie das Datenschutz-Gütesiegel vom ULD oder das *European Privacy Seal* von EuroPriSe existieren bereits, ganz zu schweigen von für auf Datenschutz setzende Unternehmen vorteilhaften rechtlichen und gesellschaftlichen Rahmenbedingungen (Bock 2012: 313 ff.).

Insbesondere für deutsche und europäische Unternehmen könnte diese Situation ein enormes Potential, sich im hart umkämpften und zugleich höchst dynamischen IT Markt von der übermächtigen amerikanischen Konkurrenz abzuheben, beinhalten (Hofer 2014). Diese wiederum beginnt zusehends eigene mehr und weniger ernst gemeinte Vorkehrungen zumindest gegenüber nachrichtendienstlicher Überwachung vorzunehmen, um weltweit zerstörtes Vertrauen in ihre Produkte und Dienstleistungen zu-

[55] Ein weiteres Beispiel ist die vom Verschlüsselungsexperten und Erfinder des Verschlüsselungsstandards PGP (Pretty Good Privacy) Phil Zimmermann mit gegründete Firma Silent Circle (mit Sitz in der Schweiz), die zusammen mit dem spanischen Smartphonehersteller Geeksphone ein abhörsicheres Smartphone entwickelt und auf den Markt gebracht hat (Hamann 2014). Das sogenannte *Blackphone* war im ersten Jahr seiner Einführung 2014 nach bereits wenigen Wochen ausverkauft (Steier 2014) und auch das Nachfolgemodell im Jahr 2015 erfreut sich größter Beliebtheit. Da vor allem auch Unternehmen zu den Kunden von Silent Circle gehören, stellt der *business-to-business*-Bereich mittlerweile den umsatzstärksten und gewinnträchtigsten Geschäftsbereich dar (Kühl 2015), womit insbesondere Herstellern wie BlackBerry Konkurrenz gemacht wird.

[56] Allerdings wirft der Erfolg dieser Unternehmen und ihren zumeist kostenpflichtigen Angeboten Fragen im Hinblick auf die grundrechtliche Gewährleistung von Datenschutz auf und birgt die Gefahr einer weiteren Verschärfung des sogenannten *Privacy Divide*, einen in Anlehnung an den *Digital Divide* (vgl. Marr 2005: 22 ff.) entstandenen Begriff, der die Unterschiede im Zugang zu digitaler Sicherheitstechnik aufgrund von sozio-ökonomischen Faktoren und technischem Know-how problematisiert (vgl. Stevens et al. 2014: 543).

rückzugewinnen.[57] Allerdings hat dies zwei Haken: Zum einen unterliegen diese Unternehmen einem Interessenkonflikt, der mit dem Grad der finanziellen Abhängigkeit von datenbasierten Geschäftsmodellen zunimmt; zum anderen sind in den USA ansässige Unternehmen (also auch deutsche) gemäß USA PATRIOT Act und *Communications Assistance for Law Enforcement Act* (CALEA) dazu verpflichtet, Strafermittlungs- und Nachrichtendienstbehörden weitreichenden Zugriff auf Daten ihrer inländischen, also auf US-amerikanischem Hoheitsgebiet befindlichen, als auch – und das ist neu – im Ausland stehenden Server zu gewähren (vgl. Karaboga et al. 2014: 7). Obwohl der Zugriff US-amerikanischer Sicherheitsbehörden auf in der EU gespeicherte personenbezogene Daten ohne spezielle Rechtsgrundlage im Widerspruch zu europäischem und deutschem Datenschutzrecht steht, wurde dieses Vorgehen erst kürzlich durch ein US-Bezirksgericht bestätigt (U.S. District Court 2014; Gibbs 2014).[58]

Während das Verlangen staatlicher Sicherheitsbehörden, umfangreichen Zugriff auf privatwirtschaftlich kontrollierte Daten zu erhalten, häufig auf wenig Gegenliebe vonseiten der bisher diskutierten IKT-Unternehmen stößt,[59] zeigt sich beim sogenannten sicherheitsindustriellen Komplex eine große Konvergenz von eben jenen Wirtschafts- und Sicherheitsinteressen (Monroy 2009; Rodrigues 2015).[60] Im Internet ist diese Konvergenz vor allem zwischen einer neuen Form von Cybersicherheitsunternehmen, die sich auf den Verkauf von Spionage- und Datenanalysesoftware spezialisiert haben, und sicherheitspolitischen Akteuren wie dem Bundeskriminalamt (BKA) oder dem BND zu beobachten. Konkrete Projekte waren hier die Entwicklung verschiedener Trojanerprogramme (vgl. Abschnitt 3.3) oder auch die Nutzbarmachung von IT-Sicherheitsschwachstellen, sogenannten *Zero Day Exploits* (Hayes 2009; Talbot 2011).

[57] Im Gegensatz zu Google hat Apple mittlerweile bei seinem Kurznachrichten-Dienst iMessage eine starke Ende-zu-Ende-Verschlüsselung eingeführt (Schmidt 2014), und auch WhatsApp reagierte nach anhaltender Kritik: In Zusammenarbeit mit den Entwicklern von TextSecure, einem von Datensicherheitsexperten hoch geschätzten, verschlüsselten Messenger-Dienst, soll WhatsApp dieselbe Form von Verschlüsselung erhalten (Greenberg 2014), deren Implementierung im Praxistest allerdings gravierende Mängel attestiert wurden (Scherschel 2015).

[58] Dies steht im Gegensatz zur weitverbreiteten Meinung, dass die Nutzung von Servern US-amerikanischer Unternehmen, die sich im Ausland befinden, vor Überwachung durch US-amerikanische Behörden schützen könnte. Bei Weigerung der Zugriffserteilung durch das Unternehmen drohen massive strafrechtliche Konsequenzen durch die Behörden, wie der Fall des auf Ende-zu-Ende-Verschlüsselung setzenden und von Snowden genutzten Emailanbieters Lavabit gezeigt hat (Greenwald 2013b; Greis 2013; Levison 2014). Und auch deutsche Unternehmen, die auf dem US-amerikanischen Markt aktiv sind, laufen Gefahr, dass bei Zuwiderhandeln Klagen oder Lizenzentzüge gegen sie eingeleitet werden, wie dies 2008 der Schweizer Bank UBS angedroht wurde, die sich zunächst erfolgreich weigerte, vertrauliche Kundendaten an US-amerikanische Finanzbehörden weiterzugeben, bevor sie sich dem Druck fügen musste (NZZ 2009).

[59] Vgl. z. B. die Initiative „Reform Government Surveillance" führender US-amerikanischer IT-Unternehmen (AOL et al. 2014). Vgl. dagegen Zurawski (2014: 17) für eine kritische Perspektive auf das vorgebrachte Argument.

[60] Der Begriff des sicherheitsindustriellen Komplexes lehnt an den von Dwight Eisenhower geprägten Ausdruck eines militärisch-industriellen Komplexes an, der auf das Gefahrenpotential einer Verflechtung von Rüstungsunternehmen, Militär und staatlicher Verwaltung in den USA der 1950er Jahre hinsichtlich der Untergrabung demokratischer Strukturen verweist (vgl. Mills 1956: 199 ff.; Leisegang 2011: 83 f.).

4.2 Sicherheitsinteressen

Die hier beleuchteten zivilen Sicherheitsinteressen werden vorwiegend von Vertretern der Strafermittlungs-, Strafverfolgungs- und Nachrichtendienstbehörden, der zuständigen Innenministerien und der Sicherheitsindustrie verfolgt. Da der Schutz des menschlichen Lebens in den Vordergrund gestellt wird, stehen Strategien und Maßnahmen im Vordergrund, die eine Minimierung von Gefahren und eine Maximierung von Sicherheit zum Ziel haben. Welch hohe Bedeutung Sicherheit dabei beigemessen wird, zeigte sich exemplarisch, als der frühere Bundesinnenminister Friedrich kurz nach den ersten Snowden-Enthüllungen die Überwachungsprogramme mit der Aussage, dass Sicherheit ein „Supergrundrecht" sei, zu rechtfertigen versuchte (Bewarder und Jungholt 2013, Gössner 2010: 880).[61] Andere Aspekte wie wirtschaftspolitische oder bürgerrechtliche Positionen müssen nach dieser Auffassung notwendigerweise in den Hintergrund rücken.[62]

Die Frage nach dem richtigen Verhältnis von Freiheit und Sicherheit ist seit jeher zentraler Bestandteil politikwissenschaftlicher Auseinandersetzungen (vgl. Voigt 2012) und spiegelt ebenfalls eine der zentralen Fragen im Datenschutz wider (Hoffmann-Riem 2014). Im Deutschland der Nachkriegsgeschichte wurde dieses Spannungsverhältnis bereits in den 1970er Jahren durch den Terror der Roten Armee Fraktion sowie die teils unverhältnismäßigen politischen Reaktionen auf die Probe gestellt (vgl. Lepsius 2004: 64).[63] Hatten diese Reaktionen aber noch vergleichsweise geringe globale Auswirkungen, läutete der islamistische Terrorismus Anfang dieses Jahrtausends und der damit einhergehende Schock über die Vulnerabilität westlicher Gesellschaften tiefgreifende Veränderungen internationaler und nationaler Sicherheitspolitiken ein (Busch 2012b).[64]

Allen voran der 11. September 2001 in den USA, aber auch die Anschläge in Madrid 2004 und in London 2005 waren zentrale Auslöser dieses sicherheitspolitischen Para-

[61] Und auch im Fall der im Frühling 2015 aufgenommenen, aber schließlich wieder eingestellten Ermittlungen gegen den Blog Netzpolitik.org wegen des Verdachts auf Landesverrat zeigt sich eben jene unverhältnismäßig starke Priorisierung sicherheitspolitischer Interessen in Kombination mit einer bedenkenswerten Verselbstständigung des Sicherheitsapparates (hier des Bundesamtes für Verfassungsschutz), dessen Kurs jedoch ein Großteil der politischen Exekutive willfährig folgt. Im konkreten Fall war dies die Aufnahme von Ermittlungen durch den damaligen Generalbundesanwalt Harald Range, maßgeblich gebilligt vom Bundeskanzleramt, Innen- und Justizministerium (Gebauer 2015).

[62] Diese besonders in der praktischen Politik immer wieder anzutreffende Wahrnehmung von Wertigkeit und Hierarchie einzelner Politik- und Themenfelder – die in der Politikwissenschaft u. a. durch das Konzept der *high* und *low politics* beschrieben wird (vgl. Hoffmann 1966; Ripsman 2006) – ist ein bisher nur wenig erforschter Aspekt in der Policy-Forschung. Zudem sei an dieser Stelle auf weiteren Forschungsbedarf hinsichtlich des Arguments, dass es sich bei Datenschutz weniger um ein Politikfeld, denn um ein querschnittsartiges Themenfeld handelt, hingewiesen. Hier könnte das jüngst im Zusammenhang mit der Popularität von Netzpolitik gewachsene Interesse der Policy-Forschung an der Entstehung von Politik- und Themenfeldern eine begriffliche und theoretische Präzisierung ermöglichen (vgl. dazu die Schwerpunktbeiträge in *der moderne staat – Zeitschrift für Public Policy, Recht und Management*, Jg. 8, Nr. 1 (2015) zum Thema „Entstehung und Wandel von Politikfeldern").

[63] Damals wie heute äußert sich in den Reaktionen der klassischen Vertreter von Sicherheitsinteressen zugleich auch eine Engführung auf bestimmte Formen des Terrorismus: Während seinerzeit besonders der Linksterrorismus und heutzutage islamistischer Terrorismus im Fokus staatlicher Sicherheitsorgane steht, wird Rechtsterrorismus trotz seiner ungebrochenen Kontinuität und selbst angesichts schwerer Terroranschläge wie dem Oktoberfestattentat 1980 oder dem NSU-Skandal mit nachrichtendienstlicher und behördlicher Verwicklungen selten als ähnlich bedrohlich wahrgenommen (siehe u. a. BpB 2013, Hofmann 2013).

[64] Allein auf EU-Ebene wurden seit dem 11. September 2001 mindestens 239 Gesetze und sonstige politische Maßnahmen – darunter 88 rechtsverbindliche Maßnahmen, z. B. Verordnungen, Richtlinien und Beschlüsse – zur Bekämpfung von Terrorismus verabschiedet (Hayes und Jones 2013: 25).

digmenwechsels auch in Europa. Diesseits und jenseits des Atlantiks waren die Jahre danach von einer Politik der sogenannten „Versicherheitlichung" geprägt, in deren Folge immer mehr Politikbereiche als sicherheitsrelevant angesehen wurden und die vormals getrennten Sphären äußerer, innerer und sozialer Sicherheit in zunehmendem Maße ineinander übergehen ließen (Daase und Deitelhoff 2013: 24). Da sich Datenschutz gegenüber etablierten Politikfeldern als ein Querschnittsthema verhält, war es gleich mehrfach von dieser Entwicklung betroffen. Dazu kommt, dass es die zunehmende Verbreitung von IKT unabdingbar machte, Sicherheitspolitiken auch auf den digitalen Raum auszuweiten.

Während sich die US-amerikanische Regierung im Rahmen ihrer Cybersicherheitspolitik nach 9/11 zunächst vornehmlich auf terroristische, nichtstaatliche Akteure konzentrierte, führte in den Folgejahren eine veränderte Risikobewertung der Gefährdungslage, ausgelöst durch konkurrierende Mächte wie China (vgl. Paul 2015) und Russland, zu einem Strategiewechsel, der die militärische Abschreckung durch den Ausbau digitaler Überwachungs- und Offensivkapazitäten sowie der Androhung ernstzunehmender digitaler Vergeltungsschläge in den Vordergrund rückte (Bendiek 2014: 17; The White House 2011). Die EU propagiert mit ihrer Cybersicherheitspolitik dagegen das Ziel, die Sicherheit von Informationstechnologien zu gewährleisten sowie fundamentale europäische Werte und Rechte zu verteidigen. Der Entwicklung militärischer und nachrichtendienstlicher Kapazitäten sowie der Kriminalitätsbekämpfung wird dabei eine eher untergeordnete Rolle beigemessen (EU-Kommission 2013a).

Die Dominanz von Sicherheitsinteressen äußerte sich im Laufe des vergangenen Jahrzehnts in den Ergebnissen zahlreicher internationaler und auch innenpolitischer Auseinandersetzungen darüber, inwiefern auf personenbezogene Daten zum Zwecke der Gewährleistung von Sicherheit zugegriffen werden darf. Der starke Einfluss sicherheitspolitischer Positionen soll im Folgenden anhand der prominenten Fallbeispiele Fluggast- und Banktransaktionsdatenübermittlung zwischen EU und USA, der Vorratsdatenspeicherung in Deutschland sowie nachrichtendienstlicher Überwachung verdeutlicht werden.

4.2.1 Fluggastdatenübermittlung

Als Folge von 9/11 wurden in den USA verschiedene Gesetze erlassen, die den Zugriff auf national und international erhobene Personendaten kontinuierlich ausweiteten. Mit dem im November 2001 verabschiedeten *Aviation and Transportation Security Act* (U.S. Congress 2001) wurden Fluggesellschaften, die Flüge in, aus oder durch die USA anbieten, dazu verpflichtet, Zugang zu ihren Fluggastdaten – dem sogenannten *Passenger Name Record* (PNR) – zu gewähren.[65] In Verhandlungen mit der EU verlangte das zuständige US-Heimatschutzministerium einen vollständigen Zugriff auf Fluggastdaten bei einem weitgehend unkontrollierten Zugang. Zwar stemmte sich der europäische Verhandlungspartner, die Generaldirektion Binnenmarkt der EU-Kommission, anfangs gegen diese Forderungen, doch wurde dem enormen Druck von US-amerikanischer Seite insbesondere aufgrund der Androhung eines Landeverbots für Flugzeuge aus der EU nachgegeben (Busch 2012a: 418).

So schloss der EU-Ministerrat 2004 ein erstes Fluggastdatenabkommen mit den USA, welches von der EU-Kommission als angemessen im Hinblick auf die EU-Datenschutzrichtlinie eingestuft wurde. Doch das EU-Parlament zog im selben Jahr vor

[65] Ein PNR wird bei jeder Buchung und Durchführung einer Flugreise erstellt und beinhaltet ein Datenset, bestehend aus über dreißig personenbezogenen Merkmalen. Darunter befinden sich neben dem Namen, Kreditkarteninformationen, der Anschrift und ggf. IP-Adresse auch Details über Speisewünsche und den gesundheitlichen Zustand des Reisenden (Busch 2012a: 420 f.).

den EuGH, der das Abkommen 2006 annullierte. Die Gründe für diese Entscheidung waren allerdings weniger inhaltlicher als vielmehr prozeduraler Natur: Demzufolge verfügte der EU-Ministerrat nicht über die Befugnis zum Abschluss des Abkommens und die EU-Kommission nicht über die Kompetenz der Formulierung eines Angemessenheitsbefundes im Rahmen der EU-Datenschutzrichtlinie. Daraufhin wurde der gesamte Sachverhalt aus der vergemeinschafteten ‚ersten Säule' der EU in die ‚dritte Säule' (die intergouvernementale Kooperation in den Bereichen Justiz und Inneres) verlegt. Durch diesen *forum shift* waren anstelle der Generaldirektion Binnenmarkt nun die nationalen Innen- und Justizminister sowie der EU-Justizkommissar für die Verhandlungen zuständig (Busch 2012a: 428 ff., Hummer 2011: 238 ff.).

In Folge dessen handelte der nun zuständige EU-Justizkommissar gemeinsam mit Wolfgang Schäuble, dem damaligen deutschen Bundesinnenminister und amtierenden Präsidenten des Ministerrats, unter Umgehung des Europäischen Parlaments 2007 ein neues Abkommen mit den USA aus, das u. a. aufgrund der Verlängerung der Vorhaltungsdauer der PNR-Daten von 3,5 auf bis zu 15 Jahre als ein weiteres Zugeständnis gegenüber den Wünschen des transatlantischen Verhandlungspartners gewertet wurde (Rötzer 2007). Obwohl der *forum shift* zunächst zu einer Schwächung der Mitwirkungsrechte des EU-Parlaments führte, fand durch das Inkrafttreten des Vertrags von Lissabon 2009 eine faktische Aufwertung der Kompetenzen des Parlaments in diesem Bereich statt.[66] Auf Grundlage der neuen Kompetenzen wurde das erneuerte PNR-Abkommen Mitte 2010 abgelehnt und die Kommission zur Ausarbeitung eines neuen Abkommens unter Einhaltung bestimmter durch das Parlament definierter Mindeststandards aufgefordert (Busch 2012a: 430). Diesem neuen *transatlantischen Abkommen zum Transfer von Flugpassagierdaten* stimmte das EU-Parlament 2012 schließlich mit einfacher Mehrheit zu (VoteWatch Europe 2012).

Verglichen mit der europäischen Position zu Beginn der Verhandlungen gilt das finale Abkommen als ein weitgehendes Entgegenkommen der EU gegenüber den Forderungen der US-Regierung (Krempl 2012). Obwohl die Europäische Union und insbesondere das EU-Parlament anfangs vielfach Datenschutzbedenken äußerten, hatte sich die eher ablehnende Haltung im Laufe der Jahre dermaßen stark gewandelt, dass nicht nur mit weiteren Staaten wie Kanada und Australien PNR-Abkommen geschlossen wurden, sondern die EU-Kommission 2007 sogar eine eigene Initiative für die europäische Fluggastdatensammlung startete (EU-Kommission 2011). Nachdem das EU-Parlament noch im November 2014 in Anbetracht des EuGH-Urteils zur Vorratsdatenspeicherung dafür stimmte, das geplante PNR-Abkommen zwischen Kanada und der EU dem EuGH zur Prüfung vorzulegen, um damit auch eine Signalwirkung in Richtung bestehender Abkommen mit den USA auszusenden (VoteWatch 2014a), signalisierte eine große Mehrheit von EU-Parlamentariern im Februar 2015 – mit dem Verweis auf die Terroranschläge in Paris Anfang desselben Jahres – nunmehr ihre grundsätzliche Zustimmung zu einer innereuropäischen Fluggastdatensammlung (Greis 2015).

4.2.2 Banktransaktionsdatenübermittlung im Rahmen von SWIFT

Noch während der Anfänge der europaweiten Kontroverse um ein PNR-Abkommen mit den USA entbrannte ein weiterer Konflikt, als durch einen Bericht der New York Times im Jahre 2006 bekannt wurde, dass sich die US-Regierung im Rahmen des *Terrorist Finance Tracking Program* (TFTP) Zugriff auf weltweite Finanztransaktionsdaten verschafft hatte (Lichtblau und Risen 2006).

[66] Mit der Einbeziehung der polizeilichen und justiziellen Zusammenarbeit im Rahmen des in Art. 14. EU-Vertrag geregelten ordentlichen Gesetzgebungsverfahrens erhielt das EU-Parlament eine faktische Vetoposition.

