ITeG | Interdisciplinary Research on Information System Design | 6

Barbara Büttner | Christian L. Geminn |
Charlotte Husemann |
Nadine Miedzianowski

Die Arena der Datenschutz-Grundverordnung

ITeG Research Center for Information System Design

kassel university press

ITeG – Interdisciplinary Research on Information System Design

Band 6 / Vol. 6

Herausgegeben von / Edited by
ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung
an der Universität Kassel

Universität Kassel
ITeG Wissenschaftliches Zentrum
für Informationstechnik-Gestaltung
Pfannkuchstraße 1
D-34121 Kassel

Barbara Büttner, Christian Geminn,
Charlotte Husemann, Nadine Miedzianowski

Die Arena der Datenschutz-Grundverordnung

kassel university press

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

ISBN 978-3-7376-0564-9 (print)
ISBN 978-3-7376-0565-6 (e-book)
DOI: http://dx.medra.org/10.19211/KUP9783737605656
URN: http://nbn-resolving.de/urn:nbn:de:0002-405654

www.upress.uni-kassel.de/

Printed in Germany

VORWORT DER HERAUSGEBER

Privatheit ist zu einem umstrittenen und unsicheren Begriff geworden. Nicht nur für Staaten entstehen neue Überwachungsmöglichkeiten, auch für Unternehmen eröffnen sich Geschäftsmodelle, die klassische Vorstellungen von Privatheit in Frage stellen. Das BMBF-Projekt „Kartografie und Analyse der Privacy-Arena" untersuchte deshalb die politischen Prozesse, die diesen Wandel von Privatheit vorantreiben, begrenzen und bewerten. Exemplarisch untersucht wurden dafür öffentliche Auseinandersetzungen rund um Privatheit – dazu gehörten die Verhandlungen um die Ausgestaltung der Datenschutz-Grundverordnung.

Die Datenschutz-Grundverordnung bedeutet eine fundamentale Neuordnung des Datenschutzrechts in Europa. Ihrem Inkrafttreten gingen zähe und komplexe Verhandlungen voraus, in deren Kern die Frage nach einem wirksamen Schutz von Privatheit und informationeller Selbstbestimmung im digitalen Zeitalter stand. In diesen Debatten versammelten sich verschiedene Akteure und Instanzen mit all ihren widerstreitenden Interessen und Problemdeutungen um einen geeigneten Umgang mit den neuen Unsicherheiten im Zuge der Digitalisierung zu finden. Der Verhandlungsprozess um die Ausgestaltung der Datenschutz-Grundverordnung kann deshalb als relevanter Ausschnitt der Privacy-Arena verstanden werden, in dem koalierend und konfligierend die Zukunft des Privaten und die Verfasstheit der digitalen Welt verhandelt wird.

Das Buch untersucht den Werdegang der Datenschutz-Grundverordnung aus einer interdisziplinären Perspektive. In diesem Werdegang zeigt sich beispielhaft, wie verschiedene soziale Welten mit ihren jeweils eigenen Logiken um die Deutung und Gestaltung von Privatheit und informationeller Selbstbestimmung kämpfen. So debattierten und rangen seit der Veröffentlichung des ersten Entwurfs im Jahr 2012 Mitgliedstaaten, die Europäische Union, zahllose Interessenverbände, die Digitalwirtschaft, die Wissenschaft und Nutzer um die Zukunft des Datenschutzes in Europa. Unterschiedlichste Vorstellungen von Datenschutz prallten aufeinander und mussten mediiert werden.

Dabei spielten routinierte Praktiken, Machtstrukturen, Zugangswege und viele weitere Faktoren eine Rolle. Ihrer Aufarbeitung aus soziologischer und rechtswissenschaftlicher Perspektive sind die folgenden Ausführungen gewidmet.

Kassel, im Frühjahr 2018

Jörn Lamla, FG Soziologische Theorie

Alexander Roßnagel, FG Öffentliches Recht

VORWORT DER AUTOREN

Dieses Buch enthält Ergebnisse des Forschungsprojekts „Privacy-Arena - Explorationsprojekt zur Kartografie und Analyse der Privacy-Arena“. Das Projekt wurde vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der Initiative „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt“ (Forum Privatheit) gefördert (FKZ 16KIS0098). Projektpartner war neben der Universität Kassel das Internationale Zentrum für Ethik in den Wissenschaften (IZEW) der Eberhard Karls Universität Tübingen.

Das Buch gibt gemeinsame Ergebnisse der Teilprojekte Rechtswissenschaft und Soziologie wieder. Diese Teilprojekte wurden verantwortet von der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) unter Leitung von Prof. Dr. Alexander Roßnagel und dem Fachgebiet Soziologische Theorie unter Leitung von Prof. Dr. Jörn Lamla.

Die Ergebnisse wurden künstlerisch aufbereitet und im Rahmen einer Ausstellung vom 1. bis zum 11. Dezember 2016 in Kassel der Öffentlichkeit zugänglich gemacht. Die künstlerische Aufarbeitung erfolgte durch ein Team der Kunsthochschule Kassel unter Leitung von Prof. Joel Baumann.

Eine begleitende Internetseite ist unter www.privacy-arena.net abrufbar.

Eine gekürzte Fassung des Textes ist bereits erschienen in Baumann, Joel / Lamla, Jörn (Hrsg.): Privacy-Arena – Kontroversen um Privatheit im digitalen Zeitalter, Kassel: Kassel University Press, 2017.

Die Autoren danken Herrn Niels Boeckhorst für die Erstellung der im Buch abgedruckten Abbildungen.

Kassel, im Frühjar 2018

Barbara Büttner

Christian Geminn

Charlotte Husemann

Nadine Miedzianowski

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abs. ..... Absatz

ABl. ..... Amtsblatt

AG ..... Aktiengesellschaft

AEUV ..... Vertrag über die Arbeitsweise der Europäischen Union

ALDE ..... Allianz der Liberalen und Demokraten für Europa

Art. ..... Artikel

Az. ..... Aktenzeichen

BayLDA ..... Bayerische Landesamt für Datenschutzaufsicht

BDSG..... Bundesdatenschutzgesetz

BGBl. ..... Bundesgesetzblatt

BfDi ..... Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

BMI..... Bundesministerium des Innern

BR-Drs. ..... Bundesrats-Drucksache

BMWi..... Bundesministerium für Wirtschaft und Energie

BMJV..... Bundesministerium der Justiz und für Verbraucherschutz

BvD ..... Berufsverband der Datenschutzbeauftragten Deutschlands

BVDW..... Bundesverband Digitale Wirtschaft

BVMW ..... Bundesverband mittelständische Wirtschaft

BVerfG ..... Bundesverfassungsgericht

BVerfGE..... Sammlung der Entscheidungen des BVerfG

CCC..... Chaos Computer Club

CDU ..... Christlich Demokratische Union

COD ..... Kommissionsvorschlag im Rahmen einer „co-decision procedure"

COREPER..... French Comité des représentants permanents

CSU ..... Christlich-Soziale Union

DSAnpUG-EU Datenschutz-Anpassungs- und -Umsetzungsgesetz EU

DSGVO .....Datenschutz-Grundverordnung

DuD .....Zeitschrift Datenschutz und Datensicherheit

GRCh.....Charta der Grundrechte der Europäischen Union

e.V. .....ehrenamtlicher Verein

ECR.....European Conservatives and Reformists

EDRi .....European Digital Rights

EG .....Europäische Gemeinschaft

EAG .....Europäische Atomgemeinschaft

EFA.....Europäische Freie Allianz

EPP .....European People's Party

EU .....Europäische Union

EuGH .....Europäischer Gerichtshof

EUV .....Vertrag über die Europäische Union

Euratom .....Europäische Atomgemeinschaft

FISA.....Foreign Intelligence Surveillance Act

GCHQ .....Government Communications Headquarters

GmbH.....Gesellschaft mit beschränkter Haftung

o. J. .....ohne Jahreszahl

Harv. L. Rev. ..Harvard Law Review

HS .....Halbsatz

Inc. .....Incorporated

IT.....Informationstechnologie

KOM.....Mitteilung der Kommission

LIBE.....Ausschuss für Bürgerrechte, Justiz und innere Angelegenheiten des europäischen Parlaments

MEP.....Mitglied des Europäischen Parlaments

NGO .....Non-Governmental Organisation

Nr. .....Nummer

NSA .....National Security Agency

PRISM ..... Planning Tool for Resource Integration, Synchronization and Management

Rn. ..... Randnummer

Rs. ..... Rechtssache

S. ..... Seite

SE ..... Societas Europaea

SPD ..... Sozialdemokratische Partei Deutschlands

UKlaG ..... Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen

Urt. ..... Urteil

USA ..... United States of America

v. ..... vom

vzbv ..... Verbraucherzentrale Bundesverband

Genderklausel

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Dies impliziert jedoch keine Benachteiligung des weiblichen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein. Sämtliche Personenbezeichnungen gelten gleichermaßen für beide Geschlechter.

1 NEUE UNSICHERHEITEN AUFGRUND DER DIGITALEN VERARBEITUNGSMÖGLICHKEITEN PERSONENBEZOGENER DATEN

Von Januar 2012 bis Dezember 2015 wurde in Brüssel die europäische Datenschutz-Grundverordnung[1] verhandelt. Sie wird ab Ende Mai 2018 in der gesamten Europäischen Union geltendes Recht sein. Die Verordnung bringt eine fundamentale Überarbeitung und Neuordnung des Datenschutzrechts in Europa mit sich.

„Vor 17 Jahren nutzten weniger als 1 % der Bevölkerung das Internet. Heute werden große Mengen an personenbezogenen Daten übermittelt und ausgetauscht, über den gesamten Globus – innerhalb von Bruchteilen von Sekunden."[2]

Mit diesen Worten begann Viviane Reding, seinerzeit EU-Kommissarin für Justiz, Grundrechte und Bürgerschaft sowie Kommissionsvizepräsidentin, die Vorstellung des Kommissionsentwurfs der Datenschutz-Grundverordnung am 25.1.2012.[3]

Die Vernetzung nahezu aller Lebensbereiche ist in den vergangenen Jahren massiv fortgeschritten. „Smart Home", „Smart Car" und „Smart City" stehen exemplarisch für das Ubiquitous Computing – die allgegenwärtige rechnergestützte Informationsverarbeitung. So werden derzeit immer mehr Gegenstände miteinander vernetzt, weshalb sich auch der Begriff „Internet der Dinge" durchgesetzt hat. Durch die Digitalisierung entstehen enorme Datenmengen, die etwa Big Data-Anwendungen möglich machen und die Voraussetzung für umfangreiche Profilbildungen darstellen. Zudem steigt die Zahl datengetriebener Geschäftsmodelle, denn mit den gesammelten Daten lässt sich etwa gezielt werben, sodass diesen Daten ein nicht unerheblicher Vermögenswert zukommt. Daneben eröffnen sich auch für Geheimdienste bisher ungeahnte Möglichkeiten der Informationskontrolle. Dem Nutzen und Komfort smarter Anwendungen stehen daher die Möglichkeit

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. 119/1; im Folgenden als „Datenschutz-Grundverordnung", „DSGVO" oder „Verordnung" bezeichnet.

2 Europäische Kommission 2012.

3 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr v. 25.1.2012, KOM (2012) 11 endg., 2012/0011 (COD).

der Verletzung von Persönlichkeitsrechten und die Verunsicherung althergebrachter Routinen der Privatheit gegenüber. Privatheit wird in dieser Situation zu einem zentralen Streitgegenstand. Dabei ist jedoch selten klar, was Privatheit überhaupt sein soll[4] – etwa ein zentraler Grundstein für eine gelingende Demokratie oder doch ein längst überholtes Konzept – noch wie in Zukunft damit umgegangen werden soll. Im Angesicht der grundlegenden Irritation der Privatheitsroutinen und -praktiken versammeln sich verschiedene Akteure[5] und Instanzen um den Gegenstand der Privatheit und versuchen Lösungen für diese neuen Unsicherheiten der Digitalisierung zu finden. Dabei prallen nicht nur verschiedene Ansätze mit dem Problem umzugehen, sondern auch unterschiedliche Interessen und Problemdeutungen aufeinander. Der Vorschlag zur Datenschutz-Grundverordnung war einer dieser Lösungsansätze, der versuchte den neuen Herausforderungen mit Hilfe einer rechtlichen Regelung auf europäischer Ebene zu begegnen. Der Ansatz der Einführung einer Verordnung kann somit als eine Reaktion auf die Krise der Privatheit verstanden werden, ausgelöst durch die Unsicherheiten in Zeiten digitaler Transformationen und deren Implikationen für Privatheit. Privatheit wird in diesen Reaktionen selten isoliert verhandelt, vielmehr geht es immer auch um die Gestaltung der digitalen Welt insgesamt. Der Umgang mit Krisen der Privatheit sagt deshalb nicht nur etwas darüber aus, wie mit digitalen Krisen generell umgegangen wird, sondern auch etwas über die demokratische Verfasstheit der digitalen Welt. Reaktionen mit diesen Unsicherheiten der Privatheit umzugehen, geben somit Einblicke in die grundlegende institutionelle Strukturierung der Gesellschaft und ihres demokratischen Gemeinwesens insgesamt.

[4] Der Begriff der „Privatheit" als Übertragung des englischen Begriffs „Privacy" ist ebenso wie der der „Privatsphäre" für das Recht und die Rechtswissenschaft in Deutschland schwer fassbar. Insbesondere dem Begriff der Privatsphäre liegt im Vergleich zu dem der informationellen Selbstbestimmung ein unterschiedliches Verständnis und Schutzkonzept zugrunde. S. hierzu ausführlich Geminn/Roßnagel 2015: S. 703 ff.

[5] Im folgenden Text werden anstelle der Doppelbezeichnungen die Personen und Funktionsbezeichnungen in männlicher Form verwendet, stehen aber jeweils für die weibliche und männliche Form.

1.1 Die Datenschutz-Grundverordnung als ein Lösungsansatz für die Krise der Privatheit

Die Europäische Kommission[6] hat in einer Mitteilung vom 25. Januar 2012 an das Europäische Parlament, den Rat der Europäischen Union, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen dafür plädiert, die EU-Datenschutzvorschriften aus dem Jahr 1995 zu reformieren, da in der neuen digitalen Umgebung weiterhin ein hohes Schutzniveau für den Einzelnen bei der Verarbeitung personenbezogener Daten gewährleistet sein müsse.[7] Die Datenschutzrichtlinie[8] litt nach Auffassung der Kommission vor allem an zwei Schwachstellen, die es zu beheben galt: Sie entstand in einer Zeit, in der das Internet noch in den Kinderschuhen steckte und war daher für eine Art der Datenerfassung und Datenverarbeitung konzipiert, die sich zwischenzeitlich grundlegend verändert hatte. Zudem fehlte es an einem einheitlichen europäischen Datenschutzrecht. Die 27 EU-Mitgliedstaaten[9] hatten die Vorschriften der Richtlinie unterschiedlich umgesetzt, was zu teils großen Unterschieden im Datenschutzniveau einzelner Mitgliedstaaten führte[10] und mit Kosten für die Wirtschaft und mit Rechtsunsicherheit auf Seiten der Bürger verbunden war.

Um diese Probleme zu beheben, trat die Datenschutz-Grundverordnung mit den Zielen einer umfassenden Modernisierung und Harmonisierung des Datenschutzes in Europa an, um zum einen die Rechte der EU-Bürger zu schützen und die Umsetzung der Grundrechte auf Schutz des Privatlebens aus Art. 7 und auf Schutz personenbezogener Daten aus Art. 8 der Grundrechtecharta[11] zu gewährleisten. Zum anderen wollte die Kommission gleichzeitig das Wirtschaftswachstum ankurbeln und damit die Wettbe-

---

6 Im Folgenden auch „Kommission" genannt.

7 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert", vom 25.1.2012, KOM(2012) 9 endgültig, 5.

8 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; im Folgenden auch „Richtlinie" genannt.

9 Zur Zeit der Verhandlungen.

10 Europäischen Kommission 2012.

11 Im Folgenden auch mit „Charta" oder „GRCh" abgekürzt.

werbsfähigkeit der Europäischen Union steigern. Dies sollte auf zwei verschiedenen Wegen erreicht werden. Einerseits mittelbar über den Grundrechtsschutz. Ein hohes Datenschutzniveau soll das Vertrauen der europäischen Verbraucher in Online-Dienste stärken und so die digitale Wirtschaft ankurbeln. Andererseits soll ein einheitlicher Rechtsrahmen auf EU-Ebene Hindernisse für den Marktzutritt überwinden und so weiteres Wirtschaftswachstum generieren.

Macht man sich die unterschiedlichen Ziele deutlich, so wird schnell verständlich, warum es sich um einen schwierigen und langwierigen Reformprozess gehandelt hat. Der Schutz personenbezogener Daten, wie er in Art. 8 Abs. 1 GRCh verankert ist, ist kein Selbstzweck, sondern dient dem Schutz der informationellen Selbstbestimmung des Einzelnen. Gleichzeitig kann er aber auch Mittel zur Durchsetzung wirtschaftlicher Interessen sein, obwohl er teilweise in eklatantem Widerspruch zu diesen wirtschaftlichen Interessen steht.

1.2 Vorgehensweise bei der Analyse der Arena der Datenschutz-Grundverordnung

Das Projekt orientiert sich methodisch an der Situationsanalyse von Adele Clarke (2005), die das Konzept der sozialen Welten und Arenen von Anselm Strauss (1978, 1993) mit verschiedenen Formen der Kartierung verknüpft. Der technische Wandel und die zunehmende Digitalisierung führen zu Unsicherheiten vieler Privatheitsroutinen und -vorstellungen. Verschiedene Akteure versammeln sich um den Gegenstand der Privatheit und versuchen den neuen Unsicherheiten im Zuge des digitalen Wandels zu begegnen. Die Arena stellt den Schauplatz der Auseinandersetzung dieser kollektiven Aushandlungsprozesse dar. Anstelle Privatheit vorab zu definieren, sollen die Verhandlungen um den Streitgegenstand Privatheit selbst betrachtet und analysiert werden. In dieser Arena diskutieren, verhandeln und kämpfen die sozialen Welten um die Ausgestaltung von Privatheit. Ein Lösungsvorschlag innerhalb dieser Arena ist die Datenschutz-Grundverordnung. Es handelt sich dabei um einen transnationalen, rechtlichen Lösungsansatz, mit dem Ziel das Datenschutzrecht auf europäischer Ebene zu modernisieren und zu harmonisieren. Die Verhandlungen um die Datenschutz-Grundverordnung können somit als Segment der „Privacy-Arena“ verstanden werden, in der verschiedene Akteure und Instanzen um die Zukunft

von Privatheit verhandeln. Der Fokus der folgenden Analysen liegt auf eben jenem Segment – der Arena der Datenschutz-Grundverordnung.[12]

Die Untersuchungen des Aushandlungsprozesses der Datenschutz-Grundverordnung konzentrieren sich auf die Verhandlungen nach Bekanntgabe des Kommissionsentwurfs am 25. Januar 2012, wodurch das Gesetzgebungsverfahren offiziell eröffnet wurde. Die Verhandlungen rund um die Verordnung dauerten insgesamt vier Jahre. Während dieser Zeit versammelten sich verschiedene Akteure und Instanzen um den Streitgegenstand der „Datenschutz-Grundverordnung" und diskutierten und kämpften um ihre Ausgestaltung. In dieser „Arena der Datenschutz-Grundverordnung" ging es selten nur um den Streitgegenstand selbst. Vielmehr wurden verschiedene Interessen und Deutungen mitverhandelt, die die digitale Welt insgesamt betreffen; sei es nun der Stellenwert ökonomischer Interessen in modernen Nationalstaaten oder ein bestimmtes Verständnis davon, wie demokratische Gesellschaften gestaltet und regiert werden sollten. In den Verhandlungen trafen all diese verschiedenen Interessen, Ziele und Werte aufeinander. Diese sind nicht zwangsläufig an einzelne Akteure gebunden.[13] In Anlehnung an Strauss Theorie sozialer Welten und Arenen stehen nicht die Handlungen oder Interaktionen Einzelner im Mittelpunkt; vielmehr geht es um die Rekonstruktion kollektiver Aushandlungsprozesse und deren Implikationen für die Neuordnung der Arena. Deshalb konzentriert sich die Analyse auf verschiedene soziale Welten und deren Vertreter.[14] Soziale Welten können als kollektive Akteure verstanden werden, denen eine geteilte Kernpraktik gemein ist, d. h. eine Aktivität, die alle Mitglieder der sozialen Welt ausüben wie etwa die Verwertung personenbezogener Daten zur Profitgenerierung. Diese Tätigkeit wird meist auf eine bestimmte Art und Weise ausgeführt, man könnte auch sagen sie folgt im weitesten Sinne einer bestimmten Technik. Das kann beispielsweise das Schreiben von Algorithmen sein. Schließlich finden die Tätigkeiten an einem be-

[12] Innerhalb einer Arena können sich Sub-Arenen herausbilden, die sich mit Teilaspekten der Gesamtarena auseinandersetzen. Die Arena der Datenschutz-Grundverordnung kann somit als ein Segment der Gesamtarena um Privatheit verstanden werden.

[13] Jemand kann als Mitglied eines Unternehmens großes Interesse an der Verwertung von Daten haben und sich als Elternteil gleichzeitig für den Datenschutz der eigenen Kinder einsetzen.

[14] Vgl. Soziale Welten und Arena-Theorie (Strauss 1978; 1993); Situationsanalyse (Clarke 2005).

stimmten Ort statt, wie zum Beispiel in einem Bürogebäude. Vertreten werden die sozialen Welten in der Regel durch verschiedene Repräsentanten, beispielsweise Internetunternehmen als Vertreter der Welt der Digitalwirtschaft. Soziale Welten sind nicht als statische Gebilde zu verstehen, ihre Grenzen und Ordnungen sind fluide. Welten können mit anderen Welten in Beziehung treten, sich austauschen,[15] Verhandlungen eingehen, Kompromisse schließen bis hin zum Führen von harten Auseinandersetzungen und Kämpfen. Eine Welt kann in sich widersprüchlich sein und aus Uneinigkeiten können neue Subwelten[16] hervorgehen. Auch nicht-menschliche Elemente wie das Recht selbst beeinflussen den Verhandlungsprozess.[17] Die Kartografierung dieser Prozesse dient dabei nicht nur als Arbeitswerkzeug, sondern auch dazu der Komplexität des Aushandlungsprozesses gerecht zu werden. Die Aufschlüsselung der verschiedenen Schichten der Kontroverse ermöglicht eine differenzierende Darstellung und einen vertiefenden Einblick verschiedener Aspekte der Verhandlungen.[18]

Im Folgenden wird daher zunächst aufgezeigt, welche Welten und wichtigen Vertreter an den Aushandlungen um die Datenschutz-Grundverordnung beteiligt waren und welche Positionen sie eingenommen haben. Anschließend wird dargestellt, wie sich die Verhandlungen im Zeitverlauf entwickelten. Zuletzt soll die Art und Weise des Aushandlungsprozesses selbst einer tiefergehenden Reflektion unterzogen sowie ein Ausblick in die Zukunft der Europäischen Datenschutz-Grundverordnung gegeben werden.

---

15 Die so entstandenen Verknüpfungen bezeichnet Strauss als „Intersektionen" (Strauss 1978: 122).

16 Strauss spricht hier von „Segmentationen" (Strauss 1978: 123). Innerhalb von Welten kann es zu Uneinigkeiten kommen – beispielsweise aufgrund unterschiedlicher Praktiken oder Ziele. Teile einer Welt können sich absondern und es können neue Subwelten entstehen.

17 Beispielsweise stecken rechtliche Normen den Handlungsspielraum zahlreicher Akteure zu einem gewissen Grad ab und wirken so mittelbar auf den Verhandlungsprozess ein.

18 Venturini 2012.

2 DIE ARENA DER DATENSCHUTZ-GRUNDVERORDNUNG ALS VERSAMMLUNG VERSCHIEDENER WELTEN

Um zu verstehen, wer in dieser „Arena der Datenschutz-Grundverordnung“ warum welche Interessen vertrat, folgt eine Beschreibung der an den Verhandlungen beteiligten sozialen Welten und der im Verhandlungsprozess relevanten kollektiven menschlichen als auch nicht-menschlichen[19] Akteure. Die Grafik illustriert diese Welten sowie deren Repräsentanten in den Verhandlungen.

[19] Der Fokus unserer Analyse nicht-menschlicher Akteure in der Arena liegt hier insbesondere auf rechtlichen Akteuren.

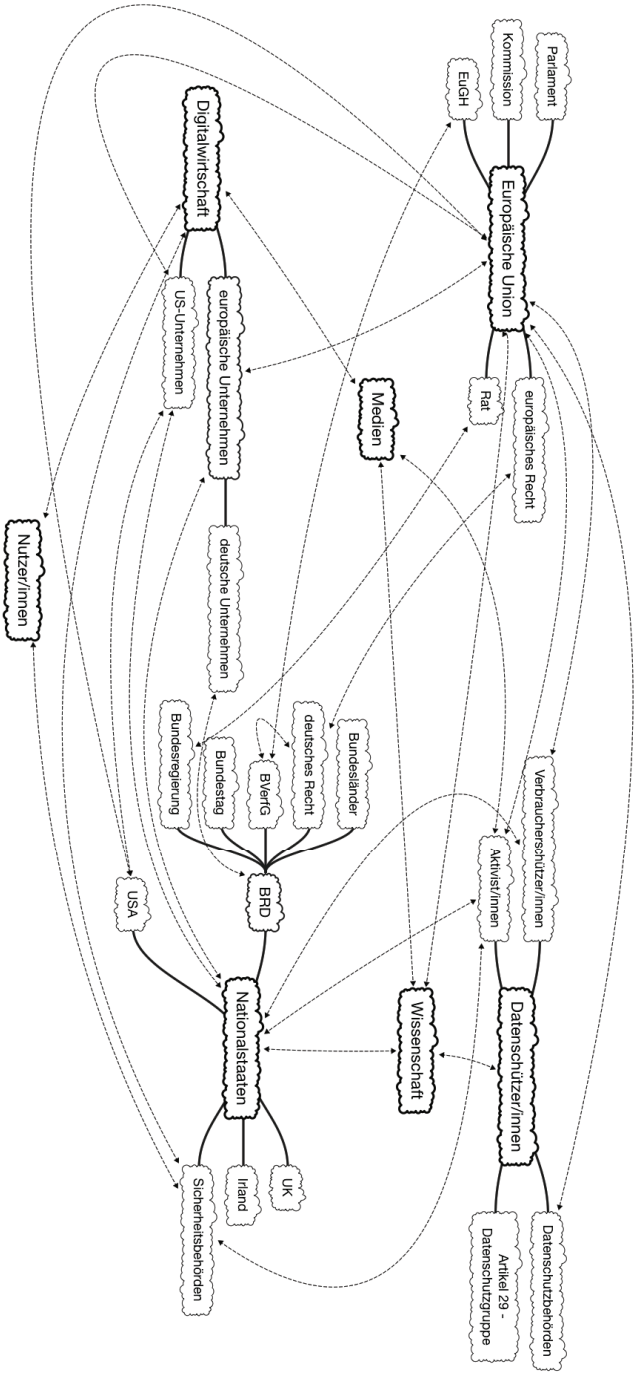

Abbildung 1: Die Arena der Datenschutz-Grundverordnung

2.1 Die Welt der Europäischen Union

Die Datenschutz-Grundverordnung setzt als rechtlicher Lösungsansatz auf europäischer Ebene an. Die europäische Union spielt somit in den Verhandlungen der Datenschutz-Grundverordnung eine rahmengebende Rolle, insofern sie die institutionellen Infrastrukturen und Leitlinien des Gesetzgebungsprozesses vorgibt. Anfänglich mit dem Ziel der Förderung der wirtschaftlichen Zusammenarbeit gegründet, deckt die Europäische Union heute zahlreiche Politikfelder ab.[20] Die Welt der Europäischen Union versucht beständig die eigene Stellung als politischer Akteur auszubauen, ihre Handlungsfähigkeit zu stärken und die Integration der Europäischen Union voranzutreiben.[21]

Die europäische Integration geht auf ein kurz nach Beendigung des Zweiten Weltkriegs von dem Franzosen Jean Monnet entwickeltes Konzept zurück, das durch den französischen Außenminister Robert Schuman aufgegriffen wurde. Der Grundgedanke des sogenannten Schuman-Plans war es, durch die Eingliederung Deutschlands in ein supranationales System zusammen mit anderen Staaten die deutsche Produktion von Kohle und Stahl, als wirtschaftlich und militärisch bedeutende Faktoren, unter internationale Kontrolle zu bringen und so eine Bedrohung des europäischen Friedens durch ein wiedererstarkendes Deutschland auszuschließen.[22] Am 1./2. Juni 1955 beschlossen die Außenminister der Mitgliedstaaten der Europäischen Gemeinschaft für Kohle und Stahl die Integration auf alle Wirtschaftsbereiche auszudehnen. Infolgedessen wurden am 25. März 1957 die Römischen Verträge unterzeichnet. Dies waren der Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft, der die Errichtung eines gemeinsamen Marktes und die Annäherung der nationalen Wirtschaftspolitiken zum Ziel hatte, sowie der Vertrag zur Gründung der Europäischen Atomgemeinschaft (Euratom/EAG), der die Förderung der friedlichen Nutzung der Kernenergie bezweckte.[23] Die Europäische Union wurde schließlich mit dem am 1. November 1993 in Kraft getretenen Vertrag über die Europäische Union gegründet. Dieser Vertrag bildet durch die Gründung der Europäischen Union die Grundlage für die Vollendung der Europäischen Wirt-

[20] Europäische Union o. J. a.
[21] Europäische Union o. J. b.
[22] Herdegen 2015: § 4 Rn. 1.
[23] Streinz 2016: § 2 Rn. 20.

schafts- und Währungsunion bis zum Jahr 1999 sowie für weitere politische Integrationsschritte, insbesondere eine gemeinsame Außen- und Sicherheitspolitik und eine verstärkte polizeiliche und justizielle Zusammenarbeit in Strafsachen.[24]

Am 1. Dezember 2009 trat der Vertrag von Lissabon zur Reform der EU-Institutionen in Kraft. Ziel war unter anderem die Demokratisierung der Institutionen sowie der Ausbau von Kompetenzen der Europäischen Union. Im Zuge dessen kam es zur Ausweitung der Rechte des Parlaments sowie zur Stärkung nationaler Parlamente.[25] Außerdem wurde die Charta der Grundrechte der europäischen Union rechtsverbindlich.[26] Die Unionsorgane und EU-Mitgliedstaaten sind an dieses Recht gebunden. Die Einhaltung dieser Rechte kann in Verfahren vor dem Europäischen Gerichtshof sowie vor nationalen Gerichten geltend gemacht werden.

Die Europäische Union ist eine supranationale Institution. Es handelt sich insofern weder um einen Bundesstaat, der regelmäßig aus einem die Souveränität innehabenden Gesamtstaat und verschiedenen Gliedstaaten besteht,[27] noch um einen Staatenbund. Der Staatenbund ist eine rein völkerrechtliche Beziehung zwischen Staaten.[28] Er beruht auf einem völkerrechtlichen Vertrag und seine Mitgliedstaaten bleiben souverän.[29] Die Europäische Union ist aber etwas zwischen diesen beiden Gebilden. Während der Staatenbund einen loseren Zusammenschluss beschreibt, ist der Bundesstaat zu fest, als dass er die Europäische Union angemessen charakterisieren würde. Das Bundesverfassungsgericht hat insofern den Begriff des „Staatenverbunds“ geprägt.[30] Dadurch soll zum Ausdruck kommen, dass die Europäische Union von den Mitgliedstaaten abhängig ist, da diese die „Herren der Verträge“ sind. Die Europäische Union hat jedoch die Möglichkeit in bestimmten Bereichen eigenständig Recht zu setzen. Die Mitgliedstaaten behalten aber ihre Souveränität und haben nur einzelne Souveränitätsrechte zugunsten einer Überstaatlichkeit an die Europäische Union übertragen. Dies führt dazu, dass das Unionsrecht die Rechtsordnungen der Mitglied-

24 Arndt/Fischer/Fetzer 2015: S. 9.
25 Zandonella 2009.
26 EUR-Lex 2016.
27 Sodan/Ziekow 2016: § 8 Rn. 1.
28 Maurer 2010: § 10 Rn. 7.
29 Maurer 2010: § 10 Rn. 7.
30 BVerfGE 89, 155 (181).

staaten überlagern und ersetzen kann, um zugunsten des Integrationsprozesses eine eigenständige, staatenübergreifende Rechtsordnung zu gewährleisten. Die Rechtsetzungskompetenz der Europäischen Union im Bereich des Datenschutzes und damit die Befugnis der Union zum Erlass der Datenschutz-Grundverordnung ergibt sich aus Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV).

Der Integrationsprozess verläuft jedoch bis heute auf unterschiedlichen Ebenen (wirtschaftlich, rechtlich, sozial, etc.) und in unterschiedlichen Geschwindigkeiten. Dabei ringt die Welt der Europäischen Union immer wieder mit ihrer eigenen Identität und ihrem Selbstverständnis wahlweise als Wirtschaftsunion, Rechtsunion oder Werteunion. Gerade diese unterschiedlichen Vorstellungen davon, wie die Integration gelingen kann, führen innerhalb der Welt zu Konflikten. Ursächlich hierfür sind auch die zahlreichen Institutionen und Organisationen der Europäischen Union. So herrschte während der Verhandlungen immer wieder Uneinigkeit darüber, ob die Datenschutz-Grundverordnung vordringlich dem Schutz der Grundrechte oder der Stärkung des europäischen Binnenmarkts dienen soll.

Die wichtigsten Organe der Europäischen Union sind die Europäische Kommission, das Europäische Parlament sowie der Rat der Europäischen Union. Diese teile sich die Rechtsetzungsgewalt in der Europäischen Union und entwickeln gemeinsam im ordentlichen Gesetzgebungsverfahren politische Strategien und Rechtsvorschriften für die Europäische Union. Der Gerichtshof der Europäischen Union ist für die Einhaltung des EU-Rechts zuständig und somit ein weiterer wichtiger Akteur in der Arena der Datenschutz-Grundverordnung. Nachfolgend konzentrieren sich die Analysen auf folgende Vertreter dieser Welt:

- Europäische Kommission
- Europäisches Parlament
- Rat der Europäischen Union
- Recht der Europäischen Union
- Europäischer Gerichtshof

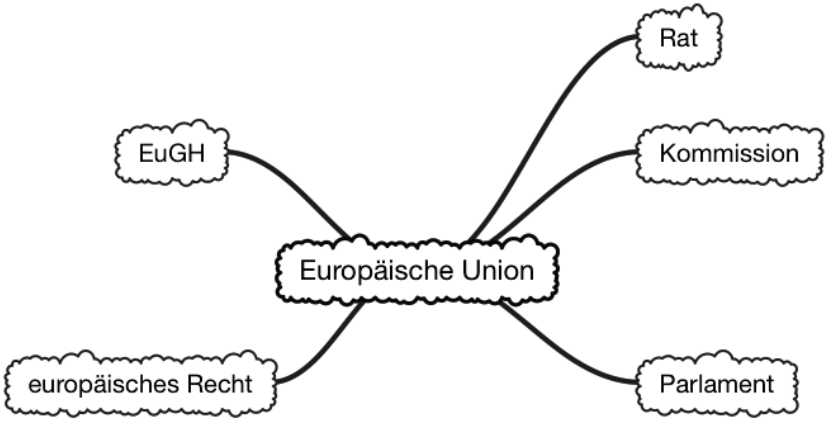

Abbildung 2: Die Welt der Europäischen Union

2.1.1 Europäische Kommission

„Der Schutz personenbezogener Daten ist zwar ein Grundrecht aller Europäer, aber die EU-Bürger haben nicht immer das Gefühl, dass sie vollständige Kontrolle über ihre personenbezogenen Daten haben. Die heute vorgeschlagenen Änderungen werden das Vertrauen in Onlinedienste stärken, weil die Bürger künftig besser über ihre Rechte informiert sein und größere Kontrolle über ihre Daten haben werden. Die Reform wird zudem die Geschäftstätigkeit der Unternehmen einfacher und kostengünstiger machen. Eine straffe, eindeutige und einheitliche Regelung auf EU-Ebene wird dazu beitragen, das Potenzial des digitalen Binnenmarkts freizusetzen und Wirtschaftswachstum, Innovation und Beschäftigung zu fördern." (Viviane Reding, Justizkommissarin von 2010 bis 2014)[31]

Die Europäische Kommission hat den entscheidenden Impuls für die Reform des europäischen Datenschutzrechts gegeben. Nachdem sie im Jahr 2009 eine öffentliche Konsultation durchführte, legte sie im November 2010 eine Mitteilung zum „Gesamtkonzept für den Datenschutz in der Europäischen Union" vor. Im Januar 2012 präsentierte die damalige Justizkommissarin Viviane Reding sodann den Gesetzesentwurf der Kommission für eine

[31] Europäische Kommission 2012.