Diese werden durch die in Belgien ansässige Genossenschaft *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) mit über 10.000 Finanzinstitutionen in über 200 Ländern als Mitglieder erfasst und elektronisch verarbeitet. Im Rahmen von SWIFT werden sowohl personenbezogene Daten als auch strategisch wertvolle Unternehmensdaten erhoben. Bis 2009 verfügte SWIFT neben einem Rechenzentrum in den Niederlanden über ein weiteres in den USA, auf dem die Daten des niederländischen Servers zum Zwecke der Ausfallsicherheit gespiegelt wurden. Durch eine sogenannte *Subpoena* – eine straf- oder zivilrechtliche Anordnung in den USA, die den Adressaten unter Androhung einer Erzwingungsstrafe zu der Herausgabe bestimmter Informationen oder anderweitiger Kooperation verpflichtet – wurde SWIFT dazu gezwungen, die in den USA gespiegelten Daten an US-Behörden weiterzureichen. Das Bekanntwerden des aus europäischer Sicht illegalen US-Zugriffs auf die Daten führte sowohl auf EU-Ebene (hier insbesondere beim EU-Parlament) als auch bei Wirtschaftsverbänden und Datenschützern zu massiver Kritik (Bonse 2006). Indem SWIFT beschloss, dem *Safe-Harbor*-Abkommen beizutreten und das US-Finanzministerium der europäischen Position insofern entgegenkam, als versichert wurde, dass die Daten ausschließlich zur Terrorbekämpfung verwendet und nach fünf Jahren wieder gelöscht würden, fand die Auseinandersetzung vorerst ein Ende (Busch 2012a: 430).

2009 entschied sich SWIFT jedoch, das in den USA genutzte Rechenzentrum in die Schweiz zu verlagern, wodurch ein neues Abkommen notwendig wurde. Auf Beschluss der EU-Außenminister verabschiedete die EU-Kommission unter vollständiger Missachtung der Bedenken des EU-Parlaments am 30. November 2009 – einen Tag vor Inkrafttreten des Vertrags von Lissabon – ein auf neun Monate angelegtes Interimsabkommen, das jedoch schon zwei Monate später mit großer Mehrheit der EU-Parlamentarier abgelehnt wurde (Hummer 2011: 227 ff.). Im Sommer 2010 stimmte schließlich eine qualifizierte Mehrheit von Liberalen, Christ- und Sozialdemokraten im EU-Parlament für ein neues Abkommen mit teilweise strengeren Auflagen (VoteWatch Europe 2010). Kritiker bemängelten jedoch weiterhin, dass die auf Anfrage zu übermittelnden Daten immer noch zu umfangreich seien, der Rechtsweg für Betroffene schwierig bleibe und mit Europol eine polizeiliche und keine richterliche Stelle über den Datentransfer wachen solle (Krempl 2010, Hummer 2011: 233 ff.).

Nach den Snowden-Enthüllungen und dem Bekanntwerden des mutmaßlichen NSA-Zugriffs auf das SWIFT-Netzwerk kam es in der Folge zu massiver Kritik vonseiten des EU-Parlaments, und selbst EU-Innenkommissarin Cecilia Malmström drohte mit einer Aussetzung des Abkommens (Hecking 2013b). Nachdem das EU-Parlament sich im Rahmen mehrerer Plenarsitzungen mit dem SWIFT-Abkommen auseinandergesetzt hatte, forderte es schließlich im Oktober 2013 dessen Aussetzung (EU-Parlament 2013c). Malmström allerdings lehnte dies letzten Endes unter Verweis auf ausstehende Zusicherungen der US-Seite ab (EU Commission 2013b). Diese Zusicherung wurde im weiteren Verlauf im Rahmen einer Kommissionsmitteilung zur „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“ (EU-Kommission 2013b) Ende November 2013 gemeinsam mit einer Reihe von Berichten zur Effektivität des SWIFT-Abkommens hinsichtlich der Terror-Abwehr bekannt gegeben.[67] Laut der Mitteilung habe es im Ergebnis offizieller Konsultationen eine schriftliche Zusicherung der US-Seite gegeben, der zufolge keine „direkte Datensammlung“ erfolgt sei, mit der gegen das Abkommen verstoßen worden wäre.

Die im Zuge des Aushandlungsprozesses des SWIFT- (aber auch PNR-) Abkommens offensichtlich gewordenen transatlantischen Differenzen im Umgang mit personenbezogenen Daten hatten die EU-Kommission zudem bereits 2010 dazu veranlasst, Ver-

[67] Vgl. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0843:FIN:EN:PDF (11.09.2015).

handlungen über ein Datenschutzabkommen (dem gegenwärtig diskutierten sogenannten *Umbrella Agreement*) aufzunehmen (EU-Kommission 2010).[68]

4.2.3 Die Vorratsdatenspeicherung in Deutschland

In Deutschland wurde die gesellschaftliche Debatte um Versicherheitlichung von keinem anderen Regierungsvorhaben so geprägt wie von der Vorratsdatenspeicherung, also der auf Vorrat (mit einer bestimmten Speicherfrist belegten) beim Provider gespeicherten Telekommunikationsverbindungsdaten (auch Verkehrsdaten genannt), die u. a. Informationen über den in Anspruch genommenen Telekommunikationsdienst, die Nummer oder Kennung der beteiligten Anschlüsse (z. B. Telefon- und Faxnummern sowie IP-Adressen), eventuelle Standortdaten (z. B. bei Smartphones), Beginn und das Ende der jeweiligen Verbindung sowie die übermittelten Datenmengen beinhalten (vgl. § 96 TKG).

Nachdem die EU im Jahre 2006 auf Druck Großbritanniens und in Folge der Madrider und Londoner Anschläge eine Richtlinie über die Vorratsspeicherung von Daten verabschiedet hatte (Europäische Union 2006), setzte die Große Koalition diese mit Unterstützung des BKA ein Jahr später in nationales Recht um. Mit einer gesetzlichen Einbettung der Vorratsdatenspeicherung in das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (2007) wurden Internet Service Provider (ISPs) und Telefonnetzanbieter dazu verpflichtet, die Verbindungsdaten von Kunden für einen Zeitraum von sechs Monaten zu speichern und diese bei Vorliegen einer richterlichen Anordnung Strafverfolgungsbehörden zur Bekämpfung schwerer Verbrechen und von Terrorismus zur Verfügung zu stellen (Fritz 2013: 136 ff.).

Kritiker der Vorratsdatenspeicherung bemängelten vor allem deren unzureichende Verhältnismäßigkeit und Effektivität, mahnten zudem aber auch das große Missbrauchspotential und den Umstand an, dass alle Bürger unter Generalverdacht gestellt würden (Meister 2008). Das Festhalten der Regierung an der Vorratsdatenspeicherung führte daraufhin zu den wohl größten Protesten gegen staatliche Überwachung seit dem Volkszählungsurteil von 1983 (vgl. Abschnitt 4.3.1). Flankiert wurden die Bemühungen der Kritiker durch mehrere Verfassungsbeschwerden. Schließlich erklärte das BVerfG 2010 die gesetzliche Grundlage zur Vorratsdatenspeicherung für verfassungswidrig (insbesondere nicht vereinbar mit dem Telekommunikationsgeheimnis aus Art. 10 (1) GG) und somit ungültig (BVerfG 2010). Allerdings wurde nur der konkreten gesetzlichen Grundlage und nicht dem Instrument der Vorratsdatenspeicherung im Allgemeinen eine Absage erteilt, so dass die Tür für eine neue, verfassungskonforme Gesetzesregelung offen blieb, wenngleich hohe Hürden für diese formuliert wurden: *Erstens* unterliegt die Datensicherheit besonders hohen technischen Standards, *zweitens* darf der Zugriff auf die Daten ausschließlich für überragend wichtige Aufgaben des Rechtsgüterschutzes erfolgen und *drittens* muss der Gesetzgeber hinreichende Vorkehrungen zur Transparenz der Datenverwendung sowie zur Gewährleistung eines effektiven Rechtsschutzes treffen (Papier 2012: 72 f.). Die Entscheidung des BVerfG wurde zudem im April 2014 durch den EuGH insofern bestätigt, als auch die EU-Richtlinie über die Vorratsspeicherung von Daten wegen des Verstoßes gegen europäische Grundrechte – hier insbesondere Art. 7 (Achtung des Privat- und Familienlebens)

[68] Das *Umbrella Agreement*, dem aktuell der US-Kongress und formell der EU-Rat sowie EU-Parlament noch zustimmen müssen, soll gemeinsame Datenschutzstandards im Datenaustausch zwischen US- und EU-Justizbehörden schaffen und europäischen Bürgern vereinzelte Rechte wie das Klagerecht vor US-Gerichten im Falle eines Missbrauchs ihrer Daten einräumen (EU Commission 2015).

und Art. 8 (Schutz personenbezogener Daten) EU-Grundrechte-Charta – für verfassungswidrig und somit nichtig erklärt wurde (EuGH 2014a).

Nachdem eine erneute Einführung der Vorratsdatenspeicherung immer wieder auf Widerstand gestoßen war (vgl. Abschnitt 3.4), gelang es deren Befürwortern in Deutschland schließlich, erst durch die Anschläge von Paris im Januar 2015 beflügelt, eine politische Mehrheit auf sich zu vereinen.

4.2.4 Nachrichtendienstliche Überwachung

Der hohe politische Stellenwert von Sicherheitsinteressen zeigt sich besonders in der umfangreichen Befähigung von Nachrichtendiensten zur Massenüberwachung elektronischer Kommunikation. In den USA wird der kontinuierliche Ausbau nachrichtendienstlicher Arbeit im Rahmen einer effektiven Umsetzung der Cybersicherheitspolitik als essentiell angesehen (Gellmann und Miller 2013). Eine Vielzahl von unterschiedlichen Programmen kommt dabei zur Anwendung, um dem Ziel, über die Daten von *jedermann*, *jederzeit* und *überall* verfügen zu können, Schritt für Schritt näher zu kommen (Risen und Poitras 2013). Als Spitze des Eisbergs entpuppten sich dabei die Überwachungsprogramme PRISM und Tempora: Während PRISM Aufschluss über die enge Kooperation der NSA mit amerikanischen IT Unternehmen wie Apple und Google gab und somit verdeutlichte, dass die Grenzen zwischen privatwirtschaftlicher Datenerhebung und staatlicher Nachrichtendienstüberwachung verschwimmen (The Washington Post 2013), verwies Tempora – ein Überwachungsprogramm in Kooperation mit dem britischen Nachrichtendienst *Government Communications Headquarter* (GCHQ) – auf die technische Machbarkeit eines kompletten Abschöpfens der Verkehrs- und Inhaltsdaten durch das Anzapfen von Internetknotenpunkten und transatlantischen Glasfaserkabeln (MacAskill et al. 2013).[69]

Neben der Zusammenarbeit von NSA und GCHQ findet eine enge Kooperation im Kreis der sogenannten *Five Eyes*, einem nachrichtendienstlichen Bündnis zwischen den USA, Großbritannien, Australien, Kanada und Neuseeland, statt (Cox 2012). Aber auch jenseits der *Five Eyes* ist es gängige Praxis unter NATO-Partnern bzw. militärischen Verbündeten nachrichtendienstliche Informationen regelmäßig auszutauschen und bei Überwachungsaktivitäten zu kooperieren (Appelbaum und Poitras 2013; Becker et al. 2013). Trotz anderslautender Einschätzungen seitens des BND – etwa im Falle der Vereitelung eines Terroranschlags durch die sogenannte Sauerland-Gruppe – deuten die bislang vorliegenden Informationen darauf hin, dass die Zusammenarbeit zwischen NSA und dem für die deutsche Auslandsaufklärung zuständigen BND weniger auf gleichberechtigter Basis als vielmehr auf einer sehr einseitig ausgeprägten Zuarbeit vonseiten des BNDs stattfindet, wie dies bei der Operation Eikonal (Mascolo et al. 2014) oder der Beschaffung von Informationen auf Grundlage von durch die NSA vorgegebenen Suchbegriffen (sogenannten Selektorenlisten) der Fall war (Biermann und Beuth 2015).[70] Hier wird deutlich, dass sicherheitspolitischen Erwägungen, zu denen auch die strategisch wichtige Pflege des transatlantischen Verhältnisses zählt, eine

[69] Obwohl in Umfang und Beweiskraft einzigartig, waren die Snowden-Enthüllungen nicht die ersten ihrer Art. Bereits 1996 wurden erste Details zu einem bis dato einzigartigen, weltumspannenden US-amerikanischen Spionagenetzes namens Echelon bekannt (Hager 1996), das der Überwachung von über Satellit geleiteten Telefonaten, Fax- und Internetverbindungen diente. Dies führte in der Folge zu einer Untersuchung des EU-Parlaments (2001; Dix 2000), deren mediale Aufarbeitung jedoch auch aufgrund der Anschläge vom 11. September 2001 und einem daraus resultierenden Paradigmenwechsel in der Sicherheitspolitik und öffentlichen Sicherheitswahrnehmung weltweit verpuffte.

[70] Zudem wird immer wieder der Vorwurf laut, dass die NSA auch Wirtschaftsspionage in Deutschland betreibe (vgl. Krempl 2015).

weitaus wichtigere Rolle zukommt als dem Schutz deutscher Grundrechtsträger vor anlassloser Überwachung.

Allerdings greift auch der BND selbst auf umstrittene, sich am Rande der Legalität befindende Überwachungspraktiken im Ausland zurück (Spiegel Online 2014b), die sich in den meisten Fällen – wie bei der NSA und dem GCHQ – eher nach politikstrategischen Erfordernissen als nach der Verträglichkeit mit Verfassungen anderer Länder oder mit international verbrieften Menschenrechten richten (Leisegang 2013b; Weichert 2013).

Rechtliche Grundlage für das Wirken deutscher Nachrichtendienste – das sind die Verfassungsschutzbehörde(n) des Bundes und der Länder, der Militärische Abschirmdienst (MAD) und der BND – ist das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel-10-Gesetz).[71] Spezifische Rechtsnormen wie das BND-Gesetz, die Strukturen und konkrete Befugnisse der jeweiligen Nachrichtendienste regeln, schränken jedoch die Anwendung deutschen Datenschutzrechts in diesem Bereich massiv ein. Und auch Strafermittlungsbehörden wie dem BKA oder den Kriminalämtern der Länder (LKAs) sind durch Gesetz umfangreiche Spielräume in der Überwachung von Bürgern gestattet,[72] obwohl hier – anders als bei der nachrichtendienstlichen Überwachung – die Gewaltenteilung durch Richtervorbehalt und die Möglichkeit der gerichtlichen Überprüfung (der Rechtsweg steht dem Betroffenen im Fall von strafrechtlichen Ermittlungen gegen ihn offen) gewährleistet werden soll.

Auf der einen Seite ist das europäische und deutsche Datenschutzrecht hinsichtlich der Kontrolle nachrichtendienstlicher Überwachung deswegen nur sehr eingeschränkt wirksam. Auf der anderen Seite kommt ihm indirekt eine Schlüsselrolle in eben jener Regulierung zu, da – wie PRISM gezeigt hat – ein Großteil der nachrichtendienstlichen Informationen von privaten Anbietern bezogen wird, die bei der Datenerhebung in Deutschland wiederum voll und ganz deutschem und europäischem Datenschutzrecht unterliegen. In diesem Zusammenhang gibt es momentan Versuche, die Weitergabe von in der EU zu kommerziellen und anderen Zwecken erhobenen Daten an Gerichte oder Behörden von Drittstaaten, die über keine eindeutige gesetzliche Grundlage oder internationalen Abkommen mit der EU oder einzelnen Mitgliedsstaaten verfügen, zu untersagen.

[71] Das Artikel-10-Gesetz wurde in Folge der kurz zuvor vorgenommenen verfassungsrechtlichen Einschränkung des Post- und Fernmeldegeheimnisses (Ergänzung des Art. 10 GG um Abs. 2) im Rahmen der Notstandsgesetze im Jahre 1968 verabschiedet. Begleitet von umfangreichen gesellschaftlichen Protesten, die als wichtiger Meilenstein im Entstehungsprozess der sogenannten 68er-Bewegung in Deutschland gelten können, war die Einführung einer Notstandsverfassung in Verbindung mit einer rechtsstaatlichen Regelung zur Post- und Fernmeldeüberwachung Voraussetzung für die Ablösung der alliierten Vorbehaltsrechte (Foschepoth 2012). Obwohl es bereits zuvor Überlegungen einer Ablösung gab (Schäfer 1966), wurden erst mit der Großen Koalition und ihrer notwendigen Zweidrittelmehrheit im Parlament die umstrittenen Grundgesetzänderungen möglich. Von da an galten geheime Verwaltungsvereinbarungen mit den drei Westmächten, die BND und Verfassungsschutz zur Kooperation mit französischen, englischen und US-amerikanischen Nachrichtendiensten verpflichteten (Gutschker und Wehner 2013; Greven 2013; Foschepoth 2014). Die Vereinbarungen mit Großbritannien und den USA wurden erst im August 2013 – wahrscheinlich auch als direkte Reaktion auf die Snowden-Enthüllungen – aufgekündigt (Auswärtiges Amt 2013; Sawall 2013).

[72] Sowohl die Strafprozessordnung (§ 100a StPO) als auch die Polizeigesetze der Länder bzw. des Bundes ermöglichen eine Telekommunikationsüberwachung (TKÜ) von Personen, die im Verdacht stehen, schwerwiegende Straftaten begangen zu haben. Darüber hinaus sind die mittlerweile auf deutscher und europäischer Ebene als verfassungswidrig eingestufte Vorratsdatenspeicherung, die Telekommunikationsüberwachungsverordnung (TKÜV) sowie das höchst umstrittene Instrument der Online-Durchsuchung bzw. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) zu nennen.

So sah beispielsweise die Ende 2011 geleakte Vorversion des Kommissionsentwurfs zur DS-GVO noch eine sogenannte *Anti-FISA-Klausel* (Artikel 42) vor, die eben jene Weitergabe unter Strafe stellte (EU Commission 2011). Auf Druck der US-Administration (Fontanella-Khan 2013b) wurde die Klausel im finalen Kommissionsentwurf allerdings vollständig gestrichen (EU-Kommission 2012a) und erst im Nachgang der Snowden-Enthüllungen durch das EU-Parlament in Artikel 43a wieder aufgenommen (EU-Parlament 2013a). Darüber hinaus ist geplant, massive Strafzahlungen bei besonders schwerwiegenden Datenschutzrechtsverstößen einzuführen, womit Datenschutzbehörden ein effektives Sanktionsinstrument an die Hand gegeben (vgl. Fn. 41) und damit auch der *Anti-Fisa-Klausel* zusätzliche Wirkungskraft verliehen werden würde. Ob und inwieweit diese Bestimmungen am Ende der Trilog-Verhandlungen jedoch Bestand haben werden, bleibt abzuwarten.

Neben der europaweiten Reform des Datenschutzrechts wird seit Bekanntwerden der weltweiten Massenüberwachung und insbesondere des Abhörens führender Politiker Europas verstärkt über eine Reform der Nachrichtendienste selbst diskutiert.[73] Jenseits des im Sommer 2015 verabschiedeten USA FREEDOM Act, der jedoch vor allem den Zugriff der NSA auf Verbindungsdaten innerhalb der USA beschränken soll (Ackerman 2015)[74] und des *Umbrella Agreement*, resultierten diese Diskussionen bislang in keiner tragfähigen nationalen oder auch internationalen Lösung.

In Deutschland wurde die Debatte um eine Reform der Geheimdienste allerdings nicht allein vor dem Hintergrund der NSA-Spähaffäre, sondern insbesondere auch im Lichte des 2011 bekannt gewordenen NSU-Skandals geführt, der sowohl das eklatante Scheitern von Verfassungsschutzämtern und der Polizei als auch deren Verwicklung in die NSU-Mordserie offenkundig machte (vgl. z. B. Förster 2014; Aust et al. 2015). Allerdings führten weder NSA- noch NSU-Skandal bisher zu nennenswerten Reformprozessen in Deutschland: Ganz im Gegenteil wird neben einer besseren Vernetzung der Nachrichtendienste untereinander (bzw. zwischen Polizei und Nachrichtendiensten) und teilweise erweiterten Kompetenzbereichen insbesondere der massive Ausbau personeller und technologischer Kapazitäten vorangetrieben, nicht zuletzt auch um den Rückstand gegenüber konkurrierenden Nachrichtendiensten aufzuholen (Goetz et al. 2014).[75] Demgegenüber steht – ähnlich wie bei den chronisch unterfinanzierten Daten-

[73] Die demokratische Kontrolle von Nachrichten- und Geheimdiensten (für eine begriffliche Differenzierung siehe Gusy 2014) gestaltet sich als grundsätzlich problematisch, da sie im Verborgenen agieren und ihre zumeist der Geheimhaltung unterliegenden Aktivitäten somit in einem strukturellen Spannungsverhältnis zu der notwendigen Schaffung von mehr Transparenz und Öffentlichkeit stehen (Weidemann 2014: 7). Zudem operieren deutsche Nachrichtendienste in der Praxis häufig nicht nur am Rande der Legalität, sie werden dabei bisher auch nur unzureichend von parlamentarischen Organen wie dem PKGr oder der G-10-Kommission kontrolliert (vgl. Fn. 35).

[74] Schon die seit Anfang 2014 angekündigten Vorschläge für eine Reform US-amerikanischer Überwachungspraktiken (Keller et al. 2014) blieben weit hinter den Forderungen der für die Ausarbeitung von Reformvorschlägen zuständigen *President's Review Group on Intelligence and Communications Technologies* (Diersch 2014), des *Privacy and Civil Liberties Oversight Board* (PCLOB) (Medine et al. 2015) sowie den Erwartungen der Zivilgesellschaft (EFF 2014) und der Wirtschaft (AOL et al. 2014) zurück (Rumold und Reitman 2015; Dilanian 2015). Und auch der viel diskutierte und zumeist als umfassende NSA-Reform bezeichnete USA FREEDOM Act entpuppte sich als wenig wirksam bzgl. der Einschränkung nachrichtendienstlicher Aktivitäten in den USA bzw. als gar nicht wirksam hinsichtlich der Auslandsüberwachung von Nicht-US-Bürgern.

[75] Der Ausbau polizeilicher und nachrichtendienstlicher Überwachungskapazitäten wird häufig mit deren Effektivität in der Bekämpfung von Kriminalität und Terrorismus legitimiert. Obwohl die Effektivität sicherheitspolitischer Maßnahmen regelmäßig Gegenstand kontroverser Auseinandersetzungen ist (Kreissl et al. 2015: 151 ff.) und in Frage gestellt wird (Gaycken 2014), finden nur vereinzelt umfassende, unabhängige Untersuchungen zu diesem Thema statt. Bei der Vorratsdatenspeicherung ist dies vor allem eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht (2011), die allerdings aufgrund des

schutzbehörden (vgl. Abschnitt 3.5) – ein geradezu zaghafter personeller Ausbau des PKGr von fünf auf zehn (bis dreizehn) Mitarbeiter (Tretbar 2014). Eine von Bürgerrechtsseite geforderte umfassende Reform der nachrichtendienstlichen Kontrolle, wie etwa Möglichkeiten, die Öffentlichkeit über Missstände zu informieren, bleibt weiterhin aus (Reuter und Stognienko 2014).

4.3 Bürgerrechtsinteressen

Der Schutz von Privatheit und personenbezogenen Daten stellt ein klassisches Bürgerrechtsinteresse dar. Neben den bereits im dritten Abschnitt besprochenen Akteuren findet eine Vertretung dieser Interessen insbesondere durch zivilgesellschaftlich organisierte Bürgerrechtsgruppen statt. Im Folgenden wird sich auf jene zivilgesellschaftlichen Vertreter von Bürgerrechtsinteressen fokussiert, von denen anzunehmen ist, dass sie Überwachung jeglicher Art größtenteils ablehnen und dem Schutz von Persönlichkeitsrechten Vorzug gegenüber Wirtschafts- und Sicherheitsinteressen einräumen.

Obwohl sich auch klassische Menschenrechtsorganisationen wie Amnesty International oder Human Rights Watch mit Datenschutzfragen auseinandersetzen, hat sich in Deutschland insbesondere die netzpolitische Aktivistenszene mit zahlreichen Nichtregierungsorganisationen (NGOs) dieses Themas in den letzten zehn Jahren verstärkt angenommen. Datenschutz ist seither zentraler Bestandteil politischer Aktionen geworden und nimmt innerhalb netzpolitischer Debatten einen prominenten Platz ein (Fritz 2013; Wendelin und Löblich 2013). Doch Fragen der Privatheit und des Datenschutzes beschäftigen Bürgerrechtler schon weitaus länger.

4.3.1 Geschichte des zivilgesellschaftlichen Datenschutzes

Die Bürgerrechtsdebatten um Datenschutz der 1970er und 1980er Jahre fanden besonders vor dem Hintergrund eines Abschwellens der Planungseuphorie des vorangegangenen Jahrzehnts, der Verbreitung von oftmals staatlich betriebenen Großrechnern im Bereich elektronischer Verwaltungsautomation und computergestützter Kriminalistik sowie einer neuen Politik der inneren Sicherheit statt (Berlinghoff 2013: 93). Die für damalige Verhältnisse umfangreichen Möglichkeiten staatlicher Überwachung wurden durch das Bekanntwerden mehrerer Nachrichtendienstaffären gegen Ende der 1970er Jahre (Foschepoth 2012: 235 ff.) und mit der zur Terrorismusbekämpfung 1979 eingeführten Rasterfahndung sichtbar. Zwar fanden die konkreten Datenschutzdebatten der 1970er überwiegend im Kreis von Datenschutzexperten statt (Bieber 2012), doch die von der 68er-Bewegung geäußerte Staatsskepsis und die darin enthaltene Kritik an den massiv in Grundrechte eingreifenden Notstandsgesetzen erfasste weite Teile der Gesellschaft. Befürchtet wurde, dass die neue Datenmacht des Staates schon bald nicht nur gegen RAF-Terroristen und ausländische Agenten, sondern auch gegen sonstige politisch unliebsame Personen – wie dies beim Radikalenerlass von 1972 zum Teil der Fall war – eingesetzt werden könnte (Berlinghoff 2013).[76] Die historischen Erfahrungen mit

Vorwurfs politischer Einflussnahme umstritten ist (Janisch und Käppner 2012). Und auch die Effektivität der Massenüberwachung von Verbindungsdaten durch die NSA zur Terrorbekämpfung wird in einer ersten Studie angezweifelt (Bergen et al. 2014). Da die Wirksamkeit von Überwachungsmaßnahmen nicht nur ein Kernargument in der öffentlichen Debatte um deren Akzeptanz ist, sondern auch in der verfassungsrechtlichen Prüfung der Verhältnismäßigkeit eine zentrale Rolle spielt, kommt der wissenschaftlichen Begutachtung von Effektivität in diesem Kontext eine entscheidende Bedeutung zu. Hier besteht insbesondere aus interdisziplinärer Perspektive verstärkt Forschungsbedarf.

[76] Der auf Vorschlag der Innenministerkonferenz von Bundeskanzler Willy Brandt und den Regierungschefs der Bundesländer verabschiedete Radikalenerlass sah von 1972-76 vor, dass Bewerber für den öffentlichen Dienst einer Gesinnungsüberprüfung unterzogen werden mussten.

dem systematischen und folgenschweren Missbrauch personenbezogener Daten durch das nationalsozialistische Regime nährten zusätzlich die Skepsis gegenüber einer ausschweifenden Datenmacht des Staates (Goos et al. 2015: 58 f.). Ohnehin rückte das „Orwelljahr" 1984 näher und diente als Chiffre für Befürchtungen, die über die Bevölkerung gespeicherten Daten könnten im Falle eines politischen Umsturzes zur Herstellung eines totalen Überwachungsstaates genutzt werden (Busch und Jakobi 2011: 301). Schließlich mündeten diese Ängste in massiven, landesweiten Protesten gegen die geplante Volkszählung von 1983, der Androhung eines Volkszählungsboykotts und mehreren hundert Verfassungsbeschwerden gegen die Volkszählung (Der Spiegel 1983). Aus diesen Verfassungsbeschwerden erwuchs im weiteren Verlauf das wegweisende BVerfG-Urteil, welches das Recht auf informationelle Selbstbestimmung begründete.

Die durch das Urteil gefühlte Stärkung des Datenschutzes, das Ausbleiben der Orwell'schen Dystopie sowie die zunehmende Verbreitung bezahlbarer Personal Computer am Arbeitsplatz und in Privatwohnungen führten jedoch in der Folge zu einer gegenläufigen Tendenz: Die Angst vor den negativen Folgen der Computerisierung wich in Deutschland Ende der 1980er Jahre einer positiven, auf Chancen und Potentiale ausgerichteten Wahrnehmung (Berlinghoff 2013: 106 ff.). Weitere Konfliktpotentiale, z. B. im Rahmen der Internationalisierung der Datenschutzpolitik im Laufe der 1990er Jahre, verblieben auf institutioneller Ebene und konnten keinen vergleichbaren breitenwirksamen Politisierungseffekt entfalten (Bieber 2012: 38 f.).

4.3.2 Zivilgesellschaftlich organisierte Datenschützer

Zivilgesellschaftlich organisierten Datenschützern ist der Schutz der Bürgerrechte im digitalen Informationszeitalter gemein, doch je nach Organisation bestehen hier Unterschiede in der Ausrichtung.[77] So rückt beispielsweise der 1981 gegründete CCC neben der Forderung von Transparenz staatlichen Handelns und entsprechender Infrastrukturen die Informationsfreiheit und ungehinderte Kommunikation in den Vordergrund seiner Arbeit (CCC 2015), während der *Digitalcourage e. V.* (bis Ende 2012 bekannt unter dem Namen *FoeBuD*) seine Arbeit über das Thema Datenschutz hinaus in einen explizit breiteren gesellschaftlichen Kontext stellt, indem er sich auch für Bürger- und Arbeitnehmerrechte sowie Friedensprojekte engagiert (Digitalcourage 2011). Weitere wichtige NGOs sind das 1984 gegründete *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FIfF), die *Deutsche Vereinigung für Datenschutz* (DVD), die *Gesellschaft für Datenschutz und Datensicherheit* (GDD), die stärker aktionistisch ausgerichtete *Aktion Freiheit statt Angst* sowie die 2010 gegründete *Digitale Gesellschaft*.[78] Bezeichnend für einen Großteil dieser zivilgesellschaftlich organisierten

[77] Für eine Auflistung weiterer Organisationen siehe: https://www.forum-privatheit.de/forum-privatheit-de/inhalt/wissenswertes-und-links.php (15.08.2015). Die hier genannten Bürgerrechtsbewegungen sind zudem von sogenannten Cyberutopisten bzw. Cyberliberalen oder auch Cypherpunks zu unterscheiden. Zwar ähneln sich die Ansichten mit Blick auf das Internet als Raum der Freiheit und hinsichtlich informationeller Selbstbestimmung als zentral zu schützendes Gut, doch erfreuen sich im Umfeld der Cyberliberalen vor allem verschiedene Spielarten des Libertarismus und Anarchismus, gepaart mit einem radikalen Individualismus sowie der Ablehnung jeglicher Staatsstrukturen, großer Beliebtheit. Idealtypisch spiegeln sich diese Haltungen in John Perry Barlows (1996) berühmter E-Mail *A Declaration of the Independence of Cyberspace* wider. Bürgerrechtler dagegen weisen eine nicht gänzlich ablehnende, sondern vielmehr ambivalent-distanzierte Haltung gegenüber staatlichen Institutionen auf (Karaboga et al. 2014: 8 f.). Für eine Kritik an cyberliberalen Vorstellungen siehe Horvath 1996, Lovink und Schultz 1996 sowie Fischbach 2009.

[78] Auf europäischer Ebene vereinigt der Dachverband *European Digital Rights* (EDRi) mit Sitz in Brüssel 34 NGOs aus 19 unterschiedlichen europäischen Ländern (EDRi 2014). Neben koordinierten Kampagnen auf nationaler und europäischer Ebene praktiziert EDRi projektweise Kooperationen mit weiteren bekannten

Datenschützer ist zudem deren Distanz zu politischen Parteien, die stets betont wird und sich auch in Auseinandersetzungen mit der häufig ähnliche Interessen vertretenden Piratenpartei widerspiegelt (Fritz 2013: 89; Wendelin und Löblich 2013: 69).[79] Mangels finanzieller Ressourcen ist zudem ein Großteil der genannten NGOs verstärkt auf Spenden und das ehrenamtliche Engagement ihrer Mitglieder angewiesen (Dobusch 2014: 12 f.). [80]

4.3.3 Einfluss von Bürgerrechtsinteressen

Jenseits des mittlerweile als historisch geltenden gesellschaftlichen Widerstands gegen die Volkszählung 1983 zogen zuletzt vor allem die Proteste gegen die Vorratsdatenspeicherung im Rahmen der mittlerweile jährlich stattfindenden „Freiheit statt Angst"-Demonstrationen Aufmerksamkeit auf sich. Zahlreiche Bürgerrechtsorganisationen wie der CCC, DVD, Digitalcourage u. v. m., die sich ein Jahr zuvor unter dem Dach des freien Zusammenschlusses des *Arbeitskreis Vorrat* gesammelt hatten, riefen erstmalig 2006 zu dieser Demonstration für mehr Datenschutz und gegen wachsende staatliche Überwachung auf. Die Demonstrationen mit vielen zehntausenden Teilnehmern und einer begleitenden Unterschriftenkampagne für eine Verfassungsbeschwerde vor dem BVerfG im Jahre 2008 (34.443 Unterschriften) waren nicht nur darin erfolgreich, ein breites Bündnis aus Bürgerrechtsgruppen, der politischen Opposition und bedeutenden Teilen der Internetwirtschaft zu mobilisieren, sie rückten auch das Thema Überwachung und Datenschutz nachhaltig in den medialen Fokus. Obwohl eine verfassungsgerichtliche Aufhebung der Vorratsdatenspeicherung (sowohl in Deutschland als auch auf EU-Ebene) erreicht und eine politische Wiederaufnahme des Vorhabens erschwert werden konnte (vgl. Fritz 2013: 145 ff.), scheiterten zivilgesellschaftlich organisierte Datenschützer letztendlich daran, einen erneuten Gesetzesvorstoß zur Vorratsdatenspeicherung zu verhindern.

Allerdings ist seit den massiven Protesten gegen die Vorratsdatenspeicherung in Verbindung mit den ersten (und seitdem ausbleibenden) Wahlerfolgen der Piratenpartei das generelle Interesse der Politik an netzpolitischen Themen stetig gewachsen. Gefragt sind Vertreter von NGOs wie dem CCC insbesondere aufgrund ihrer technischen Expertise. Sie sind inzwischen nicht nur in Talkshows und anderen öffentlichen Veranstaltungen gerngesehener Gast, sondern nehmen auch regelmäßig an parlamentarischen und parteipolitischen Diskussions- und Beratungsrunden teil (Wendelin und Löblich 2013).

NGOs wie *Privacy International* (PI) aus Großbritannien oder *La Quadrature du Net* aus Frankreich (ebd.: 12).

[79] Seit dem Erfolg sozialer Medien und der daraus neu entfachten gesellschaftlichen Debatte um digitale Privatheit hat neben den einschlägigen Bürgerrechtsorganisationen zudem eine meist unter dem Begriff *Post-Privacy* subsumierte Bewegung eine gewisse, jedoch zeitlich begrenzte Popularität erfahren. Kennzeichnend für Post-Privacy-Positionen sind eine technophile, die positiven Seiten der Digitalisierung hervorhebende Betrachtungsweise des Internet, die für eine radikale, vor allem online praktizierte Offenheit aller Personen (aber auch privatwirtschaftlicher und staatlicher Organisationen) vor dem Hintergrund eines als sinnlos erachteten und ohnehin bereits verloren geglaubten Kampfes um Privatheit eintritt (Heller 2011; Bluhm 2012). Diese Vorstellung eines auch als *Transparenzgesellschaft* bezeichneten Gesellschaftsmodells wurde vielfach kritisiert (Han 2012) und im Angesicht der historisch kontingenten Tendenz zu Monopolbildungen, insbesondere im Medienbereich, auf die damit verbundenen Machtasymmetrien zwischen Politik bzw. Wirtschaft und Zivilgesellschaft in Verbindung mit daraus resultierenden Manipulations- und Kontrollmöglichkeiten hingewiesen (vgl. dazu etwa Goldsmith und Wu 2008; Wu 2012).

[80] So gibt es bei Digitalcourage lediglich fünf und bei Digitale Gesellschaft nur zwei hauptamtlich Beschäftigte. In den übrigen Organisationen beschränken sich die Stellen sogar ausschließlich auf bezahlte Praktika und Werkverträge (Dobusch 2014: 6). Auf EU-Ebene verhält es sich ähnlich (EDRi hat gerade einmal sechs bezahlte Mitarbeiter (EDRi 2014: 26)), während beispielsweise die US-amerikanische *Electronic Frontier Foundation* (EFF) weit über 50 festangestellte Arbeitskräfte beschäftigt (EFF 2015).

Prominente Beispiele sind die Teilnahme von Padeluun (Digitalcourage) auf Vorschlag der FDP, Markus Beckedahl von netzpolitik.org auf Vorschlag der Grünen und Constanze Kurz vom CCC auf Vorschlag der Linken als Sachverständige in der Enquete-Kommission „Internet und digitale Gesellschaft" (Deutscher Bundestag 2013a), die durch das BVerfG veranlasste Beauftragung des CCC mit der Erstellung eines Gutachtens zur Vorratsdatenspeicherung (CCC 2009) oder auch die Stellungnahme von Frank Rieger (CCC) im NSA-Untersuchungsausschuss (Caspari 2014). Mit der institutionellen Einbindung der zivilgesellschaftlich organisierten Datenschützer scheint auch deren Einfluss auf die Politik gewachsen zu sein.[81] Trotz dieses Umstands und damit einhergehender Versuche, das politische Agenda-Setting aktiv mitzugestalten, tun sich erwähnte NGOs stellenweise schwer, alternative Lösungskonzepte zu formulieren, und verharren stattdessen in weitgehendem Protest gegenüber privatwirtschaftlichen und sicherheitspolitischen Akteuren (Dobusch 2014).

Insbesondere die Aufarbeitung der Massenüberwachung durch aus- und inländische Nachrichtendienste hat zivilgesellschaftlich organisierte Datenschützer an ihre Grenze stoßen lassen. Obwohl sich ein Großteil der deutschen Bevölkerung klar gegen Massenüberwachung ausspricht (Pew Research Center 2014), hat es den Anschein, als ob gesellschaftliche Reaktionen und Proteste, anders als das relativ große Interesse der Medien am Überwachungsskandal vermuten lässt, eher verhalten bleiben.[82]

Sowohl die Bestimmung des Ausmaßes der gesellschaftlichen Reaktionen (auf den NSA-Skandal im Besonderen und in Datenschutzfragen im Allgemeinen) als auch die Auseinandersetzung mit möglichen Gründen dafür werfen sozialwissenschaftliche Fragestellungen auf, die bisher allerdings kaum von der Politikwissenschaft und verwandten Fächern beleuchtet wurden und die es im Rahmen künftiger Forschung zu untersuchen gilt.[83]

[81] Zusätzlich haben es zivilgesellschaftlich organisierte Datenschützer in Deutschland erfolgreich verstanden, prominente Fürsprecher in den Medien zu gewinnen bzw. dort zu platzieren, um sich so gegenüber einer breiteren Öffentlichkeit besser Gehör verschaffen zu können. Zu den einflussreichsten Formaten gehören u. a. die Kolumnen von Constanze Kurz (2010) *Aus dem Maschinenraum*, die seit 2010 regelmäßig in der FAZ erscheint, Sascha Lobos Kolumne *S.P.O.N. - Die Mensch Maschine* (seit Anfang 2011 bei Spiegel Online) sowie der von Markus Beckedahl initiierte und mehrfach ausgezeichnete Blog netzpolitik.org.

[82] Neben kleineren deutschlandweiten Kundgebungen mit wenigen Hundert Teilnehmern konnten selbst zu den größeren Demonstrationen lediglich etwa 10.000 Menschen im Juli 2013 (Breuer und Reißmann 2013), etwa 15.000 Menschen zur Teilnahme an der alljährlichen „Freiheit statt Angst"-Demonstration Anfang September 2013 (Reißmann 2013) und Ende August 2014 nur noch etwa 5.000 Teilnehmer mobilisiert werden (Horchert 2014).

[83] Eine erste Auseinandersetzung mit Erklärungsansätzen zu diesem Themenkomplex deutet darauf hin, dass eine Priorisierung anderer, drängenderer Probleme wie z. B. Migration und Arbeitslosigkeit gegenüber Datenschutzfragen erfolgt (Forschungsgruppe Wahlen 2014; Statista 2015), viele Menschen für sich persönlich keine konkreten negativen Auswirkungen durch Überwachung entstehen sehen (Dobusch 2014) und Überwachung digitaler Kommunikation gegenüber analogen Überwachungsformen subtiler und schwerer greifbar stattfindet (Nau 2014). Darüber hinaus betrachten sich überwachte Personen nicht als Eigengruppe, die es gegenüber einer klar benennbaren Fremdgruppe zu schützen gilt, und deren Interessen es dementsprechend an Durchsetzungsfähigkeit mangelt (ebd.).Datenschutz ist zudem nach wie vor ein sehr technisch-elitär geprägtes Themenfeld, das Berührungsängste von nicht technikaffinen Menschen entstehen lässt (Karaboga et al. 2014: 8 ff.). Schließlich fehlen weitestgehend gesamtgesellschaftlich akzeptierte Alternativkonzepte zu kommerziell und politisch geförderten Überwachungsstrukturen, z. B. im Internet, wodurch es häufig zu Fatalismus und einer empfundenen Ausweglosigkeit auf Seiten der Bevölkerung und Techniknutzer kommt.