Datenschutz-Grundverordnung.[32] An dem Rechtsetzungsprozess in der Europäischen Union ist die Kommission insbesondere durch die Einbringung von Vorschlägen beteiligt. Die meisten europäischen Rechtsakte können nur auf Initiative der Kommission erlassen werden – in den Bereichen Justiz und Inneres teilt sie sich das Initiativrecht mit den EU-Staaten. Der Entwurf zielte auf ein einheitliches und modernisiertes Datenschutzrecht mit praxisgerechten und rechtsklaren Vorgaben innerhalb der Europäischen Union ab, um die uneinheitlichen Datenschutzregelungen der EU-Mitgliedstaaten durch ein einheitliches Datenschutzgerüst zu ersetzen. Dabei sollte für die neuen Datenverarbeitungspraktiken und datengetriebenen Geschäftsmodelle ein einheitlicher rechtlicher Rahmen geschaffen werden. Zugleich sollten aber auch die Rechte der EU-Bürger geschützt werden. Beispielhaft hierfür sind das „Recht auf Vergessenwerden", die Grundsätze „Privacy-by-Design" und „Privacy-by-Default" sowie die Wahrung des Verhältnismäßigkeitsprinzips.

Zusammen mit dem Europäischen Gerichtshof bildet die Europäische Kommission die reinste Ausprägung eines supranationalen Organs. Zu ihren Befugnissen gehören das Initiativrecht für die Rechtsetzung auf europäischer Ebene, Koordinierungs- und Exekutivfunktionen sowie die Vertretung der Europäischen Union nach außen.[33] Die Kommission wird auch als „Hüterin der Verträge" bezeichnet, da sie die Umsetzung von europäischen Rechtsakten überwacht. Die Ausübung der Exekutivbefugnisse nimmt die Kommission mit den ihr nachgelagerten Stellen wahr, insbesondere mit den Exekutivagenturen und anderen Ämtern. Im Hinblick auf die Vertretung der Europäischen Union nach außen, ist die Kommission für die Vertretung vor den mitgliedstaatlichen Gerichten und vor dem Europäischen Gerichtshof sowie für die Außenbeziehungen zuständig. Darunter fällt die Aushandlung von Abkommen mit Drittstaaten und internationalen Organisationen, wozu auch die Beitrittsabkommen mit neuen Mitgliedstaaten gehören. Die Aufgaben und Befugnisse der Kommission ergeben sich aus Art. 17 Abs. 1 und 2 des Vertrags über die Europäische Union (EUV).

---

[32] Europäische Kommission, Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) v. 25.01.2012, 2012/0011 COD.

[33] Europäische Kommission o. J.

Die Kommission setzt sich aus je einem Vertreter jedes Mitgliedstaats zusammen. Diese sind in der Wahrnehmung ihrer Aufgaben völlig unabhängig und allein den allgemeinen Interessen der Union verpflichtet. Aus Art. 17 Abs. 3 EUV ergibt sich, dass die Mitglieder der Kommission Weisungen von einer Regierung, einem Organ, einer Einrichtung oder jeder anderen Stelle weder einholen noch entgegennehmen dürfen. Die Kommission bildet damit den Gegenpol zum Rat der Europäischen Union, der die Interessenvertretung der nationalen Regierungen darstellt. Diese Unabhängigkeit ist Voraussetzung für die Ernennung der Kommissionsmitglieder. So heißt es in Art. 17 Abs. 3 S. 2 EUV:

„Die Mitglieder der Kommission werden aufgrund ihrer allgemeinen Befähigung und ihres Einsatzes für Europa unter Persönlichkeiten ausgewählt, die volle Gewähr für ihre Unabhängigkeit bieten."

Die Amtszeit der Kommission beträgt gemäß Art. 17 Abs. 3 EUV fünf Jahre. Das gilt für die gesamte Kommission. Die Beschlüsse innerhalb der Kommission werden mit absoluter Mehrheit gefasst. Die Europäische Kommission besteht derzeit einschließlich ihres Präsidenten aus 28 Mitgliedern.

2.1.2 Europäisches Parlament

„Ich habe eine klare Botschaft für den Rat: Jede weitere Verschiebung wäre unverantwortlich. Die Bürger Europas erwarten von uns, dass wir eine starke EU-weite Datenschutzverordnung verabschieden. Wenn einige Mitgliedstaaten nach zweijährigen Verhandlungen nicht liefern wollen, dann sollte die Mehrheit ohne sie voranschreiten." (Jan Philipp Albrecht, Abgeordneter des Europäischen Parlaments)[34]

Das Europäische Parlament[35] ist das einzige Organ, das direkt von den Unionsbürgern gewählt wird. Es ist gemäß Art. 14 Abs. 1 EUV gemeinsam mit dem Rat für die Gesetzgebung zuständig und übt mit diesem zusammen die Haushaltsbefugnisse aus. Innerhalb des Parlaments sind verschiedene Parteien und Gruppierungen vertreten, es gibt aber anders als in den nationalen Parlamenten keine Regierungs- und Oppositionsfraktionen. Die Abgeordneten unterliegen damit keinem Koalitionszwang und können flexibler auf Gesetzesentwürfe reagieren. Gleichwohl sind die Parlamentarier in Fraktionen organisiert; das Parlament setzt sich derzeit aus sieben Fraktio-

[34] Europäisches Parlament 2014.

[35] Im Folgenden auch „Parlament" genannt.

nen zusammen.[36] Voraussetzung für die Bildung einer Fraktion ist eine gemeinsame weltanschauliche Ausrichtung. Das Europäische Parlament bereitet seine Sitzungen in 20 ständigen Ausschüssen vor und bildet Delegationen und Konferenzen, in denen sich die Parlamentarier mit Mitgliedern anderer Parlamente austauschen können. Den Vorsitz des Parlaments bilden ein Präsident[37] und 14 Vizepräsidenten.

Das Parlament nahm seine Arbeit nach der Veröffentlichung des Kommissionsentwurfs zur Datenschutz-Grundverordnung am 25. Januar 2012 auf. Nachdem der Rechtsausschuss des Europäischen Parlaments dem Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE), der für den Großteil der Rechtsvorschriften und für die demokratische Überwachung von politischen Maßnahmen im Bereich Justiz und Inneres zuständig ist, im Oktober 2012 eine Stellungnahme zum Vorschlag für eine Datenschutz-Grundverordnung zukommen ließ, stellte Jan Philipp Albrecht[38] am 9. und 10. Januar 2013 einen etwa 200 Seiten umfassenden Berichtsentwurf mit Änderungen zur Datenschutz-Grundverordnung vor. Nach langem Ringen um den Parlamentsvorschlag für eine Datenschutz-Grundverordnung und der Bearbeitung von über 3.000 Änderungsanträgen, verabschiedete das Europäische Parlament ihn mit einer Mehrheit von über 95 Prozent der abgegebenen Stimmen. Der Vorschlag wurde sodann im Rat weiter verhandelt.

„Der aktuelle datenschutzrechtliche Zustand ist unhaltbar. (...) Wenn Daten nicht geschützt werden, können etliche private Informationen an jeden gelangen, der genug dafür zahlt. (...) Der Rat hat die Überarbeitung der Datenschutzrichtlinie jahrelang blockiert! Die Länder haben damit den Schutz der Grundrechte ihrer Bürger verhindert. Und sie werden auch im Trilog versuchen, eine verwässerte Version durchzubringen." (Birgit Sippel, Abgeordnete der SPD und Sprecherin / Koordina-

---

[36] Fraktion der Europäischen Volkspartei, Fraktion der Progressiven Allianz der Sozialisten und Demokraten im Europäischen Parlament, Fraktion der Allianz der Liberalen und Demokraten für Europa, Europäische Konservative und Reformisten, Fraktion der Grünen/Europäische Freie Allianz, Konföderale Fraktion der Vereinigten Europäischen Linken/Nordische Grüne Linke, Fraktion „Europa der Freiheit und der Demokratie" und eine kleine Anzahl fraktionsloser Mitglieder.

[37] Von 2012 bis 2017 Martin Schulz.

[38] Jan Philipp Albrecht ist Abgeordneter des Europäischen Parlaments für „Die Grünen/EFA" und war für die Datenschutz-Grundverordnung zuständiger Berichterstatter des Parlaments.

torin der S&D-Fraktion (Fraktion der Progressiven Allianz der Sozialisten & Demokraten))[39]

Der Entwurf des Parlaments forderte unter anderem eine frei abgegebene und spezifische Einwilligung des Betroffenen und sah Höchststrafen für Datenschutzverstöße von bis zu 100 Millionen Euro oder fünf Prozent des Jahresumsatzes eines Unternehmens vor,[40] wohingegen die EU-Kommission noch von maximal zwei Prozent des Geschäftsvolumens sprach. Ebenso befürwortete das Parlament das Recht auf Vergessenwerden sowie die Möglichkeit der Datenportabilität. Die Anforderungen für das Erstellen von Persönlichkeitsprofilen wurden verschärft. Für die Übermittlung von Daten europäischer Bürger an Drittstaaten sollte jede Firma eine vorherige Genehmigung einer nationalen Datenschutzbehörde benötigen.

2.1.3 Rat der Europäischen Union

„Heute sind wir einem modernen und einheitlichen Rahmen für den Datenschutz in der Europäischen Union einen großen Schritt näher gekommen. Ich bin sehr zufrieden, dass wir nach über drei Jahren Verhandlungen endlich einen Kompromiss über den Text erzielt haben. Mit der neuen, an die Erfordernisse des digitalen Zeitalters angepassten Datenschutzverordnung werden die individuellen Rechte unserer Bürger gestärkt und ein hohes Schutzniveau gewährleistet." (Dzintars Rasnačs, Lettischer Justizminister)[41]

Der Rat der Europäischen Union[42] besteht aus je einem Vertreter jedes Mitgliedstaats auf Ministerebene. Daher stammt auch die informelle Bezeichnung „Ministerrat", die allerdings insofern irreführend ist, als nicht nur die Bundesminister, sondern auch die Minister aus den Länderregierungen an den Ratssitzungen teilnehmen können. Deutschland entsendet zudem auch Staatssekretäre in den Rat, die ebenfalls über ein volles Stimmrecht verfügen. Der Rat hat im Gegensatz zu den anderen europäischen Institutionen keine ständigen Mitglieder, vielmehr tagt er in unterschiedlichen Zusam-

---

39 Mies 2015.

40 Europäisches Parlament 2014.

41 „Today we have moved a great step closer to modernised and harmonised data protection framework for the European Union. I am very content that after more than 3 years of negotiations we have finally found a compromise on the text. The new data protection regulation, adapted to the needs of the digital age, will strengthen individual rights of our citizens and ensure a high standard of protection.", Rat der Europäischen Union 2015.

42 Im Folgenden auch „Rat" genannt.

mensetzungen, je nach betreffender Angelegenheit. Welche Minister oder Staatssekretäre an den Sitzungen teilnehmen, hängt von dem auf der Tagesordnung stehenden Themengebiet ab. So werden etwa Minister aus den Länderregierungen entsandt, wenn schwerpunktmäßig ausschließliche Gesetzgebungsbefugnisse der Bundesländer betroffen sind. Das ist zum Beispiel in den Bereichen schulische Bildung, Kultur und Rundfunk der Fall. Voraussetzung für die Entsendung in den Rat ist, dass der jeweilige Vertreter befugt ist, für die Regierung des von ihm vertretenen Mitgliedstaates verbindlich zu handeln und das Stimmrecht auszuüben. Den Vorsitz im Rat hat in allen seinen Zusammensetzungen mit Ausnahme des Rates „Auswärtige Angelegenheiten" nach einem Rotationsprinzip immer für sechs Monate ein anderer Mitgliedstaat. Im Rat „Auswärtige Angelegenheiten" wechselt der Vorsitz nicht. Hier nimmt der Hohe Vertreter der Union für Außen- und Sicherheitspolitik den Vorsitz während seiner Amtszeit wahr, der allerdings nicht stimmberechtigt ist. Im Gegensatz zum Parlament sind Verhandlungen des Rats nicht öffentlich zugänglich. Die Datenschutz-Grundverordnung ist unter dem luxemburgischen und dem niederländischen Ratsvorsitz entstanden.

Der Rat ist das Bindeglied zwischen der Europäischen Union und den Mitgliedstaaten. Während idealtypisch gesprochen die Europäische Kommission und das Europäische Parlament europäische Interessen verfolgen, vertreten die Ratsmitglieder die Interessen der Mitgliedstaaten, die sie entsenden. Insgesamt gestaltete sich der Verhandlungsprozess des Rats aufgrund interner Streitigkeiten und auseinanderklaffender Interessenlagen der einzelnen Länder sehr zäh. Am 6. Juni 2013 scheiterte der Entwurf einer Datenschutzverordnung der irischen Ratspräsidentschaft im Rat der Europäischen Union. Nach langen Verzögerungen einigte sich der EU-Ministerrat am 15. Juni 2015 schließlich auf eine gemeinsame Fassung der Verordnung.[43]

Der Entwurf des Rats erfuhr viel öffentliche Kritik.[44] Insgesamt wurde das Datenschutzniveau im Vergleich zum Entwurf des Parlaments und der Kommission abgeschwächt. Für die Verarbeitung von Daten sollte eine „unzweideutige" Einwilligung notwendig sowie die Verarbeitung für andere

---

43 Rat der Europäischen Union, 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) v. 11.06.2015, 2012/0011 COD.

44 Krempl 2015.

Zwecke bei „berechtigten Interessen" von Drittparteien zulässig sein. Die Nutzung persönlicher Daten für Direktmarketing war prinzipiell erlaubt, konnte aber durch ein sogenanntes „opt out" nachträglich vom Nutzer widerrufen werden. Der Grundsatz der Datenminimierung wurde zu einer bloßen Verhältnismäßigkeitsprüfung herabgestuft. Das Recht auf Vergessenwerden war weiterhin Bestandteil des Entwurfs. Um für mehr Transparenz zu sorgen, wurden die Möglichkeiten über die Verarbeitung personenbezogener Daten Auskunft zu erhalten und die Pflichten für den Verarbeiter, dafür Sorge zu tragen, dass diese Rechte ausgeübt werden können, ausgebaut. Die Möglichkeiten des Profilings wurden ebenfalls eingeschränkt, ließen aber Spielraum für abweichende nationale Regelungen. Die Höchststrafe für Verstöße wurde auf 250.000 Euro oder 0,5 Prozent des Jahresumsatzes eines Unternehmens festgelegt.

2.1.4 Recht der Europäischen Union

Die Europäische Union ist eine Rechtsunion, die sich dadurch auszeichnet, dass sie eine eigenständige Rechtsordnung hat. Das Unionsrecht kann allerdings keiner der herkömmlichen Rechtskategorien zugeordnet werden. Es handelt sich weder um nationales noch um internationales Recht oder um Völkerrecht. Aus diesem Grund wird das Unionsrecht auch als supranationales Recht bezeichnet. Es regelt Rechtsbeziehungen zwischen den EU-Organen untereinander, zwischen der Europäischen Union und den einzelnen Mitgliedstaaten, zwischen den Mitgliedstaaten untereinander, zwischen der Europäischen Union und natürlichen Personen sowie Unternehmen der Mitgliedstaaten sowie zwischen den Mitgliedstaaten und natürlichen Personen und auch zwischen der Union und Drittstaaten.

Unter das Europarecht im engeren Sinne fallen der Vertrag über die Europäische Union, der Vertrag über die Arbeitsweise der Europäischen Union sowie der Vertrag zur Gründung der Europäischen Atomgemeinschaft (EAUV). Über Art. 6 EUV ist auch die Charta der Grundrechte der Europäischen Union Bestandteil des Europarechts im engeren Sinne. Diese werden zugleich als primäres Unionsrecht bezeichnet, zu dem auch die ungeschriebenen allgemeinen Rechtsgrundsätze des Unionsrechts und das Gewohnheitsrecht gehören. Der Vertrag über die Europäische Union und der Vertrag über die Arbeitsweise der Europäischen Union enthalten unter anderem Bestimmungen über die grundlegenden Werte und Ziele der Union, über die demokratischen Grundsätze, über die Struktur und Arbeitsweise der Organe der Union, über die Außenpolitik sowie über die Grundfreihei-

ten, über Wettbewerbsregeln und die Wirtschafts- und Währungspolitik. Im dritten Teil des Vertrags über die Arbeitsweise der Europäischen Union sind in 24 Kapiteln alle innenpolitischen Bereiche aufgeführt, in denen die Union tätig werden kann. Es werden jeweils Ziele, Mittel und Entscheidungsverfahren genannt, die dabei angewendet werden können. Aus diesen Rechtssätzen wird sodann das sekundäre Unionsrecht abgeleitet. Hierunter fallen gemäß Art. 288 AEUV Verordnungen, Richtlinien, Beschlüsse sowie Empfehlungen und Stellungnahmen. Das Primärrecht wird auch als Verfassung der Union bezeichnet und ist Prüfungsmaßstab für die Rechtmäßigkeit des Sekundärrechts.

Das Unionsrecht bedarf zum einen des nationalen Vollzugs und zum anderen müssen manche Rechtsakte der Europäischen Union, etwa Richtlinien, durch nationales Recht umgesetzt werden. Auch die nach Art. 114 AEUV vorgesehene Rechtsangleichung hat nicht immer eine Vollharmonisierung zur Folge.[45] Liegt keine Sperrwirkung vor und erlässt auch die nationale Legislative Gesetze, so ist es durchaus möglich, dass für einen Regelungsbereich zwei Gesetze und gleichzeitig zwei verschiedene Rechtsordnungen anwendbar sind. Daher stellt sich die Frage nach dem Rangverhältnis zwischen Unionsrecht und dem nationalen Recht der Mitgliedstaaten. Soweit ein Rechtsakt der Europäischen Union unmittelbare Wirkung entfaltet, richtet er sich zum einen direkt an die Unionsbürger, sodass diesen daraus Rechte und Pflichten entstehen können. Zum anderen müssen die Gerichte und die Verwaltung diesen Rechtsakt wie das nationale Recht anwenden. Das Unionsrecht genießt gegenüber dem nationalen Recht insofern grundsätzlich einen Anwendungsvorrang, sodass entgegenstehendes nationales Recht unanwendbar wird.

Verordnungen – und somit auch die Datenschutz-Grundverordnung – haben allgemeine Geltung, sind in allen ihren Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat. Es bedarf keines Umsetzungsaktes durch die Mitgliedstaaten, vielmehr müssen Gerichte und Verwaltungsbehörden der Mitgliedstaaten Verordnungen mit ihrem In-Kraft-Treten anwenden und auch Individuen werden möglicherweise unmittelbar berechtigt oder verpflichtet. Verordnungen regeln eine unbestimmte Vielzahl von Fallgestaltungen generell und abstrakt und entsprechen damit auf nationa-

[45] Durch die Angleichung von unterschiedlichen Rechts- und Verwaltungsvorschriften in den Mitgliedstaaten der Europäischen Union soll das Funktionieren des Binnenmarktes gewährleistet werden.

ler Ebene einem Gesetz. Die Datenschutz-Grundverordnung genießt somit Anwendungsvorrang vor dem nationalen Datenschutzrecht. Entgegenstehendes nationales Recht wir durch die Verordnung unanwendbar.

Im Gegensatz dazu sind Richtlinien für jeden Mitgliedstaat, an den sie gerichtet werden, nur hinsichtlich ihres zu erreichenden Ziels verbindlich; die Wahl der Form und Mittel ist jedoch den staatlichen Stellen überlassen. Richtlinien richten sich damit nicht direkt an die Bürger, sondern an die Mitgliedstaaten, die verpflichtet sind, die Richtlinien binnen einer festgelegten Frist in nationales Recht umzusetzen. Der nationale Gesetzgeber muss also in aller Regel ein Gesetz erlassen oder modifizieren. Großbritannien, Dänemark, Slowenien und Ungarn haben sich im Laufe der Verhandlungen zur Grundverordnung dafür ausgesprochen, statt der Verordnung eine neue Datenschutz-Richtlinie zu erlassen. Auch in Deutschland wurde dieser Wunsch geäußert.[46]

Die nationalen Datenschutzgesetze verlieren mit Inkrafttreten der Datenschutz-Grundverordnung aber nicht ihre Wirksamkeit, sie dürfen nur dann nicht angewendet werden, wenn sie dem Unionsrecht direkt oder indirekt entgegenstehen, die nationalen Regelungen denen der Verordnung also widersprechen, und wenn Gleiches oder Weitergehendes in der Verordnung geregelt wird. Demgegenüber finden die nationalen Datenschutzvorschriften dann weiter Anwendung, wenn eine nationale Vorschrift die Vorgaben der europäischen Verordnung lediglich ergänzt, ferner dann, wenn die europäische Regelung nicht hinreichend bestimmt und nicht unbedingt formuliert ist sowie im Fall impliziter oder expliziter Öffnungsklauseln.[47] Insbesondere der Rat der Europäischen Union drängte darauf, den öffentlichen Bereich mit Hilfe von Öffnungsklauseln aus der Verordnung auszunehmen.

2.1.5 Europäischer Gerichtshof

Der Europäische Gerichtshof (EuGH) hat die Aufgabe das Unionsrecht bei dessen Auslegung und Anwendung zu bewahren. Er soll die einheitliche Interpretation des EU-Rechts und die Achtung des Rechts durch die EU-Staaten und Institutionen gewährleisten. Der Gerichtshof besteht gemäß Art. 19 Abs. 2 UAbs. 1 EUV aus einem Richter je Mitgliedstaat und wird dabei von neun Generalanwälten unterstützt. Die Generalanwälte geben be-

[46] Der deutsche Bundesrat erhob sogar eine Subsidiaritätsrüge gegen den Entwurf der Kommission; vgl. auch beispielhaft Roßnagel/Kroschwald 2014: S. 495.

[47] S. hierzu ausführlich Roßnagel 2017.

gründete Schlussanträge zu den beim Gerichtshof anhängigen Rechtssachen ab, denen die Richter des EuGH in den meisten Fällen folgen.

Der Europäische Gerichtshof bildet zusammen mit dem Gericht der Europäischen Union (EuG) und dem Gericht für den öffentlichen Dienst (EuGöD) den Gerichtshof der Europäischen Union. Während das Gericht für Klagen der Mitgliedstaaten und von Privaten gegen die EU-Organe zuständig ist, entscheidet das EuGöD über Streitigkeiten aller Organe, Einrichtungen und Agenturen der Union mit ihren eigenen Bediensteten.

Der EuGH hat sich in der jüngeren Vergangenheit durchaus für den Datenschutz verdient gemacht. So hat er schon im Jahr 2003 in der Lindqvist-Entscheidung[48] festgestellt, dass die Verwendung personenbezogener Daten auf einer Webseite eine automatisierte Verarbeitung im Sinne der EG-Richtlinie 95/46/EG ist, so dass grundsätzlich die Richtlinie Anwendung findet, und dass der Begriff der personenbezogenen Daten weit zu verstehen ist. Was Suchmaschinen angeht, hat der EuGH in der Google-Spain Entscheidung[49] geurteilt, dass der Betreiber einer Suchmaschine verpflichtet sein kann, Einträge aus der Ergebnisliste zu entfernen, wenn der betroffenen Person ansonsten ein Schaden entstehen würde und führt das auf die Art. 7 und 8 GRCh zurück. In seinem ersten Urteil zur Vorratsdatenspeicherung[50] hat der Gerichtshof festgestellt, dass die Verpflichtung zur Vorratsspeicherung von Daten und der Gestattung des Zugangs der zuständigen nationalen Behörden zu diesen einen besonders schwerwiegenden Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellt und aus diesem Grund die Richtlinie über die Vorratsspeicherung von Daten für ungültig erklärt. In dieser Linie steht auch das Facebook-Urteil des EuGH, in dem er das sogenannte Safe-Harbor-Abkommen zwischen den USA und der Europäischen Union gekippt hat. Demnach seien die persönlichen Daten europäischer Nutzer in den USA nicht ausreichend vor dem Zugriff der Sicherheitsbehörden geschützt.

Der Europäische Gerichtshof wird mit Inkrafttreten der Datenschutz-Grundverordnung einen deutlichen Zuwachs an Einfluss im Bereich des Datenschutzrechts gewinnen. Viele Fragen der praktischen Ausgestaltung

48 EuGH, Urt. v. 6.11.2003, Rs. C-101/01.
49 EuGH, Urt. v. 13.5.2014, Rs. C-131/12.
50 EuGH, Urt. 8.4.2014, Rs. C-293/12.

der neuen Verordnung sind noch nicht geregelt und werden zum Teil vor Gericht geklärt werden müssen.

2.2 Die Welt der Nationalstaaten

Die Welt der Nationalstaaten vertritt und verteidigt ihre nationalstaatlichen Interessen. Die Praktiken des Regierens sind dabei stets an nationalstaatliche Territorien gebunden. Die Datenschutzinteressen der einzelnen Mitgliedsländer variieren entsprechend je nach den verschiedenen Datenschutzkulturen sowie den wirtschaftlichen und politischen Bedingungen, die vor Ort herrschen. Diese Diversität erschwert die Kompromissbildung zwischen den Nationalstaaten und führte in den Verhandlungen um die Datenschutz-Grundverordnung immer wieder zu Verzögerungen. Während der Verhandlungen um die Datenschutz-Grundverordnung haben insbesondere Großbritannien sowie die Bundesrepublik Deutschland den Einigungsprozess gebremst. Die USA wiederum verfolgten in den Debatten eigene Interessen und versuchten den Verhandlungsprozess zu ihren Gunsten zu beeinflussen. Ebenfalls immer wieder Gegenstand der Diskussionen war Irland, das als europäischer Zufluchtsort vieler Firmen galt, die strenge Datenschutzregeln umgehen wollten. Auch die Rolle der Sicherheitsbehörden wurde kontrovers diskutiert. Somit werden die folgenden kollektiven Akteure der Welt der Nationalstaaten näher betrachtet:

- Bundesrepublik Deutschland
- Irland
- Vereinigtes Königreich
- USA
- Sicherheitsbehörden

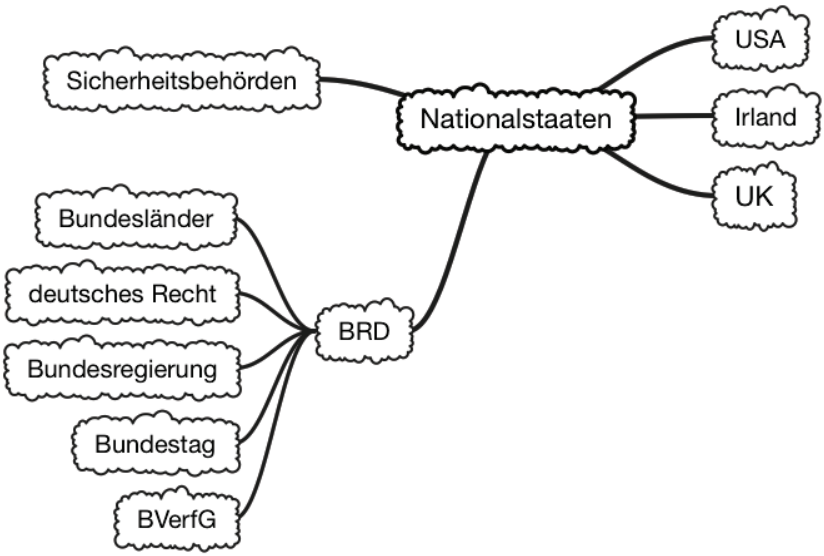

Abbildung 3: Die Welt der Nationalstaaten

2.2.1 Bundesrepublik Deutschland

Als wirtschaftlich leistungsfähigster und bevölkerungsreichster Mitgliedstaat der Europäischen Union hat die Bundesrepublik Deutschland großes Gewicht bei Entscheidungen auf europäischer Ebene – auch beim Datenschutz. Innerhalb der Bundesrepublik Deutschland kann zwischen folgenden Akteuren differenziert werden:

- Bundesregierung
- Bundestag
- Bundesländer
- Deutsches Recht
- Bundesverfassungsrecht

2.2.1.1 Bundesregierung

Die Bundesregierung ist mit ihren Ministern im Rat der Europäischen Union vertreten. Den Bundesministern gegenüber hat die Bundeskanzlerin eine Richtlinienkompetenz inne. Als wirtschaftlich leistungsfähigster und bevöl-

kerungsreichster Mitgliedstaat der Europäischen Union hat die Bundesrepublik Deutschland großes Gewicht bei Entscheidungen auf europäischer Ebene – auch beim Datenschutz.

Im Koalitionsvertrag aus dem Jahr 2013 heißt es zur Datenschutz-Grundverordnung:

„Die EU-Datenschutzgrundverordnung muss zügig weiter verhandelt und schnell verabschiedet werden, um europaweit ein einheitliches Schutzniveau beim Datenschutz zu garantieren. Die strengen deutschen Standards beim Datenschutz, gerade auch beim Datenaustausch zwischen Bürgern und Behörden wollen wir bewahren. Europa braucht ein einheitliches Datenschutzrecht für die Wirtschaft, in dem alle Anbieter, die in Europa ihre Dienste anbieten, dem europäischen Datenschutzrecht unterliegen (Marktortprinzip). Die Grundsätze der Zweckbindung, der Datensparsamkeit und -sicherheit, der Einwilligungsvorbehalt, das Recht auf Löschen und das Recht auf Datenportabilität müssen in der Verordnung gewahrt bleiben."[51]

In den Verhandlungen zur Datenschutz-Grundverordnung galt die Bundesregierung fast durchgängig als Vertreterin einer eher wirtschaftsfreundlichen Position:

„Wir müssen hohe Datensicherheit haben, aber wenn wir uns das Big Data Management, wenn wir uns die Möglichkeit der Verarbeitung großer Datenmengen durch einen falschen rechtlichen Rahmen zu sehr einengen, dann wird nicht mehr viel Wertschöpfung in Europa stattfinden. Das wäre für uns von großem Nachteil." (Angela Merkel)[52]

2.2.1.2 Bundestag

„Der Deutsche Bundestag fordert die Bundesregierung darüber hinaus auf, sich von Anbeginn der bereits für Juni 2015 angesetzten Trilogverhandlungen für weitere Verbesserungen einzusetzen, mit denen ein höchstmögliches Schutzniveau für die Bürgerinnen und Bürger erzielt und keinesfalls weiteren Verschlechterungen der Rechtspositionen zugestimmt wird." (Bündnis 90/Die Grünen)[53]

---

51 Deutschlands Zukunft gestalten, Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Legislaturperiode, 149.

52 Merkel 2015.

53 Antrag der Abgeordneten Dr. Konstantin von Notz, Luise Amtsberg, Volker Beck (Köln), Katja Keul, Renate Künast, Monika Lazar, Irene Mihalic, Özcan Mutlu, Hans-Christian Ströbele und der Fraktion BÜNDNIS 90/DIE GRÜNEN zu dem Vorschlag einer EU-Datenschutzverordnung KOM (2012) 11, Stellungnahme gegenüber der Bundesregierung, 10.06.2015, BT-Drs. 18/5102, 2.

In der Bundesrepublik Deutschland bildet der Bundestag zusammen mit dem Bundesrat als Vertretung der Bundesländer die Legislative. Die Verlagerung von Gesetzgebungsbefugnissen auf die Europäische Union bedeutet einen teilweisen Einflussverlust für den Deutschen Bundestag. Einige Kritiker sehen darin gleichzeitig eine Schwächung der demokratischen Rückkopplung der Rechtsetzung, da sie der Europäischen Union ein Demokratiedefizit attestieren.[54] Dies gilt auch für den Wechsel von der Datenschutzrichtlinie zur Datenschutz-Grundverordnung. Wo eine europäische Richtlinie noch ein nationales Umsetzungsgesetz erfordert, bei dem ein gewisser Umsetzungsspielraum verbleibt, gilt eine europäische Verordnung direkt und ohne Umsetzungsakt in den Mitgliedstaaten. Die endgültige Fassung der Datenschutz-Grundverordnung enthält jedoch zahlreiche Öffnungsklauseln. Diese ermöglichen es den Mitgliedstaaten in bestimmten Bereichen eigene Vorschriften beizubehalten oder zu erlassen, sodass der Wechsel vom Instrument der Richtlinie zur Verordnung abgemildert wird. Anzahl und Reichweite der Öffnungsklauseln sind jedoch höchst umstritten.

Zur Zeit der Aushandlungen der Datenschutz-Grundverordnung stellten von den fünf im Deutschen Bundestag vertretenen Parteien drei die Bundesregierung (CDU, CSU und SPD) und waren somit indirekt an den Verhandlungen zur Datenschutz-Grundverordnung beteiligt. Die Opposition bestand im 18. Bundestag aus den Parteien „Die Linke" und „Bündnis 90/Die Grünen".

„Wir leben im Zeitalter der digitalen Revolution, in der Daten die neue Währung sind. (...) Aus diesem Grund müssen wir die Privatsphäre unserer Bürger noch besser als zuvor schützen, denn sie haben ein Recht darauf, dass ihre Daten geheim bleiben. In diesem Grundsatz dürfen wir uns nicht beirren lassen. Datenschutz ist ein Grundrecht! Dabei ist es wichtig, dass die Standards trotz erheblicher Verbesserungen für die Nutzer auch für die Wirtschaft noch praktikabel bleiben. (...) Bei der Ratsposition handelt es sich um kein geschriebenes Gesetz, es ist lediglich eine Ausgangslage für die anstehenden Verhandlungen. Sowohl das Parlament als auch die Mitgliedstaaten sollten den Mut haben, auch von der eigenen Position abzurücken und den Text zu verbessern, um den bestmöglichen Datenschutz zu gewährleisten." (Axel Voss, Mitglied und stellvertretender Vorsitzender des Rechtsausschusses des

[54] Klein 2014.

Europäischen Parlaments und Berichterstatter seiner Fraktion CDU/CSU für die Überarbeitung der EU-Datenschutzverordnung)[55]

Eine indirekte Beteiligung aller genannten Parteien an den Verhandlungen zur Datenschutz-Grundverordnung ergab sich über das Europäische Parlament, dem wiederum Mitglieder der im Deutschen Bundestag vertretenen Parteien angehören, und die dort zusammen mit gleichgesinnten Abgeordneten anderer Mitgliedstaaten der Europäischen Union Interessengemeinschaften gebildet haben.

Nicht vertreten im Deutschen Bundestag ist die „Piratenpartei Deutschland", für die der Datenschutz und der Schutz der Privatsphäre in der digitalen Welt programmatische Schwerpunkte darstellen. Die Partei war zwischenzeitlich in verschiedenen deutschen Landesparlamenten vertreten, hat aber mittlerweile nur noch einen Abgeordneten im Europäischen Parlament.[56]

2.2.1.3 Bundesländer

„Der Bundesrat hat heute eine Subsidiaritätsrüge gegen den Verordnungsvorschlag erhoben, mit dem die europäische Kommission einen neuen Rechtsrahmen zum Schutz personenbezogener Daten schaffen möchte. Der Vorschlag lege nicht ausreichend dar, warum eine verbindliche Vollregelung des Datenschutzes auf europäischer Ebene erforderlich sein soll. Zudem führe er mit seinem umfassenden verbindlichen Geltungsanspruch zur nahezu vollständigen Verdrängung mitgliedstaatlichen Datenschutzes und gehe weit über die Kompetenzzuweisung der EU hinaus. Er widerspreche damit den Prinzipien der Subsidiarität und Verhältnismäßigkeit (...)" (Bundesrat)[57]

Aufgrund der föderalen Struktur der Bundesrepublik Deutschland existieren in allen Bundesländern eigene Landesdatenschutzgesetze, die den Umgang mit personenbezogenen Daten durch die öffentliche Verwaltung regeln. Der Datenumgang der jeweiligen Landespolizei ist wiederum meist in den Polizeigesetzen der Länder geregelt. Daneben existieren weitere landesspezifische Spezialgesetze zum Datenschutz. Auch diese Gesetze sind vom Erlass der Datenschutz-Grundverordnung betroffen und müssen bis zum

55 Mies 2015.
56 Julia Rede, seit 2014.
57 Bundesrat 2012.

Geltungsbeginn der Verordnung im Jahr 2018 überarbeitet und angepasst werden.