5
Fazit und Ausblick

Obwohl der deutsche und europäische Datenschutz eine hohe Regulierungsdichte aufweist sowie grundlegende Fragen nach Legitimation von Herrschaft, Machtverteilung und demokratischer Kontrolle aufwirft, hat die Politikwissenschaft bis auf wenige Ausnahmen dieses Thema bislang stiefmütterlich vernachlässigt. Mit ihrem Versuch einen ersten Überblick zum Thema Datenschutz aus politikwissenschaftlicher Perspektive zu liefern, haben die Autoren dieses Aufsatzes deswegen größtenteils wissenschaftliches Neuland betreten.

Mit Blick auf die historische Entwicklung ist Datenschutz nicht mehr nur als reines Abwehrrecht gegenüber staatlichen und privatwirtschaftlichen Akteuren zu verstehen, sondern beinhaltet im Kontext des 1983 geschaffenen Konzeptes der informationellen Selbstbestimmung vielmehr ein Befähigungsrecht zu demokratischer Partizipation, Teilhabe und Wahrnehmung anderer Grundrechte (vgl. Abschnitt 2). Datenschutz ist somit beides: individuell und vor allem gesellschaftlich relevant.

Da IKT und die daran anknüpfende Verarbeitung personenbezogener Daten jedwede Bereiche heutiger Informations- und Wissensgesellschaften durchdringen, liegt das Themenfeld Datenschutz quer zu gesellschaftlichen Teilbereichen wie Zivilgesellschaft, Wirtschaft und Politik. Die Analyse zentraler Regulierungsakteure in der deutschen Datenschutzpolitik hat gezeigt, dass unterschiedliche Sichtweisen und Einstellungen gegenüber Datenschutz, vornehmlich geprägt durch idealtypisch beschriebene, aber in der Praxis häufig verschwimmende Interessenlagen (Sicherheits-, Wirtschafts- und Bürgerrechtsinteressen), existieren, die die Art und Weise, wie Datenschutzregulierung stattfindet, stark beeinflussen.

So agiert die politische Exekutive sowohl auf EU- als auch auf Bundes- und Landesebene häufig ambivalent in Fragen des Datenschutzes, da sich die unterschiedlichen Interessenlagen und Grundüberzeugungen zu Sicherheit, Wirtschaft und Bürgerrechten in den Innen-, Wirtschafts- und Justizministerien mal mehr, mal weniger stark widerspiegeln und aufeinanderprallen (vgl. Abschnitt 3.1). Allerdings kann der Exekutive insgesamt ein starker Hang zur Priorisierung von sicherheitspolitischen Interessen attestiert werden, wie in den Auseinandersetzungen um PNR, SWIFT, Vorratsdatenspeicherung und nachrichtendienstlicher Überwachung deutlich wurde (vgl. Abschnitt 4.2). Wirtschaftspolitische Positionen, die zum Thema Datenschutz ebenfalls ein ambivalentes Verhältnis aufweisen (vgl. Abschnitt 4.1), werden zwar häufig nachrangig, aber immer noch mit einer hohen Priorität verfolgt, während Datenschutzfragen aus Bürgerrechtsperspektive tendenziell weniger Beachtung geschenkt wird.

Obwohl eine ähnliche Priorisierung auf Seiten der Legislative beobachtbar ist, befassen sich Parlamente aufgrund des strukturellen Einbezugs der Opposition und als Teil ihrer Kontrollfunktion gegenüber der Exekutive stärker mit Datenschutzthemen unter Betonung bürgerrechtlicher Aspekte (vgl. Abschnitt 3.2). Diese Beobachtungen hängen jedoch in starkem Maße davon ab, aus welchen Parteien sich Regierung und Opposition zusammensetzen und welche parteipolitischen Präferenzen dominieren. Während die großen Volksparteien CDU/CSU und SPD vor allem sicherheits- und wirtschaftspolitische Erwägungen ins Zentrum ihrer Wahlprogramme und späteren Regierungs- bzw. Oppositionspolitik zu rücken scheinen, stehen FDP (vor allem bzgl. sicherheitspolitischer Themen), Grüne und Linke Bürgerrechts- und Datenschutzfragen generell aufgeschlossener gegenüber (vgl. Abschnitt 3.4).

Insbesondere dem BVerfG kommt als Teil der Judikative eine immer wichtiger werdende Rolle in der Aufrechterhaltung verfassungsrechtlicher Normen zu, indem unverhältnismäßig stark in die informationelle Selbstbestimmung eingreifende Gesetze regelmäßig kassiert und die Bundes- bzw. Landesregierung(en) so in rechtsstaatliche Schranken

verwiesen werden (vgl. Abschnitt 3.3). Aber auch die deutschen Datenschutzbehörden nehmen – schon von Amts wegen – eine den Datenschutz stärkende Position ein. Dabei unterscheiden sie sich jedoch teilweise erheblich in der Wahrnehmung ihres Regulierungsauftrages, ihrer Kommunikationsstrategie (Konsens vs. Konfrontation) und Durchschlagskraft, vor allem bedingt durch den Führungsstil des jeweiligen Datenschutzbeauftragten (vgl. Abschnitt 3.5).

Jenseits dieser Institutionen stellen zivilgesellschaftlich organisierte Datenschützer weitere wichtige Vertreter von Bürgerrechtsinteressen dar (vgl. Abschnitt 4.3). Während allerdings insbesondere das BVerfG und die Datenschutzbehörden in ihren Entscheidungen zum Datenschutz auf ein Abwägen verfassungsrechtlicher Normen bzw. einen Interessenausgleich der beteiligten Akteure hinarbeiten, tendieren zivilgesellschaftlich organisierte Datenschützer dazu, ihre Interessen einseitiger und kompromissloser zu verfolgen.

Die letztendliche Dominanz von Sicherheits- bzw. Wirtschaftsinteressen in der Datenschutzregulierung verweist allerdings nicht bloß auf die Schwäche bürgerrechtlicher Positionen, sondern vielmehr auf ein Bündel gesamtgesellschaftlicher Herausforderungen, denen Datenschutz gegenübersteht (vgl. Fn. 83). Zudem hat Datenschutz schon immer im Kontext rasant fortschreitender technologischer Entwicklungen stattgefunden, die es gesellschaftlichen Prozessen des kollektiven Aushandelns von Normen kaum ermöglichen, Schritt zu halten. Nach der Einführung des PCs, dem Internet-Boom und der Smartphone-Revolution sind es heute vor allem Entwicklungen wie das Internet der Dinge (vgl. Karaboga et al. 2015) und Big Data, die den Datenschutz vor neue Herausforderungen stellen.

Allerdings sind diese weniger technischer als vielmehr sozialer und politischer Natur, wie die aktuellen Diskussionen um eine Reform und bessere Kontrolle von Geheimdiensten, die Verhandlungen zum Transatlantischen Freihandelsabkommen TTIP und zur europäischen DS-GVO zeigen. Hier gilt es demokratisch und transparent eine aus den Fugen geratene Balance zwischen eben jenen Sicherheits-, Wirtschafts- und Bürgerrechtsinteressen wiederherzustellen. Es ist Aufgabe der Politikwissenschaft und anderer Disziplinen, diese Entwicklungen im weiteren Verlauf kritisch zu begleiten.

Literaturverzeichnis

Ackerman, Spencer (2015): „Barack Obama and surveillance reform: a story of vacillation, caution and fear", The Guardian, 03.06.2015, http://www.theguardian.com/us-news/2015/jun/03/barack-obama-surveillance-reform-vacillation-caution-fear (zugegriffen am 19.8.2015).

Acquisti, Alessandro (2010): „The Economics of Personal Data and the Economics of Privacy", Conference: Joint WPISP-WPIE Roundtable, Paris: OECD, http://www.oecd.org/sti/ieconomy/46968784.pdf (zugegriffen am 22.9.2015).

Acquisti, Alessandro und Jens Grossklags (2007): „What can behavioral economics teach us about privacy", in: Acquisti, Alessandro u. a. (Hrsg.): Digital Privacy: Theory, Technologies and Practices, New York: Auerbach Publications, S. 363-377.

Albrecht, Jan Philipp (2013): „Lobbyismus zur EU-Datenschutzreform", Homepage von Jan Phillipp Albrecht, MdEP, http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/lobbyismus-zur-eu-datenschutzreform.html (zugegriffen am 2.9.2014).

--- (2014): Finger weg von unseren Daten, München: Knaur.

AOL u. a. (2014): „Global Government Surveillance Reform", http://reformgovernmentsurveillance.com/ (zugegriffen am 6.3.2015).

Appelbaum, Jacob und Laura Poitras (2013): „Als Zielobjekt markiert. Der Enthüller Edward Snowden über die geheime Macht der NSA", Der Spiegel, 28/2013, S. 22-24, http://www.spiegel.de/spiegel/print/d-102241618.html (22.9.2015).

Aust, Stefan, Per Hinrichs und Dirk Laabs (2015): „Wie nah war der Verfassungsschutz den NSU-Mördern?", Welt Online, 01.03.2015, http://www.welt.de/politik/deutschland/article137918258/Wie-nah-war-der-Verfassungsschutz-den-NSU-Moerdern.html (zugegriffen am 19.8.2015).

Auswärtiges Amt (2013): „Verwaltungsvereinbarungen zum G10-Gesetz mit USA und Großbritannien außer Kraft", http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Meldungen/2013/130802-G10Gesetz.html (zugegriffen am 9.2.2015).

Bacon, Francis (1597): Meditationes Sacrae, 11. Artikel „De Haeresibus". 1. Ausgabe.

BAG (2013): „Urteil vom 20.06.2013", Bundesarbeitsgericht, 2 AZR 546/12, http://www.bag-urteil.com/20-06-2013-2-azr-546-12/ (zugegriffen am 28.1.2015).

Bannas, Günter (2014): „Abhör-Affäre. Opposition klagt in Karlsruhe wegen Snowden-Vernehmung", Frankfurter Allgemeine Zeitung, 26.09.2014, http://www.faz.net/aktuell/politik/abhoer-affaere-opposition-klagt-wegen-snowden-vernehmung-in-karlsruhe-13175658.html (zugegriffen am 26.2.2015).

Barczok, Achim (2014): „Stille Post: Was Android-Geräte nach Hause funken", c't 05/14, S. 82-85, http://www.heise.de/artikel-archiv/ct/2014/05/082_Stille-Post (22.9.2015).

Barlow, John Perry (1996): „A Declaration of the Independence of Cyberspace", https://projects.eff.org/~barlow/Declaration-Final.html (zugegriffen am 22.9.2015).

Barnes, Susan B. (2006): „A privacy paradox: Social networking in the United States", First Monday 11/9, http://firstmonday.org/ojs/index.php/fm/article/view/1394 (zugegriffen am 8.4.2015).

Baum, Gerhart R., Constanze Kurz und Peter Schantz (2013): „Datenschutz. Das vergessene Grundrecht", Frankfurter Allgemeine Zeitung, 26.02.2013, http://www.faz.net/aktuell/feuilleton/debatten/datenschutz-das-vergessene-grundrecht-12095331.html (zugegriffen am 6.2.2015).

Baumann, Max Otto (2013): „Datenschutz im Web 2.0", in: Ackermann, Ulrike (Hrsg.): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter, Frankfurt: Humanities Online, S. 15-52.

Becker, Konrad (Hrsg.) (2002): Die Politik der Infosphäre. World-Information. Org., Schriftenreihe der Bundeszentrale für politische Bildung, Opladen: Leske+ Budrich.

Becker, Sven u. a. (2013): „Obamas Zwerge. Im Skandal um Amerikas Lauschangriff auf den Rest der Welt kuschen Regierungen reihenweise vor Washington. Die Deutschen wollen von nichts gewusst haben – dabei wird jetzt klar, dass die Geheimdienste beider Länder eng kooperieren", Der Spiegel, 28/2013, S. 14-21, http://www.spiegel.de/spiegel/print/d-102241612.html (22.9.2015).

Bender, Steffen u. a. (2015): „Die ideologisch-programmatischen Positionen der Parteien bei der Bundestagswahl 2013: Eine Analyse mit dem Duisburger-Wahl-Index (DWI)", in: Korte, Karl-Rudolf (Hrsg.): Die Bundestagswahl 2013. Analysen der Wahl-, Parteien-, Kommunikations- und Regierungsforschung, Wiesbaden: Springer Fachmedien, S. 165-184.

Bendiek, Annegret (2014): „Tests of partnership. Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection", SWP Research Paper, RP 5, http://mercury.ethz.ch/serviceengine/Files/ISN/177974/ipublicationdocument_singledocument/ae33514a-d88d-4b66-b158-86b0200416b4/en/2014_RP05_bdk.pdf (zugegriffen am 12.10.2014).

Bennett, Colin J (1992): Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Ithaca: Cornell University Press.

Bennett, Colin J. und Charles D. Raab (2006): The Governance of Privacy: Policy Instruments in Global Perspective, 2nd and updated edition, Cambridge Mass.: MIT Press.

Bergen, Peter u. a. (2014): „Do NSA's Bulk Surveillance Programs Stop Terrorists?", Washington, D.C.: New American Foundation, http://pierreghz.legtux.org/streisand/autoblogs/frglobalvoicesonlineorg_0e319138ab63237c2d2aeff84b4cb506d936eab8/media/e1982452.Bergen_NAF_NSA20Surveillance_1_0.pdf (zugegriffen am 12.4.2015).

Berke, Jürgen (2014): „Deutsche gegen US-Konzerne. Bitkom wegen NSA-Affäre gespalten", Wirtschaftswoche, 15.02.2014, http://www.wiwo.de/unternehmen/it/deutsche-gegen-us-konzerne-bitkom-wegen-nsa-affaere-gespalten/9482462.html (zugegriffen am 7.9.2015).

Berlinghoff, Marcel (2013): „‚Totalerfassung' im ‚Computerstaat'. Computer und Privatheit in den 1970er und 1980er Jahren", in: Ackermann, Ulrike (Hrsg.): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter, Frankfurt: Humanities Online, S. 93-110.

Bersing, Holger (2014): „Die Knallharte", Der Freitag, 31.10.2014, https://www.freitag.de/autoren/der-freitag/die-knallharte (zugegriffen am 20.2.2015).

Betz, Tobias (2010): „Trügerische Entspannung", The European, 01.07.2010, http://www.theeuropean.de/tobias-betz/2322-de-maizire-vs-leutheusser-schnarrenberger-2 (zugegriffen am 19.1.2015).

Beuth, Patrick (2015a): „Safe Harbor: Der EuGH hat ein Monster erschaffen“, Zeit Online, 10.08.2015, http://www.zeit.de/digital/datenschutz/2015-10/safe-harbor-eugh-konsequenzen (zugegriffen am 19.10.2015).

--- (2015b): „EU-Datenschutzverordnung: Bundesregierung hofiert Lobbyisten“, Zeit Online, 03.10.2015, http://www.zeit.de/digital/datenschutz/2015-03/eu-datenschutzgrundverordnung-ministerrat-bundesregierung-lobbyplag (zugegriffen am 2.4.2015).

Bewarder, Manuel und Thorsten Jungholt (2013): „Friedrich erklärt Sicherheit zum ‚Supergrundrecht‘“, Welt Online, 16.07.2013, http://www.welt.de/politik/deutschland/article118110002/Friedrich-erklaert-Sicherheit-zum-Supergrundrecht.html (zugegriffen am 20.4.2015).

BfDI (2015): „Andrea Voßhoff: Die EU Kommission muss jetzt Klartext reden!“, Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/01_AndreaVosshoffDieEUKommissionMussJetztKlartextReden.html (zugegriffen am 12.2.2015).

BFH (2012): „Urteil des VII. Senats vom 19.6.2012“, Bundesfinanzhof, VII R 43/11, http://www.bundesfinanzhof.de/entscheidungen/entscheidungen-online (zugegriffen am 28.1.2015).

BGH (2007): „Beschluss vom 31.01.2007: Unzulässigkeit einer "verdeckten Online-Durchsuchung““, Neue Juristische Wochenschrift (NJW) Heft 13, S. 930-932.

--- (2014): „Urteil des VI. Zivilsenats vom 1.7.2014“, Bundesgerichtshof, VI ZR 345/13, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=68159&linked=pm (zugegriffen am 22.9.2015).

Bieber, Christoph (2012): „Datenschutz als politisches Thema“, in: Schmidt, Jan-Hinrik und Thilo Weichert (Hrsg.): Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bonn: Bundeszentrale für politische Bildung, Bd. 1190, S. 34-44.

Biermann, Kai (2011): „Staatstrojaner: Überwachungstrojaner kommt aus Bayern“, Zeit Online, 10.10.2011, http://www.zeit.de/digital/datenschutz/2011-10/ccc-staatstrojaner-bayern (zugegriffen am 7.2.2015).

--- (2012): „Netzpolitik: Unionspolitiker gründen Internetlobby CNetz“, Zeit Online, 04.02.2012, http://www.zeit.de/digital/internet/2012-04/c-netz-union (zugegriffen am 25.2.2015).

--- (2014): „Überwachungsaffäre: NSA-Ausschuss sieht nur schwarz“, Zeit Online, 09.09.2014, http://www.zeit.de/politik/deutschland/2014-09/nsa-ausschuss-akten-geschwaerzt (zugegriffen am 25.2.2015).

Biermann, Kai und Patrick Beuth (2015): „Bundesnachrichtendienst: Was sind eigentlich Selektoren?“, Zeit Online, 24.04.2015, http://www.zeit.de/digital/datenschutz/2015-04/bundesnachrichtendienst-bnd-nsa-selektoren-eikonal (zugegriffen am 14.8.2015).

Biermann, Kai und Lenz Jacobsen (2013): „Bundestag: Eine Datenschutzbeauftragte, die Daten nicht schützen will“, Zeit Online, 19.12.2013, http://www.zeit.de/digital/datenschutz/2013-12/datenschutzbeauftragte-vosshoff-bundestag-gewaehlt (zugegriffen am 2.3.2015).

Biermann, Kai und Karsten Polke-Majewski (2014): „Datenschutz: Der Spion in der Tasche“, Zeit Online, 28.05.2014, http://www.zeit.de/digital/mobil/2014-05/handy-smartphone-sensor-datenschutz-ueberwachung (zugegriffen am 7.4.2015).

BITKOM (2014): „Unternehmen investieren stark in Online-Marketing“, Berlin: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM), http://www.bitkom-research.de/Presse/Pressearchiv-2014/Unternehmen-investieren-stark-in-Online-Marketing (zugegriffen am 11.2.2015).

Bluhm, Franziska (2012): „Privatsphärenverlust im Alltag?“, in: Schmidt, Jan-Hinrik und Thilo Weichert (Hrsg.): Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bonn: Bundeszentrale für politische Bildung, Bd. 1190, S. 237-242.

BMBF (2015): „Sicher in der digitalen Welt“, Bundesministerium für Bildung und Forschung, http://www.bmbf.de/de/73.php (zugegriffen am 19.1.2015).

BMWi, BMI und BMVI (2014): „Digitale Agenda 2014 - 2017“, Bundesministerium für Wirtschaft und Energie, Bundesministerium des Innern, Bundesministerium für Verkehr und digitale Infrastruktur, München: PRpetuum GmbH, http://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6 (zugegriffen am 25.2.2015).

Bó, Ernesto Dal (2006): „Regulatory Capture: A Review“, Oxford Review of Economic Policy 22/2, S. 203-225.

Bock, Kirsten (2012): „Marktwirtschaftlicher Datenschutz“, in: Schmidt, Jan-Hinrik und Thilo Weichert (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, Bonn: Bundeszentrale für politische Bildung, Bd. 1190, S. 310-321.

Böhm, Maria Laura (2011): Der„ Gefährder“ und das„ Gefährdungsrecht“: Eine rechtssoziologische Analyse am Beispiel der Urteile des Bundesverfassungsgerichts über die nachträgliche Sicherungsverwahrung und die akustische Wohnraumüberwachung, Bd. 15, Göttinger Studien zu den Kriminalwissenschaften, Göttingen: Universitätsverlag Göttingen.

Bonse, Eric (2006): „SWIFT: Industriespionage statt Antiterrorkampf?“, Handelsblatt, 07.11.2006, http://www.handelsblatt.com/politik/international/swift-industriespionage-statt-antiterrorkampf/2678574.html (zugegriffen am 24.8.2015).

Borking, John u. a. (1995): „Privacy-Enhancing Technologies: The Path to Anonymity“, GA Rijswijk (Netherlands): Registratiekamer.

BpB (2013): „Zeitleiste Rechtsterrorismus“, Bundeszentrale für politische Bildung, http://www.bpb.de/politik/extremismus/rechtsextremismus/167786/zeitleiste-rechtsterrorismus (zugegriffen am 9.1.2015).

Breuer, Theresa und Ole Reißmann (2013): „10.000 Menschen protestieren gegen NSA-Überwachung“, Spiegel Online, 27.07.2013, http://www.spiegel.de/politik/deutschland/10-000-menschen-protestieren-gegen-nsa-ueberwachung-a-913513.html (zugegriffen am 25.2.2015).

BSG (2014): „Urteil des 1. Senats vom 18.11.2014“, Bundessozialgericht, B 1 KR 35/13 R, http://juris.bundessozialgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bsg&Art=tm&Datum=2014&nr=13640 (zugegriffen am 28.1.2015).

Budras, Corinna (2014): „Google weiß, wo die Grippe lauert“, Frankfurter Allgemeine Zeitung, 15.11.2014, http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google-flu-trends-big-data-kann-helfen-uns-gegen-krankheiten-zu-wappnen-13268389-p4.html?printPagedArticle=true#pageIndex_4 (zugegriffen am 31.7.2015).

Buermeyer, Ulf und Matthias Bäcker (2009): „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO“, HRRS - Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht Heft 10, S. 433-441.

Buess, Katharina (2014): „Datensicherheit bei Emails: Kleiner Berliner Dienst, hoher Schutz“, Berliner Zeitung, 01.01.2014, http://www.berliner-zeitung.de/berlin/datensicherheit-bei-emails-kleiner-berliner-dienst–hoher-schutz,10809148,25766396.html (zugegriffen am 12.1.2015).

Bündnis 90/Die Grünen (2013): „Zeit für den grünen Wandel. Teilhaben. Einmischen. Zukunft schaffen. Bundestagswahlprogramm von Bündnis90/Die Grünen, beschlossen auf der 35. Ordentlichen Bundesdelegiertenkonferenz von Bündnis90/Die Grünen vom 26. bis 28. April 2013 in Berlin“, Berlin: Bündnis90/Die Grünen, http://www.gruene.de/fileadmin/user_upload/Dokumente/Gruenes-Bundestagswahlprogramm-2013.pdf (zugegriffen am 27.1.2015).

Busch, Andreas (2005): „The Politics of Transborder Data Flows: Competing Values, Interests, and Institutions“, Conference: Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities, Oxford Internet Institute, 8.-10. September 2005, http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/andreas_busch.pdf (zugegriffen am 24.9.2014).

--- (2007): „Von der Reformpolitik zur Restriktionspolitik? Die Innen- und Rechtspolitik der zweiten Regierung Schröder“, in: Egle, Christoph und Reimut Zohlnhöfer (Hrsg.): Ende des rot-grünen Projektes, Wiesbaden: VS Verlag für Sozialwissenschaften, S. 408-430.

--- (2012a): „Die Regulierung transatlantischer Datenströme“, in: Busch, Andreas und Jeanette Hofmann (Hrsg.): Politik und die Regulierung von Information, Baden-Baden: Nomos, S. 408-440.

--- (2012b): „Freiheits- und Bürgerrechte nach 9/11“, in: Jäger, Thomas (Hrsg.): Die Welt nach 9/11. Auswirkungen des Terrorismus auf Staatenwelt und Gesellschaft, Wiesbaden: VS Verlag für Sozialwissenschaften/Springer Fachmedien, S. 861-881.

--- (2013): „Die notwendige Kontrolle des Sicherheitsstaates“, in: Beckedahl, Markus und Andre Meister (Hrsg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte, Berlin: newthinking communications in Kooperation mit epubli GmbH, S. 138-144, https://netzpolitik.org/wp-upload/Ueberwachtes-Netz-Markus-Beckedahl-Andre-Meister.pdf (28.9.2015).

Busch, Andreas und Tobias Jakobi (2011): „Die Erfindung eines neuen Grundrechts. Zu Konzept und Auswirkungen der ‚informationellen Selbstbestimmung‘“, in: Hönnige, Christoph, Sascha Kneip und Astrid Lorenz (Hrsg.): Verfassungswandel im Mehrebenensystem, Wiesbaden: VS Verlag für Sozialwissenschaften, S. 297-320.

Butler, Declan (2013): „When Google got flu wrong“, Nature 494/7436, S. 155-156.

BVerfG (1983): „Urteil des Ersten Senats vom 15.12.1983“, Bundesverfassungsgericht, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, https://web.archive.org/web/20101116085553/http://zensus2011.de/fileadmin/material/pdf/gesetze/volkszaehlungsurteil_1983.pdf (zugegriffen am 27.7.2015).

--- (2008): „Urteil des Ersten Senats vom 27. Februar 2008“, Bundesverfassungsgericht, 1 BR 370/07, 1 BvR 595/07, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html;jsessionid=614127F096C6368E52BB5D0829655777.2_cid383 (zugegriffen am 5.2.2015).

--- (2010): „Urteil des Ersten Senats vom 2. März 2010“, Bundesverfassungsgericht, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs

20100302_1bvr025608.html;jsessionid=7B4DD7BE23A8D847A995A360AAEB5CC6.2_cid393 (zugegriffen am 19.1.2015).

BVerwG (2014): „Urteil vom 22. Oktober 2014“, Bundesverwaltungsgericht, BVerwG 6 C 7.13, http://www.bverwg.de/presse/pressemitteilungen/pressemitteilung.php?jahr=2014&nr=63 (zugegriffen am 27.1.2015).

Cáceres, Javier (2013): „Internetkonzerne schreiben bei Datenschutzregeln mit“, Süddeutsche.de, 02.11.2013, http://www.sueddeutsche.de/digital/lobby-einfluss-auf-neue-eu-verordnung-internetkonzerne-schreiben-bei-datenschutzregeln-mit-1.1596560 (zugegriffen am 2.9.2014).

Callas, Jon (2011): „Internetdienstleister: Google, Facebook und der Staat“, Zeit Online, 29.09.2011, http://www.zeit.de/2011/40/Jon-Callas-ueber-Facebook (zugegriffen am 30.11.2014).

Caspari, Lisa (2014): „Überwachung: ‚Wir können die NSA totrüsten‘“, Zeit Online, 26.06.2014, http://www.zeit.de/politik/deutschland/2014-06/nsa-ausschuss-bnd-ueberwachung/komplettansicht (zugegriffen am 26.2.2015).

Castro, Daniel (2013): „How Much Will PRISM Cost the U.S. Cloud Computing Industry?“, Washington, D.C.: The Information Technology & Innovation Foundation, http://www2.itif.org/2013-cloud-computing-costs.pdf (22.9.2015).

Cavoukian, Ann (2012): „Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era“, in: Yee, George O.M. (Hrsg.): Privacy Protection Measures and Technologies in Business Organizations. Aspects and Standards, Hershey, PA: IGI Global.

CCC (2009): „Chaos Computer Club veröffentlicht Stellungnahme zur Vorratsdatenspeicherung“, Chaos Computer Club, http://www.ccc.de/updates/2009/vds-gutachten (zugegriffen am 25.2.2015).

--- (2015): „Chaos Computer Club“, Chaos Computer Club, http://www.ccc.de/de/club (zugegriffen am 25.2.2015).

CDU/CSU (2013): „Gemeinsam erfolgreich für Deutschland. Regierungsprogramm 2013 - 2017, beschlossen auf der Gemeinsamen Vorstandssitzung von CDU und CSU am 23. Juni 2013 in Berlin“, Berlin: CDU/CSU, http://www.cdu.de/sites/default/files/media/dokumente/regierungsprogramm-2013-2017-langfassung-20130911.pdf (zugegriffen am 27.1.2015).

Clauß, Ulrich (2014): „So würde Europas ‚Schengen-Internet‘ funktionieren“, Welt Online, 31.03.2014, http://www.welt.de/politik/deutschland/article126343060/So-wuerde-Europas-Schengen-Internet-funktionieren.html (zugegriffen am 13.2.2015).

Cox, James (2012): „Canada and the Five Eyes Intelligence Community“, Strategic Studies Working Group Papers, Canadian Defence and Foreign Affairs Institute and Canadian International Council, http://opencanada.org/wp-content/uploads/2012/12/SSWG-Paper-James-Cox-December-2012.pdf.pdf (zugegriffen am 19.1.2015).

Culnan, Mary J. und Robert J. Bies (2003): „Consumer Privacy: Balancing Economic and Justice Considerations“, Journal of Social Issues 59/2, S. 323-342.

Daase, Christopher und Nicole Deitelhoff (2013): „Privatisierung der Sicherheit: Eine sozialwissenschaftliche Expertise“, Schriftenreihe Sicherheit.

Dammann, Ulrich (2014): „§24 Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“, in: Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, Nomos Kommentar, 8. Aufl., Baden-Baden: Nomos, S. 1143-1155.

De Maizière, Thomas (2014): „Das Netz - Raum der Chancen und der Freiheit“, Frankfurter Allgemeine Zeitung, 17.08.2014, http://www.faz.net/aktuell/politik/die-gegenwart/digitale-agenda-das-netz-raum-der-chancen-und-der-freiheit-13102900.html?printPagedArticle=true#pageIndex_2 (22.9.2015).

Denkler, Thorsten (2014): „Datenschutzbeauftrage - ‚Einen Maulkorb braucht sie nicht‘“, Süddeutsche.de, 09.04.2014, http://www.<deutsche.de/digital/datenschutzbeauftrage-einen-maulkorb-braucht-sie-nicht-1.2115727 (zugegriffen am 2.3.2015).

Der Spiegel (1983): „Volkszählung: Laßt 1000 Fragebogen glühen“, Der Spiegel, 13/1983, S. 28-32, http://www.spiegel.de/spiegel/print/d-14022649.html (23.9.2015).

Der Tagesspiegel (2015): „Widerstand der Parteibasis. SPD-Mitgliederbegehren gegen Vorratsdatenspeicherung“, Der Tagesspiegel, 28.07.2015, http://www.tagesspiegel.de/politik/widerstand-der-parteibasis-spd-mitgliederbegehren-gegen-vorratsdatenspeicherung/12116420.html (zugegriffen am 11.9.2015).

Deutscher Bundestag (2012): „Fünfter Zwischenbericht der Enquete-Kommission ‚Internet und digitale Gesellschaft‘. Datenschutz, Persönlichkeitsrechte“, Drucksache 17/8999, Berlin: Deutscher Bundestag, http://dipbt.bundestag.de/doc/btd/17/089/1708999.pdf (zugegriffen am 25.2.2012).

--- (2013a): „Schlussbericht der Enquete-Kommission ‚Internet und digitale Gesellschaft‘“, Drucksache 17/12550, Berlin: Deutscher Bundestag, http://dipbt.bundestag.de/dip21/btd/17/125/1712550.pdf (zugegriffen am 25.2.2015).

--- (2013b): „Aktueller Begriff: Big Data“, Wissenschaftliche Dienste, Berlin: Deutscher Bundestag, http://www.bundestag.de/blob/194790/c44371b1c740987a7f6fa74c06f518c8/big_data-data.pdf (zugegriffen am 23.9.2015).

--- (2014a): „Antrag der Fraktionen CDU/CSU, SPD, DIE LINKE. Und BÜNDNIS 90/DIE GRÜNEN. Einsetzung eines Untersuchungsausschusses“, Drucksache 18/843, Berlin: Deutscher Bundestag, http://dip21.bundestag.de/dip21/btd/18/008/1800843.pdf (zugegriffen am 25.2.2015).

--- (2014b): „Kritik an Statusänderung der Voßhoff-Behörde“, Deutscher Bundestag, http://www.bundestag.de/dokumente/textarchiv/2014/kw49_pa_innen/341938 (zugegriffen am 25.2.2015).

--- (2015): „Stellungnahmen der Sachverständigen“, Deutscher Bundestag, http://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848 (zugegriffen am 19.1.2015).

Die Linke (2013): „100 % Sozial. Wahlprogramm zur Bundestagswahl 2013, beschlossen auf dem Bundestagswahlparteitag, vom 14. bis 16. Juni 2013 in Dresden“, Wahlprogramm, Dresden: Die Linke, http://www.die-lin-ke.de/fileadmin/download/wahlen2013/bundestagswahlprogramm/bundestagswahlprogramm2013_langfassung.pdf (zugegriffen am 27.1.2015).

Diersch, Verena (2014): „The President's Review Group on Intelligence and Communications Technologies (2014): The NSA Report. Liberty and Security in a Changing World (Rezension)", Zeitschrift für Außen- und Sicherheitspolitik (ZfAS) 03/2014, S. 417-419.

Digitalcourage (2011): „Datenschutz und Bürgerrechte", Digitalcourage, https://digitalcourage.de/themen/datenschutz-und-buergerrechte (zugegriffen am 25.2.2015).

Dilanian, Ken (2015): „Surveillance tweaks illustrate little change after Snowden", The Washington Times, 02.03.2015, http://www.washingtontimes.com/news/2015/feb/3/obama-tightens-rules-on-use-of-bulk-intelligence-d/ (zugegriffen am 28.9.2015).

DIVSI (2014): „DIVSI Studie: Daten – Ware und Währung"Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), https://www.divsi.de/publikationen/studien/divsi-studie-daten-ware-und-waehrung/ (zugegriffen am 23.9.2015).

Dix, Alexander (2000): „ECHELON auf dem parlamentarischen Prüfstand", DuD - Datenschutz und Datensicherheit 24/9, S. 659-662.

--- (2013): Datenschutz und transatlantische Freihandelszone, Karlsruhe: KIT Scientific Publishing.

Dobusch, Leonhard (2014): „Digitale Zivilgesellschaft in Deutschland: Stand und Perspektiven 2014", Discussion Paper, Berlin: School of Business & Economics, http://www.econstor.eu/handle/10419/95863 (zugegriffen am 12.12.2014).

Düsseldorfer Kreis (2010): „Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht- öffentlichen Bereich am 28./29. April 2010 in Hannover", Hannover: Düsseldorfer Kreis, https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10neu.pdf (zugegriffen am 23.9.2015).

Ebbinghaus, Uwe, Thomas Thiel und Stefan Schulz (2014): „Europäische Datenschutzreform Machtprobe mit Silicon Valley", Frankfurter Allgemeine Zeitung, 11.03.2014, http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/europas-it-projekt/digitale-agenda-machtprobe-mit-silicon-valley-12842407.html (zugegriffen am 25.2.2015).

EDRi (2014): „Annual Report. January 2014 - December 2014", Brüssel: European Digital Rights, https://edri.org/wp-content/uploads/2013/09/EDRi_Annual_Report_2014.pdf (zugegriffen am 29.1.2015).

EFF (2014): „International Principles on the Application of Human Rights to Communications Surveillance", Electronic Frontier Foundation, https://en.necessaryandproportionate.org/ (zugegriffen am 6.3.2015).

--- (2015): „EFF's Staff", Electronic Frontier Foundation, https://www.eff.org/about/staff (zugegriffen am 29.1.2015).

EU Commission (2010): „A comprehensive approach on personal data protection in the European Union", Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Brussels: EU Commission,

http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (zugegriffen am 21.7.2014).

--- (2011): „Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf (zugegriffen am 17.4.2015).

--- (2013a): „Informal Justice Council in Vilnius", Memo, http://europa.eu/rapid/press-release_MEMO-13-710_en.htm (zugegriffen am 11.9.2015).

--- (2013b): „Statement by Commissioner Malmström on the European Parliament's resolution on the EU-US TFTP agreement", Memo, Brussels: EU Commission, http://europa.eu/rapid/press-release_MEMO-13-928_de.htm (zugegriffen am 20.1.2015).

--- (2015): „Questions and Answers on the EU-US data protection ‚Umbrella agreement'", Press Release. European Commission - Fact Sheet, http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm (zugegriffen am 9.9.2015).

EuGH (2010): „Urteil des Gerichtshofes (Große Kammer) vom 9. März 2010", Europäischer Gerichtshof, 2010 I-01885, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd9e087557e0d947ba9d7fa32135a7d8f1.e34KaxiLc3qMb40Rch0SaxuPb3n0?text=&docid=79752&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=368452 (zugegriffen am 20.2.2015).

--- (2012): „Urteil des Gerichtshofs (Große Kammer) vom 16. Oktober 2012", Europäischer Gerichtshof, C-614/10, http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 (zugegriffen am 31.7.2015).

--- (2014a): „Urteil des Gerichtshofes (Große Kammer) vom 08.04.2014", Europäischer Gerichtshof, 2009 I-00593, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=DE (zugegriffen am 20.2.2015).

--- (2014b): „Urteil des Gerichtshofes (Große Kammer) vom 13. Mai 2014", Europäischer Gerichtshof, C-131/12, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=370443 (zugegriffen am 20.2.2015).

--- (2015): „Urteil des Gerichtshofes (Große Kammer) vom 6. Oktober 2015", Europäischer Gerichtshof, C-362/14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=111420 (zugegriffen am 19.10.2015).

EU-Kommission (2010): „Europäische Kommission will Datenschutzabkommen mit den USA mit strengen Regeln für den Schutz der Privatsphäre", Brüssel: EU-Kommission, http://europa.eu/rapid/press-release_IP-10-609_de.htm?locale=en (zugegriffen am 11.9.2015).

--- (2011): „Bekämpfung von schwerer Kriminalität und Terrorismus: EU-Vorschlag zur Verwendung von Fluggastdaten", Brüssel: Europäische Kommission, http://europa.eu/rapid/press-release_IP-11-120_de.htm?locale=en (zugegriffen am 26.11.2014).

--- (2012a): „Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF (zugegriffen am 23.9.2015).

--- (2012b): „Vorschlag für Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52012PC0010&from=EN (zugegriffen am 29.7.2015).

--- (2013a): „Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Cybersicherheitsstrategie der Europäischen Union - ein offener, sicherer und geschützter Cyberraum“, Brüssel: EU-Kommission, http://www.eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_de.pdf (23.9.2015).

--- (2013b): „Mitteilung der Kommission an das Europäische Parlament und den Rat: Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“, Brüssel: EU-Kommission, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52013DC0846&from=de (zugegriffen am 11.9.2015).

EU-Parlament (2001): „Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON)“, 2001/2098(INI), Berichterstatter: Gerhard Schmid, Brüssel: Nichtständiger Ausschuss über das Abhörsystem Echelon, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//DE (zugegriffen am 23.9.2015).

--- (2013a): „Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//DE (zugegriffen am 29.7.2015).

--- (2013b): „Bericht über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0403+0+DOC+PDF+V0//DE (zugegriffen am 29.7.2015).

--- (2013c): „Parlament fordert Aussetzung des SWIFT-Abkommens wegen NSA-Abhörskandal“, Pressemitteilung, http://www.europarl.europa.eu/news/de/news-room/content/20131021ipr22725 (zugegriffen am 18.10.2014).

--- (2014): „Parlament droht mit Konsequenzen, falls USA Massenüberwachung nicht einstellt“, Pressemitteilung, http://www.europarl.europa.eu/news/de/news-room/content/20140307IPR38203/html/Parlament-droht-mit-Konsequenzen-falls-USA-Massen%C3%BCberwachung-nicht-einstellt (zugegriffen am 12.2.2015).

EU-Rat (2015): „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Vorbereitung einer allgemeinen Ausrichtung“, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf (zugegriffen am 29.7.2015).

Europäische Union (1995): „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“, Amtsblatt der Europäischen Gemeinschaften Nr. L 281, S. 31-50, http://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX:31995L0046 (22.8.2014).

--- (2002): „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)“, Amtsblatt der Europäischen Gemeinschaften Nr. L 201, S. 37-47, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32002L0058 (29.7.2015).

--- (2006): „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“, Amtsblatt der Europäischen Union L 105/54, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32006L0024 (zugegriffen am 3.12.2014).

--- (2009): „Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz“, Amtsblatt der Europäischen Union Nr. L 337, S. 11-36, http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:32009L0136 (29.7.2015).

--- (2010): „Charta der Grundrechte der Europäischen Union“, Amtsblatt der Europäischen Union C 83, S. 389-403, http://eur-lex.europa.eu/legal-content/de/ALL/?uri=OJ:C:2010:083:TOC (29.7.2015).

Europarat (1981): „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“, http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm (zugegriffen am 27.7.2015).

FAZ (2012): „EU-Innenkommissarin Cecilia Malmström: ‚Wir waren sehr geduldig mit Deutschland‘“, Frankfurter Allgemeine Zeitung, 07.03.2012, http://www.faz.net/aktuell/politik/europaeische-union/eu-innenkommissarin-cecilia-malmstroem-wir-waren-sehr-geduldig-mit-deutschland-11808962.html?printPagedArticle=true#pageIndex_2 (zugegriffen am 20.2.2015).

--- (2014a): „Grundsatzurteil: Anonyme Äußerungen im Netz bleiben anonym“, Frankfurter Allgemeine Zeitung, 07.01.2014, http://www.faz.net/aktuell/finanzen/meine-finanzen/urteil-bgh-staerkt-anonymitaet-im-internet-13020471.html (zugegriffen am 27.1.2015).