Über den Bundesrat können die Landesregierungen Einfluss auf den Gesetzgebungsprozess auf Bundesebene nehmen.

„Der Bundesrat weist darauf hin, dass Besetzungs- und Entscheidungsverfahren des europäischen Datenschutzausschusses jedenfalls bei seiner Ausgestaltung als europäischer Einrichtung mit verbindlichen Entscheidungsbefugnissen wegen der damit verbundenen Verlagerung von Verwaltungskompetenzen der Länder bereits im Rahmen der vorgeschlagenen Datenschutz-Grundverordnung so ausgebildet werden müssen, dass sie mit der innerstaatlichen Kompetenzverteilung in Einklang gebracht werden können. Die Anforderungen an die Entsendung mitgliedstaatlicher Vertreter sollten deshalb so ausgeformt werden, dass innerstaatliche Abstimmungsprozesse der Datenschutzaufsichtsbehörden, wie sie zum Beispiel im Bereich der Zusammenarbeit von Bund und Ländern in EU-Angelegenheiten erprobt sind, durch das Unionsrecht weder formal noch durch verfahrensrechtliche Anforderungen wie etwa kurze Entscheidungsfristen ausgeschlossen werden." (Bundesrat)[58]

Anfänglich äußerte sich der Bundesrat kritisch zur Verordnung und sah darin eine Kompetenzüberschreitung des europäischen Gesetzgebers. Auch im weiteren Verfahren setzte er sich immer wieder für nationale Spielräume bei der Ausgestaltung des Datenschutzrechts ein.

2.2.1.4 Deutsches Recht

„Anstatt Unternehmen, wie bisher, mit einer Vielzahl verschiedener Gesetze, mit teils unzureichender Passgenauigkeit und Konkretisierung, zu konfrontieren, kann die EU-Datenschutzverordnung ein einheitliches Regelwerk für alle betroffenen Märkte schaffen. Hier kann die deutsche Gesetzgebung als Vorbild dienen, da diese, trotz historisch bedingter fehlender Berücksichtigung digitaler Medien, bereits ein selbstbestimmtes Verständnis von Datenschutz geschaffen hat. Dabei ist insbesondere der Wahrnehmung entgegenzutreten, deutsche Datenschutzstandards würden den Einsatz moderner Marketinginstrumente wie Personalisierung, Profilierung und Tracking verbieten und damit einen generellen Nachteil schaffen. Denn grundsätzlich dürfen deutsche Unternehmen das Gleiche wie Unternehmen in den USA – mit dem Unterschied, dass sie hierzu eine wirksame Einwilligung des jeweils be-

[58] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr v. 28.11.2014, COM (2012) 11 final, BR-Drs. 550/14, 6.

troffenen Nutzers einholen müssen, wenn sie personenbezogene Daten verwenden." (Bundesverband Digitale Wirtschaft e.V.)[59]

Das deutsche Datenschutzrecht wurde von vielen Akteuren gerade innerhalb der Diskussionen in Deutschland als ein „best practice Beispiel" hochgehalten und als Vorbild für die Datenschutz-Grundverordnung propagiert. Dieses setzt sich aus dem Verfassungsrecht und verschiedenen einfachgesetzlichen Vorschriften zusammen. Wenn von den Vorzügen des deutschen Datenschutzes die Rede ist, wird insbesondere die Errungenschaft des Rechts auf informationelle Selbstbestimmung, welches das Bundesverfassungsgericht im Jahr 1983 aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz hergeleitet hat, hervorgehoben. Dieses gibt jedem das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Auf diese Weise soll den Veränderungen und neuen Risiken der Informations- und Kommunikationstechnologien entgegengewirkt werden.

Zu den einfachgesetzlichen Vorschriften des deutschen Datenschutzrechts gehören das Bundesdatenschutzgesetz, das Telemediengesetz, das Telekommunikationsgesetz sowie weitere fachspezifische Einzelvorschriften, wobei das Bundesdatenschutzgesetz aus dem Jahr 1977 die zentrale Datenschutzvorschrift des deutschen Rechts darstellt. Ferner hat jedes Bundesland neben dem Bundesdatenschutzgesetz ein eigenes Landesdatenschutzgesetz. Sofern es bereichsspezifische Vorschriften in Bezug auf spezielle Lebensbereiche gibt, die präzisere, weitergehende oder abweichende Regelungen treffen, als das Bundesdatenschutzgesetz in diesen Bereichen, tritt dieses in der Anwendung gegenüber den bereichsspezifischen Vorschriften zurück. So wird das Telemediengesetz angewandt, sofern personenbezogenen Daten im Internet verarbeitet werden und das Telekommunikationsgesetz, wenn es zum Einsatz von Telekommunikationstechniken kommt.

Das deutsche Recht und das Unionsrecht sind grundsätzlich zwei eigenständige und voneinander getrennte Rechtsordnungen.[60] Beide haben eine eigenständige Daseinsberechtigung. In der Praxis existieren aber ganz erhebliche Verflechtungen der beiden Rechtsordnungen. Das deutsche Datenschutzrecht wurde zum Teil von europäischen Vorgaben geprägt, hat diese

[59] BVDW e.V. 2013.

[60] Roßnagel 2017: S. 67 Rn. 3.

aber auch selbst beeinflusst. Die EU-Datenschutzrichtlinie[61] trat im Jahr 1995 in Kraft und musste in den folgenden drei Jahren von den europäischen Mitgliedstaaten in nationales Recht umgesetzt werden.[62] Ergänzt wurde die Datenschutzrichtlinie durch die Richtlinie 2002/58/EG[63], mit der erkannten Defiziten der Datenschutzrichtlinie im Bereich der elektronischen Kommunikation entgegengewirkt werden sollte. Da das nationale und das europäische Datenschutzrecht in einer Zeit entwickelt wurden, in der das heutige Internet mit seinen Informations- und Kommunikationstechnologien sowie Geschäftsmodellen noch nicht existierte, war eine Überarbeitung der bestehenden Rechtsgrundsätze notwendig. Die Risiken, die aufgrund der Verarbeitung und Erzeugung von personenbezogenen Daten durch neue Technologien in allen gesellschaftlichen Bereichen entstehen, waren zu den Entstehungszeiten des Bundesdatenschutzgesetzes und der EU-Datenschutzrichtlinie noch nicht bekannt und absehbar. Daher war es das Ziel der Europäischen Union das europäische Datenschutzrecht zu modernisieren, sodass die Datenschutz-Grundverordnung ausgearbeitet wurde. Die Verordnung wird mit ihrem Geltungsbeginn die EU-Datenschutzrichtlinie ablösen und das Bundesdatenschutzgesetz in weiten Teilen ersetzen. Das Unionsrecht und das deutsche Datenschutzrecht gelten dann nebeneinander, da die Europäische Union keine Kompetenz besitzt, deutsche Gesetze außer Kraft zu setzen.[64] Grundsätzlich haben EU-Verordnungen somit keinen Geltungsvorrang gegenüber den nationalen Gesetzen, auch wenn sie für die europäischen Mitgliedstaaten verbindlich sind. Hinzu kommt, dass sich in der Datenschutz-Grundverordnung zahlreiche Öffnungsklauseln finden, die es den europäischen Mitgliedstaaten ermöglichen, eigene Regelungen in bestimmten datenschutzrechtlichen Bereichen zu schaffen. Dadurch entsteht eine unübersichtliche Rechtslage, bei der sich Regelungen widersprechen können oder unklar ist, welche Vorschriften zur Anwendung kommen. In solchen Konfliktsituationen genießt das Unionsrecht daher einen Anwendungsvorrang gegenüber den nationa-

---

61 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt L 281/31 vom 23.11.1995.

62 In Deutschland erfolgte die Umsetzung allerdings erst im Jahr 2001.

63 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Amtsblatt L 201/37 vom 31.07.2002.

64 Roßnagel 2017: S. 68 Rn. 4.

len Vorschriften.[65] Das bedeutet, dass die Datenschutz-Grundverordnung zur Anwendung kommt und die entsprechenden innerstaatlichen Bestimmungen nicht angewandt werden dürfen.[66]

Vor diesem Hintergrund sind viele Anpassungen und Überarbeitungen des bestehenden deutschen Datenschutzrechts notwendig. Denn obwohl die Verordnung nach ihrem Inkrafttreten im Mai 2018 unmittelbar ein Teil der Rechtsordnung jedes Mitgliedstaats wird, wird diese Wirkung durch viele Ausnahmeregelungen in der Verordnung eingeschränkt. Die Anpassung des nationalen Rechtsrahmens für den Datenschutz obliegt dem deutschen Gesetzgeber. Um dieser Aufgabe gerecht zu werden, muss er bestehende Vorschriften prüfen und gegebenenfalls neue Regelungen erlassen, um so die Lücken der Verordnung auszufüllen und die Vorschriften der Datenschutz-Grundverordnung unter Umständen zu ergänzen und zu präzisieren. Dies tut er beispielsweise durch die Schaffung eines neuen Bundesdatenschutzgesetzes. Dabei ist stets das Regelungsziel der Verordnung zu beachten und in der Durchsetzung zu unterstützen. Darüber hinaus sind die abstrakten und weit gefassten Regelungen der Verordnung in der Praxis sowohl durch den Europäischen Gerichtshof als auch durch nationale Gerichte und Aufsichtsbehörden zu konkretisieren.

2.2.1.5 Bundesverfassungsgericht

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden." (BVerfGE 65, 1 (43), 15.12.1983).

Das Bundesverfassungsgericht ist „Hüter des Grundgesetzes" und wacht über die Einhaltung deutscher Grundrechte. Im Jahr 1983 erkannte es in seinem Volkszählungsurteil[67] das Grundrecht auf informationelle Selbstbestimmung an, das seither den grundrechtlichen Rahmen für die Verarbeitung personenbezogener Daten in der Bundesrepublik Deutschland bildet. Das Grundrecht „gewährleistet die Befugnis des Einzelnen, grundsätzlich

[65] Roßnagel 2017: S. 68 Rn. 5.

[66] Vgl. hierzu ausführlich Roßnagel 2017: S. 67 ff.

[67] BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83.

selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ und damit „selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“.[68]

Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist auf den Umgang mit personenbezogenen Daten beschränkt. Diese sind nach der Definition des § 3 Abs. 1 Bundesdatenschutzgesetz „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Auf die Qualität des Datums kommt es dabei nicht an. Vielmehr stellte das Gericht schon im Jahr 1983 fest, dass es gerade durch den technischen Fortschritt und der damit verbundenen Möglichkeit des Sammelns und des Kombinierens von Daten „kein belangloses Datum“ mehr gibt. Jede für sich gesehen noch so unerhebliche Information kann in Verknüpfung mit anderen Daten Rückschlüsse auf die Betroffenen, ihren Lebensweg und ihre Persönlichkeit ermöglichen. Einzelinformationen können so zu einem „weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden“. Unterschiedliche Sphären existieren beim Recht auf informationelle Selbstbestimmung daher nicht; vielmehr ist die Selbstbestimmung über jede Information, die die Betroffenen betrifft, in gleichem Maße schutzwürdig.[69]

Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt in jeder fremdbestimmten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten. Beschränkungen der informationellen Selbstbestimmung bedürfen einer „(verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht“.

Auf europäischer Ebene stehen dem Bundesverfassungsgericht der Europäische Gerichtshof und der Europäische Gerichtshof für Menschenrechte gegenüber, die über die Einhaltung der Charta der Grundrechte der Europäischen Union bzw. der Europäischen Menschenrechtskonvention wachen.

2.2.2 Irland

Irland spielt in der Datenschutzdebatte eine gewichtige Rolle. Viele datenverarbeitende Großkonzerne wie etwa Facebook Inc., Google Inc., Twitter

[68] BVerfGE 65, 1 (42).

[69] BVerfGE 65, 1 (42).

Inc. und Microsoft Corporation haben das Land als Standort für ihre Niederlassungen und den Bau großer Datenzentren gewählt. Die Datenschutzaufsicht durch den Data Protection Commissioner of Ireland wurde indes als im europäischen Vergleich schwach wahrgenommen. Lediglich 28 Mitarbeiter[70] hat der Hauptstandort in Portarlington; daneben existiert noch eine Nebenniederlassung in Dublin. Darüber hinaus herrscht eine bezogen auf die Umstände der Datenverarbeitung im Vergleich zu Deutschland und den meisten EU-Mitgliedstaaten deutlich großzügigere Mentalität vor.

Irland stand deshalb im Kern der Debatte um das sogenannte „Forum Shopping", einer Praxis, bei der ein Unternehmen bewusst den Staat mit den niedrigsten – in diesem Zusammenhang datenschutzrechtlichen – Beschränkungen als Sitz seiner Niederlassungen wählt; ein vor allem im Kontext von Steuervermeidung bekanntes Vorgehen (sog. Treaty Shopping). Die Datenschutz-Grundverordnung ist unter anderem mit dem erklärten Ziel angetreten, das Forum Shopping zu beenden.

Irland und die dortige Niederlassung von Facebook Inc. standen auch im Fokus des sogenannten Safe Harbor-Urteils des Europäischen Gerichtshofs.[71]

2.2.3 Vereinigtes Königreich

Das Vereinigte Königreich hat infolge eines am 23. Juni 2016 abgehaltenen, nicht bindenden Referendums seinen Willen zum Austritt aus der Europäischen Union erklärt. Dies wird sich auch auf den Datenschutz auswirken. Insbesondere bedeutet es, dass das Vereinigte Königreich nach erfolgtem Austritt nicht mehr direkt an europäisches Datenschutzrecht gebunden sein wird. Die euroskeptische Haltung Großbritanniens zeigte sich auch in deren Position während der Verhandlungen um die Datenschutz-Grundverordnung. Großbritannien drängte immer wieder darauf die Verordnung in eine Richtlinie umzuwandeln und so größtmöglichen nationalen Spielraum zu bewahren.

Viel spricht jedoch dafür, dass sich das Vereinigte Königreich in Sachen Datenschutz auch nach erfolgtem Austritt aus der Europäischen Union an deren datenschutzrechtlichen Bestimmungen orientieren wird – zu einem gewissen Grad auch orientieren muss. Sollte der Austritt bis zum 25. Mai 2018

70 Stand Ende 2015.

71 EuGH, Urt. v. 06.10.2015, Az. C-362/14, ECLI:EU:C:2015:650.

nicht erfolgt sein, gilt die Datenschutz-Grundverordnung ohnehin zunächst unmittelbar auch im Vereinigten Königreich. Die britische Premierministerin Theresa May hat den offiziellen Austrittsantrag nach Art. 50 EUV am 29. März 2017 gestellt.[72] Mit dem Austritt des Vereinigten Königreichs ist damit nicht vor März 2019 zu rechnen.

Aufgrund des Marktortprinzips der Datenschutz-Grundverordnung sind Unternehmen ohnehin an diese gebunden, sofern sie Waren und Dienstleistungen in der Europäischen Union anbieten. Hier dürfte es ein großes Interesse geben, nicht zwei unterschiedlichen Datenschutzregimes unterworfen zu sein – dem europäischen und einem neu zu schaffenden britischen. Vielmehr wird die Wirtschaft höchstwahrscheinlich Druck auf die neue Regierungschefin ausüben, um Kosten zu sparen.

2.2.4 USA

„Another concern we have is the regulation's requirement for explicit consent in all circumstances. We are concerned that a one-size-fits-all consent requirement would frustrate individual users because of the sheer number of consent requests they would be faced with, leading eventually to users just clicking through instead of making informed choices. At the same time, explicit consent can make it difficult for companies to use personal data in innovative ways to offer better services to consumers.(…) Furthermore, in the financial sector context, the 'right to be forgotten' could also lead to moral hazard, where defaulting parties demand their credit histories be deleted, putting the European financial system at risk. We also have concerns about the very limited protection to the freedom of expression that the regulation offers." (William E. Kennard, US-Botschafter der Europäischen Union)[73]

Die US-Regierung hat wiederholt versucht Einfluss auf die Verhandlungen der Datenschutz-Grundverordnung auszuüben und ihr Verständnis von Privatheit und Datenschutz in den Prozess einzubringen.

Von den meisten Mitgliedstaaten der Europäischen Union unterscheiden sich die USA durch ein deutlich unterschiedliches Verständnis von Privacy und Datenschutz.

Der Begriff „Privacy" ist im Text der Verfassung der Vereinigten Staaten von Amerika und ihrer Zusätze nicht enthalten; Gleiches gilt für den Begriff „Private Life". Vielmehr finden sich einzelne Aspekte von Privatheit im

72 Al-Serori/Brunner/Fürst/Munzinger 2017.

73 Hogan Lovells 2012 a.

First, Fourth, Fifth, Ninth und Fourteenth Amendment, die sich zu einem Schutz der Privatsphäre vor staatlichen Eingriffen summieren. Hervorzuheben ist vor allem der im Jahr 1791 ratifizierte vierte Verfassungszusatz, der ein Abwehrrecht gegen unangemessene Durchsuchungen, Festnahmen und Beschlagnahmen enthält. Die „Invasion of Privacy" spielt allerdings vor allem im amerikanischen Deliktsrecht eine Rolle. Als Auslöser für die Entwicklung eines „Right to Privacy" gilt ein Artikel von Warren und Brandeis aus dem Jahr 1890. Die Autoren beklagten, die Presse übertrete „in every direction the obvious bounds of property and decency. Gossip is no longer the resource of the idle and the vicious, but has become a trade, which is pursued with industry".[74]

Privacy wird vor allem von der sogenannten „Castle Doctrine" her gedacht. Diese geht auf einen Ausspruch des englischen Rechtsgelehrten Coke aus dem Jahr 1628 zurück:

„For a man's house is his castle – et domus sua cuique est tutissimum refugium."[75]

Hieraus hat sich im Gegensatz zu Deutschland ein eigenes „Privacy Law" herausgebildet, das vornehmlich mit personenbezogenen Daten befasst ist. Der Begriff „Privacy Law" ist demnach häufig auf die Erhebung und Verwendung personenbezogener Daten reduziert, also „Information Privacy". Daneben lassen sich jedoch noch die Bereiche „Bodily Privacy", „Privacy of Communication" und „Territorial Privacy" identifizieren.

In besonders starkem Kontrast steht der Ansatz, das Sammeln und Speichern von Daten und die Zuordnung zu einem Pseudonym solle noch kein Eingriff in die Rechte der Bürger sein, sondern erst das bedarfsorientierte „Anfassen" der Daten etwa durch staatliche Behörden zur Verbrechensaufklärung.

2.2.5 Sicherheitsbehörden

„Wir brauchen eine Technologieoffensive. Wir müssen unsere Sicherheitsbehörden noch viel mehr als bisher technisch ertüchtigen. (…) Wir müssen uns auch technologisch weiterentwickeln, etwa beim Einsatz von Biometrie. (…)"(Thomas de Maizière, Bundesminister des Innern)[76]

---

74 Warren/Brandeis Harv. L. Rev. 4/1890, 193, übersetzter Nachdruck DuD 2012, 755.
75 Coke, 3 Inst, Kapitel 73, 162.
76 De Maizière 2016.

Im Juni 2013 begannen die Zeitungen „The Guardian“ und „The Washington Post“ geheime Dokumente zu veröffentlichen, die sie von Edward Snowden, einem ehemaligen Mitarbeiter der amerikanischen „National Security Agency“ (NSA), erhalten hatten. Dies war der Beginn der sog. Snowden-Enthüllungen, die ein weltweites Netzwerk von Spionagesystemen vor allem rund um den Geheimdienst National Security Agency und den britischen Geheimdienst „Government Communications Headquarters“ (GCHQ) aufdeckten. Die Dokumente zeigten, dass sie mit ihren Partnerdiensten und unter Einsatz von „PRISM“ (Planning Tool for Resource Integration, Synchronization and Management) jede Form von elektronischer Kommunikation überwachen wollen. PRISM ist ein Programm zur Überwachung und Auswertung von elektronischen Medien und elektronisch gespeicherten Daten.[77] So wurden beispielsweise die Weltbank, einige Botschaften, Google Inc., Yahoo Corporation, WikiLeaks, Unicef, zahlreiche Politiker und Staatsoberhäupter ausspioniert und/oder gehackt, 122 Regierungschefs aus aller Welt abgehört, darunter auch Bundeskanzlerin Angela Merkel sowie in den Jahren 2001 bis 2015 in den USA sämtliche Verbindungsdaten des E-Mail-Verkehrs und der Telefongespräche gespeichert.[78] Die Enthüllungen erinnern stark an den Echelon-Skandal aus dem Jahr 1997, bei dem der amerikanische Geheimdienst das gleichnamige System zum Abhören kommerzieller Telekommunikationssatelliten verwendete. Dabei wurden Telefonkabel angezapft und Aufklärungsmaterial durch Abhörstationen gesammelt. Im Mittelpunkt des Vorgehens standen heikle Informationen über Personen, Institutionen, Wirtschaftsunternehmen und Regierungen, was das Abhören der internationalen Kommunikation ermöglichte.[79] Klar ist, dass sowohl mit Hilfe von Echelon als auch unter dem Einsatz von PRISM ebenso die normale Bevölkerung ausgespäht wurde. Ein solches Vorgehen zielt zunächst darauf ab, verdächtige Personen aufzuspüren, die zuvor innerhalb des Polizeisystems unauffällig waren. Zugleich kann aber aufgrund der überwachten Personen nicht nur die Terrorbekämpfung ein vordergründiges Ziel der Geheimdienste gewesen sein. Es ging daher wohl auch um die eigenen wirtschaftlichen und politischen Interessen der ausführenden Länder.[80] Diese Praktiken der Geheimdienste gerieten in den

77 Ulfkotte 2013.
78 Beuth 2013.
79 Campbell 2000.
80 Beuth 2013.

letzten Jahren vermehrt in die öffentliche Kritik, nicht zuletzt aufgrund zahlreicher Leaks. Die Ausspähpraktiken insbesondere ausländischer Geheimdienste und die Möglichkeiten diese zu unterbinden, waren daher auch Thema in den Verhandlungen um die Datenschutz-Grundverordnung.

Die Sicherheitsbehörden sammeln zur Erfüllung ihrer Aufgaben personenbezogene Daten und versuchen jede Art der elektronischen Kommunikation zu unterwandern. Dies führt jedoch zu einem Spannungsverhältnis zwischen dem Sicherheitsauftrag, den die Behörden haben, und den Interessen der Bürger an ihrer Privatheit. Diese Problematik ist ursächlich für einen enormen Anstieg an verschlüsselten Internetverbindungen. Auch Großkonzerne wie Google Inc., Microsoft Corporation oder Apple Inc. bauen ihre Verschlüsselungstechniken zum Schutz ihrer Kundendaten aus. Zugleich schützen sich die Unternehmen auf diese Weise selbst. Denn indem sie selbst keine Möglichkeiten mehr haben auf die Kommunikation ihrer Kunden zuzugreifen, werden Sicherheitsbehörden solche Informationen nicht anfragen. Die aktuellen Bestrebungen der Geheimdienste fokussieren sich daher vermehrt auf das Aufbrechen solcher Verschlüsselungssysteme.[81] Sie erschweren die Arbeit der Geheimdienste oder können es sogar technisch unmöglich machen eine elektronische Kommunikation zu überwachen. Dies führte schließlich zu einem Aufleben der sog. Kryptodebatte innerhalb der Gesellschaft und der Politik. Die Sicherheitsbehörden wünschen sich daher gesetzliche Ermächtigungsgrundlagen diese Verschlüsselungen aufheben oder den Einsatz von Hintertüren bei Verschlüsselungssystemen anwenden zu dürfen.[82]

Auch innerhalb Deutschlands gibt es ähnliche Bestrebungen, indem z. B. die Vorratsdatenspeicherung um Messengerdienste und E-Mail-Dienste ausgeweitet werden soll,[83] da diese vermehrt auf Verschlüsselungstechnologien setzen. Außerdem wird eine neue Behörde des Bundesinnenministeriums mit der Bezeichnung „Stelle für Informationstechnik im Sicherheitsbereich" (Zitis) eingerichtet, die von den Medien bereits jetzt als Mini-NSA bezeichnet wird.[84]

81 Greis 2016.
82 Geminn 2015: S. 546 f.
83 Greis 2016.
84 Flade 2016.

In Deutschland besitzen sowohl der Bund als auch die Bundesländer jeweils eigene Sicherheitsbehörden mit eigenen Aufgaben. Im Sinne des sog. Trennungsgebots werden die Aufgaben der Polizei und der Nachrichtendienste durch verschiedene und organisatorisch voneinander getrennte Behörden wahrgenommen. Die Gesetzgebungs- und Verwaltungskompetenzen liegen auf dem Gebiet der Sicherheitsbehörden in erster Linie bei den Bundesländern. Auf dieser Ebene wird zwischen den Landeskriminalämtern und den Landes-Verfassungsschutzbehörden unterschieden.[85] Auf Bundesebene ist das Bundesamt für Verfassungsschutz der Inlandsnachrichtendienst des Bundes und untersteht dem Bundesministerium des Innern. Dessen Hauptaufgabe besteht gemäß § 3 Bundesverfassungsschutzgesetz in der Beobachtung derjenigen, die Bestrebungen gegen die freiheitliche demokratische Grundordnung, gegen den Bestand und die Sicherheit des Bundes oder eines Landes vornehmen. Der Bundesnachrichtendienst ist der deutsche Auslandsnachrichtendienst, der Informationen über bedeutsame und Deutschlands Sicherheit betreffende Sachverhalte im Ausland sammelt und auswertet. Die Bundespolizei und das Bundeskriminalamt bilden die Polizeibehörden des Bundes. Die Hauptaufgabe des Bundeskriminalamts besteht in der Abwehr von Gefahren des internationalen Terrorismus. Aufgrund der unterschiedlichen Befugnisse der verschiedenen Sicherheitsbehörden müssen sie sich im sog. „Gemeinsamen Terrorismusabwehrzentrum“ untereinander über ihre Tätigkeiten austauschen. Für den Bereich des Rechtsextremismus wurde eine eigene Behörde eingerichtet („Gemeinsames Abwehrzentrum gegen Rechtsextremismus“), in der die Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zusammenarbeiten. Im Jahr 2012 wurde die Behörde um die Abteilung des „Gemeinsamen Extremismus- und Terrorismusabwehrzentrums“ erweitert, die sich um die Bereiche des Ausländerextremismus bzw. -terrorismus, des Linksextremismus bzw. -terrorismus und der Spionage kümmert.[86]

2.3 Die Welt des Datenschutzes

Die Welt des Datenschutzes versucht ein zuverlässiges und starkes Datenschutzniveau innerhalb Deutschlands, der Europäischen Union oder aber auch weltweit zu etablieren. Im Zentrum steht nicht der Schutz der Daten an sich, sondern der Schutz der Rechte des Einzelnen auf Privatheit und

[85] Kriminalpolizei o. J.

[86] BMI o. J.

Selbstbestimmung als Voraussetzung für eine freie und offene Gesellschaft. Ein besonderes Anliegen der Welt des Datenschutzes ist deshalb der Ausgleich von Machtasymmetrien zwischen Individuen und Organisationen. So gibt es zum einen Aktivisten, die alleine oder im Verbund auf ihrer Meinung nach unrechtmäßige Praktiken im Bereich des Datenschutzes aufmerksam machen wollen und gegen diese vorgehen. Zum anderen setzen sich staatliche Behörden für die Einhaltung der Datenschutzbestimmungen ein und stehen den Bürgern beratend zur Seite. Für Unternehmen werden Daten aufgrund der Digitalisierung zu einem immer wichtigeren Gut, sodass der Datenschutz auch in den Fokus des Verbraucherschutzes gerückt ist.

„EDRi welcomes the European Commission's proposal for a new data protection Regulation. Europe needs a comprehensive reform in order to ensure the protection of its citizens' personal data and privacy, while enhancing legal certainty and competitiveness in a single digital market." (European Digital Rights)[87]

Datenschutz dient den Datenschützern nicht als Selbstzweck, sondern wird häufig mit einem höheren Wert verknüpft. Oft findet man den Bezug zur informationellen Selbstbestimmung und zu Privatheit als Wert, den es zu verteidigen gilt. Was Privatheit in diesen Kontexten genau bedeutet, wird nicht explizit ausbuchstabiert.

„Beim Datenschutz geht es nicht um den Schutz von Daten. Im Mittelpunkt steht das informationelle Selbstbestimmungsrecht des Einzelnen und damit der Mensch." (Andrea Voßhoff, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)[88]

Wenngleich die unterschiedlichen Vertreter der Welt ein gemeinsames Ziel verfolgen, so unterscheiden sie sich doch hinsichtlich des Mitteleinsatzes, um dieses Ziel zu erreichen, sowie hinsichtlich einer unterschiedlichen Rechtfertigungslogik. So macht es einen Unterschied, ob man institutionelle Mittel wie das Recht aktiviert (beispielsweise in Form von Klagen), oder ob man versucht durch öffentlichen Druck Veränderungen herbeizuführen. Der Schutz der Privatheit kann mit weiteren gesellschaftlichen Zielen verknüpft und als kollektives Gut betrachtet werden, das dem Wohle der Gemeinschaft dient. So wird beispielsweise Privatheit als Bedingung für De-

87 EDRi 2012.

88 BfDi o. J. a.

mokratie angesehen.[89] Privatheit kann aber ebenso als individuelle Angelegenheit im Sinne eines persönlichen Anspruchs betrachtet werden, was etwa für die Autonomie des Individuums gilt. Aufgrund der unterschiedlichen Strategien und Logiken lassen sich in den Verhandlungen vier Vertreter identifizieren:

- Datenschutzaktivisten
- Datenschutzbehörden
- Verbraucherschützer
- Artikel 29-Datenschutzgruppe

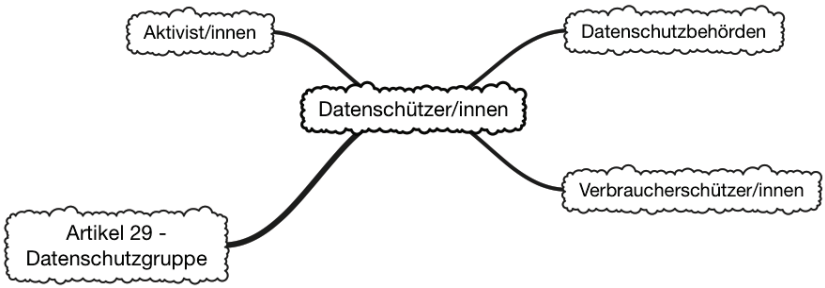

Abbildung 4: Die Welt des Datenschutzes

2.3.1 Datenschutzaktivisten

„Why we need a Regulation (and not a Directive): An EU wide, unified approach to securing an appropriately high level of data protection, and to the safeguarding of essential elements of democratic societies such as privacy and free speech is long overdue. It is crucial in a fast changing digital environment." (European Digital Rights)[90]

Die Datenschutzaktivisten möchten den Datenschutz stärken und die informationelle Selbstbestimmung des Einzelnen sowie Privatheit als Wert verteidigen. In der Rechtfertigung ihrer Tätigkeit wird dabei häufig auf höhere Werte Bezug genommen. Datenschutz ist demnach kein Selbstzweck, vielmehr setzt ihrer Meinung nach eine demokratische Gesellschaft zum

[89] Für einen Überblick zur Rolle von Privatheit und Öffentlichkeit für die Demokratie siehe Geminn 2016: S. 601 ff.

[90] EDRi 2012.

Funktionieren und Überleben ein hohes Maß an informationeller Selbstbestimmung und an Privatheit als Bedingung voraus. Datenschutz wird nicht nur als individuelles Recht gesehen, sondern auch als gesellschaftlicher Wert wahrgenommen.[91] Die Datenschutz-Grundverordnung soll beides gewährleisten.

Datenschutzaktivisten versuchen daher auf die Gesetzgebung einzuwirken sowie die Bevölkerung in Bezug auf datenschutzrechtliche Themen und Probleme zu sensibilisieren. Die Aktivisten orientieren sich dabei an Werten wie Freiheit, Transparenz und Rechtsstaatlichkeit. Zu ihren Praktiken zählen unter anderem öffentliche Stellungnahmen oder die Veröffentlichung von Leaks. Durch den Zusammenschluss von Interessengemeinschaften, Vereinen oder sonstigen Organisationen können sich Aktivisten mobilisieren und auf diese Weise ihre Rechtsposition erheblich verbessern sowie politischen Druck erzeugen. Bürger können sich diesen Bündnissen anschließen oder diese in Form von Spenden oder Unterschriften unterstützen. Es gibt zahlreiche Zusammenschlüsse, die sich international für den Datenschutz einsetzen und versucht haben, bei den Verhandlungen um die Datenschutz-Grundverordnung Einfluss zu nehmen. Beispielhaft hierfür sind der Chaos Computer Club e.V. (CCC), Digitalcourage e.V., die Digitale Gesellschaft e.V., Privacy International, Article 19, Initiative für Netzfreiheit oder European Digital Rights. Während des Verhandlungsprozesses wurden insbesondere Forderungen nach einem starken Datenschutz, einer europäischen Harmonisierung und einheitlicher Durchsetzbarkeit des Datenschutzrechts sowie mehr Transparenz politischer Aushandlungsprozesse laut.

Gleichzeitig versuchten die Datenschutzaktivisten immer wieder durch öffentliche Stellungnahmen oder die Veröffentlichung von Leaks Einfluss auf den Verhandlungsprozess zu nehmen. Eine besonders tragende Rolle nahm die Plattform Lobbyplag ein. Sie verfolgte den Gesetzgebungsprozess von Anfang an und veröffentlichte immer wieder interne Dokumente, die die Einflussnahme von Interessengruppen und insbesondere Wirtschaftsunternehmen auf die Verhandlungen transparent machen sollten. Diese Leaks bekamen vor allem durch die mediale Berichterstattung Aufmerksamkeit in der breiten Öffentlichkeit.[92]

---

91 Vgl. etwa Digitalcourage e.V. o. J., Privacy International o. J. a oder EDRi o. J.

92 Lischka/Stöcker 2013.

Auf internationaler Ebene ist Privacy International ein wichtiger datenschutzrechtlicher Akteur, der es sich zur Aufgabe gemacht hat, für die Privatheit zu kämpfen, sich für ihren Schutz einzusetzen und internationale Überwachungstätigkeiten aufzudecken. Der Verbund von Menschenrechtsanwälten aus zwanzig Ländern versteht sich als globale Bewegung. Dabei schützen sie das Recht auf Privatheit, indem sie ihre Expertise bei lokalen, regionalen sowie internationalen Debatten einbringen.[93] Von der Datenschutz-Grundverordnung ist die Menschenrechtsbewegung eher enttäuscht, da sie dem technischen Fortschritt der digitalen Welt nicht gerecht werde. Insbesondere seien technische Problemfelder wie „privacy by design" oder die Profilbildung nicht genug berücksichtigt worden.[94]

„If the purpose of this reform was to strengthen people's control over their personal information and improve enforcement, our governments have achieved the exact opposite. The Council revisions to the draft data protection Regulations have done their best to disembowel some of the fundamental principles and further disempower individuals and their representatives by weakening rights. Moreover, any notion of harmonised, predictable rules across the Union have gone out of the window; in over a quarter of all the articles of this Regulation individual governments can develop their own rules." (Anne Fielder, Vorstandsvorsitzende Privacy International)[95]

Auf deutscher Ebene gehört der CCC als größte europäische Hackervereinigung zu den stärksten Datenschutzaktivisten. Sie engagieren sich als Vermittler in Spannungsfeldern, die sich aus technischen und sozialen Entwicklungen ergeben.[96] Sie möchten insbesondere auf Datenschutzproblemfelder und die Datensammelpraktiken von Großkonzernen aufmerksam machen.[97] So forderten sie etwa zu Beginn der Verhandlungen um die Datenschutz-Grundverordnung zusammen mit anderen Datenschutzaktivisten in einem offenen Brief an den damaligen Bundesminister des Innern, Hans-Peter Friedrich, harmonisierte und auch durchsetzbare Datenschutzregeln für die gesamte Europäische Union.[98]

---

93 Privacy International o. J. b.

94 Privacy International 2015.

95 Privacy International 2015.

96 Chaos Computer Club e.V. o. J.

97 Kloiber/Welchering 2016.

98 Chaos Computer Club e.V./Digitalcourage e.V./Digitale Gesellschaft e.V./Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung 2013.

Ein weiteres Beispiel für einen solchen Zusammenschluss ist die Online-Plattform „netzpolitik.org“. Sie engagiert sich für digitale Freiheitsrechte und ihre politische Umsetzung. Dabei thematisiert sie Fragen der Politik, des Internets und der Gesellschaft und möchte dabei aufzeigen, wie die Politik mit Regularien das Internet verändert. Ferner bietet das Portal seinen Lesern Lösungen an, wie sie sich eigenständig für die digitale Freiheit einsetzen können.[99]

Neben Bürgerinitiativen oder Aktivistengruppen können auch die Aktivitäten von Einzelpersonen als Teil der politischen Aktivisten eine enorme Ausstrahlwirkung im Bereich des Datenschutzrechts haben. Ein populäres Beispiel aus den Medien ist der Rechtsstreit[100] des österreichischen Juristen Maximilian Schrems gegen die irische Datenschutzbehörde, der bekannt wurde als Schrems vs. Facebook. Dieser führte dazu, dass der Europäische Gerichtshof das sogenannte „Safe Harbor-Abkommen“ mit den USA für ungültig erklärte. Zunächst klagte Schrems in Österreich, um zu erreichen, dass Facebook Inc. sich an das europäische Datenschutzrecht hält. Nach den Enthüllungen von Edward Snowden entschied er sich gegen die Tochtergesellschaft von Facebook, „Facebook Ireland Ltd.“, gerichtlich vorzugehen, da diese für alle Facebook-Nutzerkonten außerhalb der USA zuständig ist.[101] Hinter Schrems stand unter anderem der von ihm gegründete Verein „europe-v-facebook.org“, der ihn mit Spenden unterstützte.

„It is good to see that this case was won overall, but one needs to remember that this legal fight over two years and up to the highest court in Europe was only to get the Irish DPC to simply open an investigation. It will be very interesting to see if they now also take action, or if they will again find reasons to not do their job in providing protection to users of Irish services. Given my experience I doubt that what is today mainly a 'tech business protection authority' will wake up tomorrow and turn into real 'data protection authority' – but I guess we'll see soon." (Maximilian Schrems, österreichischer Jurist und Datenschutzaktivist)[102]

Der Einfluss von politischen Aktivisten und die Verbreitung von Leaks kann somit zu weitreichenden Folgen für die gesamte Internetwirtschaft führen. Auch die Aufdeckungen von Edward Snowden machen diesen Ef-

99 Netzpolitik.org o. J.
100 EuGH, Urt. v. 06.10.2015, Az. C-362/14, ECLI:EU:C:2015:650.
101 Europe-v-facebook.org 2016.
102 Europe-v-facebook.org 2016.

fekt deutlich. So ist der Artikel 48 der Datenschutz-Grundverordnung, der die Vollstreckbarkeit und Anerkennung von Gerichts- und Verwaltungsbehördenentscheidungen von Drittländern behandelt, auf seine Enthüllungen zurückzuführen.

2.3.2 Datenschutzbehörden

Datenschutzbehörden existieren sowohl auf europäischer (Europäischer Datenschutzbeauftragter) als auch auf nationaler Ebene (nationale Datenschutzbehörden). Die Behörden sind für die Einhaltung des geltenden Datenschutzrechts sowie bei Datenschutzrechtsverstößen für eine entsprechende Sanktionierung zuständig und laut Gesetz unabhängige Institutionen. Die Aufsichtsfunktion umfasst den Schutz der Datensubjekte vor unrechtmäßigen Zugriffen sowohl durch den Staat als auch durch Unternehmen. Die Behörden setzen Datenschutz mit Hilfe der Datenschutzgesetze und der Gerichte durch. Der Begriff der Privatheit ist dem deutschen Recht jedoch weitgehend fremd. Um Privatheit dennoch schützen zu können, muss der Begriff zuerst in die Sprache des Rechts transformiert werden. Der Schutz erfolgt deshalb aus einem Rückgriff auf verschiedene Grundrechte, im Kontext von Datenverarbeitung insbesondere auf das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts.

Die institutionelle Anbindung der Datenschutzbehörden ermöglichte es ihnen, sich in den Verhandlungen um die Datenschutz-Grundverordnung Gehör zu verschaffen, schränkte aber gleichzeitig auch ihren Handlungsspielraum ein, indem es sie an institutionelle Routinen bindet. Vielfach mahnten die Datenschutzbehörden, die gesetzliche Durchsetzbarkeit von Gesetzen auch zu gewährleisten und die Behörden mit entsprechenden Ressourcen auszustatten, da Gesetze sonst wirkungslos blieben.[103] Gleichwohl existieren hinsichtlich der inhaltlichen Ausrichtung zwischen den einzelnen Datenschutzbehörden große Unterschiede. Während die irische Datenschutzbehörde regelmäßig mit dem Vorwurf konfrontiert wird, sehr wirtschaftsfreundlich zu agieren, gelten deutsche Datenschutzbehörden als weitaus datenschutzfreundlicher, wenngleich auch hier regionale Unterschiede bestehen.

[103] Büschemann 2015.

Auf europäischer Ebene fungiert der Europäische Datenschutzbeauftragte als unabhängige Kontrollbehörde und überwacht das Datenschutzsystem.[104] Er ähnelt den nationalen Datenschutzbeauftragten innerhalb der Mitgliedstaaten. Nach Art. 1 Abs. 1 HS 1 der EG-Verordnung Nr. 45/2001[105], müssen die Organe und Einrichtungen der Europäischen Gemeinschaft den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleisten. Der Europäische Datenschutzbeauftragte kontrolliert und überwacht gemäß Art. 1 Abs. 2 der Verordnung 45/2001, ob alle Verarbeitungen durch die Organe und Einrichtungen der Union dieser Verpflichtung nachkommen. Der bis zum Jahr 2014 amtierende Europäische Datenschutzbeauftragte Peter Hustinx bemängelte den Ausschluss von Polizei und gesetzlichen Autoritäten im Kommissionsentwurf zur Datenschutz-Grundverordnung, sprach sich aber auch dafür aus, mehr nationale Spielräume einzubauen.[106] Sein Nachfolger Giovanni Buttarelli kritisierte wiederum die Detailverliebtheit der drei Entwurfsversionen von EU-Kommission, Rat und Europäischem Parlament.[107] Sie seien nicht flexibel genug, um auf den künftigen technischen Wandel reagieren zu können.

Jede europäische Institution beschäftigt einen Datenschutzbeauftragten der Europäischen Kommission. Ihre Aufgabe ist es, sicherzustellen, dass die Verordnung innerhalb der Europäischen Union zur Anwendung kommt. Dabei handeln sie in enger Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten. Darüber hinaus bestellt jedes Organ und jede Einrichtung der Gemeinschaft gemäß Art. 24 Abs. 1 S. 1 der Verordnung 45/2001 mindestens eine Person als behördlichen Datenschutzbeauftragten für personenbezogene Daten.

---

104 Zweiter Erwägungsgrund der Verordnung Nr. 45/2001 des Europäischen Parlaments und des Rates vom
18.12.2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe
und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, Amtsblatt L 8/1 vom 12.01.2001.

105 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates v. 18.12.2000 zum Schutz natürlicher Personen bei der verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, L 8/1; im Folgenden mit Verordnung 45/2001 abgekürzt.

106 Fox 2012.

107 Stupp 2015.

Während der Europäische Datenschutzbeauftragte auf europäischer Ebene agiert, beschäftigt jeder Mitgliedstaat der Europäischen Union einen nationalen Datenschutzbeauftragten. Für Deutschland ist dies derzeit die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, die auf Vorschlag der Bundesregierung vom Deutschen Bundestag gewählt wurde. Sie ist für jegliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen des Bundes sowie im Bereich der Privatwirtschaft für Telekommunikations- und Postunternehmen zuständig.[108] Seit dem Jahr 2016 untersteht ihre Behörde nicht mehr dem Bundesinnenministerium; sie ist seither unabhängig und nur noch gegenüber dem Parlament verantwortlich.[109] Innerhalb Deutschlands hat jedes Bundesland einen Landesbeauftragten für den Datenschutz bzw. den sog. Datenschutzbeauftragten. Zu seinen Aufgaben gehört das Beraten und Überprüfen aller öffentlichen Stellen des Landes (z. B. Industrie- und Handelskammern, Behörden, Gemeinden oder Hochschulen) im Bereich des Datenschutzes. In den meisten Bundesländern ist er zugleich die zuständige Aufsichtsbehörde für nicht-öffentliche Stellen (z. B. Parteien, Vereine oder Wirtschaftsunternehmen). Sofern Privatpersonen Fragen im Bereich des Datenschutzes haben, können sie sich von ihm oder der entsprechenden Aufsichtsbehörde kostenlos beraten lassen.[110]

„Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der Datenschutz-Grundverordnung an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. (...) Jede Verarbeitung scheinbar 'belangloser' Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je." (Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder)[111]

Die unabhängigen Datenschutzbehörden des Bundes und der Länder bilden als Zusammenschluss die sogenannte Datenschutzkonferenz. Zu den Mitgliedern gehören die Bundesbeauftragte für den Datenschutz, die Beauftrag-

[108] Datenschutzbeauftragter INFO 2014.
[109] Krempl 2016.
[110] Datenschutzbeauftragter INFO 2014.
[111] Landesbeauftragte für den Datenschutz Bremen 2012.

ten für den Datenschutz der Länder und der Präsident des Bayerischen Landesamtes für Datenschutz. Die Ziele des Zusammenschlusses sind die Wahrung und der Schutz der relevanten Grundrechte sowie das Erreichen einer einheitlichen Anwendung des Datenschutzrechts innerhalb Deutschlands.[112] Aus diesem Grund hat die Datenschutzkonferenz von Beginn an die Datenschutzreform um die Datenschutz-Grundverordnung mit dem Ziel unterstützt, einen modernen und stabilen Datenschutzrechtsrahmen für die Europäische Union bereitzustellen, ohne aber das derzeit herrschende Datenschutzniveau zu unterbieten.[113] Dabei kritisierte sie besonders das Fehlen spezifischer Anforderungen zur Profilbildung oder der Videoüberwachung und mahnte bei den Verhandlungen, die Autonomie des Einzelnen, die Transparenz und Zweckbindung bei der Datenverarbeitung sowie die Verantwortlichkeit der/des Datenverarbeitenden nicht außer Acht zu lassen.

2.3.3 Verbraucherschützer

„Der Datenschutz ist vor allem durch die digitale Entwicklung zu einem immer wesentlicheren Teil des Verbraucherschutzes geworden. Eine Modernisierung ist dringend notwendig, um den Schutz der persönlichen Daten und die Privatsphäre der Verbraucher auch in Zukunft zu gewährleisten und gleichzeitig die Rechtssicherheit und Wettbewerbsfähigkeit der europäischen Unternehmen zu stärken." (Verbraucherzentrale Bundesverband e.V.)[114]

Das Anliegen der Verbraucherschützer ist es den Datenschutz zu stärken, um es den Verbrauchern zu ermöglichen, ihre Rechte besser zu wahren und um Wettbewerbsgleichheit zwischen den unterschiedlichen Akteuren auf dem Markt zu erreichen.

Sie vertreten die Interessen der Verbraucher gegenüber Unternehmen und versuchen Chancengleichheit zwischen diesen herzustellen. Während der Verhandlungen veröffentlichten sie immer wieder Stellungnahmen und Kommentare.[115]

Die Verbraucher sollen die Kontrolle über ihre Daten zurückgewinnen und ihre Autonomie gegenüber den Unternehmen behaupten. Im Zentrum steht das Individuum, dessen individuelle Privatheit es zu schützen gilt.

---

112 Dankert 2016.
113 Hessischer Datenschutzbeauftragter 2015.
114 vzbv 2012.
115 Vgl. etwa vzbv o. J. oder BEUC o. J.

„In der digitalen Welt hinterlassen Verbraucher viele Daten. Wenn Unternehmen Daten kombinieren, entstehen umfassende Persönlichkeitsprofile. Die Profile sind für die Wirtschaft wertvoll, können für Verbraucher aber böse Nebenwirkungen haben. Dazu gehören unter anderem unerwünschte Werbung, höhere Versicherungsprämien, Nachteile bei der Wohnungssuche oder eine eingeschränkte Kreditfähigkeit." (Verbraucherzentrale Bundesverband e.V.)[116]

Innerhalb Deutschlands bündelt der gemeinnützige Verbraucherzentrale Bundesverband e.V. (vzbv) als Dachverband 16 Verbraucherzentralen der Länder und 25 verbraucherpolitische Verbände. Er klagt Verbraucherrechte vor Gericht ein und ist formell lediglich den Verbrauchern verpflichtet. Dabei fungiert er als eine Art Marktwächter, indem er Verbraucherprobleme aufzeigt, Lösungen anbietet und sich für deren Umsetzung einsetzt. Indem der Bundesverband für starke Verbraucherrechte kämpft, sollen auf fairen Märkten unbedenkliche Produkte und Dienstleistungen angeboten werden. Seine Arbeit zielt auf klare Verbraucherinformationen, verlässliche und praktisch durchsetzbare Rechte sowie auf den Schutz der Verbraucher vor Übervorteilung durch Unternehmen ab. Aufgrund des digitalen Wandels setzt sich der Verband darüber hinaus vermehrt für diejenigen Verbraucherrechte ein, die durch die Digitalisierung immer mehr an Bedeutung gewinnen. So möchte er dazu beitragen, dass sich neue technische Innovationen im rechtlichen Rahmen bewegen, ohne dass Verbraucherrechte missachtet oder Innovationen gehemmt werden. Zu den häufigsten Klagegründen des Verbraucherzentrale Bundesverbands gehören Datenschutzverstöße in allgemeinen Geschäftsbedingungen.[117]

„Technischer Fortschritt und gesetzliche Regelungen müssen in der digitalen Welt miteinander Schritt halten und weiter -entwickelt werden." (Jutta Gurkmann, Leiterin Geschäftsbereich Verbraucherpolitik der vzbv)[118]

Auf staatlicher Ebene ist das Bundesministerium der Justiz und für Verbraucherschutz innerhalb der Bundesregierung für den Bereich der Verbraucherpolitik zuständig.

---

116 vzbz 2014.
117 vzbz 2017.
118 vzbz 2017.

2.3.4 Artikel 29-Datenschutzgruppe

Die „Article 29 Working Party", die auch als „Artikel 29-Datenschutzgruppe" bezeichnet wird, wurde im Rahmen der Datenschutzrichtlinie[119] eingerichtet. Sie ist im Bereich des Datenschutzes das wichtigste Beratungsgremium der EU-Kommission bei der Zusammenarbeit mit den Mitgliedstaaten der Europäischen Union. Sie handelt in einer unabhängigen Beratungsfunktion und besteht aus einem Vertreter der Kontrollstelle/n, die von jedem EU-Mitgliedstaat eingerichtet wird/werden, einem Vertreter der Behörde/n, die für die EU-Institutionen und EU-Organe geschaffen wird/werden und einem Vertreter der Europäischen Kommission. Innerhalb der Gruppe treffen die Datenschutzaufsichtsbehörden aller Mitgliedstaaten der Europäischen Union einen Konsens bezüglich verschiedener Datenschutzfragen und beraten dahingehend die EU-Kommission.[120] Darüber hinaus hat die Arbeitsgruppe Expertenmeinungen bezüglich Fragen des Datenschutzes auf der Ebene der Mitgliedstaaten für die EU-Kommission bereitzustellen und eine einheitliche Auslegung der Datenschutzrichtlinie innerhalb aller europäischer Mitgliedstaaten sowie Norwegen, Liechtenstein und Island zu fördern. Ziel der Gruppe ist es, eine Harmonisierung des Datenschutzes innerhalb der Europäischen Union herbeizuführen.[121]

Während der Verhandlungen zur Datenschutz-Grundverordnung versuchte die Arbeitsgruppe durch Veröffentlichung von Dokumenten und Einschätzungen stets dazu beizutragen, dass ein hohes Datenschutzniveau innerhalb der Europäischen Union sichergestellt wird. Gleich zu Beginn der Verhandlungen veröffentlichte die Arbeitsgruppe im Jahr 2012 eine detaillierte Stellungnahme[122] zu dem Entwurf der Datenschutz-Grundverordnung. Dabei legte sie besonderen Wert auf die Pseudonymisierung, den Schutz und die Stärkung der Rechte Betroffener, die Stärkung der Position der Aufsichtsbehörden sowie auf eine umfassende und aufgrund der technischen Möglichkeiten (z. B. technische Identifizierungsmöglichkeiten wie IP-Adressen) angemessene Definition des Begriffs „personenbezogene Daten".[123] Auch

[119] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281/31.

[120] BfDI o. J. b.

[121] BfDI o. J. b.

[122] Artikel 29-Datenschutzgruppe 2012.

[123] Artikel 29-Datenschutzgruppe 2015 b.

wenn die Gruppe grundsätzlich eine positive Haltung gegenüber dem Vorhaben einnahm und besonders Aspekte wie das Recht auf Vergessenwerden, die Datenminimierung und die Vorschriften für die Verarbeitung von personenbezogenen Daten von Kindern lobte, hatte diese auch viele Kritikpunkte. So waren ihr einige Ausführungen der Verordnung nicht präzise genug. Sie betonte in diesem Zusammenhang die Wichtigkeit des Begriffs der „Einwilligung" und verbesserter Schutzmechanismen für die Betroffenen. Auch bei den Trilog-Verhandlungen nahm die Artikel 29-Datenschutzgruppe ihre Beratungsaufgaben wahr. So wünschte sie sich klare, einfache und effektive Lösungen, die zum einen den Betroffenen einen hohen Schutz ihrer Daten ermöglichen, aber zum anderen auch die Unternehmen nicht im Wettbewerb und im Kampf um Innovationen hemmen. Damit die Verordnung in den Mitgliedstaaten besser und einfacher implementiert werden kann, möchte die Arbeitsgruppe einen Aktionsplan als Richtwert zur Implementierung der Datenschutz-Grundverordnung entwickeln.[124]

Im Zuge des Geltungsbeginns der Datenschutz-Grundverordnung wird die Datenschutzrichtlinie zum 25. Mai 2018 aufgehoben und die Artikel 29-Datenschutzgruppe durch den Europäischen Datenschutzausschuss ersetzt.[125] Der Europäische Datenschutzausschuss wird als Einrichtung der Union mit eigener Rechtspersönlichkeit handeln. Er wird durch einen Vorsitz vertreten und besteht aus dem Leiter einer oder mehrerer Aufsichtsbehörde/n jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten. Die EU-Kommission ist berechtigt ohne Stimmrecht an den Tätigkeiten und Sitzungen des Ausschusses teilzunehmen und ist von diesem stets über seine Tätigkeiten zu informieren. Die Aufgaben des Ausschusses umfassen beispielsweise:

- Überwachung und Sicherstellung einer ordnungsgemäßen Anwendung der Datenschutz-Grundverordnung
- Beratung der EU-Kommission bei allen Fragen bezüglich des Schutzes personenbezogener Daten

124 Artikel 29-Datenschutzgruppe 2015 a.

125 Erwägungsgrund 139 der Verordnung 2016/679 des Europäischen Parlaments und des Rates v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1.

- Bereitstellen von Leitlinien, Empfehlungen und bewährten Verfahren zur Löschung von Links zu personenbezogenen Daten oder Kopien dieser Daten sowie zur näheren Bestimmung der Kriterien und Bedingungen für die Übermittlung personenbezogener Daten
- Förderung der Ausarbeitung von Verhaltensregeln und der Einrichtung von datenschutzspezifischen Zertifizierungsverfahren sowie Datenschutzsiegeln und Datenschutzprüfzeichen

2.4 Die Welt der Digitalwirtschaft

„Noch vor Straßenbau und noch vor Schienenwegebau ist nichts so sinnvoll wie die Modernisierung der Energie- und der ICT-Infrastruktur (Anm. d. Verf.: information and communication technology)." (Günther Oettinger, EU-Kommissar für die digitale Wirtschaft und Gesellschaft)[126]

Die Welt der Digitalwirtschaft betreibt Geschäftsmodelle, die auf den Umgang mit Daten angewiesen sind. Dies umfasst sowohl Unternehmen, deren Kerngeschäft auf dem Sammeln oder der Verarbeitung von Daten basiert, wie etwa Google Inc. und Facebook Inc., als auch Unternehmen, die täglich eine große Menge an Daten verarbeiten, um einen reibungslosen Geschäftsvorgang zu gewährleisten, deren Kerntätigkeiten jedoch nicht datengetrieben sind. Das gilt beispielsweise für Unternehmen der Finanzbranche und des Gesundheitswesens. Je nach Geschäftsmodell ergeben sich hierdurch unterschiedliche Interessen an Daten und Datenschutz. Während Datenschutz für datenbasierte Geschäftsmodelle häufig als hinderlich wahrgenommen wird, kann es für Bereiche wie die Telekommunikationsbranche oder den Finanzsektor essentiell sein ein hohes Datenschutzniveau einzuhalten, um das Vertrauen der Kunden nicht zu verlieren. Zudem mag es im Interesse der Unternehmen sein, das Gut „Daten" zu schützen, um die eigenen Geschäftsgeheimnisse zu bewahren. Dabei unterscheiden sich Unternehmensinteressen und -ziele nicht nur aufgrund unterschiedlicher Geschäftsmodelle, sondern häufig auch aufgrund der Unternehmensgröße oder des jeweiligen Standortes. Gemein ist jedoch allen, dass Datenschutz insbesondere dann eine Rolle spielt, wenn er den übergeordneten Geschäftsinteressen dient. In den Verhandlungen propagierten viele Vertreter der Welt der Digitalwirtschaft immer wieder die zukunftsweisenden Verhei-

[126] n-tv 2014.

ßungen digitaler Technologien für die Wirtschaft.[127] Zugleich wurden Selbstregulierungsmaßnahmen, sei es auf Seiten der Unternehmen in Form von Selbstverpflichtungen oder auf Seiten der Verbraucher, im Sinne von Selbstdatenschutz propagiert. Ebenso wurden ein Glaube an Technik und deren gesellschaftlichen Mehrwert sowie die Freiheit des Internets und die Autonomie des Individuums als Werte hervorgehoben.

Der Wirtschaftszweig der Digitalwirtschaft ist gekennzeichnet durch permanente Veränderungen und durch zahlreiche Neuerungen. Großkonzerne wie Amazon.com, Inc. oder Facebook Inc. müssen sich besonders aus rechtlicher Sicht regelmäßig neuen Herausforderungen und Veränderungen stellen. Zudem unterscheiden sich Unternehmensinteressen und -ziele häufig aufgrund der Unternehmensgröße oder des jeweiligen Standortes. Unterschiede ergeben sich dabei hinsichtlich:

- Europäischer Unternehmen
- Deutscher Unternehmen
- US-Unternehmen

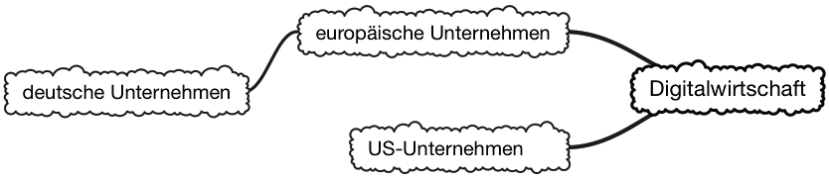

Abbildung 5: Die Welt der Digitalwirtschaft

2.4.1 Europäische Unternehmen

„Europe needs a data protection regulation that allows it to embrace the data-driven innovations that are helping transform the economy, while at the same time granting enough protection to personal data to ensure that citizens trust the technologies." (DigitalEurope)[128]

Im globalen Wettbewerb nimmt die Europäische Union in der Digitalwirtschaft eine vergleichsweise untergeordnete Rolle ein. Europäische Unter-

[127] Vgl. etwa Bitkom 2015 oder DigitalEurope 2014.
[128] DigitalEurope 2015.

nehmen der Informations-, Kommunikations-, Software- und Internetbranche bleiben in einigen Bereichen deutlich hinter Firmen aus den USA oder China zurück. Dies führt zu einer gewissen Abhängigkeit Europas in diesen Bereichen. Um im internationalen Vergleich bestehen zu können und eine größere Unabhängigkeit herbeizuführen, fordern Vertreter aus der Wirtschaft in erster Linie seitens der Politik eine deutliche Stärkung des Handels im digitalen Bereich. Europäische Unternehmen verlangen den Abbau von Kosten durch zu viel Bürokratie, die Förderung von Innovationsmöglichkeiten und die Wahrnehmung von Chancen durch Big Data.[129]

„Big Data relies on the collection and processing of large amounts of data. While not all of this data will be personal data, we acknowledge that personal data will play an important role in Big Data applications. Therefore the take-up and success of Big Data will depend heavily on the EU's future Data Protection Regulation, which is currently being negotiated." (Digital Europe)[130]

Datenschutz wird durch europäische Unternehmen deshalb sehr zwiegespalten wahrgenommen. Einerseits erhoffen sie sich durch ein gewisses Datenschutzniveau das Kundenvertrauen zu stärken und potentielle Wettbewerbsvorteile gegenüber außereuropäischen Unternehmen zu gewinnen. Andererseits werden immer wieder Stimmen laut, die ein zu hohes Datenschutzniveau als Bedrohung für Innovation und Wachstum betrachten. Um entgegen solcher Befürchtungen im internationalen Wettbewerb bestehen zu können, sei eine Kombination aus Risikokapital, internationalem Talent, der Wissenschaft sowie politischer Unterstützung zielführend, welche ganz dem großen amerikanischen Vorbild des Silicon Valley entnommen werden könne.[131] Dass ein solches Vorhaben möglich ist, werde am Beispiel des Unternehmens Airbus deutlich. Im Jahr 1965 entschieden sich Deutschland, Frankreich und Großbritannien zur gemeinsamen Entwicklung eines Passagierflugzeuges. Fünf Jahre später gründeten sie die Firma Airbus Industries.[132] Im Laufe der Zeit ist das Unternehmen zum direkten Konkurrenten des amerikanischen Konzerns „The Boeing Company" aufgestiegen und gilt seither als Paradebeispiel einer gelungenen europäischen Zusammenarbeit.

129 DigitalEurope 2014.
130 DigitalEurope 2014.
131 Scherzer 2014.
132 Austrian Wings 2008.

Ziel der Europäischen Union ist es, dem Beispiel von Airbus als Vorreiter einer europäischen Zusammenarbeit zu folgen und auch in der Digitalwirtschaft konkurrenzfähige IT-Unternehmen zu etablieren, die im globalen Wettbewerb mithalten können und die Europäische Union bei der Technologieführerschaft weiter vorantreiben. Auf diese Weise soll ein europäisches Gegengewicht geschaffen werden, das der Übermacht amerikanischer Konzerne entgegenwirkt. Besonders im Zuge der NSA-Affäre wurde der Wunsch nach europäischen IT-Großkonzernen und nach europäischen Alternativen wieder aktuell.

„Was wollen wir in Europa können? So, wie wir einmal entschieden haben, dass wir Airbus als eine Alternative zu Boeing aufbauen, und so, wie wir seit Jahren – nicht immer besonders schnell – daran arbeiten, ein Alternativsystem zu GPS namens Galileo aufzubauen, so wird sich auch die Frage stellen, welche technologischen Fähigkeiten wir im Internetbereich, in der Sicherheitstechnik, die dazu gehört, und im Bereich all der Hardware-Komponenten in Europa eigentlich noch haben wollen. Ansonsten kommen wir in Abhängigkeiten, die dann auch dazu führen, dass wir bestimmte Systeme gar nicht mehr bis ins Tiefste hinein durchschauen. Ich glaube, ein Kontinent wie Europa sollte diesen Anspruch haben, und die europäische Gemeinsamkeit könnte uns dabei auch helfen." (Angela Merkel)[133]

Der internationale Erfolg des Airbus-Konzerns ist primär dem politischen Willen der europäischen Länder geschuldet. Damit diesem Beispiel auch in der Digitalwirtschaft gefolgt werden kann, fordern Stimmen aus der Politik und der europäischen Wirtschaft den Aufbau von IT-Unternehmen in der Europäischen Union gezielt zu fördern und die rechtlichen Rahmenbedingungen dahingehend zu stärken sowie zu vereinfachen. Für die Europäische Union würden entsprechende wirtschaftspolitische Maßnahmen erfolgreich sein, sofern im digitalen Bereich ein regulatorischer Rahmen für die Europäische Union beschlossen wird. Hierbei müssten besonders Freiräume geschaffen werden, die Innovationen und Wachstum ermöglichen sowie die Kreativität fördern, zugleich aber auch entsprechende Wettbewerbsbedingungen schaffen.[134]

„Wenn die Politik das gleiche Engagement, das sie in der Automobilbranche zeigt, in der IT-Sicherheitsbranche entwickeln würde, dann wären wir erfolgreicher. Aber da muss sich Europa an die eigene Nase fassen. Warum machen wir es Start-ups in

133 Washietl 2014.

134 Bundesministerium für Wirtschaft und Energie, Industrie 4.0 und Digitale Wirtschaft.

Europa so schwer, an Kapital zu kommen? Wir investieren große Summen in Forschung und Entwicklung, aber dann machen wir nicht den nächsten Schritt, daraus erfolgreiche Unternehmen zu machen." (Udo Helmbrecht, Leiter der europäischen Agentur für Netz- und Informationssicherheit)[135]

2.4.2 Deutsche Unternehmen

„Eine EU-weite Datenschutz-Grundverordnung (EU-DSGVO) bietet die große Chance, das Datenschutzrecht in Europa umfassend zu modernisieren und zu harmonisieren und damit den europäischen Binnenmarkt zu stärken. Der BVMW begrüßt diese Bestrebungen. Der vorliegende Entwurf bedarf jedoch einer Mittelstandsklausel, damit der europäische Mittelstand im internationalen Wettbewerb bestehen kann. Die überwiegend mittelständisch geprägte Digitale Wirtschaft in Deutschland braucht eine verfügbare und leistungsfähige IT-Infrastruktur sowie eine nachhaltige Datenpolitik, um einen verantwortungsvollen Umgang mit Daten zu ermöglichen und global konkurrenzfähig zu sein." (Bundesverband mittelständische Wirtschaft)[136]

Deutschland bildet im internationalen Vergleich den fünftgrößten Markt in der Informations- und Kommunikationstechnologie-Branche – hinter den USA, China, Japan und Großbritannien.[137] Der rasante Fortschritt in diesem Bereich führt dazu, dass sich die Märkte und Marktstrukturen sehr schnell verändern und neue Marktführer die Digitalwirtschaft erobern. Ein Beispiel hierfür ist das Unternehmen Zalando SE. Der Online-Versandhändler ist, bezogen auf den Umsatz, bereits wenige Jahre nach seiner Gründung im Jahr 2008, zum drittgrößten Versandhändler Deutschlands aufgestiegen. Dabei sieht das Unternehmen in strengen Datenschutzvorschriften vor allem einen Wettbewerbsnachteil gegenüber US-Unternehmen.

„Bevor wir uns der Schaffung neuer Regularien zuwenden, sollten zunächst die bestehenden gesetzlichen Regelungen genutzt und im Einzelfall – wenn nötig – an die veränderten Gegebenheiten der digitalen Welt angepasst werden. Aus unserer Sicht bremst eine weitere Regulierung vor allem Innovationen in Deutschland und Europa, fördert damit Rechtsunsicherheit und Bürokratie für junge und unerfahrene Start-ups und schafft so letztlich Markteintrittsbarrieren." (Zalando SE)[138]

135 Visser 2013.
136 BVMW 2014.
137 BMWi 2015: S. 7.
138 Menz 2016.

Aufgrund der schnellen konzeptionellen aber auch rechtlichen Veränderungen wird sich die deutsche Digitalwirtschaft permanent neu justieren müssen. Insbesondere die in Deutschland besonders vertretenen kleinen und mittelständischen Unternehmen fürchten die im Zuge der Datenschutz-Grundverordnung auf sie zukommenden Änderungen und die aus den notwendigen Umstellungen resultierenden Kosten. Daher setzten sie sich während der Verhandlungen für weniger Bürokratisierung ein.[139]

„Das neue Datenschutzreglement soll keine unnötigen bürokratischen Hürden für Unternehmen schaffen, sondern die Wettbewerbsfähigkeit europäischer Unternehmen unterstützen. Deswegen brauchen wir gleiche Wettbewerbsbedingungen für eine starke europäische Wirtschaft sowie differenziertere Standards für kleine, mittelständische- und große Unternehmen." (Axel Voss, Mitglied und stellvertretender Vorsitzender des Rechtsausschusses des Europäischen Parlaments und Berichterstatter seiner Fraktion CDU/CSU für die Überarbeitung der EU-Datenschutzverordnung)[140]

Welche deutschen Unternehmen hiervon betroffen sind, zeigt sich beispielhaft an den Mitgliedern des Digitalverbands „Bitkom e.V.". Dieser setzt sich laut Selbstbeschreibung für eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein. Er vertritt mehr als 2400 Unternehmen der digitalen Wirtschaft, davon 1000 Mittelständler und mehr als 300 Start-ups. Hierzu gehören beispielsweise Amazon Deutschland, Deutsche Telekom AG, 1&1 Telecom GmbH oder Deutsche Bahn AG. Darüber hinaus gehören zu dem deutschen Verband auch global agierende Unternehme wie Apple GmbH, SAP SE, Toshiba Europe GmbH, Microsoft Deutschland GmbH oder Facebook Germany GmbH. So vereint der Verband in seinem Netzwerk zahlreiche Firmen im digitalen Bereich. Bitkom versuchte sich bei den Verhandlungen um die Datenschutz-Grundverordnung für eine klarere Ausgestaltung der Verantwortlichkeiten bei der Datenverarbeitung, eine neue Definition des Begriffs „pseudonymisierte Daten" und einen stärkeren Anreiz für den Umgang mit pseudonymisierten Daten innerhalb der Verordnung einzusetzen.[141] Zu der endgültigen Fassung der Verordnung äußerte sich Susanne Dehmel, Mitglied der Geschäftsleitung Vertrauen und Sicherheit Bitkom e.V., wie folgt:

---

139 BVMW 2014.

140 Mies 2015.

141 Bitkom 2014.

„Viele Regelungen der neuen Datenschutzverordnung sind so allgemein formuliert, dass nicht auf den ersten Blick klar ist, wie sie in der Praxis umgesetzt werden sollen. Das wird in der Anfangszeit zu einer gewissen Rechtsunsicherheit führen.“[142]

Noch strikter sieht dies der Bundesverband „Digitale Wirtschaft e.V.“, der die Interessen von Unternehmen der Digitalwirtschaft vertritt und dahingehend im ständigen Dialog mit der Öffentlichkeit und Politik steht. Diese Unternehmen stehen der Datenschutz-Grundverordnung kritisch gegenüber. So zeige die Verordnung, dass es an einem grundlegenden Verständnis der heutigen Informationsgesellschaft fehle und es keine Differenzierung und Risikoabstufung bei dem Umgang mit Daten gebe. Sichtbar werde dies an einer nicht ausreichend implementierten Pseudonymisierung und Verschlüsselung der Daten.[143]

2.4.3 US-Unternehmen

„Das Internet hat uns gehört. Unsere Firmen haben es gebaut, verbreitet und perfektioniert, so dass andere nicht mithalten können. Und hinter den intellektuellen Positionen der Kritiker steckt das Interesse, diesen kommerziellen Erfolg auszuhöhlen. Zur Verteidigung von Google und Facebook muss man sagen, dass die europäische Reaktion manchmal mehr wirtschaftsgetrieben ist als alles andere.“ (Barack Obama, US-Präsident von 2009 bis 2017)[144]

Die USA sind Heimat der bedeutendsten datenverarbeitenden Unternehmen der Welt. Insbesondere das kalifornische Silicon Valley gilt als Herz der Computer- und Softwareindustrie. Hier haben Firmen wie Facebook Inc., Hewlett Packard Inc., Apple Inc., Google Inc. und dessen Holding Alphabet Inc. und viele weitere ihren Sitz. Die amerikanischen Unternehmen prägen und dominieren die Digitalwirtschaft und nehmen eine überlegene Position auf dem digitalen Markt ein.