--- (2014b): „Europaparlament: Bildung einer rechtsextremen Fraktion gescheitert“, Frankfurter Allgemeine Zeitung, 24.06.2014,

http://www.faz.net/aktuell/politik/europaeische-union/buendnisverhandlungen-der-rechtspopulisten-scheitern-13006706.html (zugegriffen am 21.2.2015).

FDP (2013): „Bürgerprogramm 2013. Damit Deutschland stark bleibt. Nur mit uns, beschlossen auf dem Bundesparteitag vom 4. bis 5. Mai 2013 in Nürnberg“, Nürnberg: FDP, http://www.fdp.de/files/408/B_rgerprogramm_A5_Online_2013-07-23.pdf (zugegriffen am 27.1.2015).

Fischbach, Rainer (2009): „Internet: Zensur, technische Kontrolle und Verwertungsinteressen“, in: Bisky, Lothar, Konstanze Kriese und Jürgen Scheele (Hrsg.): Medien – Macht – Demokratie. Neue Perspektiven, Berlin: Karl Dietz Verlag, S. 109-133.

Fontanella-Khan, James (2013a): „Victory for tech giants on EU data laws“, Financial Times, 25.10.2013, http://www.ft.com/cms/s/5ad18e46-3d8c-11e3-9928-00144feab7de,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F5ad18e46-3d8c-11e3-9928-00144feab7de.html%3Fsiteedition%3Duk&siteedition=uk&_i_referer= (zugegriffen am 9.2.2015).

--- (2013b): „Washington pushed EU to dilute data protection“, Financial Times, 06.12.2013, http://www.ft.com/intl/cms/s/0/42d8613a-d378-11e2-95d4-00144feab7de.html (zugegriffen am 17.10.2014).

Forschungsgruppe Wahlen (2014): „Politbarometer Januar I 2014“, Forschungsgruppe Wahlen e. V., http://www.forschungsgruppe.de/Umfragen/Politbarometer/Archiv/Politbarometer_2014/Januar_I_2014/ (zugegriffen am 30.9.2015).

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

--- (2014): „In Deutschland gilt auch US-Recht“, Süddeutsche.de, 08.11.2014, http://www.sueddeutsche.de/politik/deutsch-amerikanische-beziehungen-in-deutschland-gilt-auch-us-recht-1.2084126 (zugegriffen am 13.8.2014).

Foucault, Michel (1977): Überwachen und Strafen: Die Geburt des Gefängnisses, übers. von Walter Seitter, 19. Aufl., Frankfurt am Main: Suhrkamp Verlag.

Förster, Andreas (Hrsg.) (2014): Geheimsache NSU: Zehn Morde, von Aufklärung keine Spur, Tübingen: Klöpfer und Meyer.

Fritz, Johannes (2013): Netzpolitische Entscheidungsprozesse. Datenschutz, Urheberrecht und Internetsperren in Deutschland und Großbritannien, Baden-Baden: Nomos.

Fürstenau, Marcel (2014): „Sicherheitspolitik: Geheimdienste ‚unter die Lupe nehmen‘“, Deutsche Welle, http://www.dw.de/geheimdienste-unter-die-lupe-nehmen/a-17361828 (zugegriffen am 22.4.2015).

Garfinkel, Simson und Beth Rosenberg (2009): „Gesichtserkennung: Clever oder unheimlich?“, Technology Review, 13.03.2009, http://www.heise.de/tr/artikel/Gesichtserkennung-Clever-oder-unheimlich-276193.html (zugegriffen am 11.2.2015).

Garstka, Hansjürgen (2008): „Der Mensch als Datenzuträger. Was Sie schon immer über Ihren Nachbarn wissen wollten“, in: Herwig, Rita (Hrsg.): Wissen als Begleiter!?: das Individuum als lebenslanger Lerner, Münster: LIT Verlag, S. 133-138.

Gaycken, Sandro (2014): „Cyberwar-Experte: Die Speicherung von Vorratsdaten ist eine Technik von gestern“, Cicero, 14.04.2015, http://www.cicero.de/berliner-republik/datenschutz-cyberwar-experte-die-vorratsdatenspeicherung-hilft-strafverfolgern-nicht/57396 (zugegriffen am 18.9.2015).

Gebauer, Matthias (2015): „Affäre um Landesverrat: Maaßen informierte Kanzleramt über Netzpolitik.org-Fall", Spiegel Online, 27.08.2015, http://www.spiegel.de/politik/deutschland/netzpolitik-org-kanzleramt-wusste-frueh-von-landesverrat-ermittlungen-a-1050004.html (zugegriffen am 15.9.2015).

Gellman, Barton und Greg Miller (2013): „'Black budget' summary details U.S. spy network's successes, failures and objectives", The Washington Post, 29.08.2013, http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (zugegriffen am 28.11.2014).

Gellman, Barton und Laura Poitras (2013): „U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", The Washington Post, 06.07.2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (zugegriffen am 11.5.2014).

Gibbs, Samuel (2014): „US court forces Microsoft to hand over personal data from Irish server", The Guardian, 29.04.2014, http://www.theguardian.com/technology/2014/apr/29/us-court-microsoft-personal-data-emails-irish-server (zugegriffen am 22.4.2015).

Giddens, Anthony (1995): Die Konstitution der Gesellschaft. Grundzüge einer Theorie der Strukturierung, Frankfurt am Main: Campus Verlag.

Ginsberg, Jeremy u. a. (2009): „Detecting influenza epidemics using search engine query data", Nature 457/7232, S. 1012-1014.

Goetz, John, Hans Leyendecker und Frederik Obermaier (2014): „BND will Technik massiv aufrüsten", Süddeutsche.de, 06.03.2014, http://www.sueddeutsche.de/digital/geheimdienste-bnd-plant-ausforschen-auf-augenhoehe-1.1982334 (zugegriffen am 26.2.2015).

Goldsmith, Jack und Tim Wu (2008): Who Controls the Internet? Illusions of a Borderless World, New York: Oxford University Press.

González-Fuster, Gloria (2014): The Emergence of Personal Data Protection as a Fundamental Right of the EU, Law, Governance and Technology Series, Volume 16, Cham; Heidelberg; New York: Springer.

Goos, Kerstin u. a. (2015): "The co-evolution of surveillance technologies and surveillance practices", in: Wright, David und Reinhard Kreissl (Hrsg.): Surveillance in Europe, 1. Aufl., Abingdon; New York: Routledge, S. 51-100.

Gössner, Rolf (2010): „Staatlicher Antiterrorkampf - Im Namen der Sicherheit und auf Kosten der Bürgerrechte?", in: Soeffner, Hans-Georg (Hrsg.): Unsichere Zeiten. Herausforderungen gesellschaftlicher Transformationen. Verhandlungen des 34. Kongresses der Deutschen Gesellschaft für Soziologie in Jena 2008, Bd. 2, 1. Aufl., Wiesbaden: VS Verlag für Sozialwissenschaften, S. 877-882.

GPEN (2014): „Global Privacy Enforcement Network Sweep 2014", Ottawa: Global Privacy Enforcement Network (GPEN), https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp (zugegriffen am 7.4.2015).

Greenberg, Andy (2014): „Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users", Wired.com, 18.11.2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/ (zugegriffen am 12.1.2015).

Greenwald, Glenn (2013a): „NSA collecting phone records of millions of Verizon customers daily“, The Guardian, 06.06.2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (zugegriffen am 9.5.2014).

--- (2013b): „Email service used by Snowden shuts itself down, warns against using US-based companies“, The Guardian, 08.09.2013, http://www.theguardian.com/commentisfree/2013/aug/09/lavabit-shutdown-snowden-silicon-valley (zugegriffen am 13.2.2015).

Greis, Friedhelm (2013): „Snowdens Mailprovider: Lavabit-Gründer bot dem FBI Metadaten für 3.500 Dollar an“, Golem.de, 10.10.2013, http://www.golem.de/news/snowdens-mail-provider-lavabit-gruender-bot-dem-fbi-metadaten-fuer-3-500-dollar-an-1310-102065.html (zugegriffen am 13.2.2015).

--- (2015): „Fluggastdatenspeicherung: EU-Parlament macht Weg für PNR-Datenbank frei“, Golem.de, 11.02.2015, http://www.golem.de/news/fluggastdatenspeicherung-eu-parlament-macht-weg-fuer-pnr-datenbank-frei-1502-112303.html (zugegriffen am 13.2.2015).

Greven, Ludwig (2013): „Historiker Foschepoth im Interview: ‚Die USA dürfen Merkel überwachen‘“, Zeit Online, 25.10.2013, http://www.zeit.de/politik/deutschland/2013-10/nsa-uerberwachung-merkel-interview-foschepoth/komplettansicht (zugegriffen am 9.2.2015).

Gude, Hubert und Annett Meiritz (2014): „NSA-Affäre: Kanzleramt droht Ausschuss mit Strafanzeige“, Spiegel Online, 16.10.2014, http://www.spiegel.de/politik/deutschland/nsa-affaere-kanzleramt-droht-ausschuss-mit-strafanzeige-a-997468.html (zugegriffen am 25.2.2015).

Gusy, Christopher (2014): „Architektur und Rolle der Nachrichtendienste in Deutschland“, Aus Politik und Zeitgeschichte (APuZ), 64/18-19/2014 (Ausgabe: Überwachen), S. 9-14.

Gutschker, Thomas und Markus Wehner (2013): „NSA-Affäre: Der große Bruder“, Frankfurter Allgemeine Zeitung, 07.07.2013, http://www.faz.net/aktuell/politik/inland/nsa-affaere-der-grosse-bruder-12273323.html?printPagedArticle=true#pageIndex_2 (zugegriffen am 13.8.2014).

Gutwirth, Serge (2002): Privacy and the Information Age, Lanham; Boulder; New York; Oxford: Rowman & Littlefield Publishers.

Hager, Nicky (1996): Secret power, Nelson (New Zealand): Craig Potton.

Hamann, Götz (2014): „Silent Circle: ‚Wir haben alles zerstört‘“, Die Zeit, Nr. 47/2014, 13.11.2014, http://www.zeit.de/2014/47/spionage-silent-circle-edward-snowden (zugegriffen am 13.8.2015).

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

Handelsblatt (2014): „Entscheidung des Bundessozialgerichts: Gesundheitskarte verstößt nicht gegen Datenschutz“, Handelsblatt, 18.11.2014, http://www.handelsblatt.com/finanzen/recht-steuern/urteile-entscheidungen/entscheidung-des-bundessozialgerichts-gesundheitskarte-verstoesst-nicht-gegen-datenschutz/10998390.html (zugegriffen am 27.1.2015).

Hansen, Markus und Andreas Pfitzmann (2007): „Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme“, Deutsche Richterzeitung 8, S. 225-228.

--- (2008): „Windei Bundestrojaner“, c’t 25/08, http://www.heise.de/ct/artikel/Windei-Bundestrojaner-291808.html (zugegriffen am 3.2.2015).

Hänßler, Boris (2014): „Skandal! Egal?“, Technology Review 06/2014, 05.06.2014, S. 24-28, http://www.heise.de/tr/artikel/Skandal-Egal-2215573.html (23.9.2015).

Hayes, Ben (2009): „NeoConOpticon: The EU Security-Industrial Complex“, Amsterdam/London: Transnational Institute/Statewatch, http://www.statewatch.org/analyses/neoconopticon-report.pdf (zugegriffen am 10.4.2015).

Hayes, Ben und Chris Jones (2013): „Catalogue of EU Counter-Terrorism Measures Adopted since 11 September 2001“, Deliverable 2.1 (Catalogue of Measures) of the EU-funded project (FP7) SECILE (Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness), London: Statewatch, http://www.statewatch.org/news/2013/dec/secile-catalogue-of-EU-counter-terrorism-measures.pdf (zugegriffen am 25.2.2015).

Hecking, Claus (2013a): „Deutsche Beamte bremsen Europas Datenschutz aus“, Spiegel Online, 12.02.2013, http://www.spiegel.de/netzwelt/netzpolitik/deutsche-beamte-bremsen-europas-datenschutz-aus-a-936704.html (zugegriffen am 4.9.2014).

--- (2013b): „NSA-Spionage: EU-Kommission droht USA mit Ende des Swift-Abkommens“, Spiegel Online, 13.09.2013, http://www.spiegel.de/netzwelt/netzpolitik/eu-kommission-droht-usa-mit-ende-des-swift-abkommens-a-922131.html (zugegriffen am 11.9.2015).

Hecking, Claus, Gregor Peter Schmitz und Christoph Schult (2014): „Neue EU-Kommission: Junckers Handelschefin im Kreuzfeuer“, Spiegel Online, 29.09.2014, http://www.spiegel.de/politik/ausland/ttip-junckers-handelschefin-malmstroem-in-der-kritik-a-994247.html (zugegriffen am 3.4.2015).

Heise Online (2007a): „Innenministerium: Verfassungsschutz, MAD und BND können Online-Durchsuchungen durchführen“, Heise Online, 24.03.2007, http://www.heise.de/newsticker/meldung/Innenministerium-Verfassungsschutz-MAD-und-BND-koennen-Online-Durchsuchungen-durchfuehren-161153.html (zugegriffen am 2.2.2015).

--- (2007b): „Verfassungsbeschwerde gegen Online-Durchsuchungen in NRW eingelegt“, Heise Online, 09.02.2007, http://www.heise.de/newsticker/meldung/Verfassungsbeschwerde-gegen-Online-Durchsuchungen-in-NRW-eingelegt-144446.html (zugegriffen am 29.1.2015).

--- (2014): „Verfassungsschutz soll mehr zur IT-Sicherheit beitragen“, Heise Online, 19.08.2014, http://www.heise.de/newsticker/meldung/Verfassungsschutz-soll-mehr-zur-IT-Sicherheit-beitragen-2294924.html (zugegriffen am 2.3.2015).

Heller, Christian (2011): Post Privacy. Prima leben ohne Privatsphäre, München: C.H. Beck.

Hess, Thomas und Michel Schreiner (2012): „Ökonomie der Privatsphäre“, DuD - Datenschutz und Datensicherheit 36/2, S. 105-109.

Heumann, Stefan und Ben Scott (2013): „Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany“, Joint Publication of Program "European Digital Agenda" of stiftung neue verantwortung and the Open Technology Institute of the New America Foundation, Berlin: Stiftung Neue Verantwortung (SNV), http://www.stiftung-nv.de/sites/default/files/impulse.pdf (zugegriffen am 28.8.2015).

Hofer, Joachim (2014): „Wir punkten mit Datensicherheit“, Handelsblatt, Nr. 47, 07.03.2014, S. 14.

Hoffmann, Stanley (1966): „Obstinate or Obsolete? The Fate of the Nation-State and the Case of Western Europe“, Daedalus 95/3, S. 862-915.

Hoffman-Riem, Wolfgang (2014): „Der Staat als Garant von Freiheit und Sicherheit“, Vortrag, Akademie für politische Bildung Tutzing, http://www.jura.uni-hamburg.de/public/personen/hoffmann-riem/14.pdf (zugegriffen am 20.4.2015).

Hofmann, Gunther (2013): „Radikalenerlass von 1972: Nazis rein, Linke raus“, Die Zeit, Nr. 29/2013, 21.07.2013, http://www.zeit.de/2013/29/berufsverbote-radikalenerlass-1972/komplettansicht (zugegriffen am 8.12.2014).

Horchert, Judith (2014): „‚Freiheit statt Angst‘: Tausende demonstrieren in Berlin gegen Überwachung“, Spiegel Online, 30.08.2014, http://www.spiegel.de/netzwelt/netzpolitik/freiheit-statt-angst-demonstration-gegen-ueberwachung-in-berlin-a-989016.html (zugegriffen am 28.1.2015).

Hornung, Gerrit (2007): „Ermächtigungsgrundlage für die ‚Online-Durchsuchung ‘?“, DuD - Datenschutz und Datensicherheit 31/8, S. 575-580.

--- (2012): „Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012“, Zeitschrift für Datenschutz (ZD) 3/2012, S. 99-106.

Horvath, John (1996): „Die Unabhängigkeit des Internet und der Massengeist“, Telepolis, http://www.heise.de/tp/artikel/1/1019/ (zugegriffen am 25.2.2015).

Hughes, Krista (2014): „Data privacy shapes up as a next-generation trade barrier“, Reuters, 27.03.2014, http://www.reuters.com/article/2014/03/27/us-usa-trade-tech-analysis-idUSBREA2Q1K120140327 (zugegriffen am 12.2.2015).

Hummer, Waldemar (2011): „Die SWIFT-Affäre. US-Terrorismusbekämpfung versus Datenschutz“, Archiv des Völkerrechts 49/3, S. 203-245.

Iseli, Marc (2015): „Whatsapp-Rivale Threema startet in den USA durch“, Handelszeitung, 22.06.2015, http://www.handelszeitung.ch/unternehmen/whatsapp-rivale-threema-startet-den-usa-durch-801320 (zugegriffen am 12.8.2015).

Janisch, Wolfgang und Joachim Käppner (2012): „Gutachten zur Vorratsdatenspeicherung: Ein Institut, zwei Meinungen“, Süddeutsche.de, 20.03.2012, http://www.sueddeutsche.de/digital/gutachten-zur-vorratsdatenspeicherung-ein-institut-zwei-meinungen-1.1307175 (zugegriffen am 16.9.2015).

Jungholt, Thorsten (2015): „Terror zwingt Maas und de Maizière in den Konflikt“, Welt Online, 18.01.2015, http://www.welt.de/politik/deutschland/article136504726/Terror-zwingt-Maas-und-de-Maiziere-in-den-Konflikt.html (zugegriffen am 19.1.2015).

Kamp, Meike und Sarah Thomé (2012): „Die Kontrolle der Einhaltung der Datenschutzgesetze“, in: Schmidt, Jan-Hinrik und Thilo Weichert (Hrsg.): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, Bonn: Bundeszentrale für politische Bildung, Bd. 1190, S. 298-309.

Karaboga, Murat u. a. (2014): „White Paper Selbstdatenschutz“, Hrsg.: Peter Zoche u. a., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, 2. Aufl., Karlsruhe: Fraunhofer ISI, https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf (zugegriffen am 25.2.2015).

--- (2015): „White Paper Das versteckte Internet: Zu Hause - Im Auto - Am Körper“, Hrsg.: Peter Zoche u. a., Forum Privatheit und selbstbestimmtes Leben in der digitalen

Welt, 1. Aufl., Karlsruhe: Fraunhofer ISI, https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles_dokumente/White-Paper-2-Final_17.07.15-Druckversion.pdf (zugegriffen am 25.2.2015).

Keller, Josh u. a. (2014): „Obama's Changes to Government Surveillance", The New York Times, 17.01.2014, http://www.nytimes.com/interactive/2014/01/17/us/nsa-changes-graphic.html?_r=0 (zugegriffen am 8.1.2015).

Kerkmann, Christof (2013): „Kommentar: Politischer Kuhhandel beim Datenschutz", Handelsblatt, 17.12.2013, http://www.handelsblatt.com/meinung/kommentare/kommentar-politischer-kuhhandel-beim-datenschutz/9230896.html (zugegriffen am 2.3.2015).

Kiometzis, Michael (2014): „E-Mail made in Germany", DuD - Datenschutz und Datensicherheit 38/10, S. 709-713.

Kreissl, Reinhard u. a. (2015): „Surveillance: Preventing and detecting crime and terrorism", in: Wright, David und Reinhard Kreissl (Hrsg.): Surveillance in Europe, 1. Aufl., Abingdon; New York: Routledge, S. 150-210.

Krempl, Stefan (2010): „EU-Parlament verabschiedet neues SWIFT-Abkommen zum Bankdatentransfer", Heise Online, 08.07.2010, http://www.heise.de/newsticker/meldung/EU-Parlament-verabschiedet-neues-SWIFT-Abkommen-zum-Bankdatentransfer-1034690.html (zugegriffen am 11.3.2015).

--- (2012): „EU-Parlament segnet Fluggastdaten-Transfer in die USA ab", Heise Online, 19.04.2012, http://www.heise.de/newsticker/meldung/EU-Parlament-segnet-Fluggastdaten-Transfer-in-die-USA-ab-1542874.html (zugegriffen am 24.2.2015).

--- (2015): „Ex-BND-General: NSA wollte Wirtschaftsspionage betreiben", Heise Online, 06.03.2015, http://www.heise.de/newsticker/meldung/Ex-BND-General-NSA-wollte-Wirtschaftsspionage-betreiben-2569294.html (zugegriffen am 7.3.2015).

Kühl, Eike (2015): „Mobile World Congress: Aus Abhörwanzen sollen Datentresore werden", Zeit Online, 03.03.2015, http://www.zeit.de/digital/datenschutz/2015-03/blackphone-knox-qualcomm-sicherheit-datenschutz (zugegriffen am 13.8.2015).

Kuhn, Johannes (2013): „Mit der Handschrift von Lobbyisten", Süddeutsche.de, 02.11.2013, http://www.sueddeutsche.de/politik/lobbyplageu-zum-datenschutz-mit-der-handschrift-von-lobbyisten-1.1596685 (zugegriffen am 2.4.2015).

Kurz, Constanze (2010): „Aus dem Maschinenraum Der Hacker", Frankfurter Allgemeine Zeitung, 19.02.2010, http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/aus-dem-maschinenraum-der-hacker-1939779.html?printPagedArticle=true#pageIndex_2 (zugegriffen am 3.12.2014).

--- (2014): „Knapp ein Jahr im Amt: Die Datenschutzbeauftragte ist ein Desaster", Frankfurter Allgemeine Zeitung, 18.11.2014, http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/andrea-vosshoff-versagt-als-datenschutzbeauftragte-13269359.html?printPagedArticle=true#pageIndex_2 (zugegriffen am 19.11.2014).

Laffont, Jean-Jacques und Jean Tirole (1991): „The Politics of Government Decision-Making: A Theory of Regulatory Capture", The Quarterly Journal of Economics 106/4, S. 1089-1127.

Lazer, David u. a. (2014): „The Parable of Google Flu: Traps in Big Data Analysis", Science 343/6176, S. 1203-1205.

Leisegang, Daniel (2011): „Das Wettrüsten im Internet", Blätter für deutsche und internationale Politik 11/2011, S. 79-86.

--- (2013a): „Geheimdienste außer Kontrolle: Wer überwacht eigentlich die Überwacher“, in: Beckedahl, Markus und Andre Meister (Hrsg.): Überwachtes Netz, Edward Snowden und der größte Überwachungsskandal der Geschichte, Berlin: newthinking communications in Kooperation mit epubli GmbH, S. 133-137, https://netzpolitik.org/wp-upload/Ueberwachtes-Netz-Markus-Beckedahl-Andre-Meister.pdf (28.9.2015).

--- (2013b): „Schöne neue Überwachungswelt“, Blätter für deutsche und internationale Politik 8/2013, S. 5-8.

Lepsius, Oliver (2004): „Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland“, Leviathan 32/1, S. 64-68.

Lever, Annabelle (2006): „Privacy Rigths and Democracy: A Contradiction in Terms?“, Contemporary Political Theory 5, S. 142-162.

Levison, Ladar (2014): „Secrets, lies and Snowden’s email: why I was forced to shut down Lavabit“, The Guardian, 20.05.2014, http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email (zugegriffen am 13.2.2015).

Levy-Abegnoli, Julie (2015): „No EU data protection deal ‚before end of year‘“, The Parliament Magazine, 01.2015, https://www.theparliamentmagazine.eu/articles/news/no-eu-data-protection-deal-end-year (zugegriffen am 3.4.2015).

Lewinski, Kai von (2009): „Geschichte des Datenschutzrechts von 1600 bis 1977“, in: Arndt, Felix u. a. (Hrsg.): Freiheit - Sicherheit - Öffentlichkeit: 48. Assistententagung Öffentliches Recht, Heidelberg 2008, 1. Aufl., Baden-Baden: Nomos, S. 196-220.

--- (2014): Die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes, Tübingen: Mohr Siebeck.

Leyendecker, Hans und Georg Mascolo (2014): „Bundesanwalt ermittelt nun doch“, Süddeutsche.de, 06.03.2014, http://www.sueddeutsche.de/politik/merkels-abgehoertes-handy-karlsruher-kehrtwende-1.1984723 (zugegriffen am 19.1.2015).

Lichtblau, Eric und James Risen (2006): „Bank Data Is Sifted by U.S. in Secret to Block Terror“, The New York Times, 23.06.2006, http://www.nytimes.com/2006/06/23/washington/23intel.html (zugegriffen am 11.3.2015).

London Economics (2010): „Study on the economic benefits of privacy-enhancing technologies (PETs)“, Final Report to The European Commission - DG Justice, Freedom and Security, http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (zugegriffen am 7.9.2015).

Lovink, Geert und Pit Schultz (1996): „Der Anti-Barlow“, Telepolis, 07.05.1996, http://www.heise.de/tp/artikel/1/1030/ (zugegriffen am 25.2.2015).

MacAskill, Ewen u. a. (2013): „GCHQ taps fibre-optic cables for secret access to world’s communications“, The Guardian, 21.06.2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (zugegriffen am 25.6.2014).

Marr, Mirko (2005): Internetzugang und politische Informiertheit: Zur digitalen Spaltung der Gesellschaft, Reihe: Forschungsfeld Kommunikation, Bd. 19, UVK Verlagsgesellschaft.

Mascolo, Georg, Hans Leyendecker und John Goetz (2014): „Codewort Eikonal - der Albtraum der Bundesregierung", Süddeutsche.de, 10.04.2014, http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432 (zugegriffen am 26.2.2015).

Max-Planck-Institut für ausländisches und internationales Strafrecht (2011): „Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten", Gutachten, Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht, http://vds.brauchts.net/MPI_VDS_Studie.pdf (zugegriffen am 11.9.2015).

Mayer-Schönberger, Viktor (1998): „Generational development of data protection in Europe", in: Agre, Philip E. und Marc Rotenberg (Hrsg.): Technology and Privacy: The New Landscape, Cambridge, MA, USA: MIT Press, S. 219-241, http://dl.acm.org/citation.cfm?id=275283.275292 (zugegriffen am 1.10.2014).

Mayer-Schönberger, Viktor und Kenneth Cukier (2013): Big Data: Die Revolution, die unser Leben verändern wird, München: Redline Verlag.

Medine, David u. a. (2015): „Recommendations Assessment Report", Washington, D.C.: President's Review Group on Intelligence and Communications Technologies des Privacy and Civil Liberties Oversight Board (PCLOB), https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf (zugegriffen am 24.2.2015).

Meister, Andre (2008): „Vorratsdatenspeicherung und gesellschaftliche Kontroverse", Bachelorarbeit, Humboldt-Universität zu Berlin, https://netzpolitik.org/wp-upload/Bachelor_Meister_Vorratsdatenspeicherung.pdf (zugegriffen am 7.1.2015).

Mills, C. Wright (1956): The Power Elite, Oxford/New York: Oxford University Press.

Monroy, Matthias (2009): „Der sicherheitsindustrielle Komplex der EU", Telepolis, 25.09.2009, http://www.heise.de/tp/artikel/31/31196/ (zugegriffen am 10.4.2015).

--- (2014): „Großer Bundestrojaner ist ‚einsatzbereit', kleiner Bundestrojaner wird noch eine Zeitlang ausprobiert", Netzpolitik.org, 15.08.2014, https://netzpolitik.org/2014/grosser-bundestrojaner-inzwischen-einsatzbereit-kleiner-bundestrojaner-wird-noch-eine-zeitlang-ausprobiert/ (zugegriffen am 7.2.2015).

Nau, Johannes (2014): „'Why Protest? I've got nothing to hide' Collective Action against and Chilling Effects of Internet Mass Surveillance", Masterarbeit, Philipps Universität Marburg/University of Kent, https://www.academia.edu/9795304/_Why_protest_I_ve_got_nothing_to_hide_Collective_Action_against_and_Chilling_Effects_of_Internet_Mass_Surveillance (zugegriffen am 25.2.2015).

Naumann, Michael (2009): „Verfassungsklage gegen neues BKA-Gesetz: Jeder ist verdächtig", Die Zeit, Nr. 18 /2009, 23.04.2009, http://www.zeit.de/2009/18/BKA-Gesetz (zugegriffen am 7.2.2015).

Neskovic, Wolfgang (2013): „NSA und BND: Die Geheimdienste sind außer Kontrolle", Der Tagesspiegel Online, 18.07.2013, http://www.tagesspiegel.de/meinung/nsa-und-bnd-geheimdienstler-halten-kontrollgremium-fuer-maerchenstunde/8511232-2.html (zugegriffen am 22.4.2015).

Newman, Abraham L. (2008): „Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", International Organization 62, S. 103-130.

NZZ (2009): „Weitergabe von Kundendaten – Zahlung von 780 Millionen Dollar: Kapitulation im Steuerstreit mit den USA“, Neue Zürcher Zeitung, 18.02.2009, http://www.nzz.ch/finanzmarktaufsicht-bankgeheimnis-ubs--1.2037969 (zugegriffen am 22.4.2015).

OECD (1980): OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris: Organisation for Economic Co-operation and Development, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (zugegriffen am 27.7.2015).

Oswald, Bernd (2010): „Das Parlamentarische Kontrollgremium: Viel Stille um zu wenig Info“, Süddeutsche.de, 19.05.2010, http://www.sueddeutsche.de/politik/das-parlamentarische-kontrollgremium-viel-stille-um-zu-wenig-info-1.896020 (zugegriffen am 22.4.2015).

Papier, Hans-Jürgen (2012): „Verfassungsrechtliche Grundlegung des Datenschutzes“, Bd. 1190, in: Schmidt, Jan-Hinrik und Thilo Weichert (Hrsg.): Datenschutz: Grundlagen, Entwicklungen und Kontroversen, Bonn: Bundeszentrale für politische Bildung, Bd. 1190, S. 67-77.

Paul, Michael (2015): „Die amerikanische Schwerpunktverlagerung nach Asien“, SWP-Studie, S 5, Berlin: Stiftung Wissenschaft und Politik, http://www.swp-berlin.org/de/publikationen/swp-studien-de/swp-studien-detail/article/us_militaerpolitik_schwerpunktverlagerung_nach_asien.html (zugegriffen am 23.9.2015).

Petri, Thomas B. (2008): „Das Urteil des Bundesverfassungsgerichts zur ‚Online-Durchsuchung‘“, DuD - Datenschutz und Datensicherheit 32/7, S. 443-448.

Pew Research Center (2014): „Global Opinions of U.S. Surveillance: Germany“, Pew Research Center’s Global Attitudes Project, http://www.pewglobal.org/2014/07/14/nsa-opinion/ (zugegriffen am 25.2.2015).

Pohl, Hartmut (2007): „Zur Technik der heimlichen Online-Durchsuchung“, DuD - Datenschutz und Datensicherheit 31/9, S. 684-688.

Poullet, Yves (2010): „About the E-Privacy Directive: towards a third generation of data protection legislation?“, in: Gutwirth, Serge, Yves Poullet und Paul De Hert (Hrsg.): Data protection in a profiled world, Dordrecht/Heidelberg/London/New York: Springer-Verlag, S. 3-30.

Prantl, Heribert (2010): „BKA-Gesetz: ‚Gegen den Sicherheitsstaat‘“, Süddeutsche.de, 17.05.2010, http://www.sueddeutsche.de/politik/bka-gesetz-gegen-den-sicherheitsstaat-1.405592 (zugegriffen am 7.2.2015).

--- (2011): „Staatliche Daten-Spionage: Trojaner fressen Grundrecht auf“, Süddeutsche.de, 13.10.2011, http://www.sueddeutsche.de/digital/staatliche-daten-spionage-trojaner-fressen-grundrecht-auf-1.1158728 (zugegriffen am 3.2.2015).

--- (2013): „Große Koalition: Zu Lasten von Datenschutz und Grundrechten“, Süddeutsche.de, 28.11.2013, http://www.sueddeutsche.de/politik/schwarz-roter-koalitionsvertrag-zu-lasten-von-datenschutz-und-grundrechten-1.1829791 (zugegriffen am 18.2.2015).

--- (2014): „NSA: Harald Range ermittelt nur ein klein wenig“, Süddeutsche.de, 06.05.2014, http://www.sueddeutsche.de/politik/ermittlungen-in-der-nsa-affaere-an-der-aufklaerung-vorbeigemogelt-1.1985636 (zugegriffen am 18.2.2015).

Ramm, Arnim (2007): „§ 46 BDSG - Eine Übergangsvorschrift? - Die ‚Weitergeltung von Begriffsbestimmungen‘ nach § 46 BDSG am Beispiel der inneren Sicherheit“, DuD - Datenschutz und Datensicherheit 31/6, S. 431-433.

Rath, Christian (2015): „Heiko Maas und Vorratsdatenspeicherung: ‚Ja, das war ich'", Die Tageszeitung (taz), 27.7.2015, http://www.taz.de/Heiko-Maas-und-Vorratsdatenspeicherung/!5215559/ (zugegriffen am 17.9.2015).

Reißmann, Ole (2013): „Freiheit statt Angst 2013: Demonstration gegen NSA-Überwachung", Spiegel Online, 09.07.2013, http://www.spiegel.de/netzwelt/netzpolitik/freiheit-statt-angst-2013-demonstration-gegen-nsa-ueberwachung-a-920927.html (zugegriffen am 25.2.2015).

Reuter, Markus und Michael Stognienko (2014): „Modelle zu Reform und Abschaffung der Geheimdienste", in: Beckedahl, Markus, Anna Biselli und Andre Meister (Hrsg.): Jahrbuch Netzpolitik 2014, Berlin: epubli, S. 117-126, https://pound.netzpolitik.org/wp-upload/JahrbuchNetzpolitik2014.pdf (zugegriffen am 9.9.2015).

Reuters Institute (2014): „Reuters Institute Digital News Report 2014. Tracking the Future of News", Oxford: Reuters Institute for the Study of Journalism, University of Oxford, http://www.digitalnewsreport.org/survey/2014/ (zugegriffen am 5.4.2015).

Rieger, Frank (2011): „Ein amtlicher Trojaner Anatomie eines digitalen Ungeziefers", Frankfurter Allgemeine Zeitung, 10.09.2011, http://www.faz.net/aktuell/feuilleton/ein-amtlicher-trojaner-anatomie-eines-digitalen-ungeziefers-11486473.html (zugegriffen am 7.2.2015).

Ripsman, Norrin M. (2006): „False dichotomies: Why Economics is high politics", Ridgway Center Working Papers 11, Pittsburgh (USA): Matthew B Ridgway Center for International Security Studies, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=22143&%3Blng=en (zugegriffen am 7.8.2015).

Risen, James und Laura Poitras (2013): „N.S.A. Report Outlined Goals for More Power", The New York Times, 22.11.2013, http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html (zugegriffen am 12.11.2014).

Roberts, Andrew (2015): „A republican account of the value of privacy", European Journal of Political Theory 14/3, S. 320-344.

Rodrigues, Rowena (2015): „The surveillance industry in Europe", in: Wright, David und Reinhard Kreissl (Hrsg.): Surveillance in Europe, 1. Aufl., Abingdon/New York: Routledge, S. 103-149.

Rosenbach, Marcel und Jörg Schindler (2015): „Fehlende Auskunft der USA: Generalbundesanwalt stellt Ermittlungen zu abgehörtem Merkel-Handy ein", Spiegel Online, 12.06.2015, http://www.spiegel.de/politik/deutschland/abgehoertes-merkel-handy-generalbundesanwalt-stellt-ermittlungen-ein-a-1038458.html (zugegriffen am 11.9.2015).

Rosenbach, Marcel und Hilmar Schmundt (2009): „Aufstand der Netzbürger", Der Spiegel, 32/2009, 03.08.2009, http://www.spiegel.de/spiegel/print/d-66284673.html (zugegriffen am 25.2.2015).

Roßnagel, Alexander (2011): „Datenschutz und innere Sicherheit", in: Humanistische Union (Hrsg.): Perspektiven des nationalen und europäischen Schutzes der Bürger- und Menschenrechte. Erstes Gustav-Heinemann-Forum, Norderstedt: Books on Demand GmbH, S. 35-55.

Roßnagel, Alexander, Andreas Pfitzmann und Hansjürgen Garstka (2001): „Modernisierung des Datenschutzrechts", Gutachten im Auftrag des Bundesministeriums des Innern, Berlin: Bundeministerium des Innern,

http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile (zugegriffen am 25.9.2014).

Roßnagel, Alexander, Philipp Richter und Maxi Nebel (2012): „Internet Privacy aus rechtswissenschaftlicher Sicht", Bd. acatech Studie, in: Buchmann, Johannes (Hrsg.): Internet Privacy. Eine multidisziplinäre Bestandsaufnahme, Berlin/Heidelberg: Springer-Verlag, S. 281-326, http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Projektberichte/acatech_STUDIE_Internet_Privacy_WEB.pdf (zugegriffen am 25.11.2014).

Rost, Martin und Kirsten Bock (2011): „Privacy By Design und die Neuen Schutzziele", DuD - Datenschutz und Datensicherheit 35/1, S. 30-35.

Rötzer, Florian (2007): „EU und USA erzielen Vereinbarungen über Flugpassagier- und Finanzdaten", Heise Online, 27.06.2007, http://www.heise.de/newsticker/meldung/EU-und-USA-erzielen-Vereinbarungen-ueber-Flugpassagier-und-Finanzdaten-144928.html (zugegriffen am 11.3.2015).

Rumold, Mark und Rainey Reitman (2015): „One Year Later, Obama Failing on Promise to Rein in NSA", Electronic Frontier Foundation, 03.02.2015, https://www.eff.org/deeplinks/2015/02/one-year-later-obama-failing-promise-rein-nsa (zugegriffen am 26.2.2015).

Sauerbrey, Anna (2013): „Datenschutz unter der großen Koalition: Nicht auf dem Schirm", Der Tagesspiegel, 26.10.2013, http://www.tagesspiegel.de/meinung/datenschutz-unter-der-grossen-koalition-nicht-auf-dem-schirm/8988406.html (zugegriffen am 18.2.2015).

Sawall, Achim (2013): „G-10: Bundesregierung setzt Abhörpakt mit USA und UK außer Kraft", Golem.de, 02.08.2013, http://www.golem.de/news/g-10-bundesregierung-setzt-abhoerpakt-mit-usa-und-uk-ausser-kraft-1308-100771.html (zugegriffen am 9.2.2015).

Schaar, Peter (2012): „§55 Datenschutz und Föderalismus. Schöpferische Vielfalt oder Chaos?", in: Härtel, Ines (Hrsg.): Handbuch Föderalismus – Föderalismus als demokratische Rechtsordnung und Rechtskultur in Deutschland, Europa und der Welt, Berlin/Heidelberg: Springer-Verlag, S. 95-108.

Schäfer, Friedrich (1966): Die Notstandsgesetze. Vorsorge für den Menschen und den demokratischen Rechtsstaat, Bd. Demokratische Existenz heute, Köln/Opladen: Westdeutscher Verlag, http://nbn-resolving.de/urn:nbn:de:1111-20120810436 (zugegriffen am 12.12.2014).

Scherschel, Fabian A. (2015): „Der WhatsApp-Verschlüsselung auf die Finger geschaut", Heise Security, 30.04.2015, http://www.heise.de/security/artikel/Der-WhatsApp-Verschluesselung-auf-die-Finger-geschaut-2629020.html (zugegriffen am 13.8.2015).

Schlie, Erik, Jörg Rheinboldt und Niko Waesche (2011): Simply Seven: Seven Ways to Create a Sustainable Internet Business, Basingstoke, (UK)/New York: Macmillan Education.

Schmidt, Jürgen (2014): „Kommentar: Warum Google uns echte Verschlüsselung verweigert", Heise Security, 19.05.2014, http://www.heise.de/security/artikel/Warum-Google-uns-echte-Verschluesselung-verweigert-2191797.html (zugegriffen am 12.1.2015).

Schulte, Ulrich (2015): „SPD für Vorratsdatenspeicherung: Rebellion à la SPD“, Die Tageszeitung (taz), 20.06.2015, http://www.taz.de/!5205394/ (zugegriffen am 11.9.2015).

Schulzki-Haddouti, Christiane (2015a): „Crypto Wars 3.0: Erneuter Streit um Quellen-TKÜ“, Heise Online, http://www.heise.de/newsticker/meldung/Crypto-Wars-3-0-Erneuter-Streit-um-Quellen-TKUe-2534095.html (zugegriffen am 7.2.2015).

--- (2015b): „Deutsche Datenschutzbehörden leiden unter Personalknappheit“, c't, 17/15, 24.07.2015, S. 76-78.

Schulz, Stefan (2014): „App für Gesichtserkennung: ‚Seien Sie kein Fremder!'“, Frankfurter Allgemeine Zeitung, 13.01.2014, http://www.faz.net/aktuell/feuilleton/medien/app-fuer-gesichtserkennung-seien-sie-kein-fremder-12749493.html (zugegriffen am 13.1.2015).

Schütz, Philip (2012a): „The Set Up of Data Protection Authorities as a New Regulatory Approach“, in: Gutwirth, Serge u. a. (Hrsg.): European Data Protection: In Good Health?, Dordrecht: Springer Netherlands, S. 125-142.

--- (2012b): „Accountability and Independence of Data Protection Authorities - A Trade-Off?“, in: Guagnin, Daniel u. a. (Hrsg.): Managing Privacy through Accountability, Basingstoke: Palgrave Macmillan.