Nicht wenige dieser Unternehmen fokussieren sich auf datengetriebene Geschäftsmodelle. Sie sammeln, speichern und verkaufen personenbezogene Daten, indem sie sie zu einem handelbaren und kostbaren Gut erheben. Mittlerweile gelten personenbezogene Daten als „Rohstoff” des 21. Jahrhunderts. Durch die erfassten Datenmengen lassen sich einfach Nutzerpro-

142 Bitkom 2016.
143 BVDW 2016.
144 Schmiechen 2015.

file erstellen, die wiederum hinsichtlich der Wirtschaftsziele der Unternehmen analysiert und genutzt werden können.

Deutlich wird ein solches datenbasiertes Geschäftsmodell am Beispiel von Facebook Inc. Das Unternehmen betreibt mit seiner Plattform das erfolgreichste soziale Netzwerk weltweit. Dabei erhebt das Unternehmen aus verschiedenen Quellen und in erheblichem Umfang Daten von seinen Nutzern. Durch das systematische Erfassen dieser Daten erstellt es Nutzerprofile, die wiederum durch andere Unternehmen zu Werbezwecken verwertet werden können. Wenn sich die Nutzer auf der Internetplattform registrieren, willigen sie in diese Verwendung und Datenpraxis ein. Fraglich ist dabei jedoch, ob die Verwender sich über den Umfang ihrer Einwilligung und den Datengebrauch bewusst sind. Aufgrund von Facebooks Datenumgang und seiner marktbeherrschenden Stellung im Bereich der sozialen Medien, hat das Bundeskartellamt Anfang des Jahres 2016 ein Verfahren gegen den Konzern eingeleitet, und zwar sowohl gegen die irische als auch gegen die deutsche Niederlassung sowie gegen die US-amerikanische.[145] Dabei soll der Frage nachgegangen werden, ob Facebook durch die Ausgestaltung seiner Vertragsbestimmungen seine Marktstellung missbraucht und durch seine Nutzungsbedingungen gegen datenschutzrechtliche Vorschriften verstößt. Zusätzlich sammelt das Unternehmen mit der Hilfe des Messenger-Dienstes „WhatsApp" Nutzerdaten. So werden aufgrund der geänderten Datenschutzbestimmungen von WhatsApp künftig die bei dem Dienst erfassten Telefonnummern mit Facebook geteilt. Die Übernahme von WhatsApp durch Facebook wurde vor zwei Jahren durch die Kartellbehörden genehmigt, da zwischen den beiden Unternehmen kein Datenaustausch stattfinden sollte. Aufgrund des neuen Vorhabens des Konzerns ermittelte in dieser Angelegenheit auch die EU-Kommission gegen Facebook[146] und verhängte nach sechsmonatigen Verhandlungen eine Geldstrafe in Höhe von 110 Millionen Euro wegen falscher Angaben gegen das Unternehmen.[147]

„Marktbeherrschende Unternehmen unterliegen besonderen Pflichten. Dazu gehört es auch, angemessene Vertragsbedingungen zu verwenden, soweit diese marktrelevant sind. Für werbefinanzierte Internetdienste wie Facebook haben die Nutzerda-

145 Bundeskartellamt 2016.

146 Europäische Kommission 2016.

147 Europäische Kommission 2017.

ten eine herausragende Bedeutung. Gerade deshalb muss auch unter dem Gesichtspunkt des Missbrauchs von Marktmacht untersucht werden, ob die Verbraucher über die Art und den Umfang der Datenerhebung hinreichend aufgeklärt werden." (Andreas Mundt, Präsident des Bundeskartellamts)[148]

Amerikanische Unternehmen versuchten während der Verhandlung um die Datenschutz-Grundverordnung durch gezielte Lobbyarbeit das Datenschutzniveau zu schwächen und setzten sich für Selbstregulierungsmaßnahmen ein.[149] Sie fürchteten erhebliche Nachteile, wenn sie sich auf ein höheres Datenschutzniveau einstellen müssen, da ihre Geschäftsmodelle und Angebote zum Teil mit den Grundprinzipien des Datenschutzes kollidieren.

„Das Datensammeln ist ein lukrativer Wachstumsmarkt, auf dem strenge Regeln nur stören. Unternehmen aus den Vereinigten Staaten sind im Vorteil, weil es bei ihnen keinen Datenschutz gibt, der über einen eng gefassten Privatbereich hinausgeht. Sie dürfen Daten sammeln, so viel sie wollen und die Ausbeute als ihr Eigentum betrachten. In Europa verbietet das die Datenschutzrichtlinie aus dem Jahr 1995 – sie wird jedoch kaum umgesetzt." (Frankfurter Allgemeine Zeitung)[150]

2.5 Die Welt der Nachrichtenportale

Nachrichtenportale sind an der Herstellung von Öffentlichkeit beteiligt und berichteten regelmäßig über die Verhandlungen zur Datenschutz-Grundverordnung. Das Medien-Echo zur Datenschutz-Grundverordnung ist deshalb nicht nur nach ihrem Inkrafttreten enorm. Denn bereits während der Einigungsgespräche der EU-Organe zur Verordnung und nach der Veröffentlichung der finalen Version war das mediale Interesse an den Neuerungen des europäischen Datenschutzrechts groß. Die Nachrichtenportale bilden eine Art Schnittstelle zwischen den Bürgern und dem politischen Entscheidungsprozess und wirken als Vermittler. Sie informieren die Bevölkerung über die aktuellen Entwicklungen und die einzelnen Ergebnisse der Verhandlungsprozesse zur Datenschutz-Grundverordnung. Sie werden aber nicht nur durch professionelle Journalisten erbracht, sondern auch durch soziale Medien verbreitet. Gleichzeitig kann die mediale Berichterstattung sowohl eine kritische als auch eine positive Position einnehmen und so ihre Rezipienten beeinflussen. Diese Berichte können den Bürgern

148 Bundeskartellamt 2016.
149 Ebbinghaus/Schulz/Thiel 2014.
150 Ebbinghaus/Schulz/Thiel 2014.

wiederum als Informationsgrundlage dienen.[151] Darüber hinaus haben Nachrichtenportale aber auch selbst Einfluss auf die Debatte um die Grundverordnung nehmen können. So wurde beispielsweise durch die mediale Berichterstattung nach dem Ratsentwurf[152] der Europäischen Union der Eindruck vermittelt, dass die Verordnung den Grundsatz der Zweckbindung aufweichen wolle.[153] Indem Nachrichtenportale mobilisiert werden, kann eine rechtliche Debatte angestoßen und ein Gesetzgebungsverfahren vorangetrieben werden. Die Welt der Nachrichtenportale griff insbesondere die Leaks der Datenschutzaktivisten zu den Lobbyvorgängen während der Verhandlungen in ihrer Berichterstattung auf.

2.6 Die Welt der Wissenschaft

Die Wissenschaft spielt in der Debatte um Datenschutz allgemein und speziell um die Datenschutz-Grundverordnung vielfältige Rollen. Zum einen sind Teile der Wissenschaft, die in ihrer Forschungspraxis auf personenbezogenen Daten angewiesen sind, von der Datenschutz-Grundverordnung selbst betroffen. Zum anderen fällt der Wissenschaft die Rolle des kritisch-distanzierten Beobachters zu, der sich während der Verhandlungen mit den Wechselwirkungen von Privatheit, Technik und Gesellschaft auseinandersetzte. Schließlich formen die Wissenschaften durch technische Entwicklungen den Rahmen, in dem Datenverarbeitung stattfindet, mit. Die Welt der Wissenschaft wird so auf vielfältige Weise selbst zum Teil der Arena.

Die Rechtswissenschaft hat zunächst die Rolle eines Kommentators von Gesetzen und gerichtlichen Entscheidungen. Zudem ist sie mit der Bearbeitung bisher ungelöster Rechtsprobleme befasst. Ihre Erkenntnisse macht sie über zahlreiche Publikationsformen wie etwa Fachzeitschriften und Gesetzeskommentare der Öffentlichkeit zugänglich. Daneben berät die Rechtswissenschaft aber auch die Politik, Unternehmen, Verbände und andere Institutionen. Der Rechtswissenschaft kommt damit letztlich eine indirekt steuernde Funktion zu.

---

151 Vgl. etwa Berg/Kiefer 1996: 183.

152 Rat der Europäischen Union, 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), 2012/0011 (COD) v. 11.06.2015.

153 Roßnagel 2016; siehe hierzu genauer: Richter 2015: S. 735; Roßnagel/Nebel/Richter 2015: S. 455.

Die Informatik als mit der Verarbeitung von Informationen befasste Wissenschaft gibt softwareseitig den technischen Rahmen vor, in dem Datenverarbeitung stattfindet. Sie beeinflusst zusammen mit den technischen Wissenschaften und den Naturwissenschaften aber auch das Recht, denn nur technisch Mögliches kann vom Recht überhaupt gefordert werden. Zudem befinden sich Recht und Technik in einer Art ständigem Wettlauf, dessen Sieger nicht so leicht auszumachen ist: Einerseits geht der technische Fortschritt schneller voran, als seine rechtliche Regulierung; andererseits gibt das Recht den Rahmen für alle künftigen technischen Entwicklungen vor.

Wissenschaftliche Disziplinen wie etwa Soziologie, Ethik, Medien- und Politikwissenschaften oder Philosophie beobachten und bewerten die gesellschaftlichen Auswirkungen zunehmender Datenverarbeitung auf Individuen wie auf die Gesellschaft insgesamt. Es gibt zahlreiche Projekte, die sich mit den Folgen der Digitalisierung, dem Thema Privatheit und den Wechselwirkungen mit der Gesellschaft auseinandersetzen. Nicht zuletzt trägt das Projekt „Privacy-Arena", in dessen Rahmen die vorliegende Veröffentlichung entstanden ist, selbst dazu einen Beitrag bei. Die Grenzen zwischen passiver Beobachtung und aktiver Teilnahme am Diskurs sind dabei stets fließend. Anstatt eine allwissende Objektivität zu beanspruchen, kann das Projekt vielmehr selbst als Teil der Arena betrachtet werden, welches versucht seine Geschichte der Datenschutz-Grundverordnung zu erzählen.

2.7 Die Welt der Nutzer

In den datenschutzrechtlichen Debatten ist immer wieder die Rede von den Nutzern,[154] den Verbrauchern[155], den Bürgern[156] oder auch den Datensub-

[154] „Jenseits der eigentlichen datenschutzrechtlichen Regulierung muss jedoch auch das Problembewusstsein der Nutzer berücksichtigt werden, wenn Fragen des Wettbewerbsvorteils diskutiert werden sollen: Insbesondere die Enthüllungen von Edward Snowden zum systematischen Zugriff von Nachrichtendiensten auf Internetdienste und internetbasierte Kommunikation haben zu einem spürbaren Vertrauensverlust der Nutzer geführt.", Oetjen 2016: S. 6.

[155] „Wenn Grundprinzipien wie die Einwilligung und die Zweckbindung fallen würden, verlieren Verbraucherinnen und Verbraucher die Kontrolle über ihre eigenen Daten.", Müller 2015.

[156] „Eine starke Datenschutzverordnung würde Bürgerinnen und Bürger wieder ins Zentrum der Onlinewirtschaft rücken.", Digitale Gesellschaft e.V. 2013.

jekten[157]. Gemeint sind damit all jene Personen, deren Daten beispielsweise bei der Nutzung von Informations- und Kommunikationstechniken, sozialen Netzwerken oder bei der Wahrnehmung verschiedener Dienstleistungen des Alltags erhoben, verarbeitet und genutzt werden. Sie nehmen in der datenschutzrechtlichen Diskussion eine Art Doppelrolle ein. Sie fungieren einerseits als Subjekte, die mit Rechten ausgestattet sind oder sein sollten. Andererseits sind ihre Daten und die von ihnen hinterlassenen Datenspuren aber auch selbst Waren und werden gehandelt. Auch im Hinblick auf die Sicherheitsbehörden ergibt sich eine solche Zweiteilung. Einerseits sind die Nutzer von den Sicherheitsbehörden zu schützen. Andererseits gelten sie auch als potentielle Bedrohung, die nur durch vermehrte Kontrolle eingehegt werden kann. So fordern die einen, das Vertrauen der Nutzer oder Verbraucher, das aufgrund von Datenskandalen erschüttert wurde, zurückzugewinnen, um weiterhin Zugang zu ihren Daten zu erhalten. Andere wiederum distanzieren sich von so einem instrumentellen Zugriff und verstehen den Schutz der Bürger vor unrechtmäßigem Datenzugriff und Datenmissbrauch als notwendige Bedingung, um Demokratie zu gewährleisten oder die Autonomie der Individuen zu bewahren. Andererseits wird auch auf das ökonomische Potential der Datenverwertung hingewiesen sowie auf die Notwendigkeit, Zugang zu den Daten der Bürger zu haben, um staatliche Kontrollfunktionen ausüben zu können. Dabei kommen die Datensubjekte selten selbst zu Wort, vielmehr sind sie zumeist Gegenstand der Verhandlungen, derer sich verschiedene Parteien bedienen.

[157] „Eine Datenverarbeitung darf darüber hinaus auch beim Nachweis der Notwendigkeit für das Verfolgen 'legitimer Interessen' erfolgen, allerdings nur unter der Voraussetzung, dass dadurch nicht die Grundrechte des 'Datensubjekts' unterwandert werden.", Verein Für soziales Leben e.V. o. J.

3 Die Entwicklung der Verhandlungen im Zeitverlauf

Während der Verhandlungen rund um die Datenschutz-Grundverordnung bildeten sich verschiedene Konstellationen von Kompromissbildungen und Konfliktlinien zwischen den verschiedenen sozialen Welten sowie ihren Repräsentanten heraus. Manche dieser Verbindungen blieben konstant, andere veränderten sich im Zeitverlauf. Gelang es verschiedenen Welten ihre eigenen Interessen mit einem gemeinsamen Ziel zu verknüpfen, so entstanden Allianzen. Allianzen waren ein geeignetes Mittel, um die eigene Verhandlungsmacht in den Debatten zu stärken. Gleichzeitig gab es auch Konflikte, insbesondere dann, wenn sich die Interessen und alltäglichen Praktiken der Welten entgegenstanden.

Im Folgenden sollen die Allianzen und Konflikte sowie ihre Veränderungen im Zeitverlauf dargestellt werden.

- November 2010: Vorstellung eines neuen Gesamtkonzeptes für den Datenschutz in der Europäischen Union durch die EU-Kommission
- Januar 2012: Vorschlag der EU-Kommission für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung); Vorstellung durch Justizkommissarin Reding
- Oktober 2013: EU-Parlament legt eigenen, überarbeiteten Entwurf vor
- März 2014: EU-Parlament nimmt eigenen Entwurf an; Ablehnung durch den Europäischen Rat
- Juni 2015: Europäischer Rat legt eigenen Entwurf vor; Beginn des Trilogs
- Dezember 2015: Parlament und Rat einigen sich; Trilog endet
- Mai 2016: Veröffentlichung im Amtsblatt und Inkrafttreten
- Mai 2018: Geltungsbeginn der Datenschutz-Grundverordnung

3.1 Die Arena formiert sich

In der Anfangsphase der Verhandlungen kristallisierten sich die zwei zentralen Konfliktlinien in der Arena heraus – der Konflikt zwischen der Welt der Digitalwirtschaft und der Welt des Datenschutzes sowie der zwischen der Welt der Nationalstaaten und der Welt der Europäischen Union.

3.1.1 Die starke Rolle der Europäischen Kommission im Kommissionsentwurf stößt auf Widerstand

Viele Elemente des im Jahr 2012 veröffentlichten Kommissionsentwurfs sahen eine Stärkung der EU-Kommission in ihrer Funktion vor. Die Kommission übernimmt in der Europäischen Union Exekutivaufgaben und ähnelt daher der nationalstaatlichen Regierung. Sie ist entsprechend daran interessiert, ihre eigenen Kompetenzen zu erweitern. Dies versuchte sie durch die Integration einer Vielzahl von delegierten Rechtsakten in die Datenschutz-Grundverordnung zu erreichen, die es der Kommission erlaubt hätten, unter Umgehung des Europäischen Parlaments und des Rates, selbst unmittelbar Recht zu setzen. Bis auf zwei wurden diese Ermächtigungen der Kommission zum Erlass delegierter Rechtsakte im Laufe des Aushandlungsprozesses wieder entfernt.

Vertreter der Kommission versuchten im Nachhinein, die Aufnahme der zahlreichen delegierten Rechtsakte in ihren Entwurf als geschickte Verhandlungstaktik zu legitimieren. Diese sollten stimulierend auf Parlament und Rat wirken.

„Diese Rechnung ging auf".[158]

Eine Ausweitung der Souveränität der Europäischen Union führt zwangsläufig zu einem Souveränitätsverlust der Nationalstaaten und stößt auf entsprechenden Widerstand eben jener. Während sich für die Nationalstaaten wirtschaftliche Vorteile durch die transnationale Zusammenarbeit ergeben, ist dies aber auch immer mit einem Machtverlust auf nationaler politischer Ebene verbunden. Der Aufbruch nationalstaatlicher Rechtsräume zugunsten überstaatlicher Regularien wird deshalb insbesondere im Bereich öffentlicher Stellen von vielen Mitgliedstaaten der Europäischen Union kritisch beäugt. Einige forderten, dass die Regulierung staatlicher Datenverarbeitung im Vergleich zur privaten Datenverarbeitung unterschiedlich behandelt werde.

„Work on finding flexibility for the public sector related to Article 6(3) as well as to other parts of the draft regulation should be continued, on the understanding that it is only after this work that the assessment as to whether the regulation is capable of

158 Selmayr/Ehmann in: Ehmann/Selmayr 2017: Einführung Rn. 56.

accommodating the required level of flexibility for member states' public sector can be made." (Pressemitteilung des 3228. Ratstreffens Justice and Home Affairs)[159]

Darüber hinaus wird die starke Rolle der EU-Kommission auch von anderer Seite problematisiert. Der Entwurf sah einen Zuwachs an Kompetenzen der Kommission vor, insbesondere in Bereichen, die bisher den Datenschutzbehörden zugetragen wurden. Entsprechend kritisch äußerte sich die Artikel 29-Datenschutzgruppe gegenüber diesem Vorhaben und betonte die sich daraus ergebende Rechtsunsicherheit.[160]

Indes bezeichnet Viviane Reding[161] gerade die Datenschutzbehörden als Einfallstor für Lobbyismus und plädiert für mehr Transparenz. Laut Reding seien gerade eben solche Expertenkomitees, die im Geheimen tagen und letztendlich nicht-legitimierte Entscheidungen treffen, problematisch. Durch die Übertragung der Befugnisse (delegierte Rechtsakte) auf die Kommission würde dieses Dilemma aufgelöst werden.

3.1.2 Spannungen zwischen dem Europäischen Gerichtshof und dem Bundesverfassungsgericht

Die überragende Bedeutung von Datenverarbeitung in der modernen Gesellschaft brachte den deutschen Verfassungsrichter Masing dazu, vor einem „Abschied von den Grundrechten" zu warnen.[162] Hintergrund waren Ängste, dass mit dem Wechsel von der Richtlinie zur Verordnung deutsche Grundrechte marginalisiert werden. Insgesamt handelt es sich beim Datenschutzrecht um ein emotionales Thema in Deutschland, bei dem oft auf die lange und erfolgreiche Rechtstradition in Deutschland verwiesen wird. Die Datenschutz-Grundverordnung führe bezogen auf die Verarbeitung personenbezogener Daten zu einem Monopol des Europäischen Gerichtshofs in Fragen des Grundrechtsschutzes, jedoch handle es sich, so Masing, dabei um ein „Gericht ohne Unterbau" und um „kein Bürgergericht", das wie das

---

159 Rat der Europäischen Union 2013.

160 „The Working Party has serious reservations with regard to the extent the commission is empowered to adopt delegated and implementing acts, which is especially relevant because a fundamental right is at stake. (…) The adoption of delegated or implementing acts for a large numbers of articles may take several years and could represent legal uncertainty.", Nielsen 2012.

161 Viviane Reding war von 2010 bis 2014 Vizepräsidentin der Europäischen Kommission und stellte in dieser Funktion am 25.1.2012 den Kommissionsvorschlag für die Datenschutz-Grundverordnung vor.

162 Masing 2012.

Bundesverfassungsgericht von einzelnen Bürgern angerufen werden kann. Ein Äquivalent zur deutschen Verfassungsbeschwerde existiert nicht; einzelne Bürger können nur indirekt Fälle vor den Europäischen Gerichtshof bringen. Zudem sei dieser angesichts der Zahl der zu erwartenden Verfahren unterbesetzt.

Ausgangspunkt dieser Befürchtungen sind die durch den Wechsel entstehenden Folgen für die Geltung nationaler Grundrechte. Der Wechsel von der Richtlinie zur Verordnung wird Folgen für die Geltung nationaler Grundrechte haben. Deutsche Grundrechte etwa werden allenfalls noch dort relevant sein, wo die Datenschutz-Grundverordnung den Mitgliedstaaten Umsetzungsspielräume lässt. Diese fallen bei einer Verordnung deutlich enger aus als bei einer Richtlinie. Das grundlegende Verhältnis zwischen nationalen und europäischen Grundrechten hat das Bundesverfassungsgericht in seinen Solange-Entscheidungen[163] geklärt. Im Solange II-Urteil[164] heißt es:

„Solange die Europäischen Gemeinschaften, insbesondere die Rechtsprechung des Gerichtshofs der Gemeinschaften einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleisten, der dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im wesentlichen gleichzuachten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt, wird das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von abgeleitetem Gemeinschaftsrecht, das als Rechtsgrundlage für ein Verhalten deutscher Gerichte oder Behörden im Hoheitsbereich der Bundesrepublik Deutschland in Anspruch genommen wird, nicht mehr ausüben und dieses Recht mithin nicht mehr am Maßstab der Grundrechte des Grundgesetzes überprüfen."

Das Bundesverfassungsgericht beschränkt sich damit auf eine Art von „Mindestkontrolle" dahingehend, ob durch die Europäische Union dem „Wesensgehalt der Grundrechte generell verbürgt" wird. Dem steht der Anspruch des Europäischen Gerichtshofs gegenüber, umfassend und abschließend über Unionsrecht und dessen Anwendung zu entscheiden. Nach seinem weiten Verständnis gelten nationale Grundrechte nur, wenn keine Fallgestaltung denkbar ist, die vom Unionsrecht erfasst würde. Nach dem engen Verständnis des Bundesverfassungsgerichts kommt es indes darauf an, ob ein Sachverhalt unionsrechtlich determiniert ist.[165]

---

163 BVerfGE 37, 271.

164 BVerfGE 73, 339.

165 Vgl. hierzu ausführlich Roßnagel 2017: S. 86 ff.

Auf europäischer Seite hat sich der Europäische Gerichtshof in der Åkerberg Fransson-Entscheidung aus dem Jahr 2013 zum Verhältnis nationaler und europäischer Grundrechte geäußert. Die Unionsgrundrechte sollen „in allen unionsrechtlich geregelten Fallgestaltungen" gelten. Nationale Grundrechte können damit nur noch dann gelten, wenn keine Fallgestaltung denkbar ist, die vom Unionsrecht erfasst würde. Flankiert wurde diese Aussage durch die Melloni-Entscheidung des Europäischen Gerichtshofs. Danach gestattet der Vorrang des Unionsrechts den Mitgliedstaaten nicht, die Ausführung von Unionsrecht zu verweigern, wenn dies das höhere Schutzniveau nationaler Grundrechte verletzt. Diesem weiten Verständnis des Europäischen Gerichtshofs setzte das Bundesverfassungsgericht sein eigenes, enges Verständnis entgegen. Danach sind Vorschriften nur dann nicht am deutschen Grundgesetz zu messen, wenn sie durch Unionsrecht determiniert sind.

Das Verhältnis zwischen Europäischem Gerichtshof und Bundesverfassungsgericht war und ist also durchaus problembehaftet. Man kann von einer komplizierten und schwierigen „Kooperation" oder „Kohabitation" zwischen den beiden Gerichten sprechen. Praktische Auswirkungen hatten die Differenzen indes bisher nicht. Dies könnte sich durch die Datenschutz-Grundverordnung jedoch ändern.

3.1.3 Die Europäische Union rüstet sich gegen die Vormacht von US-Unternehmen

Der Konflikt zwischen den Souveränitätsansprüchen einzelner Länder und den Kompetenzerweiterungen der Europäischen Union entzündete sich auch an anderer Stelle. Mit der Datenschutz-Grundverordnung möchte die Europäische Union ihren Bürgern einen besseren Schutz ihrer Daten garantieren, wenn diese von US-Konzernen verwendet werden. Mit Hilfe der Verordnung wird ein einheitliches Datenschutzniveau innerhalb der Europäischen Union angestrebt, an welches sich im Sinne des Marktortprinzips auch amerikanische Konzerne halten müssen, die auf dem europäischen Markt aktiv sind. Gleichzeitig verfolgt die Europäische Union auch wirtschaftsprotektionistische Interessen. Die Verbesserung der Wettbewerbsbedingungen für europäische Unternehmen sowie die Förderung von Innovationen dient vor allem auch der Aufholjagd gegenüber amerikanischen Unternehmen, die in vielen Bereichen der Digitalökonomie der Europäischen Union weit voraus sind. Eines der Ziele der Europäischen Union ist es in der Digitalwirtschaft konkurrenzfähige IT-Unternehmen zu etablieren, die im

globalen Wettbewerb mithalten können und die Europäische Union bei der Technologieführerschaft weiter vorantreiben. Auf diese Weise soll ein europäisches Gegengewicht geschaffen werden, das der Übermacht amerikanischer Konzerne entgegenwirkt. Das Voranbringen des wirtschaftlichen Wohlstands der Europäischen Union ist eine der zentralen Rechtfertigungsrhetoriken, mit dem die Sinnhaftigkeit einer Europäischen Union begründet wird. Amerikanische Unternehmen fürchten hingegen, dass durch die Datenschutz-Grundverordnung nicht nur das Datenniveau in der Europäischen Union, sondern durch den sog. California Effekt auch in den USA angehoben wird.[166] Insbesondere datengetriebene Geschäftsmodelle, so die Angst, könnten dadurch gefährdet und die Monopolstellung einiger Unternehmen aufgebrochen werden.

3.1.4 Die US-Regierung und die Digitalwirtschaft vereint im Kampf gegen den Datenschutz

Bisher konnten amerikanische Unternehmen auf der Grundlage des Safe-Harbor-Abkommens innerhalb der USA Daten von EU-Bürgern verarbeiten. Da der Europäische Gerichtshof[167] jedoch entschieden hat, dass in den USA kein angemessenes Datenschutzniveau herrscht, wurde das Abkommen für ungültig erklärt. Ein angemessenes Datenschutzniveau ist immer dann anzunehmen, wenn dieses dem innerhalb der Europäischen Union gewährleisteten Schutzniveau entspricht bzw. als gleichwertig angesehen wird.[168] Aufgrund der Snowden-Enthüllungen verhandelte die Europäische Kommission ab November 2013 mit den USA neu und verstärkte diese nach dem Urteil des Europäischen Gerichtshofs im Oktober 2015.[169] Daraufhin präsentierte die Europäische Kommission am 29. Februar 2016 einen Entwurf des Privacy Shield-Abkommen, das schließlich am 12. Juli 2016 erlassen wurde.

Auch bei den Verhandlungen um die Datenschutz-Grundverordnung wurde die Anerkennung eines angemessenen Schutzniveaus der USA diskutiert. Dies stieß auf Widerstand der US-Regierung. Der US-Botschafter der Europäischen Union, William Kennard, forderte die Europäische Union bei den Verhandlungen dazu auf, der USA einen „adequate status“ zuzuerken-

166 O´Brien 2013.

167 EuGH, Urt. v. 06.10.2015, Az. C-362/14.

168 Bei der Beurteilung sind die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die geltenden Datenschutzvorschriften und die Rechtsprechung des EuGH zu berücksichtigen; Molnár-Gábor/Kaffenberger 2017: S. 19.

169 Schantz in: Wolff/Brink 2016: § 4b BDSG Rn. 34.

nen[170] und sprach sich für eine Rücknahme der ausdrücklichen Einwilligung bei einer Datenerhebung sowie des Rechts auf Vergessen aus.[171]

In einem von der internationalen Bürgerrechtsvereinigung „European Digital Rights" veröffentlichten Schreiben der US-Regierung warnte diese die Europäische Union vor Handelshemmnissen und den terroristischen Gefahren, sollte der Datenaustausch zwischen den beiden Kontinenten durch die Grundverordnung zu sehr beeinträchtigt werden.[172] Die USA verfolgten dabei einerseits staatliche Interessen der Kontrollausübung. So sah eine Version im Vorfeld der Veröffentlichung des offiziellen Entwurfs der EU-Kommission noch einen zusätzlichen Artikel vor, der es den USA erschwert hätte, Daten über Nutzer von Unternehmen zu verlangen. Geleakte Dokumente konnten zeigen, dass dieser Artikel aufgrund intensiver Lobbyarbeit von Seiten der US-Regierung schließlich wieder gestrichen wurde.[173] Gleichzeitig verfolgte die US-Regierung auch wirtschaftliche Interessen. Gerade die Big Player der Digitalökonomie (z. B. Facebook Inc., Google Inc., u.a.) haben ihren Sitz in den USA. Ihre Monopolstellung aufzubrechen und europäische Konkurrenz zu befruchten, ist eines der Ziele der Datenschutz-Grundverordnung. Entsprechend erzeugte dies auf Seiten der US-Regierung und Teilen der Digitalökonomie Widerstand. Beide teilen das Interesse, die USA in ihrer wirtschaftlichen und politischen Stellung abzusichern. Gerade Unternehmen, deren Geschäftsmodelle datengetrieben sind, die aber nicht vom Vertrauen der Verbraucher essentiell abhängig sind, da schlicht keine alternativen Konkurrenzangebote existieren, setzen sich für ein schwaches Datenschutzniveau ein und pochen auf Selbstregulierung.[174] Insbesondere amerikanische Technologiekonzerne haben durch Lobbyisten versucht, intensiv gegen unterschiedliche Bestimmungen der Datenschutz-Grundverordnung vorzugehen und Einfluss auf ihre Ausgestaltung zu nehmen, was zahlreiche geleakte Dokumente belegten.

---

170 Baker 2012.

171 O´Brien 2013.

172 EDRi 2013.

173 Fox 2013.

174 „'I studied in Silicon Valley and there were companies coming to the classroom not knowing there is a European among them. They were saying it very bluntly: yes, Europe has strong data protection rules, but if you just pretend to respect them, you're fine. No way can they find out what we are doing on our servers and even if they do, it will take them at least 10 years to enforce anything.'(...) Schrems said." Pop 2013.

Allerdings sind es nicht nur US-Unternehmen, die Datenschutz als Gefahr für datenbasierte Geschäftsmodelle betrachten. Auch europäische Unternehmen befürchten, dass ein zu enges Datenschutzgesetz Innovation und Wachstum in der Europäischen Union schwächen könnte. Wenngleich Unternehmen, die Daten verarbeiten, aber deren Kerntätigkeit nicht datenbasiert ist, wie zum Beispiel Unternehmen der Finanzbranche und des Gesundheitssektors, durchaus ein gewisses Interesse an Datenschutz haben, um das Vertrauen der Kunden nicht zu verlieren, so sind auch für sie strenge Regularien mit mehr Bürokratie und höheren Kosten verbunden. Europäische und amerikanische Unternehmen haben somit beide ein Interesse daran, dass Datenschutzniveau in der Europäischen Union zu schwächen.

Die Strategie der Wirtschaftsvertreter umfasste auch die Errichtung eigener Organisationen, die auf den ersten Anschein wie NGOs oder gemeinnützige Vereine wirken (sollten). Dahinter verbergen sich Organisationen, die durch große Unternehmen finanziert werden und unter der Hand deren Interessen vertreten.[175] Medial wird dieses Phänomen häufig unter dem Begriff „Astroturfing" aufgegriffen. Im Bereich Privacy setzten sich diese Organisationen meist für ein moderates Maß an Datenschutz ein, solange es den eigentlichen Geschäftsinteressen der Unternehmen nicht im Wege stand.[176]

3.1.5 Geschäftsmodelle der Digitalwirtschaft im Widerspruch mit den Grundprinzipien des Datenschutzes

Im Konflikt zwischen der Welt des Datenschutzes und der Welt der Digitalwirtschaft spiegelt sich eine der zentralen Streitlinien der gesamten Verhandlungen wider. Die Welt der Digitalwirtschaft fürchtet erhebliche Nachteile, wenn das Datenschutzniveau ihrer bisherigen Unternehmenspraxen angehoben werden muss, da deren Geschäftsmodelle und Angebote zum Teil mit den Grundprinzipien des Datenschutzes kollidieren. Datenschutz wurde von vielen Wirtschaftsvertretern als Bedrohung für den wirtschaftlichen und gesellschaftlichen Wohlstand dargestellt. Durch die Einführung des Marktortprinzips mit der Datenschutz-Grundverordnung bergen bestimmte EU-Länder, wie beispielsweise Irland, keine datenschutzrechtlichen Vorteile mehr in Form eines vergleichsweise schwachen Datenschutzniveaus, das sich US-Unternehmen bisher zu Nutze machen konnten. So z. B. Facebook Inc. mit seiner Niederlassung in Irland.

---

175 Baker 2013.

176 Vgl. Center for Democracy & Technology o. J. oder European Privacy Association o. J.

„Die Datenschutzgrundverordnung sollte innovative Big Data Anwendungen fördern, anstatt diese zu bremsen. Big Data Analysen ermöglichen die Auswertung großer Datenmengen in hoher Geschwindigkeit und gelten als eine der wichtigsten Technologien der Zukunft. Sie kommen in unterschiedlichsten Bereichen wie der Medizin, der wissenschaftlichen Forschung oder der Wirtschaft zum Einsatz. Der weiteren Entwicklung von Big Data in Europa stehen sowohl das Gebot der Datensparsamkeit als auch die sogenannte Zweckbindung bei der Datenerhebung entgegen." (Susanne Dehmel, Mitglied der Geschäftsleitung Vertrauen und Sicherheit Bitkom e.V.)[177]

Für die Digitalwirtschaft stellen Daten vor allem eine Ware dar, wie etwa der Handel mit Daten für Werbezwecke oder Nebenprodukte des alltäglichen Geschäftsablaufs. Dies können beispielsweise Kundendaten sein. Datenschutz spielt insofern eine Rolle, als er dazu dient, das Kundenvertrauen zu stärken oder die Daten des Unternehmens selbst vor fremden Zugriffen zu schützen. Jenseits dieser beiden Aspekte wird er oft als hinderlich oder zusätzlicher Mehraufwand wahrgenommen. Insbesondere die großen Global Player, die auf dem freien Markt eine monopolähnliche Stellung einnehmen, sehen in einem starken Datenschutz eine Gefahr für ihre digitalen Verwertungspraktiken. Demgegenüber stehen Unternehmen, die Datenschutz als potentielle Ressource zur Effizienz- und Funktionalitätssteigerung ihrer Produkte betrachten. Auch wenn Datenschutz prinzipiell Vorteile für einige Unternehmen mit sich bringt, so stellt er dennoch einen Kostenfaktor dar, der hinsichtlich der Effizienz und Funktionalität mit anderen Interessen abgewogen werden muss. Innerhalb der Welt der Digitalwirtschaft werden daher immer wieder Stimmen laut, die auf einen Ausgleich zwischen Datenschutz und der Ermöglichung datengetriebener Geschäftsmodelle pochen. Besonders einige europäische Unternehmen, deren Kundenbindung nicht durch eine monopolartige Stellung im Markt gesichert ist und die somit viel stärker dem freien Markt unterworfen sind, hoffen durch eine gesetzliche Regelung und verhältnismäßig starkem Datenschutz (insbesondere im Vergleich zu den USA) auf eine Verbesserung ihrer Wettbewerbsbedingungen.[178]

Für die Welt des Datenschutzes stellt der Schutz personenbezogener Daten einen Teil der Kernpraktik der Welt dar, die mit bestimmten Werten und

[177] Dehmel 2015.

[178] Matzer 2014.

Zielen, wie dem Schutz der Rechte und Freiheiten des Einzelnen, verbunden ist. Der Kampf für Datenschutz ist wertebasiert und nicht instrumentell. Somit ist Datenschutz nicht nur ein Instrument, um die eigene Kernpraktik auszuführen, vielmehr ist er selbst Bestandteil eben jener. Dieser unterschiedliche Zugang zu Datenschutz gestaltet Kompromissfindungen zwischen diesen beiden Welten teilweise sehr schwierig.

Innerhalb der Welt des Datenschutzes rücken die einzelnen Vertreter enger zusammen. So wird Datenschutz immer mehr ein Bestandteil des Verbraucherschutzes. Dies wird zum Beispiel durch das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts[179] deutlich, wonach das Unterlassungsklagengesetz auf bestimmte Datenschutzrechtsverstöße durch Unternehmen erweitert wurde. Unternehmen verarbeiten zunehmend mehr Daten der Verbraucher, ohne dass diese hierfür eine Einwilligung erteilt haben. Dies umfasst insbesondere die Datenverarbeitung für Werbung, Profiling oder den Adresshandel. Sofern ein Unternehmen gegen datenschutzrelevante Vorschriften verstößt, die dem Verbraucherschutz dienen, kann dieses auf Unterlassung in Anspruch genommen werden, da das Unterlassungsklagengesetz zum Tragen kommt. Den Anspruch können jedoch nicht die betroffenen Verbraucher selbst geltend machen, sondern sie werden dabei durch Verbände oder Institutionen vertreten.[180] Auf diese Weise können die Verbraucherschutzzentralen, wie bei anderen verbraucherschützenden Gesetzen, im Namen der Verbraucher tätig werden und das entsprechende Unternehmen verklagen oder abmahnen.[181] Hintergrund dieses Entschlusses ist der Wunsch, die Arbeit von Datenschutzbehörden durch den Rechtsschutz durch Verbraucherverbände zu ergänzen.[182] Der Bundesminister der Justiz und für Verbraucherschutz, Heiko Maas, sieht in der Ausweitung der Unterlassungsklage einen Erfolg:

„Das ist ein wichtiger Schritt zum besseren Schutz unserer Daten. Endlich bekommen Verbände bei Datenschutzverstößen ein Klagerecht. Personenbezogene Daten sind für den Wirtschaftsverkehr von unermesslicher Bedeutung. (…) Wir müssen uns darauf verlassen können, dass unsere Daten rechtlich geschützt sind und dieser

179 Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts v. 17.02.2016, BGBl. II, 233.

180 Vgl. § 3 Abs. 1 S. 1 UKlaG.

181 Ackermann 2016.

182 BMJV 2015.

Schutz auch durchgesetzt werden kann. (...) Alle darauf zu verweisen, ihre Rechte einzeln einzuklagen, ist oft ein stumpfes Schwert. Viele trauen sich nicht, gegen große Unternehmen rechtlich vorzugehen. (…)"[183]

Auch wenn sowohl die Datenschützer als auch Teile der Digitalwirtschaft ein Interesse an Datenschutz haben, können die dahinter liegenden Ziele somit teilweise konträr zueinander stehen. Während die Welt des Datenschutzes mit der Datenschutz-Grundverordnung vor allem die Rechte der Bürger stärken möchte, geht es der Welt der Digitalwirtschaft um die Verbesserung der ökonomischen Ausgangslage.

3.2 Die Fronten verhärten sich

Im Laufe der Verhandlungen bildeten sich neue Bündnisse und Spannungen entlang der zentralen Konfliktlinien heraus. Ein Kompromiss oder eine Annäherung zwischen den unterschiedlichen Positionen der sozialen Welten und ihren Repräsentanten in der Arena schien in weite Ferne zu rücken.

3.2.1 Allianz zwischen Datenschutzaktivisten und der Welt der Nachrichtenportale

Im Verlauf der Verhandlungen zur Datenschutz-Grundverordnung kam es immer wieder vereinzelt zu Leaks[184] von Dokumenten, die der Öffentlichkeit eigentlich nicht zugänglich gemacht werden sollten. Ins Zentrum der Aufmerksamkeit kamen diese Leaks vor allem durch ihre Thematisierung durch Nachrichtenportale. Datenschutzaktivisten konnten so Aufmerksamkeit für ihre Anliegen bekommen und Aufklärung betreiben. Gleichzeitig bot dies für die Welt der Nachrichtenportale die Gelegenheit, mit Hilfe eines Skandals Klickzahlen und Auflagen zu produzieren. Eine besonders tragende Rolle in den Verhandlungen nahm die Plattform Lobbyplag[185] ein. Sie verfolgte den Gesetzgebungsprozess von Anfang an und veröffentlichte immer wieder interne Dokumente, die die Einflussnahme von Interessengruppen und insbesondere Wirtschaftsunternehmen auf die Verhandlungen transparent machen sollten. Diese Leaks bekamen insbesondere durch die mediale Berichterstattung Aufmerksamkeit durch eine breite Öffentlichkeit.

183 BMJV 2015.
184 Lobbyplag o. J. b.
185 Lobbyplag o. J. a.

„Wie stark der konkrete Einfluss der Lobbyisten zuweilen ist, zeigt nun eine Internetplattform namens Lobbyplag: Sie dokumentiert in übersichtlicher Form, welche Abschnitte aus Papieren von Unternehmen und Lobby-Organisationen teils wörtlich in eine Stellungnahme des EU-Ausschusses für Binnenmarkt und Verbraucherschutz eingeflossen sind – von Amazon bis zur Amerikanischen Kammer für den Handel mit der EU, vom europäischen Bankenverband EBF bis hin zum Verband der Kreditauskunfteien." (Spiegel online)[186]

3.2.2 Die Wissenschaft macht gegen die Lobbyindustrie mobil

Im Zuge des Bekanntwerdens der großflächigen Industrielobbyarbeit versammelten sich auch einige Wissenschaftler, um eine Gegenposition im öffentlichen Diskurs zu etablieren.[187] Wissenschaftler aus ganz Europa starteten eine Onlinepetition und setzten sich für eine stärkere Regulierung des Datenschutzes ein, um zu verhindern, dass die Datenschutz-Grundverordnung aufgrund des enormen Lobbyeinflusses der Industrie verwässert wird. Zahlreiche Disziplinen, von den Rechtswissenschaften bis hin zu den Wirtschaftswissenschaften, unterzeichneten die Petition.

„The European Parliament and the European Council are now preparing their views on this new regulation. At the same time, huge lobby groups are trying to massively influence the regulatory bodies. To contribute a more objective perspective to this heated debate, we would like to bring forward some professional arguments. We want to reply to some arguments that aim to weaken data protection in Europe." (Online-Petition Data Protection in Europe)[188]

3.2.3 Uneinigkeit im Europäischen Parlament

Nach der Veröffentlichung des Kommissionsentwurfs nahm das Europäische Parlament seine Arbeit auf. Der Konflikt zwischen Datenschutz und Wirtschaftsinteressen spiegelte sich auch innerhalb des Europäischen Parlaments wider. Hier zeichnete sich eine Spaltung zwischen einer wirtschaftsfreundlichen (allen voran EPP, ALDE und ECR) und einer datenschutzaffinen (Grüne-EFA, GUE-NGL) Fraktion ab.[189] Datenschutzaktivisten und Teile des Parlaments (Grüne und European United Left/ Nordic Green Left) teilten das Interesse am Datenschutz mit dem Ziel, die Rechte des Individu-

[186] Lischka/Stöcker 2013.

[187] Initiative Data Protection in Europe 2013.

[188] Initiative Data Protection in Europe 2013.

[189] „Both the centre-right EPP and the liberal Aide groups are opposing the Greens and the European United Left/Nordic Green Left camp." Nielsen 2013 a.

ums zu stärken. Allen voran Jan Philipp Albrecht[190] forderte in öffentlichen Debatten immer wieder die Stärkung der individuellen Rechte. Der Europaabgeordnete Albrecht wurde vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) als zuständiger Berichterstatter ernannt. Seine Aufgabe bestand darin, sich federführend mit dem Kommissionsvorschlag auseinanderzusetzen und die Stellungnahme des Ausschusses vorzubereiten. Albrecht setzte sich für einen starken Datenschutz und einen offenen und transparenten Verhandlungsprozess ein.[191]

„Der Grundsatz muss heißen: im Zweifel für den Schutz der Person. Anders ist ein konsequenter Schutz auch nicht denkbar." (Jan Philipp Albrecht, Abgeordneter des Europäischen Parlaments)[192]

Am 9. und 10. Januar 2013 stellte Albrecht schließlich einen Berichtsentwurf mit Änderungen zur Datenschutz-Grundverordnung vor. Bevor dieser weiter an das Plenum zur Abstimmung gegeben werden konnte, war Albrecht zudem damit vertraut die über 3.000 Änderungsanträge einzuarbeiten. Albrecht bekam in seiner Position, die Grundrechte der europäischen Bürger zu stärken und einen starken Datenschutz durchzusetzen, öffentliche Unterstützung von der damaligen Kommissionsvorsitzenden Viviane Reding. Beide teilten das Interesse, die Integration Europas als Werteunion voranzutreiben.

„I am glad to see that the European Parliament rapporteurs are supporting the Commission's aim to strengthen Europe's data protection rules which currently date back to 1995 – pre-Internet age." (Viviane Reding, Justizkommissarin von 2010 bis 2014)[193]

Gleichzeitig übernahmen einige Parlamentarier, wie diverse Leaks zeigten, teilweise wortgleich Forderungen von großen amerikanischen IT-Unternehmen, die die Schwächung einiger Datenschutzregeln forderten.[194] Lobbying wurde aber auch von verschiedenen Bürgerrechtsorganisationen betrieben, die versuchten ihre Forderungen nach einer datenschutzfreundlichen Reform in die Verhandlungen mit einzubringen. So fanden sich hier

190 Tzschentke 2013.

191 Tzschentke 2013.

192 BvD e.V. 2013.

193 Europäische Kommission 2013.

194 So flossen Lobbytexte etwa von Amazon, Ebay und der US-amerikanischen Handelskammer in Anträge über gesetzliche Regelungen; vgl. Peters 2013.

ebenfalls wortgleiche Übernahmen durch Parlamentarier.[195] Die Anhörung verschiedener Interessengruppen zur Meinungsbildung ist kein ungewöhnlicher Prozess im europäischen Politikbetrieb, jedoch kritisierten viele Medien die Intransparenz des Verfahrens und das Übermaß an wirtschaftlicher Einflussnahme.[196]

„Lobbying is so intense and uneven on this law - Facebook alone has hired five lobbyists for this in Brussels, while on the other side, NGOs have maybe one person who also has to cover other topics too. And MEPs rarely go the extra mile of asking some independent experts or academics about it." (Maximilian Schrems, österreichischer Jurist und Datenschutzaktivist)[197]

Zudem zeichnete sich ein Machtungleichgewicht zwischen den unterschiedlichen Interessengruppen ab. Insbesondere große IT-Unternehmen sind mit enormen finanziellen Ressourcen ausgestattet, die es ihnen im Vergleich zu zahlreichen Bürger- oder Verbraucherrechtsorganisationen erlauben, ein Vielfaches an Lobbygeldern auszugeben.

Insgesamt schienen sich zu diesem Zeitpunkt die Stimmen, die eine wirtschaftsfreundlichere Strategie verfolgten, im Parlament langsam durchzusetzen.[198]

„Much of what we have said unanimously is now contested by lobbyist groups and by some members in here in the house who seem not to feel obliged by the resolution they voted on in the first place." (Jan Philipp Albrecht, Abgeordneter des Europäischen Parlaments)[199]

3.2.4 Der Rat der Europäischen Union nähert sich der europäischen Digitalwirtschaft an

Nachdem das Europäische Parlament seine Stellungnahme veröffentlichte, nahm der Rat der Europäischen Union seine Arbeit auf und verhandelte unter Ausschluss der Öffentlichkeit über die Datenschutz-Grundverordnung.

---

195 So beispielsweise Änderungsvorschläge der Internet NGO Bits of Freedom, portal liberal 2013.

196 Lischka/Stöcker 2013.

197 Pop 2013.

198 „'I can see a shift towards more of the protection, under quotation marks, of business interests and not the protection of citizen's fundamental rights.', Greek socialist MEP Dimitrios Droutsas told reporters in Brussels on Wednesday (15 May)." Nielsen 2013 b.

199 information age 2013.

Dabei drangen nur wenige interne Informationen nach außen. Die Innen- und Justizminister setzten vor allem auf den von der Ökonomie geforderten Ansatz der Selbstregulierung und den risikobasierten Ansatz. Generell schien der Rat eine unternehmensfreundliche Haltung einzunehmen.[200]

„The application of approved codes of conduct and the use of approved data protection certification mechanisms should be incentivised by establishing linkages with the risk assessment process; work on the risk-based approach should be continued by further developing criteria for enabling the controller and processor to distinguish risk levels and by further exploring the use of pseudonymous." (Pressemitteilung des 3228. Ratstreffens Justice and Home Affairs)[201]

Dem waren vielfache Warnungen europäischer Unternehmen vor den Folgen eines zu strengen Datenschutzes für den digitalen Binnenmarkt vorangegangen.

„However, the benefits of greater harmonisation are at risk of being outweighed by the costs of failing to strike the right balance between the protection of Europeans' fundamental right to privacy and data protection, and the promotion of innovation, competitiveness and growth in the Digital Single Market. If enacted in the present draft form, the Regulation would delay the launch of innovative services in Europe, cause substantial loss in revenues for businesses of all sizes and in a wide range of industries, limit opportunities for new market entrants, strongly increase administrative costs and create legal uncertainty." (Industry Coalition for Data Protection)[202]

Sowohl im Rat als auch in der europäischen Digitalindustrie setzte sich die Ansicht durch, dass ein zu strenger Datenschutz schädlich für die Europäische Union sein könnte. Die Angst, abgehängt zu werden, langfristig nicht mit den Big Playern in den USA mithalten zu können und so in der Wirtschaft und dadurch letztendlich auch in der Politik zu einer marginalen Größe zu schrumpfen, bekräftigte diese Allianz.

200 Bergemann 2013.
201 Rat der Europäischen Union 2013.
202 Industry coalition for data protection 2012.

3.3 Datenschutz erfährt durch Snowden-Enthüllungen Aufschwung

Im Zuge der Snowden Enthüllungen erfuhr die Datenschutz-Grundverordnung vermehrt öffentliche Aufmerksamkeit. Wirtschaftsfreundliche Positionen zu Lasten des Datenschutzes verloren an öffentlicher Legitimität und Vertreter dieser Positionen gerieten unter Druck sich neu zu positionieren.

3.3.1 Die Bundesregierung öffnet sich dem Datenschutz

Angela Merkel setzte sich als Reaktion auf den Snowden Skandal für den Schutz der Daten der Bürger ein.[203] Ausländische Unternehmen und Regierungen wurden so kurzzeitig zu einem gemeinsamen Feind, vor dem es die „heimischen" Daten zu schützen galt.

„Wir arbeiten zusammen im Kampf gegen den Terror, aber auf der anderen Seite muss natürlich auch der Schutz der Daten der Bürgerinnen und Bürger gewährleistet sein. Nicht alles was technisch machbar ist, das wird ja in Zukunft immer mehr sein, darf auch gemacht werden." (Angela Merkel)[204]

3.3.2 Einigung im Europäischen Parlament zugunsten des Datenschutzes

Auch das Europäische Parlament blieb von den Snowden-Enthüllungen nicht unberührt. Die internen Streitigkeiten lösten sich kurzfristig auf und das Parlament trat geschlossen für ein schnelles Ende der Verhandlungen ein. Nach der Veröffentlichung des NSA-Skandals wurde Datenschutz zu einem brisanten Thema und stärkte die Verhandlungsposition der datenschutzfreundlicheren Kräfte innerhalb des Parlaments. Im Oktober 2013 konnte das Parlament eine gemeinsame Position verabschieden.[205] Es verfolgte das Ziel, die Verhandlungen mit den Mitgliedstaaten so schnell wie möglich zu beginnen.[206] Die Position des Parlaments machte gegenüber datenschutzfreundlichen Lösungen viele Zugeständnisse und näherte sich dem Anliegen vieler Vertreter der Welt des Datenschutzes an, ein starkes Datenschutzniveau zum Wohle der Bürger zu verankern.

---

203 Die Welt 2013.

204 Merkel 2013.

205 „Dank der Aufregung um Snowden konnten Datenschützer in den Entwurf sogar ein paar Punkte wieder hineinschreiben, die die Industrie bereits hatte streichen lassen.", Biermann 2013.

206 Krempl 2013.

3.4 Die Angst der Europäischen Union vor wirtschaftlicher Abhängigkeit

Die Mitgliedstaaten der Europäischen Union fürchteten nicht nur die politische Abhängigkeit, sondern auch den Verlust ihrer Wettbewerbsfähigkeit gegenüber amerikanischen IT-Großunternehmen. Wirtschaftsfreundliche Positionen wurden in der Arena wieder dominanter. Die Drohszenarien der Welt der Digitalwirtschaft vor den vermeintlich negativen Folgen durch einen zu hohen Datenschutz hatten ihre Wirkung entfaltet, während die Snowden-Enthüllungen in den Verhandlungen kaum noch eine Rolle zu spielen schiene.

3.4.1 Der Kampf um Souveränität der Nationalstaaten

Gegen Ende des Jahres 2013 gerieten die Verhandlungen um die Datenschutz-Grundverordnung schließlich wieder ins Stocken. Im Rat der Europäischen Union, der sich als letztes Organ (nach Kommission und Parlament) auf eine gemeinsame Stellungnahme zur Verordnung einigen musste, bevor die aufgrund der wechselseitigen Ablehnung der jeweiligen Vorschläge zwischen Rat und Parlament notwendigen Trilog-Verhandlungen beginnen konnten, kam es immer wieder zu Verzögerungen. Insbesondere das Prinzip des One-Stop-Shop führte wiederholt zu Konflikten zwischen den Mitgliedstaaten.[207] Das Prinzip ist eine wesentliche Neuerung gegenüber dem bisherigen europäischen Datenschutzrecht, indem es künftig grundsätzlich eine zentrale Behördenzuständigkeit geben wird. Bei grenzüberschreitenden Datenverarbeitungen ist für das datenverarbeitende Unternehmen und deren Tochtergesellschaften gemäß Art. 56 Abs. 1 DSGVO nur noch die Aufsichtsbehörde am Sitz der Hauptniederlassung zuständig.

Einzelne Länder, darunter das Vereinigte Königreich, Dänemark, Slowenien und Ungarn, lehnten eine Verordnung generell ab und plädierten für die Umwandlung in eine Richtlinie. Im Gegensatz zu einer Verordnung würde die Umsetzung im Falle einer Richtlinie den einzelnen Staaten überlassen und mehr Raum für nationale Sonderregeln schaffen. Deutschland wiede-

[207] „An EU diplomat said Germany, with the support of Sweden and Belgium, is partly responsible for the delay. The issue revolves around a so-called one-stop shop principle, considered a central pillar of the proposal because it harmonizes decision-making across the bloc. (…) The German argument, said the contact, is that Berlin does not want the EU law to be any weaker than its domestic one. (…) But the UK has issue with the legal basis and wants to downgrade the 'regulation' into a 'directive'." Nielsen 2013 c.

rum versuchte zu verhindern, dass der öffentliche Sektor ebenfalls von der Verordnung erfasst wird.

„The delays are caused, in part, by a handful of member states that want to weaken the regulation, which aims at harmonising data protection rules across the bloc. Among the core group is the UK, along with Denmark, Hungary, and Slovenia. All four are pushing to turn the regulation into a directive. Unlike a regulation, a directive gives member states room to manoeuvre and interpret the EU law to their advantage. Germany is also among the delaying camp of member states but for different reasons. The Germans support the regulation but do not want it applied to the public sector. 'Obviously the German government is against European-wide common rules. This behaviour is irresponsible against the EU citizens.'(sagte Albrecht, Anm. d. Verf.)" (EUObserver)[208]

Der Ursprung der zähen Verhandlungen lag in der Angst der einzelnen Staaten, in relevanten Bereichen Souveränität abgeben zu müssen. Dies führte dazu, dass trotz des massiven Drucks von Kommission und Parlament die Verhandlungen nicht vor den Neuwahlen im Frühling 2014 abgeschlossen werden konnten. Erst im Dezember 2014 konnte sich der Rat schließlich auf einen Kompromiss im One-Stop-Shop-Prinzip einigen.[209] Im Juni 2015 einigte sich der Rat schließlich und veröffentlichte seine Version eines Vorschlags für eine Datenschutz-Grundverordnung.

3.4.2 Die Sorge der Bundesregierung um den nationalen wirtschaftlichen Wohlstand

Angela Merkel zweifelte mittlerweile öffentlich, ob Datenschutz als Oberziel noch zukunftsfähig ist. Vielmehr betonte sie die Wichtigkeit wirtschaftlicher Aspekte und trat für eine Stärkung der heimischen Industrie und im Zuge dessen für europäische Unternehmen ein.

„Wir müssen hohe Datensicherheit haben, aber wenn wir uns das Big Data Management, wenn wir uns die Möglichkeit der Verarbeitung großer Datenmengen durch einen falschen rechtlichen Rahmen zu sehr einengen, dann wird nicht mehr

[208] Nielsen 2014 a.

[209] „Member states on Thursday (4 December) reached a broad consensus on a key area of the EU's reformed data protection bill but some problems remain for the next EU presidency to resolve. Months of wrangling on technical details have led to an Italian EU presidency compromise text on the so-called one stop shop mechanism aimed at harmonizing data protection decisions across the EU." Nielsen 2014 b.

viel Wertschöpfung in Europa stattfinden. Das wäre für uns von großem Nachteil." (Angela Merkel)[210]

Die deutsche Bundesregierung teilte somit die Interessen vieler europäischer Unternehmen, die im Datenschutz eine Gefahr für die Konkurrenzfähigkeit der europäischen Wirtschaft sahen. Als eine Vertreterin der Welt der Nationalstaaten handelt sie im Interesse Deutschlands. Gesellschaftlicher Wohlstand wird hier eng an den ökonomischen Wohlstand gekoppelt. Europäische Unternehmen wiederum verfolgen wirtschaftliche Interessen der Profitgenerierung und möchten ihre Wettbewerbsfähigkeit verbessern. Die Forderung datengetriebene Geschäftsmodelle zu ermöglichen und verstärkt auf Selbstregulierung zu setzen, kann somit die Interessen beider Welten vereinen.

3.4.3 Der Rat der Europäischen Union unter dem Einfluss europäischer Unternehmen

Im März 2015 wurden erneut Dokumente veröffentlicht, die eine enge Kooperation des Rats der Europäischen Union und der Digitalökonomie belegen sollten. Insbesondere Deutschland, welches eine maßgebliche Rolle in den Verhandlungen einnahm, näherte sich in seiner Position der Industrie an.[211] Beim direkten Vergleich der US-amerikanischen und europäischen Digitalwirtschaften wird häufig die Meinung vertreten, dass die Europäische Union durch den Datenschutz die internationale Wettbewerbsfähigkeit ihrer Unternehmen und die europäischen IT-Innovationen hemme, es zugleich aber auch nicht-europäischen Unternehmen erschwert werde innerhalb der Europäischen Union zu bestehen. Im Juni 2015 einigte sich der Rat schließlich und veröffentlichte seine Version eines Vorschlags für eine Datenschutz-Grundverordnung. Zahlreiche Datenschutz- und Verbraucherschutzorganisationen kritisieren die endgültige Ratsversion der Verordnung als zu wirtschaftsfreundlich. Einer der Hauptvorwürfe sind die vielen

[210] Merkel 2015.

[211] „Member states have since held protracted internal debates with signs suggesting that Germany is now leading the pack in rolling back key points in the original draft." Nielsen 2015 b.

Schlupflöcher für Unternehmen, die es ihnen ermöglichen, die Daten ihrer Kunden auszuspähen.[212]

Da der ursprüngliche Entwurfsvorschlag der Europäischen Kommission aus dem Jahr 2012 sowohl vom Europäischen Parlament als auch dem Rat der Europäischen Union abgelehnt wurde und beide eigene Entwurfsversionen der Datenschutz-Grundverordnung vorschlugen, begannen Ende Juni 2015 die Trilog-Verhandlungen zwischen allen drei Parteien. Im Dezember 2015 einigten sich das Europäische Parlament, die Europäische Kommission und der Rat der Europäischen Union schließlich auf eine gemeinsame Fassung der Datenschutz-Grundverordnung. Dabei konnte sich der Rat in weiten Teilen mit seinen Vorstellungen durchsetzen.

[212] „AccessNow, a Brussels-based digital rights NGO, in a statement said companies would be allowed to 'collect and repeatedly use citizens' personal information without their knowledge' under article 6.4. The NGO accused ministers of eviscerating the bill by 'introducing so many loopholes it's not even consistent with the EU Charter of Fundamental Rights.' The European Consumer Organisation, Beuc, expressed similar concerns" (EUobeserver, 15.06.2015).

4 FAZIT

Die Verhandlungen um die Datenschutz-Grundverordnung waren äußerst vielschichtig. Es ging nicht nur um den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, wie es Art. 1 der Datenschutz-Grundverordnung letztlich als Ziel der Verordnung vorgibt, sondern weit darüber hinaus. So wurde etwa mitverhandelt, welche Bedeutung Privatheit heute und in Zukunft haben soll und haben kann und welche marktwirtschaftlichen Folgen die Verordnung für europäische Unternehmen haben wird. Außerdem wurden im Kontext der Verhandlungen die Rechtsetzungsprozesse auf europäischer Ebene von einigen Akteuren in den Blick genommen und teilweise stark kritisiert.

Darüber hinaus zeigten sich in den Verhandlungen über die Datenschutz-Grundverordnung auch Machtkämpfe sowohl zwischen den Mitgliedstaaten und der Europäischen Union als auch innerhalb letzterer selbst. In der Wahl der Verordnung als Instrument der Neuregelung des Datenschutzes lag eine Strukturentscheidung bezogen auf die zukünftige Ausgestaltung der Europäischen Union. Dies versuchte die Kommission durch die zahlreichen in ihrem Entwurf enthaltenen Ermächtigungen zu ihren Gunsten noch zu verstärken. Im Kern ging es auch und gerade um die Frage, wer über die Zukunft und Fortentwicklung des Datenschutzes in der Europäischen Union entscheidet sowie bestimmt, wie sich Demokratie und Gewaltenteilung in für die digitale Gesellschaft zentralen Bereichen entwickeln. Hätte sich während der Verhandlungen die Position der Europäischen Kommission oder des Europäischen Parlaments durchgesetzt, wäre dies eine Entscheidung zu Ungunsten der Mitgliedstaaten gewesen. Etabliert wurde aber letztlich eine Ko-Regulierung zwischen Mitgliedstaaten und Europäischer Union, die beiden Seiten gerecht werden sollte. Aufgrund der zahlreichen Übereinstimmungen zwischen Ratsentwurf und finaler Fassung der Datenschutz-Grundverordnung können der Rat und die Mitgliedstaaten letztlich wohl als Sieger in diesen Kämpfen gelten, während die Kommission mit dem Versuch des Ausbaus ihrer Kompetenzen gescheitert ist.[213]

[213] Die Kommission selbst stellt sich jedoch als Gewinnerin dar. So sei ein Machtzuwachs durch delegierte Rechtsakte nie wirklich gewollt gewesen, sondern geschickte Verhandlungstaktik mit dem Ziel, Parlament und Rat unter Druck zu setzen. So die Darstellung von Selmayr/Ehmann in: Ehmann/Selmayr 2017: Einführung Rn. 56.

Auf einer weiteren Ebene ging es schließlich darum, wer in welcher Form von den Möglichkeiten der fortschreitenden Digitalisierung profitiert. Hier fand ein Machtkampf innerhalb der Welt der Digitalwirtschaft statt. Deren wirtschaftliche Interessen stehen häufig mit datenschutzrechtlichen Prinzipien. Trennlinien verliefen unter anderem zwischen Unternehmen der Internetwirtschaft mit datengetriebenen Geschäftsmodellen und sonstigen datenverarbeitenden Unternehmen und Institutionen.

4.1 Datenschutz im gesellschaftlichen Diskurs

Datenschutz steht in einer immer stärker vernetzten und digitalisierten Welt im Zentrum der Debatte um den Schutz von Privatheit und Selbstbestimmung. Ängste bezogen auf Privatheit und Datenverarbeitung richteten sich in den 1980er Jahren vornehmlich gegen den Staat und führten zu starkem Widerstand gegen eine geplante Volkszählung. Hier spielten nicht zuletzt die Erfahrungen der Deutschen im Nationalsozialismus und die zeitgenössische Wirklichkeit einer umfassenden Überwachung der eigenen Bevölkerung durch das Ministerium für Staatssicherheit in der DDR eine Rolle. Mit dem Volkzählungsurteil aus dem Jahre 1983 schuf das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung und sicherte den Schutz personenbezogener Daten damit verfassungsrechtlich ab. In den 1990er Jahren bildeten mit dem „Großen Lauschangriff“ noch optische und akustische Überwachungsmaßnahmen den Schwerpunkt der Debatte um die Privatheit der eigenen Wohnung, während die Debatte um Privatheit in öffentlichen Räumen von der Überwachungskamera dominiert war.

Neu belebt wurden Ängste vor einer umfassenden staatlichen Überwachung im Jahr 2013 durch die Enthüllungen des Whistleblowers Edward Snowden, der die umfangreichen Abhör- und Datensammelaktivitäten anglo-amerikanischer Geheimdienste der breiten Öffentlichkeit bekannt machte.

Neben staatlichen Überwachungsmaßnahmen werden Daten aber vornehmlich von privaten Unternehmen erhoben und ausgewertet, was insbesondere in jüngerer Zeit zu gesellschaftlichen Diskussionen führte. Die Ziele sind hierbei vielfältig und reichen von handfesten Vorteilen für die Nutzer, etwa in Form von Komfort- und Sicherheitsgewinn, über das Anbieten personalisierter Werbung bis hin zur Marktforschung. Hierzu können die betroffenen Personen ihre Einwilligung erteilen oder eine gesetzliche Grundlage ermächtigt die Unternehmen zur Verarbeitung und Auswertung personenbe-

zogener Daten. Besonders greifbare Fokuspunkte der Debatte um Privatheit in einer digitalen Welt sind die Zulässigkeit von verschlüsselter Kommunikation ohne Hintertüren für Sicherheitsorgane und die anonyme Nutzung von Dienstleistungen und Kommunikationsplattformen im Internet. Staatliche und privatwirtschaftliche Interessen stehen hier, wie auch in vielen anderen Fällen, in direktem Widerstreit mit den Interessen und auch mit den Grundrechten der Bürger.

Dies spiegelte sich auch in den Verhandlungen zur Datenschutz-Grundverordnung wider. Wenngleich nicht immer explizit Bezug auf den Datenschutz genommen wurde, fanden sich doch häufig implizite Bezüge, die Aufschluss über die unterschiedlichen Vorstellungen von Datenschutz in der Arena gaben. So fanden sich einerseits individuelle Vorstellungen, die Datenschutz vor allem als Problem des Einzelnen ansehen. Datenschutz wird als ein Aspekt unter vielen betrachtet, den es im (unternehmerischen) Handeln zu berücksichtigen gilt. Ihm wird aber kein übergeordneter Wert beigemessen. Er stellt lediglich einen Faktor unter vielen dar, der wahlweise hinderlich für den gesellschaftlichen Wohlstand oder die unternehmerische Tätigkeit sein kann und dann unter dem Schlagwort „Datenschutz als Innovationsbremse" kursiert, oder aber als ein positiver Aspekt für die Geschäftsinteressen berücksichtigt wird. In diesem Fall wird Datenschutz als Wettbewerbsvorteil deklariert. In diesem Sinne wird der wirtschaftliche Wohlstand mit gesellschaftlichem Wohlstand gleichgesetzt und als dem Allgemeinwohl dienend gerahmt, während Privatheit letztendlich als persönliche Angelegenheit zu einem gewissen Grad auch abdingbar oder zumindest verhandelbar ist. Solche Bezüge finden sich häufig als Argumentationsmuster in wirtschaftsfreundlichen Positionen innerhalb der Arena.

Datenschutz kann aber auch selbst als kollektiver Wert betrachtet werden, der dem Allgemeinwohl dient. Als Voraussetzung für eine freie und offene Gesellschaft muss er demnach verteidigt und beschützt werden. Insbesondere die Argumentationsmuster datenschutzfreundlicher Positionen folgen tendenziell eher diesem Leitbild. Die einzelnen Welten bewegen sich in ihren Positionierungen in der Arena zwischen diesen beiden Polen – einerseits gilt Privatheit als individueller Aspekt, der im Zweifelsfall verhandelbar ist und in Relation zu anderen Ziel- und Wertvorstellungen gesetzt wird; ande-

rerseits wird Privatheit als fester, unverhandelbarer Wert angesehen, der als Kollektivgut dem Allgemeinwohl dienend gerahmt wird.[214]

In der Arena der Datenschutz-Grundverordnung geht es aber um mehr als nur um Datenschutz und Privatheit selbst. Mitverhandelt wurden auch immer bestimmte Vorstellungen, wie man die Gesellschaft gestalten kann. So propagierten viele Ökonomen mit einem „Mehr" an Daten eine prosperierende Wirtschaft und letztendlich ein besseres Leben für die Gesellschaft. Datenschützer sahen wiederum genau in dieser Marktgläubigkeit eine Gefahr und betrachteten Datenschutz selbst als eine grundlegende Bedingung für ein gutes und freies Leben. So zeigten sich in diesen Reaktionen in Zeiten digitaler Krisen letztendlich auch bestimmte Vorstellungen darüber, was Demokratie bedeuten kann.

Je nach Fassung des Datenschutzrechts werden bestimmte Geschäftsmodelle erst ermöglicht oder ausgeschlossen. Die Wirtschaftsinteressen sind jedoch sehr unterschiedlich. Eine deutsche Krankenversicherung wird beispielsweise völlig andere Interessen verfolgen als ein amerikanischer Internetgigant. Gerade auch der Kampf um bessere Wettbewerbsbedingungen europäischer Unternehmen gegenüber den etablierten amerikanischen Großunternehmen bestimmte ganz wesentlich die Auseinandersetzungen um die Datenschutz-Grundverordnung. Somit ging es bei den Verhandlungen auch um Marktchancen und um transatlantischen Wettbewerb. Hinzu kommt, dass sich die Informationstechnik mit einer enorm hohen Geschwindigkeit weiterentwickelt und verändert und nahezu alle Lebensbereiche erfasst. Die Novellierung des Datenschutzrechts stellte damit nicht nur eine Regulierung des Status quo, sondern gewissermaßen eine Neuordnung der digitalen Gesellschaft der Zukunft dar, da gerade auch Technologien erfasst sind, die heute noch nicht bekannt oder noch nicht entwickelt sind. In Zusammenschau mit der hohen Relevanz der Verarbeitung personenbezogener Daten wird deutlich, weshalb hart darum gekämpft wurde, wie die Verarbeitung personenbezogener Daten reguliert wird.

[214] Beide Aspekte finden sich bereits im Volkszählungsurteil des Bundesverfassungsgerichts.

4.2 Die Verhandlungen über die Datenschutz-Grundverordnung und die Zukunft der Demokratie

Zum Gegenstand der Verhandlungen wurde auch die Frage, wie die Aushandlungen selbst von statten gingen, und somit die Frage nach der Art und Weise politischer Entscheidungsprozesse. Immer wieder wurden Stimmen laut, die mehr Transparenz dieser Prozesse forderten. Die legislativen Verfahren der Europäischen Union und insbesondere das Trilogverfahren standen wegen der intransparenten Einflussnahme verschiedener Interessenvertreter auf Politiker in der Kritik. Aber auch die Modalitäten des Trilogs selbst wurden kritisiert:

„It is difficult to find out when trilogues are taking place, what is being discussed and by whom without a great deal of time and effort. (…) Making this information available should enable citizens to hold their representatives to account and to engage effectively in the legislative process." (Emily O'Reilly, Bürgerbeauftragte der Europäischen Union)[215]

Zahlreiche Lobbyisten versuchten in den Verhandlungen in Hinterzimmern zu agieren und sich der öffentlichen Sichtbarkeit zu entziehen. Die Lobbyindustrie setzte dabei verschiedene Strategien ein. Ein fester Bestandteil dieser Strategien bestand in regelmäßigen Gesprächen mit Politikern, um so Einfluss auf den Prozess nehmen zu können. Stellt Interessenvertretung auf EU-Ebene zunächst keinen ungewöhnlichen Vorgang dar, wird diese jedoch dann problematisch, wenn es einen Überhang wirtschaftlicher Einflussnahme gibt und die Prozesse der Einflussnahme intransparent sind.[216] Durch die im Vergleich zu zahlreichen Datenschutzorganisationen finanziell weitaus besser ausgestattete[217] und gut vernetzte Lobbyindustrie der Digitalwirtschaft kam es zu einem Ungleichgewicht der Einflussnahme. Die Intransparenz der zahlreichen Einflussnahmen unterläuft dabei die institutionellen Mechanismen der demokratischen Entscheidungsfindung. Während die politischen Institutionen formell zu funktionieren scheinen, fallen die eigentlichen Entscheidungen zum Teil hinter verschlossenen Türen. Wer gehört wird und wessen Stimmen zählen, folgt keinem geregelten Prozess, sondern hängt zu einem großen Teil von der Ausstattung mit Ressourcen

[215] Ombudsman Europa 2016.

[216] Griesser 2014.

[217] Zahlen für die Ausgaben der verschiedenen Interessenvertretungen in Brüssel lassen sich dem EU-Transparenzregister entnehmen.

ab. Dieser Modus der Demokratie wird auch Postdemokratie genannt.[218] Postdemokratische Züge trug etwa auch der Entwurf der Europäischen Kommission zur Datenschutz-Grundverordnung, der letztlich der Kommission die Herrschaft über die Zukunft des Datenschutzes in Europa zugesprochen hätte. Deren demokratische Legitimation ist jedoch nur vergleichsweise schwach ausgeprägt. Eine Beteiligung von Parlament und Rat wäre bezogen auf zentrale Fragen nicht mehr notwendig gewesen, wäre der Kommissionsentwurf Gesetz geworden.

Postdemokratische Tendenzen sind indes kein Alleinstellungsmerkmal der Europäischen Union, sondern sind etwa auch in der Bundesrepublik zu beobachten. Diese zeigten sich etwa in der Art und Weise, wie bestimmte richtungsweisende Gesetze mit Relevanz für den Datenschutz auf nationaler Ebene verabschiedet wurden. Eines der prominentesten Beispiele dürfte hier die Abstimmung im Deutschen Bundestag zum Gesetz zur Fortentwicklung des Meldewesens während des Halbfinalspiels zwischen Deutschland und Italien im Rahmen der Fußball-Europameisterschaft im Jahr 2012 sein.

Es gab aber auch Gegenbewegungen in der Arena. Einige Akteure stellten sich der Intransparenz des Gesetzgebungsverfahrens nicht nur auf diskursiver Ebene, sondern auch praktisch entgegen: Die Praktik des Leaking wurde benutzt, um öffentliche Sichtbarkeit zu erzeugen und verschiedene soziale Welten um den Gegenstand der Datenschutz-Grundverordnung zu versammeln. Datenschützer (insbesondere Aktivisten und Verbraucherschützer), aber auch die einige der unmittelbar am Gesetzgebungsprozess Beteiligten selbst, versuchten der Unsichtbarkeit im Aushandlungsprozess entgegen zu wirken. Sie plädierten in ihren Stellungnahmen immer wieder für mehr Transparenz in den Verhandlungen rund um die Datenschutz-Grundverordnung und initiierten durch die Veröffentlichung von Leaks auch auf praktischer Ebene eine Gegenbewegung.

Die Zuschreibung von Verantwortlichkeiten, Legitimität und Illegitimität bestimmter Praktiken in den Medien, in diesem Fall der Praktiken des Wirtschaftslobbyismus, wirkt sich auf die Meinungsbildung der Bürger aus. Somit können die Attributionshandlungen der medialen Berichterstattung in Demokratien aufgrund von Wahlentscheidungen mittelbare Konsequenzen auf politische Entscheidungsprozesse haben. Die Unterstützung solcher

[218] Vgl. Blühdorn 2006, Crouch 2008, Lamla 2013.

Praktiken durch Politiker kann potentiell zu einem negativen Einfluss auf die Karriere- und Machtchancen der Amtsinhaber führen.[219] Die Medienöffentlichkeit wurde in diesem Sinne als Ressource genutzt, nicht nur um öffentlichen Druck auf die Politiker und Akteure der Digitalökonomie zu erzeugen, sondern auch um verschiedene Akteure um das Verhandlungsobjekt der Datenschutz-Grundverordnung versammeln zu können, die sonst nicht Teil des Diskurses gewesen wären.[220]

Der Hinweis auf interne Probleme demokratischer Verfahrensweisen war eine Art Korrekturversuch. In dieser Vorgehensweise findet sich ein weiterer Demokratiemodus, der hier aktiviert wird. Dieser Modus weist auf interne Probleme der Demokratie hin, wie in diesem Fall die Regulierungsdefizite von Interessensvertretungen der Europäischen Union, und beruft sich dabei auf höhere Instanzen der Demokratie. Geltende Verfahrensordnungen und Rechtskonstruktionen werden jedoch nicht überschritten, vielmehr werden Lern- und Anpassungsprozesse der Demokratie forciert. Solch ein konstitutionalistischer Demokratiemodus[221] hält nach wie vor an institutionellen Routinen fest, ist aber um interne Reformen bemüht. Der Verhandlungsprozess oszilliert häufig zwischen diesen beiden Demokratiemodi – auf der einen Seite postdemokratische Tendenzen und auf der anderen die Aktivierung konstitutionalistischer Momente.

Die Verhandlungen beschränken sich jedoch nicht nur auf eine Oszillation dieser beiden Modi der Demokratie. Es findet sich ein dritter demokratischer Aushandlungsmodus, der die Arena mitprägt – ein demokratischer Protektionismus.[222] Dieser Demokratiemodus zeichnet sich durch ein Verharren in territorialen Logiken und politischen Routinen aus, die darauf abzielen den Status Quo der Demokratie beizubehalten. Beobachtbar wird er immer dann, wenn in den Verhandlungen die Gefahren für die Demokratie außerhalb der eigenen Institutionen und Gemeinwesen lokalisiert werden – sei es in Form ausländischer Konkurrenz oder einer als übermächtig empfundenen Europäischen Union, vor denen wahlweise der europäische Wirt-

---

219 Gerhards/Offerhaus/Rosse 2009: 552.

220 Leaks spielten in den Verhandlungen eine zentrale Rolle, dienten sie gerade für die Befürwortern eines starken Datenschutzes als Möglichkeit, Öffentlichkeit zu erzeugen, in der Debatte Gehör zu finden und die Routinen der Hinterzimmerpolitik kurzzeitig zu durchbrechen. Das Gesetzgebungsverfahren wurde dabei nicht an sich angezweifelt, sondern die Art und Weise, wie es ausgeführt wurde.

221 Lamla/Ochs 2016.

222 Ebda.

schaftsraum oder die nationalstaatliche Souveränität beschützt werden müssen. Insbesondere die Aktivierung institutioneller Logiken des Schutzes und Bewahrens nationaler Rechtssetzungen oder Wirtschaftsweisen einiger Nationalstaaten weisen ein solches Muster auf und zielen darauf ab, die Harmonisierungs- und Integrationsbestrebungen der Europäischen Union zu unterlaufen. Dabei wird auch die Frage aufgeworfen, welcher Wert höher zu bemessen ist – die Harmonisierung des europäischen Datenschutzes oder ein hohes Datenschutzniveau – denn nicht immer lassen sich beide Ziele vereinen.

Zu beobachten ist, dass insbesondere Deutschland bewahrende und damit auch machterhaltende Bestrebungen durch inhaltliche Argumentation zu untermauern suchte und dabei gerade im Kontext der notwendigen Neufassung des Bundesdatenschutzgesetzes als Reaktion auf die Datenschutz-Grundverordnung nicht selten darauf verwies, durch Abweichungen von Vorgaben der Grundverordnung und dem Ausnutzen von (teilweise umstrittenen) Regelungsspielräumen das hohe deutsche Datenschutzniveau bewahren zu wollen. Dass dabei auch faktische Absenkungen des Datenschutzniveaus unter das der Datenschutz-Grundverordnung mit diesem Verweis legitimiert werden sollten, macht deutlich, dass es sich zumindest auch um ein vorgeschobenes Argument handelte. Umgekehrt wird Verfechtern nationaler Abweichungen und Korrekturen der Grundverordnung auf nationaler Ebene nicht selten eine antieuropäische Grundhaltung unterstellt.

Letztlich ist unklar, ob der Qualität des Datenschutzes in Europa besser durch Vereinheitlichung (auch unter Inkaufnahme einer Absenkung des Schutzniveaus unter das Niveau vor Geltungsbeginn der Datenschutz-Grundverordnung) oder durch nationale Abweichungen gedient ist. Darüber hinaus stellen sich Fragen der Adäquanz des neuen europäischen Regelwerks, das in nur wenigen Artikeln materiellen Datenschutzrechts die teilweise hochkomplexen, risikoadäquaten und historisch gewachsenen nationalen Regelungen abzulösen versucht.

Wenngleich weitgehend Einstimmigkeit bezüglich der Notwendigkeit einer Erneuerung der EU-Datenschutzrichtlinie 95/46/EG bestand, so waren sich die Nationalstaaten in der Art und Weise sowie dem Ausmaß transnationaler Regelungen und somit beim Eingriff in nationale Rechtsvorschriften keineswegs einig. Dabei teilen die einzelnen Nationalstaaten nicht alle diesel-

ben Interessen,[223] vielmehr sind es gerade deren Heterogenitäten, die einen Kompromiss erschweren, aber auch überhaupt erst notwendig machen, und letztendlich in protektionistische Bestrebungen umschlagen. So zeigt sich insbesondere an den zahlreichen Öffnungsklauseln in der endgültigen Fassung der Datenschutz-Grundverordnung die partielle Durchsetzung territorialer Logiken sowie der Schutz erreichter politischer Errungenschaften. Ein wichtiger Aspekt der Verhandlungen um die Datenschutz-Grundverordnung war damit der Kampf zwischen den Nationalstaaten und der Europäischen Union um Machterhalt und die Durchsetzung eigener politischer Strömungen.

Letztendlich bleibt abzuwarten wie sich die Suchbewegungen zwischen verschiedenen Demokratiemodi wie dem demokratischen Konstitutionalismus, der Postdemokratie und dem demokratischen Protektionismus weiterentwickeln und ob sich einer diese Demokratiemodi schließlich durchsetzen wird, oder ob sich nicht eine ganz neue Form jenseits dieser idealtypischen Heuristik herausbildet, zwischen denen freilich auch fließende Übergänge bestehen. So erachtet die Europäische Union die Integration auf Basis des Neoliberalismus als erstrebenswert, das Festhalten an grundrechtlichen Errungenschaften jedoch als rückschrittlich.

Wenngleich die Datenschutz-Grundverordnung bereits verabschiedet wurde, so bedeutet dies noch keineswegs ein Ende der Verhandlungen. Vieles bleibt in der Verordnung ungeregelt und damit entweder den Mitgliedstaaten in Form von Regelungsaufträgen und Regelungsoptionen oder den Aufsichtsbehörden überlassen. Das letzte Wort in allen Fragen zum Datenschutz in der Europäischen Union wird aber der Europäische Gerichtshof haben – die Kämpfe in der Arena und mit ihr der Kampf um die Zukunft der Privatheit und Demokratie gehen weiter.

[223] Was das zugrundeliegende Schutzgut sein soll, ist dabei keineswegs unumstritten und kann somit variieren – etwa in Form eines nationalen Wirtschaftsprotektionismus oder dem Schutz der freiheitlich demokratischen Grundordnung.

5 AUSBLICK

Die Datenschutz-Grundverordnung ist mit den Zielen einer umfassenden Modernisierung und Harmonisierung des Datenschutzes in Europa angetreten. Folgende Probleme sollen durch die Datenschutz-Grundverordnung adressiert werden:

- Das Datenschutzrecht in Europa gleicht bisher, trotz des durch die Datenschutzrichtlinie bereitgestellten gemeinsamen Rahmens, einem Flickenteppich.
- Unternehmen wählten in der Vergangenheit ihre Firmensitze so, dass sie besonders strenge Datenschutzvorschriften umgehen konnten.
- Neue Technologien lassen das Datenschutzrecht unter erheblichen Druck geraten, denn sie erfordern eine stetig zunehmende Erfassung und Nutzung von Daten.
- Mit Daten lässt sich viel Geld verdienen. Einige datenverarbeitende Unternehmen haben einen höheren Unternehmenswert als klassische Industriegiganten. Zwischen den Nutzern datengetriebener Dienste und ihren Anbietern besteht ein erhebliches ökonomisches wie auch informationelles Ungleichgewicht. Diese klassischen Unternehmen wollen indes zunehmend auch selbst an den bei ihnen anfallenden Daten verdienen.
- Gesammelte Daten aus den unterschiedlichsten Quellen können zu detaillierten Profilen einzelner Personen verknüpft werden. Oft reicht es sogar aus, über Daten Dritter auf die Lebensumstände und Interessen einer Person zu schließen – mit zunehmender Genauigkeit.

Die Schwierigkeiten des Aushandlungsprozesses um die Datenschutz-Grundverordnung werden insofern im Ergebnis deutlich, als die Ziele der Verordnung nur teilweise erreicht wurden. Auf der einen Seite machen drakonische Sanktionen Druck auf Unternehmen, datenschutzrechtliche Vorgaben genau zu beachten. Zudem werden die Stellung der Aufsichtsbehörden in der Europäischen Union verbessert und die Rechte und Beschwerdemöglichkeiten des Einzelnen gestärkt. Auf der anderen Seite werden jedoch konzeptionelle Probleme des Datenschutzrechts perpetuiert.

Im Zuge der Datenschutz-Grundverordnung kommen viele Änderungen, neue Herausforderungen und zusätzliche Kosten auf deutsche und europäische Unternehmen zu. Darüber hinaus werden sich die bisherigen Regeln des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes wesentlich verändern, sodass für die Unternehmen der Digitalwirtschaft eine enorme Planungsunsicherheit entsteht. Sie müssen ihre Geschäftsprozesse grundlegend auf Kompatibilität mit den neuen rechtlichen Vorgaben und Rahmenbedingungen prüfen, was Investitionsrisiken birgt. Die neuen Vorschriften führen in vielen Bereichen zu erheblichen Pflichten und zusätzlichen Belastungen wie der Datenschutz-Folgenabschätzung, mehr Dokumentations- und Informationspflichten sowie dem Recht der Verbraucher auf Datenübertragbarkeit. In anderen Bereichen entfallen frühere Grundsätze wie risikospezifische Betroffenenrechte bei Ausnahmen der Pflichten der Verantwortlichen oder die Risikoorientierung bei der Zulässigkeit der Datenverarbeitung. Daraus folgt, dass die Pflichten der Datenschutz-Grundverordnung viele Verantwortliche nicht treffen werden. In anderen Bereichen wiederum ist der Unterschied zur bisherigen datenschutzrechtlichen Praxis jedoch eher gering. Diese Probleme, die Unterkomplexität der Verordnung sowie ihre Technikneutralität führen im Ergebnis zu einer enormen Rechtsunsicherheit. Diese Unsicherheit ist als größter Nachteil der Verordnung anzusehen, der zumindest zunächst schwerer wiegt, als der Vorteil einer Vereinheitlichung im Bereich des europäischen Datenschutzrechts. Die höheren Bußgelder bei Verstößen gegen die Verordnung bergen für Unternehmen ein größeres wirtschaftliches Risiko.[224] Diesen Herausforderungen müssen sich aber nicht nur europäische Unternehmen stellen, sondern alle in der Europäischen Union agierenden Unternehmen. Dies ist auf die Einführung des Marktortprinzips zurückzuführen, welches vorsieht, dass das europäische Datenschutzrecht auch von Unternehmen aus dem EU-Ausland beachtet werden muss, wenn diese innerhalb der Europäischen Union personenbezogene Daten verarbeiten und nach Art. 3 Abs. 2 DSGVO entweder Dienstleistungen oder Waren innerhalb der Europäischen Union anbieten oder das Verhalten betroffener Personen beobachten.

Darüber hinaus sind konkrete Aussagen zur Implementierung der Datenschutz-Grundverordnung derzeit kaum möglich. Der Bundestag hat am 27.

[224] Vgl. Art. 83 DSGVO.

April 2017 ein neues Bundesdatenschutzgesetz beschlossen, dem der Bundesrat am 12. Mai 2017 zugestimmt hat.[225] Das Gesetz wurde am 5. Juli 2017 veröffentlicht[226] und tritt am 25. Mai 2018 in Kraft. Damit sollen zum einen die (vermeintlichen) Spielräume, die die Grundverordnung dem nationalen Gesetzgeber durch die zahlreichen Öffnungsklauseln[227] lässt, genutzt werden. Zum anderen soll damit zu mehr Rechtssicherheit beigetragen werden. Der Entwurf wurde ähnlich kontrovers begleitet wie die Verordnung selbst, von verschiedenen Seiten teils heftig kritisiert und auch vielfach nachgebessert. Ob seine Regelungen vor dem Europäischen Gerichtshof bestehen können, bleibt aber abzuwarten. Die Europäische Kommission hat bereits im Entstehungsprozess des neuen Gesetzes mit einem Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland gedroht.[228] Viele der in der Verordnung verwendeten unbestimmten Rechtsbegriffe bedürfen einer Klärung durch den Europäischen Gerichtshof. Es wird daher vermutlich Jahre dauern, bis im Hinblick auf die Datenschutz-Grundverordnung Klarheit und Rechtssicherheit besteht.

„(...) Aufgrund der Unterkomplexität der Unionsregelungen sind mitgliedstaatliche Präzisierungen, Ausfüllungen und Ergänzungen notwendig, um die Verordnung problemadäquat und damit auf die faktischen Probleme, die es zu bewältigen gilt, anwendbar zu machen. In der Folge ist die Datenschutz-Grundverordnung kein homogenes, in sich geschlossenes Gesetzeswerk für den Datenschutz in der Union, sondern gleicht eher einem ‚Schweizer Käse', der zwar einige strukturierende Elemente aufweist, vor allem aber durch die Löcher dazwischen auffällt. Anders als bei einem Schweizer Käse, werden diese Löcher aber unterschiedlich gefüllt werden. In der Folge wird kein einheitliches Datenschutzrecht in allen Mitgliedstaaten zur Anwendung kommen, sondern vergleichbar viele Unterschiede wie zuvor unter der Datenschutz-Richtlinie – nur an anderen Stellen und mit erheblicher Rechtsunsi-

[225] Krempl 2017 b; Hülsmann 2017.

[226] Gesetz zu Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zu Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017, BGBl. I Nr. 44.

[227] Öffnungsklauseln ermöglichen es den Mitgliedstaaten in bestimmten Bereichen eigene Vorschriften beizubehalten oder zu erlassen. Ihre Reichweite (und sogar ihre Existenz) ist jedoch Gegenstand einer intensiven Debatte.

[228] Krempl 2017 a unter Verweis auf Äußerungen von Renate Nikolay, der Kabinettschefin der Justizkommissarin.

cherheit. (...)"(Prof. Dr. Alexander Roßnagel, Leiter des Fachgebiets Öffentliches Recht mit Schwerpunkt Recht der Technik und des Umweltschutzes)[229]

„Viele Regelungen der neuen Datenschutzverordnung sind so allgemein formuliert, dass nicht auf den ersten Blick klar ist, wie sie in der Praxis umgesetzt werden sollen. Das wird in der Anfangszeit zu einer gewissen Rechtsunsicherheit führen." (Susanne Dehmel, Mitglied der Geschäftsleitung Vertrauen und Sicherheit Bitkom e.V.)[230]

„Die Datenschutz-Grundverordnung erweitert den Anwendungsbereich des Datenschutzes, lässt zugleich aber eine für die Digitalwirtschaft notwendige Risikodifferenzierung komplett außer Acht. Das Internet als wirtschaftlicher Wachstumsmotor wird im Ergebnis überreguliert, die Wettbewerbsfähigkeit Europas im globalen Wettbewerb deutlich begrenzt. Zusätzlich führt die Reform zu einer stärkeren Überforderung der Nutzer und zu mehr Bürokratisierung. Der Datenschutz verliert zugleich an Effektivität. Anstelle ausgewogener Konzepte für echte 'privacy by design' bleibt nach wie vor die Einwilligung der Nutzer maßgeblich. Bereits erfolgreiche Ansätze wie Pseudonymisierung und Verschlüsselung sind nicht ausreichend implementiert." (Bundesverband Digitale Wirtschaft e.V.)[231]

„Das Projekt der Modernisierung des europäischen Datenschutzes ist aufgrund der Gegenwehr einiger Industriegruppen, die lieber im letzten Jahrhundert verharren wollen, leider nur teilweise geglückt. (...) Auch bedauern wir, dass es nicht gelungen ist, den schwammigen Begriff des 'berechtigten Interesses' für eine Datenverarbeitung zu reformieren. Wir sind jedoch froh, dass zumindest einige Schutzmaßnahmen ergänzt wurden. Schwerwiegender ist, dass das Vorhaben, den Datenschutz in der EU zu harmonisieren, in sein Gegenteil verkehrt wurde. Die Anzahl der Ausnahmetatbestände in der jetzigen Verordnung ist größer als die der eigentlichen Artikel in der bisher gültigen Richtlinie von 1995. (...)"(Gemeinsame Stellungnahme von European Digital Rights, Bits of Freedom, Digital Rights Ireland, Privacy International und Digitale Gesellschaft e.V.)[232]

229 Roßnagel 2016.
230 Bitkom 2016.
231 BVDW 2016.
232 Tripp 2015.

„Das Ja zur EU-Datenschutzverordnung ist eine gute Nachricht für Verbraucher und Unternehmen. Endlich gelten europaweit einheitliche und zeitgemäße Spielregeln beim Datenschutz." (Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands)[233]

„Leider zeigt der verabschiedete Kompromiss zur Datenschutz-Grundverordnung mit aller Deutlichkeit, dass der europäische Gesetzgeber die Zeichen der Zeit nicht in allen Facetten erkannt hat. Sie stellt einen realitätsfernen, einwilligungsbasierten 'One size fits all'-Ansatz dar, der erhebliche Hürden für entgeltfreie Dienste, also den Kern des Internets, schafft." (Thomas Duhr, Vizepräsident Bundesverband Digitale Wirtschaft e.V.)[234]

„Nach allem, was wir über den hinter verschlossenen Türen ausgehandelten und unter massivem Lobbyisteneinfluss geschlossenen Deal wissen, wird er nur in Einzelbereichen den Datenschutz stärken, in wichtigen Teilen aber das derzeitige Datenschutzniveau absenken: So wird das bisherige deutsche Verbot einer Protokollierung unseres Surfverhaltens im Netz durch Internet- und Medienkonzerne aufgegeben. Die offene Videoüberwachung von Büros soll weitreichend erlaubt werden – bisher war das in Deutschland nur in engen Grenzen als letztes Mittel zulässig. Außerdem soll gegen die Erstellung von Verbraucherprofilen nur ein Widerspruchsrecht bestehen." (Patrick Breyer, Piratenpartei, MdL Schleswig Holstein)[235]

233 vzbv 2016.
234 Kemper 2016: S. 9.
235 Breyer 2015.

6 ANHANG: TIMELINE

6.1 2010

4. November

- Vorstellung eines neuen Gesamtkonzeptes für den Datenschutz in der Europäischen Union durch die EU-Kommission nach einem mehrmonatigen öffentlichen Konsultationsprozess
- Ziele des Gesamtkonzeptes:
  - ✓ Überarbeitung der Datenschutzrichtlinie (RL 95/46/EG) vom 24.10.1995
  - ✓ Schutz der Daten des Einzelnen in allen Bereichen einschließlich der Strafverfolgung
  - ✓ Sicherstellung der Transparenz der Datenverarbeitung
  - ✓ Dauerhafte Löschung und Sperrung der Daten im Internet
  - ✓ Verpflichtung von Unternehmen zur Integration datenschutzfreundlicher Technologien in ihre Produkte
- Auf Grundlage des Gesamtkonzepts: nach Durchführung einer Folgenabschätzung und unter Berücksichtigung der EU-Grundrechtecharta Entstehung eines Vorschlags von Rechtsvorschriften im Jahr 2011
- Bitte an die EU-Mitgliedstaaten um Rückmeldung zum Gesamtkonzept

November 2010 bis Dezember 2011

- Durchführung einer europaweiten öffentlichen Anhörung zum Datenschutz und zur Überarbeitung der Datenschutzrichtlinie (RL 95/46/EG)

6.2 2011

November 2011

- Eine vorläufige Fassung einer Datenschutzverordnung wird über das Internet öffentlich bekannt (Version 56 (29/11/2011))

- Unter anderem starke Kritik seitens datenverarbeitender Unternehmen gegen die Einführung einer Datenschutz-Grundverordnung

Dezember 2011

- EU-Kommission: Zugänglichmachung des Entwurfs einer Datenschutz-Grundverordnung des Parlaments und des Rates zum allgemeinen Datenschutz nur für die am Rechtswerdungsprozess Beteiligten
- Der „eigentliche" Entwurf einer Datenschutz-Grundverordnung gelangt über das Internet an die Öffentlichkeit

6.3 2012

25. Januar

- Viviane Reding (seinerseits EU-Kommissarin für Justiz) stellt den Entwurf der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vor
  - ✓ Vorschlag von Änderungen gegenüber dem bisherigen Rechtsrahmen im Bereich des Datenschutzes (Datenschutzrichtlinie RL 95/46/EG)
  - ✓ Im Entwurf einer Datenschutz-Grundverordnung: Berücksichtigung von Veränderungen der Digitalisierung (Datenschutzrichtlinie war bereits vor der Entstehung teilweise veraltet)
  - ✓ Datenschutzrichtlinie: Hauptgedanke war die Vereinheitlichung der Regelungen innerhalb der Mitgliedstaaten; Ergebnis: eher Kakophonie der Gesetzeslage in den Mitgliedstaaten
  - ✓ Hauptgedanke des Entwurfs einer Datenschutz-Grundverordnung ist die Beseitigung des paneuropäischen Wirrwarrs beim Grundrechteschutz und insbesondere beim Datenschutz

28. März

- Beschluss des Innenausschusses des Bundestages über eine öffentliche Anhörung zum Thema „EU-Datenschutzreform"

30. März

- Erhebung einer Subsidiaritätsrüge gegen den Entwurf für eine Datenschutz-Grundverordnung durch den Bundesrat

9. und 10. Oktober

- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE): Durchführung einer interparlamentarischen Expertenanhörung

18. Oktober

- Entwurf einer Stellungnahme des Rechtsausschusses zum Vorschlag für eine Datenschutz-Grundverordnung für den LIBE
- Kernpunkte:
  - ✓ Stärkung des Datenschutzes bei Kindern: Erweiterung des Anwendungsbereiches des Art. 8 auf alle Güter und Dienstleistungen, nicht nur auf Dienstleistungen der Informationsgesellschaft
  - ✓ Streichung des Art. 18 (Recht auf Datenübertragbarkeit), da kein Mehrwert gegenüber Art. 15 (Auskunftsrecht)
  - ✓ Forderung nach Einführung eines allgemeinen Grundsatzes der Rechenschaftspflicht
  - ✓ Stärkung des „Rechts auf Vergessenwerden"
- Enthält 71 Änderungsanträge

6. November

- Stellungnahme des Deutschen Bundestages zum Vorschlag einer Datenschutz-Grundverordnung auf Initiative von CDU/CSU und FDP

6.4 2013

9. und 10. Januar

- Veröffentlichung und Vorstellung eines ca. 200 Seiten umfassenden Berichtsentwurfs mit Änderungsvorschlägen zur Datenschutz-Grundverordnung durch Jan Philipp Albrecht (für den Datenschutz zuständiger Berichterstatter des EU-Parlaments) v. 17.12.2012

- Johannes Masing (für den Datenschutz zuständiger Richter am Bundesverfassungsgericht) kritisiert grundsätzlich das Vorhaben der Europäischen Kommission
- Kernpunkte der Kritik:
  - ✓ Verlust der Wirkung der Grundrechte im Grundgesetz im Wirkungsbereich der Datenschutz-Grundverordnung (bei Akzeptanz des Vorrangs des Europarechts)
  - ✓ Einschränkung der Entscheidungsbefugnis des Bundesverfassungsgerichts

Januar bis Oktober

- Fraktionen im EU-Parlament: Beratung in den zuständigen Ausschüssen und Einbringung von Änderungswünschen im Hinblick auf den Berichtsentwurf von Jan Philipp Albrecht
- Überarbeitung des ersten Entwurfs einer Datenschutz-Grundverordnung unter Federführung von Jan Philipp Albrecht unter Berücksichtigung von über 3000 Änderungsanträgen

6. Juni

- Tagung des EU-Ministerrats zur Datenschutz-Grundverordnung
- Eine generelle Einigung über die Datenschutz-Grundverordnung ist nicht in Sicht
- Kernpunkte der Kritik:
  - ✓ Fehlen von Regelungen zu modernen Techniken wie Apps oder Cloud Computing
  - ✓ Fehlen von konkreten Bestimmungen für Meinungsäußerungen in sozialen Netzwerken und Quellenschutz für Journalisten
  - ✓ Fehlen von Regelungen zum anonymen Anlegen von Nutzerprofilen
- Der Entwurf einer Datenschutzverordnung scheitert im Rat der Europäischen Union

21. Oktober

- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE): Abstimmung über das Verhandlungsmandat des EU-Parlaments zur Da-

tenschutz-Grundverordnung (49 Ja-Stimmen, 1 Gegenstimme, 3 Enthaltungen)

- LIBE: Annahme des Entwurfs zur Änderung der durch die EU-Kommission vorgelegten Datenschutz-Grundverordnung
- Kernpunkte der Neuerungen im Entwurf:
  - ✓ Schaffung eines umfassenden Verbots auf Datenweitergabe ohne rechtliche Grundlage
  - ✓ Wiederaufnahme der „FISA-Klausel"
  - ✓ „Profiling" nur unter Einwilligungsvorbehalt des Betroffenen
  - ✓ Verschärfte Sanktionen
  - ✓ Pflicht zur Bereitstellung eines Betriebsdatenschutzbeauftragten bei Verarbeitung von Daten von mehr als 5000 Betroffenen innerhalb eines Jahres

6. Dezember

- Treffen des Rats der Innen- und Justizminister in Brüssel
- Keine Einigung hinsichtlich des Entwurfs einer Datenschutz-Grundverordnung

6.5 2014

12. März

- Beschluss des Plenums des EU-Parlaments: Bestätigung der formellen Fassung des Ausschusses LIBE v. 21.10.2013 ohne Änderungen in der 1. Lesung (621 Ja-Stimmen, 10 Gegenstimmen, 22 Enthaltungen

6.6 2015

März

- Herausgabe einer Synopse der konsolidierten Fassung der Datenschutz-Grundverordnung auf 630 Seiten durch den EU-Rat

8. Juni

- EU-Rat stellt seine Position zur Datenschutz-Grundverordnung in der neuesten konsolidierten Fassung zusammen

15. Juni

- Einigung im EU-Rat über die Datenschutz-Grundverordnung
- Veröffentlichung des aktuellen Entwurfs für eine Datenschutz-Grundverordnung „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) vom 11.06.2015
- Beginn des Trilogs mit dem EU-Parlament und der EU-Kommission

17. Juni

- Herausgabe von drei Stellungnahmen zu drei unterschiedlichen Entwürfen sowie einen ausführlichen Annex einer Datenschutz-Grundverordnung durch die Art. 29-Datenschutzgruppe
- Kernpunkte der Stellungnahmen:
  - ✓ Feststellung eines Fortschritts und der Modernisierung im Bereich des Datenschutzes in der Europäischen Union
  - ✓ Neue Vorschriften sollen das jetzige Datenschutzniveau nicht senken oder die Kernprinzipien nicht untergraben
  - ✓ Vorgeschlagene Regelungen im Entwurf einer Datenschutz-Grundverordnung beziehen sich ausschließlich auf den Bereich der Strafverfolgung, nicht auf die Sicherung der öffentlichen Ordnung. Folge: Senkung des Datenschutzniveaus und Erhöhung der Anzahl der Regulierungsbehörden
  - ✓ Forderung nach Einklang von Datenschutzrichtlinie und Datenschutz-Grundverordnung im Hinblick auf Definitionen, Prinzipien, Individualrechte und Befugnisse der Aufsichtsbehörden

24. Juni

- Herausgabe einer Synopse der drei Fassungen der Datenschutz-Grundverordnung durchs Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

- Kontrastierung des Vorschlags der EU- Kommission für eine Datenschutz-Grundverordnung mit den jeweiligen Beschlüssen des EU-Parlaments und des EU-Rates

Juni bis November

- Trilog-Verhandlungen zu Kapiteln I bis XI
- 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) - Preparation for trilogue - whole Regulation, 2012/0011 (COD), 14318/15 v. 27.11.2015

27. Juli

- Herausgabe einer Empfehlung einschl. Annex zur Datenschutz-Grundverordnung durch Giovanni Buttarelli (EU-Datenschutzbeauftragter)

Dezember 2015

- Planung einer konsolidierten Fassung der Datenschutz-Grundverordnung

15. Dezember

- Einigung bei den Trilog-Verhandlungen zwischen EU-Kommission, EU-Parlament und EU-Rat auf die neue Datenschutz-Grundverordnung

17. Dezember

- Zustimmung des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) zur letzten Fassung der Datenschutz-Grundverordnung

18. Dezember

- Zustimmung des Ausschuss der ständigen Vertreter der Mitgliedstaaten (COREPER) zur letzten Fassung der Datenschutz-Grundverordnung

6.7 2016

28. Januar

- Veröffentlichung einer ersten vorläufigen deutschen Fassung der Datenschutz-Grundverordnung durch den EU-Rat

12. Februar

- Politische Einigung über den Entwurf für eine Stellungnahme zur Datenschutz-Grundverordnung

17. März

- Veröffentlichung des Entwurfs für eine Stellungnahme zur Datenschutz-Grundverordnung

08. April

- Festlegung des Standpunktes des EU-Rats in der ersten Lesung im Hinblick auf den Erlass der Datenschutz-Grundverordnung, der vollständig dem Kompromisstext entspricht, auf den sich der EU-Rat und das EU-Parlament geeinigt hatte

11. April

- Mitteilung der EU-Kommission an das EU-Parlament über die Akzeptanz des Standpunktes des EU-Rates zur Datenschutz-Grundverordnung

14. April

- Die Datenschutz-Grundverordnung wurde vom EU-Parlament angenommen
- Nach einer Übergangszeit von 20 Tagen nach der Veröffentlichung, tritt die Datenschutz-Grundverordnung in Kraft (25.05.2016)
- Beginn der zweijährigen Übergangsphase bis zum Wirksamwerden der Datenschutz-Grundverordnung am 25.05.2018. In dieser Zeit müssen die EU-Mitgliedstaaten ihre Rechtsordnung an die Verordnung anpassen

21. April

- Text der Datenschutz-Grundverordnung wurde im EU-Rat verabschiedet und an das EU-Parlament zur Billigung weitergeleitet

27. April

- Finale Unterzeichnung der Datenschutz-Grundverordnung und Ende des Verfahrens

04. Mai

Veröffentlichung der Datenschutz-Grundverordnung im EU-Amtsblatt (ABl. L 119)

25. Mai

- Inkrafttreten der Datenschutz-Grundverordnung
- Die Frist zur nationalen Umsetzung der Datenschutz-Grundverordnung endet am 25.05.2018 und löst zu diesem Zeitpunkt die bisher geltende Datenschutzrichtlinie ab

LITERATUR

Ackermann, Astrid (2016): Geändertes Gesetz: Datenschutz nun auch Verbraucherschutz, 24.06.2016, https://www.datenschutzbeauftragter-info.de/geaendertes-gesetz-datenschutz-nun-auch-verbraucherschutz/ [zuletzt geprüft am 15.02.2017].

Al-Serori, Leila/Brunner, Katharina/Fürst, Dominik/Munzinger, Hannes (2017): Brexit: Wie es weitergeht, Süddeutsche Zeitung, 30.03.2017, http://www.sueddeutsche.de/politik/ueberblick-brexit-wie-es-weiter geht-1.3364145 [zuletzt geprüft am 15.02.2017].

Arndt, Hans-Wolfgang/Fetzer, Thomas/Fischer, Kristian (2015): Europarecht, 11. Auflage, Heidelberg: C.F. Müller.

Artikel 29-Datenschutzgruppe (2012): Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, WP 191, 23.03.2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_de.pdf [zuletzt geprüft am 15.02.2017].

Artikel 29-Datenschutzgruppe (2015 a): Appendix. Core topics in the view of trilogue, 17.06.2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf [zuletzt geprüft am 15.02.2017].

Artikel 29-Datenschutzgruppe (2015 b): Offener Brief der Artikel 29-Datenschutzgruppe an Frau Ilze Juhansone, 17.06.2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_msjuhansone.pdf, [zuletzt geprüft am 15.02.2017].

Austrian Wings (2008): Airbus - eine europäische Erfolgsgeschichte, 25.07.2008, https://www.austrianwings.info/2008/07/airbus-eine-europaische-erfolgsgeschichte/ [zuletzt geprüft am 15.02.2017].

Baker, Jennifer (2012): EU privacy watchdog expects no immediate change in data protection standoff with US, 05.12.2012, http://www.csoonline.com/article/2132628/privacy/eu-privacy-watchdog-expects-no-immediate-change-in-data-protection-standoff-with-us.html [zuletzt geprüft am 15.02.2017].

Baker, Jennifer (2013): Google, Microsoft, and Yahoo are secret backers behind European Privacy Association, infoworld, 20.05.2013, http://www.infoworld.com/article/2614554/startups/google--microsoft--and-yahoo-are-secret-Backers-behind-european-privacy-association.html [zuletzt geprüft am 15.02.2017].

Berg, Klaus/Kiefer, Marie-Luise (1996): Massenkommunikation V. Eine Langzeitstudie zur Mediennutzung und Medienbewertung 1964-1995. Baden-Baden: Nomos.

Bergemann, Benjamin (2013): EU-Ministerrat reitet auf Trojanischen Pferden Richtung Datenschutzreform, netzpolitik.org, 11.03.2013, https://netzpolitik.org/2013/innen-und-justizminister-reiten-auf-trojanischen-pferden-richtung-datenschutzreform/ [zuletzt geprüft am 15.02.2017].

BEUC (ohne Jahr): Privacy and personal data protection, http://www.beuc.eu/digital-rights/privacy-and-personal-data-protection [zuletzt geprüft am 27.04.2017].

Beuth, Patrick (2013): Alles Wichtige zum NSA-Skandal, Zeit online, 28.10.2013, http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal [zuletzt geprüft am 15.02.2017].

BfDI (2012): Die Europäischen Datenschutzbehörden verabschieden eine Stellungnahme zu den Reformvorschlägen zum Datenschutzrecht, 29.03.2012, https://www.bfdi.bund.de/DE/Europa_International/Europa/Reform_Datenschutzrecht/ReformEUDatenschutzrechtArtikel/Eu_Datenschutzbeh%C3%B6rden_verabsch_Stellungnahme_Reformvorschlaegen.html [zuletzt geprüft am 27.04.2017].

BfDI (ohne Jahr a): Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, https://www.bfdi.bund.de/DE/BfDI/bfdi-node.html [zuletzt geprüft am 15.02.2017].

BfDI (ohne Jahr b): Europäischer Datenschutz, http://www.bfdi.bund.de/DE/Europa_International/Europa/europa-node.html [zuletzt geprüft am 15.02.2017].

Biermann, Kai (2013): Mehr Datenschutz in der EU dank Snowden, Zeit online, 18.10.2013, http://www.zeit.de/digital/datenschutz/2013-10/eu-datenschutzreform-abstimmung-libe/komplettansicht [zuletzt geprüft am 15.02.2017].

Bitkom (2014): Stellungnahme zur Abstimmung des Europäischen Parlaments über den Entwurf für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung), 07.03.2014, https://www.bitkom.org/noindex/Publikationen/2014/Positionen/Abstimmung-des-Europaeischen-Parlaments-ueber-Verordnung-Schutz-personenbezogener-Daten-freie-Datenverkehr/20140307-BITKOM-Stellungnahme-zu-EP-Abstimmung-DSVO-3.pdf [zuletzt geprüft am 15.02.2017].

Bitkom (2015): Big Data und europäisches Datenschutzrecht, 04.02.2015, https://www.bitkom.org/Lost-Found/20150204-Stellungnahme-Big-Data-und-Datenschutz.pdf [zuletzt geprüft am 27.04.2017].

Bitkom (2016): Datenschutzverordnung sollte einheitlich angewendet werden, Pressemitteilung, 14.04.2016, https://www.bitkom.org/Presse/Presseinformation/Datenschutzverordnung-sollte-einheitlich-angewendet-werden.html [zuletzt geprüft am 15.02.2017].

Blühdorn, Ingolfur (2006): billig will Ich. Post-demokratische Wende und simulative Demokratie, in: Forschungsjournal Neue Soziale Bewegungen, 19 (4), S. 72-84.

BMI (ohne Jahr): Zusammenarbeit der Sicherheitsbehörden, http://www.bmi.bund.de/DE/Themen/Sicherheit/Terrorismusbekaempfung/Sicherheitsbehoerden/sicherheitsbehoerden_node.html [zuletzt geprüft am 15.02.2017].

BMJV (2015): Effektive Durchsetzung von Verbraucherrechten: Verbandsklagerecht bei Datenschutzverstößen, 18.12.2015, https://www.bmjv.de/SharedDocs/Artikel/DE/2015/12182015_Verbandsklagerecht.html [zuletzt geprüft am 15.02.2017].

BMWi (2015): Monitoring-Report Wirtschaft DIGITAL 2015, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/monitoring-report-wirtschaft-digital-2015.pdf?__blob=publicationFile&v=12 [zuletzt geprüft am 15.02.2017].

Breyer, Patrick (2015): Kommentar zu der Einigung auf ein EU-weit einheitliches Datenschutzrecht, Piratenpartei, MdL Schleswig Holstein, 17.12.2015, http://www.patrick-breyer.de/?p=560176 [zuletzt geprüft am 15.02.2017].

Bundeskartellamt (2016): Bundeskartellamt eröffnet Verfahren gegen Facebook wegen Verdachts auf Marktmissbrauch durch Datenschutzverstöße, 02.03.2016, http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html [zuletzt geprüft am 15.02.2017].

Bundesrat (2012): Subsidiaritätsrüge zur europäischen Datenschutz-Grundverordnung, Pressemitteilung, 30.03.2012; http://www.bundesrat.de/SharedDocs/pm/2012/051-2012.html [zuletzt geprüft am 15.02.2017].

Büschemann, Karl Heinz (2015): Große Datenfirmen könnten 'eine kleine Behörde lahmlegen', Süddeutsche Zeitung, 19.09.2015, http://www.sueddeutsche.de/digital/datenschutz-digitaler-sisyphos-1.2653568 [zuletzt geprüft am 15.02.2017].

BvD e.V. (2013): Optimistisch, dass es bis April 2014 eine Einigung gibt, BvD-News 2/2013, https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/Mitgliederbereich/Publikationen/BvD_News/z2013-02.pdf. [zuletzt geprüft am 15.02.2017].

BVDW e.V. (2013): Kommentar: EU-Datenschutz-Grundverordnung – Chance oder Risiko?, 18.10.2013, http://www.bvdw.org/medien/kommentar-eu-datenschutz-grundverordnung--chance-oder-risiko?media=5213 [zuletzt geprüft am 15.02.2017].

BVDW e.V. (2016): BVDW zur EU-Datenschutzreform: Überregulierung statt Rechtssicherheit, 15.04.2016, http://www.bvdw.org/medien/bvdw-zur-eu-datenschutzreform-berregulierung-statt-rechtssicherheit?media=7645 [zuletzt geprüft am 15.02.2017].

BVMW (2014): Positionspapier EU-Datenschutz-Grundverordnung, 20.12.2014, https://www.bvmw.de/fileadmin/download/Downloads_allg._Dokumente/politik/positionspapiere/positionspapier_eu-datenschutz-grundverordnung.pdf [zuletzt geprüft am 15.02.2017].

Campbell, Duncan (2000): Inside Echelon, 24.07.2000, https://heise.de/-3447438 [zuletzt geprüft am 15.02.2017].

Center for Democracy & Technology (ohne Jahr): Privacy & Data, https://cdt.org/issue/privacy-data/ [zuletzt geprüft am 15.02.2017].

Chaos Computer Club e.V./Digitalcourage e.V./Digitale Gesellschaft e.V./Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (2013): Offener Brief an Bundesminister Dr. Fridrich, 02.12.2013, https://digitalcourage.de/sites/default/files/media/datenschutz/02122013-brief-jirat-friedrich.pdf [zuletzt geprüft am 15.02.2017].

Chaos Computer Club e.V. (ohne Jahr): Chaos Computer Club, https://www.ccc.de/ [zuletzt geprüft am 15.02.2017].

Clarke, Adele (2005): Situational Analysis. Grounded Theory after the Postmodern Turn, Thousand Oaks, California: Sage.

Coke, Edward (1669): The Third Part of the Institutes of the Laws of England, Concerning High Treason, and Other Pleas of the Crown and Criminal Issues, 4. Aufl., London, 1669; zit.: Coke, 3 Inst.

Crouch, Colin (2008): Postdemokratie. Frankfurt am Main: Suhrkamp.

Dankert, Reinhard (2016): Vorsitz der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder übernommen, 04.01.2016, https://www.datenschutz-mv.de/presse/2016/pm-vorsitz.html [zuletzt geprüft am 15.02.2017].

Datenschutzbeauftragter INFO (2014): Datenschutzbeauftragte von Bund und Ländern, 27.05.2014, https://www.datenschutzbeauftragter-info.de/datenschutzbeauftragte-von-bund-und-laendern/ [zuletzt geprüft am 15.02.2017].

De Maizière, Thomas (2016): Deutschland bleibt ein sicheres Land, Pressekonferenz zu geplanten Maßnahmen zur Erhöhung der Sicherheit in Deutschland, 11.08.2016, http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2016/08/pressekonferenz-zu-massnahmen-zur-erhoehung-der-sicherheit-in-deutschland.html;jsessionid=19B88F99A3593058F768AE4FBDE8D9CF.2_cid364?nn=3314802 [zuletzt geprüft am 15.02.2017].

Dehmel, Susanne (2015): Nachbesserungen bei EU-Datenschutzverordnung notwendig, Pressemitteilung, 15.06.2015, https://www.bitkom.org/Presse/Presseinformation/Nachbesserungen-bei-EU-Datenschutzverordnung-notwendig.html [zuletzt geprüft am 15.02.2017].

Die Welt (2013): Merkel will internationales Datenschutzabkommen, 14.07.2013, https://www.welt.de/newsticker/dpa_nt/infoline_nt/brennpunkte_nt/article118035131/Merkel-will-internationales-Datenschutzabkommen.html [zuletzt geprüft am 15.02.2017].

Digitalcourage (ohne Jahr): Über uns, https://digitalcourage.de/ueber-uns [zuletzt geprüft am 27.04.2017].

Digitale Gesellschaft e.V. (2013): Internationale Bürgerrechtsorganisationen: Unternehmen gefährden unsere Grundrechte auf Privatsphäre und Datenschutz, 25.04.2013, https://digitalegesellschaft.de/wp-content/uploads/2013/04/EUDATAP_REPORT_DE1-0.pdf [zuletzt geprüft am 15.02.2017].

DigitalEurope (2014): Making Europe Fit for the Data Economy, 09.12.2014, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=864&language=en-US&PortalId=0&TabId=353 [zuletzt geprüft am 15.02.2017].

DigitalEurope (2015): Pressemitteilung, 15.06.2015, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=979&language=en-US&PortalId=0&TabId=353 [zuletzt geprüft am 15.02.2017].

Ebbinghaus, Uwe/Schulz, Stefan/Thiel, Thomas (2014): Machtprobe mit Silicon Valley, FAZ, 11.03.2014, http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/europas-it-projekt/digitale-agenda-machtprobe-mit-silicon-valley-12842407.html [zuletzt geprüft am 15.02.2017].

EDRi (2012): EDRi Initial Comments on the Proposal for a Data Protection Regulation, 27.01.2012, https://edri.org/commentsdpr/ [zuletzt geprüft am 15.02.2017].

EDRi (2013): Protecting privacy while maintaining global trade and security requires flexible solutions, https://edri.org/files/us_position_20130114.pdf [zuletzt geprüft am 15.02.2017].

EDRi (ohne Jahr): Why we do it, https://edri.org/why-we-do-it/ [zuletzt geprüft am 27.04.2017].

Ehmann, Eugen/Selmayr, Martin (2017): Datenschutz-Grundverordnung, Kommentar, München: C.H. Beck.

EUR-Lex (2016): Charta der Grundrechte, 17.10.2016, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM:l33501 [zuletzt geprüft am 15.02.2017].

Europäische Kommission (ohne Jahr): Organisationsstruktur, https://ec.europa.eu/info/about-european-union/organisational-structure_de [zuletzt geprüft am 15.02.2017].

Europäische Kommission (2012): Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern, Pressemitteilung, 25.02.2012, http://europa.eu/rapid/press-release_IP-12-46_de.htm [zuletzt geprüft am 15.02.2017].

Europäische Kommission (2013): Commission welcomes European Parliament rapporteurs´ support for strong EU data protection rules, 10.01.2013, http://europa.eu/rapid/press-release_MEMO-13-4_de.htm [zuletzt geprüft am 15.02.2017].

Europäische Kommission (2016): Fusionskontrolle: Kommission wirft Facebook vor, irreführende Angaben zur WhatsApp-Übernahme gemacht zu haben, 20.12.2016, http://europa.eu/rapid/press-release_IP-16-4473_de.htm [zuletzt geprüft am 15.02.2017].

Europäische Kommission (2017): Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover, press release, 18.05.2017, http://europa.eu/rapid/press-release_IP-17-1369_en.htm [zuletzt geprüft am 22.05.2017].

Europäische Union (ohne Jahr a): Die EU - kurz gefasst, https://europa.eu/european-union/about-eu/eu-in-brief_de [zuletzt geprüft am 15.02.2017].

Europäische Union (ohne Jahr b): Gerichtshof der Europäischen Union (EuGH), https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_de [zuletzt geprüft am 15.02.2017].

Europäisches Parlament (2014): Parlament verschärft Regeln zum Schutz persönlicher Daten im digitalen Zeitalter, Plenartagung Pressemitteilung, 12.03.2014, http://www.europarl.europa.eu/news/de/news-room/20140307IPR38204/parlament-verschärft-regeln-zum-schutz-persönlicher-daten-im-digitalen-zeitalter [zuletzt geprüft am 15.02.2017].

Europe-v-facebook.org (2016): Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems, 27.02.2016, http://www.europe-v-facebook.org/MU_HC.pdf [zuletzt geprüft am 15.02.2017].

European Privacy Association (ohne Jahr): Mission, http://europeanprivacyassociation.eu/mission/ [zuletzt geprüft am 15.02.2017].

Flade, Florian (2016): Deutschland bekommt jetzt seine eigene Mini-NSA, 17.08.2016, https://www.welt.de/politik/deutschland/article157722637/Deutschland-bekommt-jetzt-seine-eigene-Mini-NSA.html [zuletzt geprüft am 15.02.2017].

Fox, Benjamin (2012): Police should not be exempt from privacy rules, says EU data chief, EUobserver, 21.06.2012, https://euobserver.com/justice/116706 [zuletzt geprüft am 15.02.2017].

Fox, Benjamin (2013): EU commission ´stood firm´ on US data privacy, EUobserver, 13.06.2013, https://euobserver.com/justice/120490 [zuletzt geprüft am 15.02.2017].

Geminn, Christian L. (2015): Crypto Wars Reloaded?. In: DuD - Datenschutz und Datensicherheit 39 (8), S. 546-547.

Geminn, Christian L. (2016): Demokratie zwischen Öffentlichkeit und Privatheit. In: VerwArch - Verwaltungsarchiv 107 (4), S. 601-630.

Geminn, Christan L./Roßnagel, Alexander (2015): „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts – ein Überblick. In: JZ - JuristenZeitung 70 (14), S. 703-708.

Gerhards, Jürgen/Offerhaus, Anke/Roose, Jochen (2009): Wer ist verantwortlich? Die Europäische Union, ihre Nationalstaaten und die massenmediale Attribution von Verantwortung für Erfolge und Misserfolge. In: Politische Vierteljahresschrift 42, Wiesbaden: VS-Verlag, S. 529-558.

Greis, Friedhelm (2016): Bundesregierung will jede Art von Kommunikation auswerten, 11.08.2016, http://www.zeit.de/digital/datenschutz/2016-08/vorratsdatenspeicherung-terrorbekaempfung-darknet-bundesregierung [zuletzt geprüft am 15.02.2017].

Herdegen, Matthias (2015): Europarecht, 17. Auflage, München: C.H. Beck.

Hessischer Datenschutzbeauftragter (2015): Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung, 14.08.2015, www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/20150826_Verbesserung%20DSGrundverordnung.pdf?__blob=publicationFile&v=3 [zuletzt geprüft am 15.02.2017].

Hogan Lovells (2012 a): US Government Tells EU: "We Are Adequate", 06.12.2012, https://www.hoganlovells.com/en/blogs/hldataprotection/us-government-tells-eu-we-are-adequate [zuletzt geprüft am 15.02.2017].

Hogan Lovells (2012 b): Forum Europe's 3rd Annual European Data Protection and Privacy Conference, 04.12.2012, https://www.hoganlovells.com/en/blogs/hldataprotection/us-government-tells-eu-we-are-adequate [zuletzt geprüft am 15.02.2017].

Hülsmann, Werner (2017): Bundesrat: Zustimmung zum DSAnpUG-EU inkl. BDSG-neu, 12.05.2017, https://dsgvo.expert/bundesrat-zustimmung-zum-dsanpug-eu-inkl-bdsg-neu/ [zuletzt geprüft am 24.05.2017].

Industry coalition for data protection (2012): Reforming Europe´s Privacy Framework - How to find the right balance, September 2012, http://www.digitaleurope.org/DocumentDownload.aspx?Command=Core_Download&EntryId=545 [zuletzt geprüft am 15.02.2017].

information age (2013): Diplomats slept in tents during EU data protection talks, 07.06.2013, http://www.information-age.com/ico-at-high-risk-of-running-out-of-money-123457085/ [zuletzt geprüft am 15.02.2017].

Initiative Data Protection in Europe (2013): Positionspapier zur Datenschutz-Grundverordnung, http://web.archive.org/web/20160304212653/http://dataprotectioneu.eu/index_de.html [zuletzt geprüft am 15.02.2017].

Kemper, Frank (2016): INTERNET WORLD Business 2/2016, S. 8-10, http://heftarchiv.internetworld.de/content/download/123047/3378157/file/IWB_0216_Klein.pdf [zuletzt geprüft am 15.02.2017].

Klein, Matthias (2014): Ist die Europäische Union demokratisch genug?, bpb, 07.04.2014, https://www.bpb.de/dialog/europawahlblog-2014/181851/ist-die-europaeische-union-demokratisch-genug [zuletzt geprüft am 15.02.2017].

Kloiber, Manfred/Welchering, Peter (2016): Themen rund um die Gated Community, 02.01.2016, http://www.deutschlandfunk.de/32-chaos-communication-congress-themen-rund-um-die-gated.684.de.html?dram:article _id =341339 [zuletzt geprüft am 15.02.2017].

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2015): Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Grundverordnung, 14.08.2015, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/20150826_Verbesserung%20DSGrundverordnung.pdf?__blob=publicationFile&v=3 [zuletzt geprüft am 15.02.2017].

Krempl, Stefan (2013): EU-Parlament gibt grünes Licht für Datenschutzreform, heise online, 21.10.2013, https://heise.de/-1983124 [zuletzt geprüft am 15.02.2017].

Krempl, Stefan (2015): EU-Datenschutzreform: Zweckbindung und Datensparsamkeit ausgehebelt, heise online, 15.06.2015, https://heise.de/-2690862 [zuletzt geprüft am 15.02.2017].

Krempl, Stefan (2016): Bundesdatenschutz wird unabhängig, bleibt aber „zahnlos", heise online, 04.01.2016, https://heise.de/-3059238 [zuletzt geprüft am 15.02.2017].

Krempl, Stefan (2017 a): Datenschutzreform: EU-Kommission droht Deutschland mit Vertragsverletzungsverfahren, heise online, 20.04.2017, https://heise.de/-3689759 [zuletzt geprüft am 27.04.2017].

Krempl, Stefan (2017 b): Weniger Kontrollrechte: Bundestag beschließt Gesetz zur EU-Datenschutzreform, heise online, 28.04.2017, https://heise.de/-3699398 [zuletzt geprüft am 24.05.2017].

Kriminalpolizei (ohne Jahr): Deutsche Sicherheitsbehörden, http://www.kriminalpolizei.de/service/sicherheitsbehoerden.html [zuletzt geprüft am 15.02.2017].

Lamla, Jörn/Ochs, Carsten (2016): Der NSA-Skandal als Krise der Demokratie? Selbstreflexionen der Öffentlichkeit in der Privacy-Arena. In: Kornelia Hahn und Andreas Langenohl (Hg.): Kritische Öffentlichkeiten – Öffentlichkeiten in der Kritik. Wiesbaden: Springer VS, S. 83-112.

Lamla, Jörn (2013): Verbraucherdemokratie. Berlin: Suhrkamp.

Landesbeauftragte für den Datenschutz Bremen (2012): Entschließung: Europäische Datenschutzreform konstruktiv und zügig voranbringen!, 07./08.11.2012, https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.7507.de [zuletzt geprüft am 15.02.2017].

Lischka, Konrad/Stöcker, Christian (2013): Website entlarvt Lobby-Einfluss in Brüssel, Spiegel Online, 11.02.2013, http://www.spiegel.de/netzwelt/netzpolitik/lobbyplag-zeigt-lobby-einflussname-bei-eu-datenschutz-richtlinie-a-882567.html [zuletzt geprüft am 15.02.2017].

Lobbyplag (ohne Jahr a), http://lobbyplag.eu/governments [zuletzt geprüft am 01.12.2016].

Lobbyplag (ohne Jahr b), http://lobbyplag.eu/governments/documents [zuletzt geprüft am 01.12.2016].

Masing, Johannes (2012): Ein Abschied von den Grundrechten, Süddeutsche Zeitung, 09.01.2012, https://www.datenschutzbeauftragter-online.de/wp-content/uploads/2012/01/20120109_SZ_Masing_Datenschutz.pdf [zuletzt geprüft am 15.02.2017].

Matzer, Michael (2014): Datenschutz made in Europe, 01.07.2014, http://www.it-business.de/datenschutz-made-in-europe-a-450943/ [zuletzt geprüft am 15.02.2017].

Menz, Michael (2016): Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, Zalando SE, A-Drs. 18 (24) 97, 13.04.2016, https://www.bundestag.de/blob/418118/64f73092f5748d9cbe29a02832c2fae9/stellungnahme_menz-data.pdf. [zuletzt geprüft am 15.02.2017].

Merkel, Angela (2013): ARD-Sommerinterview, 14.07.2013, http://www.ard mediathek.de/tv/Bericht-aus-Berlin/Bericht-aus-Berlin-Sommerinter view-mit/Das-Erste/Video?bcastId=340982&document Id=15861418 [zuletzt geprüft am 01.12.2016].

Merkel, Angela (2015): Rede von Bundeskanzlerin Merkel beim 9. Nationalen IT-Gipfel, 19.11.2015, https://www.bundesregierung.de/Content/DE/Rede/2015/11/2015-11-19-merkel-it-gipfel.html [zuletzt geprüft am 15.02.2017].

Mies, Stefan (2015): Pressespiegel: Der Trilog zur europäischen Datenschutzgrundverordnung, 25.06.2015, https://www.artegic.de/blog/pressespiegel-der-trilog-zur-europaeischen-datenschutzgrundverordnung/ [zuletzt geprüft am 15.02.2017].

Molnár-Gábor, Fruzsina/Kaffenberger, Laura (2017): EU-US-Privacy-Shield – ein Schutzschild mit Löchern?. In: ZD - Zeitschrift für Datenschutz (1), S. 18-24.

Müller, Klaus (2015): EU-Datenschutzverordnung: Verbraucherrechte müssen im Trilog geschärft werden, Pressemitteilung, 16.06.2015, http://www.vzbv.de/pressemitteilung/eu-datenschutzverordnung-verbraucherrechte-muessen-im-trilog-Geschaerft-werden [zuletzt geprüft am 15.02.2017].

Münch, Ingo von/Mager, Ute (2015): Staatsrecht I. Staatsorganisationsrecht unter Berücksichtigung der europarechtlichen Bezüge, 8. Auflage, Stuttgart: Kohlhammer.

Netzpolitik.org (ohne Jahr): Über uns, https://netzpolitik.org/about-this-blog/ [zuletzt geprüft am 15.02.2017].

Nielsen, Nikolaj (2012): Commission data protection reforms under fire, EUobserver, 03.05.2012, https://euobserver.com/justice/116129 [zuletzt geprüft am 15.02.2017].

Nielsen, Nikolaj (2013 a): EU countries back pro-business data bill, EUobserver, 06.06.2013, https://euobserver.com/justice/120407 [zuletzt geprüft am 15.02.2017].

Nielsen, Nikolaj (2013 b): EU data bill exposes political rifts, EUobserver, 15.05.2013, https://euobserver.com/news/120134 [zuletzt geprüft am 15.02.2017].

Nielsen, Nikolaj (2013c): EU data protection bill 'moves backwards', 06.12.2013, https://euobserver.com/justice/122384 [zuletzt geprüft am 15.02.2017] .

Nielsen, Nikolaj (2014a): EU data bill delayed until after May elections, 24.01.2014, https://euobserver.com/justice/122853 [zuletzt geprüft am 15.02.2017].

Nielsen, Nikolaj (2014b): EU ministers back key pillar in data reform bill, EUobserver, 04.12.2014, https://euobserver.com/justice/126796 [zuletzt geprüft am 15.02.2017].

Nielsen, Nikolaj (2015a): EU ministers back weaker data protection rules, EUobserver, 15.06.2015, https://euobserver.com/justice/129122 [zuletzt geprüft am 15.02.2017].

Nielsen, Nikolaj (2015b): National governments punch holes in EU data protection bill, EUobserver, 03.03.2015, https://euobserver.com/justice/127856 [zuletzt geprüft am 15.02.2017].

n-tv (2014): Oettinger macht Digitales zu seinem Thema, 29.09.2014, http://www.n-tv.de/politik/Oettinger-macht-Digitales-zu-seinem-Thema-article13696331.html [zuletzt geprüft am 15.02.2017].

O´Brien, Kevin J. (2013): Silicon Valley Companies Lobbying Against Europe´s Privacy Proposals, The New York Times, 25.01.2013, http://www.nytimes.com/2013/01/26/technology/eu-privacy-proposal-lays-bare-differences-with-us.html?_r=1& [zuletzt geprüft am 15.02.2017].

Oetjen, Jan (2016): Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, United Internet, A-Drs. 18 (24) 97, 19.02.2016, https://www.bundestag.de/blob/409388/4813873f2e4d425b3b16cc35bac0c297/a-drs-18-24-91-data.pdf [zuletzt geprüft am 15.02.2017].

Ombudsman Europa (2016): Ombudsman O'Reilly, Emiliy calls for more trilogues transparency, Pressemitteilung, 14.07.2016, https://www.ombudsman.europa.eu/press/release.faces/en/69214/html.bookmark [zuletzt geprüft am 15.02.2017].

Peters, Roland (2013): EU-Verordnung per „Copy & Paste" – Blog deckt Lobbyeinfluss auf, n-tv, 12.02.2013, http://www.n-tv.de/politik/Blog-deckt-Lobbyeinfluss-auf-article10103291.html [zuletzt geprüft am 15.02.2017].

Pop, Valentina (2013): Facebook, Skype challenged in EU over spy affair, EUobserver, 18.07.2013, https://euobserver.com/justice/120894 [zuletzt geprüft am 15.02.2017].

portal liberal (2013): ALVARO: Grüne Datenschutzvorschläge: #fail, 08.01.2013, https://www.liberale.de/content/alvaro-gruene-datenschutzvorschlaege-fail [zuletzt geprüft am 15.02.2017].

Privacy International (2015): Privacy and Data Protection under threat from EU Council agreement, 15.06.2015, https://www.privacyinternational.org/node/597 [zuletzt geprüft am 15.02.2017].

Privacy International (ohne Jahr a): No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, https://www.privacyinternational.org/ [zuletzt geprüft am 27.04.2017].

Privacy International (ohne Jahr b): Building a Global Privacy Movement, https://www.privacyinternational.org/node/42 [zuletzt geprüft am 15.02.2017].

Rat der Europäischen Union (2013): 3228th Council meeting Justice and Home Affairs, Pressemitteilung, 07./08.03.2013, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/135901.pdf [zuletzt geprüft am 15.02.2017].

Rat der Europäischen Union (2015): EU Data Protection Reform: EU-Council Ready for Trilogue, 15.06.2015, http://www.computerundrecht.de/40876.html [zuletzt geprüft am 15.05.2017].

Richter, Philipp (2015): Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO. In: DuD - Datenschutz und Datensicherheit 39 (11), S. 735-740.

Roßnagel, Alexander (2016): Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, A-Drs. 18 (24) 94, 19.02.2016, https://www.bundestag.de/blob/409512/4afc3a566097171a7902374da77cc7ad/a-drs-18-24-94-data.pdf. [zuletzt geprüft am 15.02.2017].

Roßnagel, Alexander (Hg.) (2017): Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, 1. Auflage, Baden-Baden: Nomos.

Roßnagel, Alexander/Kroschwald, Steffen (2014): Was wird aus der Datenschutzgrundverordnung? – Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument. In: Zeitschrift für Datenschutz Heft 10/2014, S. 495-500.

Roßnagel, Alexander/Nebel, Maxi/Richter, Philipp (2015): Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO. In: Zeitschrift für Datenschutz Heft 10/2015, S. 455-460.

Scherzer, Stephan (2014): Europa braucht einen digitalen Airbus!, 13.05.2014, http://www.vdz.de/nachricht/print/98/artikel/gastkommentar-europa-braucht-einen-digitalen-airbus/ [zuletzt geprüft am 15.02.2017].

Schmiechen, Frank (2015): Das Internet hat uns gehört, Gründerszene, 16.02.2015, http://www.gruenderszene.de/allgemein/obama-recode-interview [zuletzt geprüft am 15.02.2017].

Sodan, Helge/Ziekow, Jan (2016): Grundkurs Öffentliches Recht. Staats- und Verwaltungsrecht, 7. Auflage, München: C.H. Beck.

Strauss, Anselm L. (1978): A Social World Perspective. In: Studies in Symbolic Interaction, Band 1, S. 119-128.

Strauss, Anselm L. (1993): Continual Permutations of Action. Hawthorne, New York: de Gruyter.

Streinz, Rudolf (2016): Europarecht, 10. Auflage, Heidelberg: C.F. Müller.

Stupp, Catherine (2015): EU watchdog launches transparency app for data privacy talks, euractiv, 27.07.2015, https://www.euractiv.com/section/digital/news/eu-watchdog-launches-transparency-app-for-data-privacy-talks/ [zuletzt geprüft am 15.02.2017].

Tripp, Volker (2015): Vorentscheidung zur Europäischen Datenschutzgrundverordnung: am Ende reichte es nur zur Sicherung von Mindeststandarts, Digitale Gesellschaft, 17.12.15, https://digitalegesellschaft.de/2015/12/vorentscheidung-dsgvo-mindeststandard/ [zuletzt geprüft am 15.02.2017].

Tzschentke, Karin (2013): Massives Lobbying gegen EU-Datenschutzverordnung, Der Standard, 13.02.2013, http://derstandard.at/ 1360161300194/Massives-Lobbying-gegen-Datenschutzverordnung [zuletzt geprüft am 15.02.2017].

Ulfkotte, Udo (2013): Der Krieg im Dunkeln: Die wahre Macht der Geheimdienste, Altenau: Hallenberger Media UG.

Venturini, Tomasso (2012): Building On Faults. How to represent controversies with digital methods. In: Public Understanding of Science 21, S. 796-812.

Verein Für soziales Leben e.V. (ohne Jahr): Welche Regelungen beinhaltet die Europäische Datenschutz-Grundverordnung – DSGVO-EU?, http://www.europaeische-datenschutz-grundverordnung.de/inhalt.html [zuletzt geprüft am 15.02.2017].

Visser, Corinna (2013): Wir brauchen einen Airbus für die IT-Industrie, 02.11.2013, http://www.tagesspiegel.de/wirtschaft/datensicherheit-in-unternehmen-wir-brauchen-einen-airbus-fuer-die-it-industrie/9018606.html [zuletzt geprüft am 15.02.2017].

vzbv e.V. (2012): Datenschutz-Grundverordnung: Gute Ideen, aber zu vage, Stellungnahme, 29.02.2012, http://www.vzbv.de/dokument/datenschutz-Grundverordnung-gute-ideen-aber-zu-vage [zuletzt geprüft am 15.02.2017].

vzbz e.V. (2014): EU-Datenschutzgrundverordnung: es gibt keine belanglosen Daten, 25.11.2014, http://www.vzbv.de/dokument/eu-datenschutzverordnung-es-gibt-keine-belanglosen-daten [zuletzt geprüft am 15.02.2017].

vzbv e.V. (2016): Besserer Datenschutz für Verbraucher, Pressemitteilung, 14.04.2016, http://www.vzbv.de/pressemitteilung/besserer-daten schutz-fuer-verbraucher [zuletzt geprüft am 15.02.2017].

vzbv e.V. (2017): Die Stimme der Verbraucher, http://www.vzbv.de/sites /default/files/2017_vzbv_broschuere_die_stimme_der_verbraucher_we b_1.pdf [zuletzt geprüft am 11.05.2017].

vzbv e.V. (ohne Jahr): EU-Datenschutzverodnung, http://www.vzbv.de/ eu-datenschutzverordnung [zuletzt geprüft am 27.04.2017].

Warren, Samuel D./Brandeis, Louis D. (2012 [1890]): Das Recht auf Privatheit – The Right to Privacy. Harv. L. Rev. 4/1890, 193, übersetzter Nachdruck, In: DuD - Datenschutz und Datensicherheit 36 (10): S. 755-766.

Washietl, Engelbert (2014): Der Traum vom Europa-Google, 23.01.2014, http://www.euractiv.de/section/digitale-agenda/news/der-traum-vom-europa-google/ [zuletzt geprüft am 15.02.2017].

Wolff, Amadeus/Brink, Stefan (2017): Beck´scher Online-Kommentar Datenschutzrecht, 19. Edition, Stand: 01.02.2017, München.

Zandonella, Bruno (2009): Pocket Europa. EU-Begriffe und Länderdaten, Bonn: Bundeszentrale für politische Bildung.

Die Datenschutz-Grundverordnung brachte eine fundamentale Neuordnung des Datenschutzrechts in Europa mit sich. Ihrem Inkrafttreten gingen zähe und komplexe Verhandlungen voraus, in deren Kern die Frage nach einem wirksamen Schutz von Privatheit und informationeller Selbstbestimmung im digitalen Zeitalter stand. In diesen Debatten versammelten sich verschiedene Akteure und Instanzen mit all ihren widerstreitenden Interessen und Problemdeutungen in einer „Arena", um einen geeigneten Umgang mit den neuen Unsicherheiten im Zuge der Digitalisierung zu finden.

Das Buch untersucht den Werdegang der Datenschutz-Grundverordnung aus einer interdisziplinären Perspektive. In diesem Werdegang zeigt sich beispielhaft, wie verschiedene soziale Welten mit ihren jeweils eigenen Logiken um die Deutung und Gestaltung von Privatheit und informationeller Selbstbestimmung kämpfen.

ISBN 978-3-7376-0564-9