--- (2012c): „Comparing formal independence of data protection authorities in selected EU Member States“, Conference: 4th Biennial ECPR Standing Group for Regulatory Governance Conference 2012, Exeter (UK), http://regulation.upf.edu/exeter-12-papers/Paper%20265%20-%20Schuetz%202012%20-%20Comparing%20formal%20independence%20of%20data%20protection%20authorities%20in%20selected%20EU%20Member%20States.pdf (zugegriffen am 7.10.2014).

Seeger, Jürgen (2011): „To cloud or not to cloud“, iX Magazin für professionelle Informationstechnik 11/2011, http://www.heise.de/ix/artikel/To-cloud-or-not-to-cloud-1355056.html (zugegriffen am 12.2.2015).

Sennett, Richard (1983): Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität, Frankfurt am Main: Fischer.

Seubert, Sandra (2012): „Der gesellschaftliche Wert des Privaten“, DuD - Datenschutz und Datensicherheit 36/2, S. 100-104.

Sigler, Constanze (2010): „Online-Medien und Marketing“, Online-Medienmanagement, 1. Aufl., Wiesbaden: Gabler.

Simitis, Spiros (2014): „Einleitung: Geschichte - Ziele - Prinzipien“, in: Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, Nomos Kommentar, 8. Aufl., Baden-Baden: Nomos, S. 81-196.

Simonite, Tom (2014): „Die Privatsphäre als Produkt“, Technology Review, 14.02.2014, http://www.heise.de/tr/artikel/Die-Privatsphaere-als-Produkt-2109857.html (zugegriffen am 17.8.2015).

Sokol, Bettina und Philip Scholz (2014): „§4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung“, in: Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, Nomos Kommentar, 8. Aufl., Baden-Baden: Nomos, S. 446-470.

SPD (2013): „Das Wir entscheidet. Das Regierungsprogramm 2013 - 2017, beschlossen auf dem Bundesparteitag am 14. April 2013 in Augsburg“, Wahlprogramm, Augsburg: SPD,

http://www.spd.de/linkableblob/96686/data/20130415_regierungsprogramm_2013_2017.pdf (zugegriffen am 27.1.2015).

Spiegel Online (2007): „Online-Durchsuchung: NRW-Verfassungsschutz spioniert weiter durchs Netz“, Spiegel Online, 02.06.2007, http://www.spiegel.de/netzwelt/web/online-durchsuchung-nrw-verfassungschutz-spioniert-weiter-durchs-netz-a-464631.html (zugegriffen am 2.2.2015).

--- (2013): „Brüssel: EU-Ministerrat bremst Datenschutzreform“, Spiegel Online, 06.06.2013, http://www.spiegel.de/netzwelt/netzpolitik/bruessel-eu-ministerrat-bremst-datenschutzreform-a-904266.html (zugegriffen am 3.9.2014).

--- (2014a): „Bundesverwaltungsgericht: Bayern darf Kfz-Nummernschilder erfassen“, Spiegel Online, 22.10.2014, http://www.spiegel.de/auto/aktuell/bundesverwaltungsgericht-bayern-darf-kfz-nummernschilder-erfassen-a-998640.html (zugegriffen am 27.1.2015).

--- (2014b): „BND führt Nato-Partner Türkei als Aufklärungsziel“, Spiegel Online, 16.08.2014, http://www.spiegel.de/politik/deutschland/bnd-fuehrt-nato-partner-tuerkei-als-aufklaerungsziel-spiegel-exklusiv-a-986432.html (zugegriffen am 22.9.2015).

Spiekermann, Sarah (2012): „Datenschutzgesetz: Die Verwässerer“, Zeit Online, 11.08.2012, http://www.zeit.de/2012/46/Deutsches-Datenschutzgesetz-Spiekermann (zugegriffen am 12.1.2015).

Spiekermann, Sarah, Jens Grossklags und Bettina Berendt (2001): „E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior“, Proceedings of the 3rd ACM conference on Electronic Commerce, New York: ACM, http://dl.acm.org/citation.cfm?id=501163 (zugegriffen am 8.4.2015).

Staten, James (2013): „The Cost of PRISM Will Be Larger Than ITIF Projects“, Cambridge, MA (USA): Forrester Research, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects (zugegriffen am 27.6.2014).

Statista (2015): „Welches sind Ihrer Meinung nach die wichtigsten Probleme, denen Deutschland derzeit gegenübersteht?“, Statista, http://de.statista.com/statistik/daten/studie/2739/umfrage/ansicht-zu-den-wichtigsten-problemen-deutschlands/ (zugegriffen am 30.9.2015).

Steier, Henning (2014): „Schweizer Unternehmen lanciert relativ abhörsicheres Blackphone: «99,99 Prozent der Handynutzer im Visier»“, Neue Zürcher Zeitung, 27.06.2014, http://www.nzz.ch/digital/mike-janke-interview-blackphone-1.18330071 (zugegriffen am 13.8.2015).

Steinmüller, Wilhelm u. a. (1971): „Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministerium des Innern“, Drucksache VI/3826Bonn: Deutscher Bundestag (6. Wahlperiode), http://www.maroki.de/pub/dphistory/1971_Steinmuellller_39398927-Grundfragen-Datenschutz-BAD06-3826.pdf (zugegriffen am 24.9.2014).

Stevens, Gunnar, Timo Jakobi und Kai-Oliver Detken (2014): „Mehrseitige, barrierefreie Sicherheit intelligenter Messsysteme“, DuD - Datenschutz und Datensicherheit 38/8, S. 536-544.

Stiftung Warentest (2012): „Datenschutz bei Apps: Welche Apps Ihre Daten ausspähen“, Stiftung Warentest 6/2012, S. 39-43.

Störing, Marc (2014): „EU Kommission zur Cookie-Richtlinie: Vorgaben für Cookies gelten in Deutschland“, Heise Online, 07.02.2014, http://www.heise.de/newsticker/meldung/EU-Kommission-zur-Cookie-Richtlinie-

Vorgaben-fuer-Cookies-gelten-in-Deutschland-2107770.html (zugegriffen am 25.11.2014).

Streinz, Rudolf (2011): „Die Rechtsprechung des EuGH zum Datenschutz", DuD - Datenschutz und Datensicherheit 35/9, S. 602-606.

Talbot, David (2011): „Das Geschäft mit der Netzüberwachung", Technology Review, 23.12.2011, http://www.heise.de/tr/artikel/Das-Geschaeft-mit-der-Netzueberwachung-1397385.html (zugegriffen am 21.4.2015).

Tanriverdi, Hakan (2014): „Whatsapp-Konkurrent Threema verdoppelt Nutzerzahl", Süddeutsche.de, 21.02.2014, http://www.sueddeutsche.de/digital/seit-facebook-deal-whatsapp-konkurrent-threema-verdoppelt-nutzerzahl-1.1894768 (zugegriffen am 12.1.2015).

The Washington Post (2013): „NSA slides explain the PRISM data-collection program", The Washington Post, 07.10.2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (zugegriffen am 29.8.2014).

The White House (2011): „International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World", Washington, D.C.: The White House, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (zugegriffen am 24.9.2015).

Thomé, Sarah (2015): Reform der Datenschutzaufsicht. Effektiver Datenschutz durch verselbstständigte Aufsichtsbehörden, Wiesbaden: Springer Vieweg.

Tinnefeld, Marie-Theres, Thomas Petri und Benedikt Buchner (2012): Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Aufl., München: Oldenbourg Wissenschaftsverlag.

Tomik, Stefan (2007): „Online-Durchsuchung: Die Angst vorm Bundestrojaner", Frankfurter Allgemeine Zeitung, 10.09.2007, http://www.faz.net/aktuell/politik/inland/online-durchsuchung-die-angst-vorm-bundestrojaner-1462090.html (zugegriffen am 2.2.2015).

Tretbar, Christian (2014): „Reform in homöopathischen Dosen", Der Tagesspiegel, 14.03.2014, http://www.tagesspiegel.de/politik/parlamentarisches-kontrollgremium-reform-in-homoeopathischen-dosen/9613950.html (zugegriffen am 19.8.2015).

ULD (2013): „ULD-Tätigkeitsbericht 2013: Datenschutz als globale Herausforderung", Pressemitteilung, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/presse/20130319-tb34.htm (zugegriffen am 18.2.2015).

--- (2014): „ULD begrüßt Safe-Harbor-Vorlage wegen Facebook beim EuGH", Pressemitteilung, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/presse/20140620-safe-harbor.htm (zugegriffen am 12.2.2015).

U.S. Congress (2001): „Aviation and Transportation Security Act", https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf (zugegriffen am 10.1.2015).

U.S. District Court (2014): „In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation", U.S. District Court. Southern District of New York. Judge James C. Francis, 13 Mag. 2814, http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398 (zugegriffen am 22.4.2015).

U.S. Supreme Court (1967): „Katz v. United States“, 389 U.S. 347, https://supreme.justia.com/cases/federal/us/389/347/ (zugegriffen am 27.7.2015).

Voigt, Rüdiger (Hrsg.) (2012): Sicherheit versus Freiheit: Verteidigung der staatlichen Ordnung um jeden Preis?, Wiesbaden: VS Verlag für Sozialwissenschaften.

VoteWatch Europe (2010): „Agreement between the EU and the USA on the processing and transfer of financial messaging data from the EU to the USA for purposes of the Terrorist Finance Tracking Program“, VoteWatch Europe, http://term7.votewatch.eu/en/agreement-between-the-eu-and-the-usa-on-the-processing-and-transfer-of-financial-messaging-data-from.html (zugegriffen am 12.11.2014).

--- (2011): „EU-Australia agreement on the processing and transfer of PNR data“, VoteWatch Europe, http://term7.votewatch.eu/en/eu-australia-agreement-on-the-processing-and-transfer-of-pnr-data-draft-legislative-resolution-vote-.html (zugegriffen am 29.1.2015).

--- (2012): „EU-USA agreement on the use and transfer of PNR to the US Department of Homeland Security“, VoteWatch Europe, http://term7.votewatch.eu/en/eu-usa-agreement-on-the-use-and-transfer-of-pnr-to-the-us-department-of-homeland-security-draft-legi.html (zugegriffen am 12.11.2014).

--- (2013): „Suspension of the SWIFT agreement as a result of NSA surveillance (S&D, ALDE, Greens/EFA)“, VoteWatch Europe, http://term7.votewatch.eu/en/suspension-of-the-swift-agreement-as-a-result-of-nsa-surveillance-s-d-alde-greens-efa-motion-for-res.html (zugegriffen am 29.1.2015).

--- (2014a): „Opinion of the Court of Justice - EU/Canada agreement on the transfer and processing of Passenger Name Record (PNR) data“, VoteWatch Europe, http://www.votewatch.eu/en/term8-opinion-of-the-court-of-justice-eu-canada-agreement-on-the-transfer-and-processing-of-passenger-name.html#/ (zugegriffen am 29.1.2015).

--- (2014b): „Processing of personal data for the purpose of crime prevention“, VoteWatch Europe, http://term7.votewatch.eu/en/processing-of-personal-data-for-the-purposes-of-crime-prevention-draft-legislative-resolution-vote-l.html#/ (zugegriffen am 29.1.2015).

--- (2014c): „Protection of individuals with regard to the processing of personal data“, VoteWatch Europe, http://term7.votewatch.eu/en/protection-of-individuals-with-regard-to-the-processing-of-personal-data-draft-legislative-resolutio.html#/ (zugegriffen am 29.1.2015).

Warman, Matt (2012): „EU Privacy regulations subject to ‚unprecedented lobbying‘“, The Telegraph, 02.08.2012, http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html (zugegriffen am 1.9.2014).

Warren, Samuel D. und Louis D. Brandeis (1890): „The Right to Privacy“, Harvard Law Review 4/5, S. 193-220.

Weichert, Thilo (2012): „§56 Harmonisierte Instrumente und Standards für Datenschutzkontrollen und Ermittlungsmethoden – Die Situation im föderalen Deutschland“, in: Härtel, Ines (Hrsg.): Handbuch Föderalismus – Föderalismus als demokratische Rechtsordnung und Rechtskultur in Deutschland, Europa und der Welt, Berlin/Heidelberg: Springer-Verlag, S. 109-119.

--- (2013): „PRISM, Tempora, Snowden: Analysen und Perspektiven“, in: Beckedahl, Markus und Andre Meister (Hrsg.): Überwachtes Netz, Edward Snowden und der

größte Überwachungsskandal der Geschichte, Berlin: newthinking communications in Kooperation mit epubli GmbH, S. 179-185, https://netzpolitik.org/wp-upload/Ueberwachtes-Netz-Markus-Beckedahl-Andre-Meister.pdf (28.9.2015).

--- (2014a): „Unabhängige Datenschutzbeauftragte - Gesetzesvorschlag", Legal Tribune Online, 23.09.2014, http://www.lto.de/recht/hintergruende/h/bundesdatenschutzbeauftragte-unabhaengigkeit-gesetzesvorschlag/ (zugegriffen am 25.2.2015).

--- (2014b): „Freihandelsabkommen contra Datenschutz?", DuD - Datenschutz und Datensicherheit 38/12, S. 850-856.

Weidemann, Stefan (2014): „Freiheit unter Beobachtung?", Aus Politik und Zeitgeschichte (APuZ), 64/18-19/2014 (Ausgabe: Überwachen), S. 3-8.

Welt Online (2014): „Hamburger stellen Weltrekord im Crowdfunding auf", Welt Online, 06.05.2014, http://www.welt.de/regionales/hamburg/article128756957/Hamburger-stellen-Weltrekord-im-Crowdfunding-auf.html (zugegriffen am 12.1.2015).

Wendelin, Manuel und Maria Löblich (2013): „Netzpolitik-Aktivismus in Deutschland. Deutungen, Erwartungen und Konstellationen zivilgesellschaftlicher Akteure in der Internetpolitik", M&K Medien & Kommunikationswissenschaft Jahrgang 61, Heft 1, S. 58-75.

Westin, Alan F. (1967): Privacy and Freedom, 6. Aufl., New York: Atheneum.

Whitman, James Q. (2004): „The two western cultures of privacy: Dignity versus liberty", The Yale Law Journal 113/6, S. 1151-1221.

Wolter, Clarice (2011): „Gesichtserkennung bei Facebook Gesucht, erkannt, verlinkt", Frankfurter Allgemeine Zeitung, 06.08.2011, http://www.faz.net/aktuell/technik-motor/computer-internet/gesichtserkennung-bei-facebook-gesucht-erkannt-verlinkt-1657009.html (zugegriffen am 30.11.2014).

Wu, Tim (2012): Der Master Switch. Aufstieg und Niedergang von Medienimperien, Heidelberg/München/Landsberg/Frechen/Hamburg: MITP Verlag.

Zeit Online (2013): „Facebook hat alle Daten aus Gesichtserkennung gelöscht", Zeit Online, 02.07.2013, http://www.zeit.de/digital/datenschutz/2013-02/facebook-gesichtserkennung-verfahren-caspar (zugegriffen am 11.9.2015).

Zerdick, Axel u. a. (2001): Die Internet-Ökonomie: Strategien für die digitale Wirtschaft, 3. Aufl., Berlin/Heidelberg: Springer-Verlag.

Ziercke, Jörg (2008): „Pro Online-Durchsuchung", Informatik-Spektrum 31/1, S. 62-64.

Zivadinovic, Dusan (2014): „E-Mail made in Germany: Vollständig umgesetzt, dennoch unzureichend", Heise Netze, 29.04.2014, http://www.heise.de/netze/meldung/E-Mail-made-in-Germany-Vollstaendig-umgesetzt-dennoch-unzureichend-2179269.html (zugegriffen am 13.2.2015).

Zurawski, Nils (2014): „Geheimdienste und Konsum der Überwachung", Aus Politik und Zeitgeschichte (APuZ) 64/18-19/2014 (Ausgabe: Überwachen), S. 14-19.

Abkürzungsverzeichnis

BAG	Bundesarbeitsgericht
BfDI	Bundesbeauftragte/r für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CALEA	Communications Assistance for Law Enforcement Act
CCC	Chaos Computer Club
DS-GVO	Datenschutz-Grundverordnung
DVD	Deutsche Vereinigung für Datenschutz
EuGH	Europäischer Gerichtshof
EDRi	European Digital Rights
EFF	Electronic Frontier Foundation
FIfF	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung
GCHQ	Government Communications Headquarter
GDD	Gesellschaft für Datenschutz und Datensicherheit
IKT	Informations- und Kommunikationstechnologien
IP	Internet Protokoll
LfD	Landesbeauftragte/r für den Datenschutz
LIBE	Ausschuss für bürgerliche Freiheiten, Justiz und Inneres
LKA	Landeskriminalamt
ISP	Internet Service Provider
MAD	Militärischer Abschirmdienst
NGO	Nichtregierungsorganisation
NSA	National Security Agency
NSU	Nationalsozialistischer Untergrund
RAF	Rote Armee Fraktion

PC	Personal Computer
PCLOB	Privacy and Civil Liberties Oversight Board
PostG	Postgesetz
PI	Privacy International
PET	Privacy Enhancing Technology
PGP	Pretty Good Privacy
PKGr	Parlamentarisches Kontrollgremium
PKGrG	Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes
PNR	Passenger Name Record
Quellen-TKÜ	Quellen-Telekommunikationsüberwachung
StPO	Strafprozessordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFTP	Terrorist Finance Tracking Program
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TKÜV	Telekommunikationsüberwachungsverordnung
TTIP	Transatlantic Trade and Investment Partnership
ULD	Unabhängiges Landeszentrum für Datenschutz
USA FREEDOM Act	Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

Tabelle 1: Bundesverfassungsgerichtsurteile seit 1983 im Spannungsverhältnis von Grundrechtsschutz und Sicherheitsinteressen (eigene Darstellung)

Fall	Jahr	Entscheidung	Verletzte Grundrechte	Rechtlicher Klagegrund
Rasterfahndung (I)	1995	verfassungskonform (mit Maßgaben)	–	Änderung des Artikel-10-Gesetz
Telekommunikationsüberwachung (I)	1999	in weiten Teilen verfassungswidrig	TK-Geheimnis (Art. 10 GG), Pressefreiheit (Art. 5 (1) 2 GG), Rechtsschutzgarantie (Art. 19 (4) GG)	Änderung des Artikel-10-Gesetz
Genetischer Fingerabdruck (I)	2000	verfassungswidrig	Informationelle Selbstbestimmung	Gerichtsentscheidung
Großer Lauschangriff	2004	verfassungswidrig: Änderung der StPO; verfassungskonform: Änderung von Art. 13 GG	Schutz der Menschenwürde (Art. 1 (1) GG), Rechtsschutzgarantie (Art. 19 (4) GG)	Änderung von Art. 13 (3-6) GG und der StPO
GPS-Überwachung	2005	verfassungskonform	–	Bestehende StPO
Vorbeugendes Abhören von Telefonen (Telekommunikationsüberwachung (II))	2005	verfassungswidrig	TK-Geheimnis (Art. 10 GG)	Änderung des niedersächsischen Polizeigesetzes
Rasterfahndung (II)	2006	verfassungswidrig	Informationelle Selbstbestimmung	Gerichtliche Anordnung in NRW
Standorte eingeschalteter Handys	2006	verfassungskonform	–	Änderung der StPO (§ 100 i)
Heimlicher Zugriff auf Kontenstammdaten	2007	größtenteils verfassungskonform	–	Gesetz zur Förderung der Steuerehrlichkeit
Online-Dursuchung	2008	verfassungswidrig	IT-Grundrecht	Änderung des Landesverfassungsschutzgesetzes NRW
Automatisierte Massenkontrolle von Autokennzeichen per Videokamera	2008	verfassungswidrig	Informationelle Selbstbestimmung	Änderung des Landesverwaltungsgesetzes Schleswig-Holstein (§ 184 (5)) und des hessischen Polizeigesetzes (§ 14 (5))
Genetischer Fingerabdruck (II)	2009	verfassungswidrig	Informationelle Selbstbestimmung	Gerichtsentscheidung
Vorratsdatenspeicherung	2010	in weiten Teilen verfassungswidrig	TK-Geheimnis (Art. 10 (1) GG)	Gesetz zur Neuregelung der TKÜ und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG
Bestandsdatenauskunft	2012	verfassungskonform: Speicherung; verfassungswidrig: Herausgabe von Zugangscode sowie Anschlussinhaber-Identifizierung anhand von IP-Adressen	Informationelle Selbstbestimmung bzw. TK-Geheimnis (Art. 10 (1) GG)	Änderung des TKG
Antiterrordatei	2013	in weiten Teilen verfassungswidrig	Informationelle Selbstbestimmung, TK-Geheimnis (Art. 10 (1) GG) und Unverletzlichkeit der Wohnung (Art. 13 (1) GG)	Antiterrordateigesetz

IMPRESSUM

Kontakt:
Peter Zoche
Koordinator Sicherheitsforschung und Technikfolgenabschätzung

Telefon +49 721 6809-152
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage: 200 Stück
November 2015

Druck
Stober GmbH Druck und Verlag, Eggenstein

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT HOHENHEIM
LEHRSTUHL FÜR MEDIENPSYCHOLOGIE

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein