Europäische Vorreiterrolle im Datenschutzrecht: Neue Entwicklungen in der Gesetzgebung, Rechtsprechung und internationalen Praxis der EU

Thomas Giegerich*

Inhalt

* Univ.-Prof. Dr. iur., Direktor des Europa-Instituts der Universität des Saarlandes.

A. Datenschutz im Zeitalter der digitalen Revolution und des internationalen Terrorismus

I. Technologischer Totalitarismus oder freiheitliche Demokratie?

Die digitale Revolution bewirkt neue Herausforderungen, auf die das Recht nur mit Verzögerungen reagiert, obwohl sie praktisch alle Rechtsgebiete betreffen. Eine Vielzahl von Problemen gilt es rechtlich zu bewältigen, beispielsweise die Gewährleistung von Netzsicherheit und der Schutz der Netzinfrastruktur; die Bekämpfung von Com-

puterkriminalität;[1] die Regelung der Kriegsführung mit digitalen Mitteln (sogenannter Cyberkrieg);[2] die Sicherung freier Informationsabfrage, -weitergabe und Kommunikation im Internet über nationale Grenzen hinweg; die Sicherung eines Internetzugangs für alle Menschen auch in den Entwicklungsländern; den Schutz der persönlichen Daten, der Privatsphäre und der Persönlichkeit gegen staatliche Überwachung und privatwirtschaftliche Ausbeutung; die Kontrolle der transnational agierenden Internet-Konzerne, die als Intermediäre bestimmte Bereiche der digitalen Welt geradezu monopolisieren;[3] schließlich das Internet-Regime als solches.[4] Überspitzt ausgedrückt, stehen wir vor der Alternative, einen möglicherweise von Staaten und Konzernen gemeinsam oktroyierten technologischen Totalitarismus hinzunehmen oder unsere freiheitliche Demokratie zu verteidigen. Die einzig akzeptable zweite Variante verlangt einerseits, den Primat demokratischer politischer Entscheidungen über die Wirtschaft durchzusetzen,[5] und andererseits, die Grundrechte der Einzelnen gegenüber staatlicher und nichtstaatlicher Macht auch in digitaler Form zu schützen.

Dabei dürfen aber die durch informationstechnologische Fortschritte eröffneten Chancen nicht vergessen werden: Das Internet bietet enormes Potential nicht nur zur Gefährdung, sondern auch zur Erweiterung der Freiheit, indem es die Fähigkeit der Allgemeinheit zur Kontrolle von staatlicher und nichtstaatlicher Macht exponentiell erhöht.[6] Neben die Presse als „vierte Gewalt" tritt das Internet als „fünfte Gewalt". Digitale Freiheiten können die Entwicklung und den wirtschaftlichen Wohlstand von Individuen und Gesellschaften fördern, den sozialen Zusammenhalt verbessern und zur weltweiten Verbreitung von „*good government*" beitragen.

II. Daten-, Privatsphären- und Persönlichkeitsschutz im Netz gegen staatliche und private Gefährder

Aus dem vorgenannten Bündel von rechtlichen Aufgaben greife ich im Folgenden den Daten-, Privatsphären- und Persönlichkeitsschutz im Netz heraus, weil dieser in letzter Zeit besonders wichtig geworden ist. Denn einerseits hat der internationale Terrorismus zu früher unvorstellbaren staatlichen Überwachungsmaßnahmen geführt, die unter Ausnutzung modernster technischer Möglichkeiten tief in die Grund- und

1 Vgl. u.a. das Übereinkommen über Computerkriminalität v. 23.11.2001 (CETS No. 185) mit Zusatzprotokoll betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art v. 28.1.2003 (CETS No. 189), die beide vom Europarat erarbeitet wurden.

2 *Woltag*, Cyber Warfare, in: Wolfrum (ed.), The Max Planck Encyclopedia of Public International Law (OUP online edition).

3 Vgl. *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 72 f., 79 ff.

4 Vgl. zur Internet governance u.a. *Giegerich*, Internationale Standards – aus völkerrechtlicher Perspektive, BDGIR 46 (2014), S. 131 ff. m.w.N.

5 Vgl. die Rede des Präsidenten des Europäischen Parlaments, *Martin Schulz*, am 28.1.2016 unter dem Titel „Technological Totalitarianism, Politics and Democracy", European Data Protection Law Review 1/2016, S. 11 ff.

6 Zu dieser Ambiguität vgl. u.a. *Joyce*, Internet Freedom and Human Rights, EJIL 26 (2015), S. 493 ff.

Menschenrechte eingreifen. In Bezug auf die Internet-Überwachung haben dabei die USA und Großbritannien eine Vorreiterrolle übernommen, weil sie einen Großteil der Internet-Infrastruktur (Server und Glasfaserkabel) physisch kontrollieren.[7] Ihre Ausspionierung von persönlichen Daten vieler Millionen Menschen rund um die Welt ohne physische Übergriffe auf fremdes Territorium lässt die alte Frage nach den völker- und menschenrechtlichen Grenzen der extraterritorialen Ausübung von Hoheitsgewalt in ganz neuem Licht erscheinen.[8]

Andererseits haben zumeist US-amerikanische multinationale Privatunternehmen das Geschäftsmodell des „Datenabbaus" (*data mining*) entwickelt: Die Internet-Giganten beuten die personenbezogenen Daten einschließlich besonders sensibler Daten[9] von Nutzern, die ihre Internetdienste vermeintlich kostenlos in Anspruch nehmen, als eine Art neuen Rohstoffs aus und machen damit Profite in Milliardenhöhe.[10] Einzelpersonen müssen sich deren Bedingungen unterwerfen, wollen sie nicht auf die Teilhabe an selbstverständlichen Vorteilen des modernen Lebens verzichten. Darüber hinaus kontrollieren und managen diese Konzerne die relevanten Technologien, so dass Zugriffe anderer auf persönliche Daten der Internetnutzer – seien es staatliche Stellen, seien es private Akteure – in aller Regel nur unter ihrer Mitwirkung erfolgen können.[11] Während die Konzerne zunächst mit staatlichen Überwachungsorganen regelmäßig kooperierten, haben sie sich seit den Snowden-Enthüllungen gegen staatliche Versuche, auf die personenbezogenen Daten ihrer Kunden zuzugreifen,

7 Council of Europe Commissioner for Human Rights, Issue Paper: The rule of law on the Internet and in the wider digital world, CommDH/IssuePaper(2014)1 v. 8.12.2014, https://wcd.coe.int/ViewDoc.jsp?p=&id=2268589&direct=true (1.8.2016), S. 9.

8 *Polakiewicz*, Privacy Protection in the 21st Century: The Need for Innovative Approaches, in: Casadevall u.a. (Hrsg.), Mélanges en l'honneur de Dean Spielmann, 2015, S. 508 ff.; *von Arnauld*, Freiheit und Regulierung in der Cyberwelt, BDGIR 47 (2016), S. 9 ff. Vgl. *Milanovic*, UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No right to Privacy under the ECHR, EJIL: Talk! v. 18.5.2016, www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr/ (1.8.2016); *Kim*, ECHR Jurisdiction and Mass Surveillance, EJIL: Talk! v. 9.6.2016, www.ejiltalk.org/echr-jurisdiction-and-mass-surveillance-scrutinising-the-uk-investigatory-power-tribunals-recent-ruling/?pfstyle=wp (1.8.2016).

9 Art. 6 des Datenschutz-Übereinkommens des Europarats (siehe unter C.) identifiziert die folgenden Daten als sensibel und verpflichtet die Vertragsparteien daher, deren automatische Verarbeitung besonderen Schutzbestimmungen zu unterwerfen: Daten, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen, welche die Gesundheit oder das Sexualleben betreffen sowie Daten über Strafurteile. Art. 7 DSchGrVO (siehe unter D.I.3.) verbietet grundsätzlich mit abschließend festgelegten Ausnahmen die „Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person". Art. 10 DSchGrVO erlaubt die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten nur in engen Grenzen.

10 Siehe den Cannataci-Bericht (A/HRC/31/64) v. 8.3.2016, S. 5 (Abschnitt 9), nach dem die Privatwirtschaft inzwischen mehr Daten gesammelt haben soll als die Staaten.

11 CommDH/IssuePaper(2014)1, (Fn. 7), S. 64.

teilweise gerichtlich zur Wehr gesetzt und damit als Verfechter des Daten- und Privatsphärenschutzes gegenüber staatlichen Exzessen positioniert.[12]

III. Grund- und menschenrechtliche Kontrolle privater Konzerne mit Hilfe der staatlichen Schutzpflicht

Das eklatante Machtgefälle zwischen Internet-Konzernen und einzelnen privaten Nutzern wirft die umstrittene Frage nach den grund- und menschenrechtlichen Verpflichtungen solcher privaten Wirtschaftsunternehmen auf.[13] Es ruft insbesondere die grund- und menschenrechtliche Schutzpflicht der Staaten auf den Plan. Denn diese sind völkerrechtlich, europarechtlich und zumeist auch verfassungsrechtlich verpflichtet, die Grund- und Menschenrechte nicht nur zu achten, sondern sie auch zu gewährleisten.[14] Das bedeutet, dass sie diese Rechte zunächst selbst nicht verletzen dürfen. Darüber hinaus müssen sie aber Eingriffen anderer – auch privater – Akteure entgegenwirken,[15] soweit diese nicht ihrerseits von einem schwerer wiegenden grund- oder menschenrechtlichen Gegenrecht gedeckt sind. Je nach Fallkonstellation kann es sich dabei handeln um die Informationsfreiheit (etwa von Internetnutzern), die Meinungsäußerungs- und Pressefreiheit (etwa von Medienunternehmen), die Berufs- und Gewerbefreiheit (etwa von Internet-Konzernen) und das Eigentum (etwa von Urheberrechtsinhabern).[16] Welchem der miteinander kollidierenden Grund- und Menschenrechte der Vorrang gebührt, ergibt sich aus einer Abwägung, deren Ziel die Herstellung einer praktischen Konkordanz ist.[17] Es geht mit anderen Worten darum,

12 Vgl. *Yorke*, Silencing the Canary: the lawfulness of the U.K. Investigatory Powers Bill's secrecy provisions under the ECHR, EJIL Talk! v. 17.5.2016, www.ejiltalk.org/silencing-the-canary-the-lawfulness-of-the-u-k-investigatory-powers-bills-secrecy-provisions-under-the-echr/ (1.8.2016).

13 Vgl. die vom Sonderbeauftragten des UN-Generalsekretärs *John Ruggie* ausgearbeiteten UN Guiding Principles on Business and Human Rights of 16.4.2014; Recommendation CM/Rec(2016)3 des Ministerkomitees des Europarats an die Mitgliedstaaten zu „human rights and business" v. 2.3.2016, https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec%282016%293&Language=lanEnglish&Ver=original&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864&direct=true (1.8.2016).

14 Vgl. z.B. Art. 2 Abs. 1 IPbpR; Art. 1 EMRK; zurückhaltender Art. 51 Abs. 1 Satz 2 GRCh – vgl. jedoch Art. 1 Satz 2, Art. 8 Abs. 1 GRCh. *Nowak*, U.N. Covenant on Civil and Political Rights, 2. Aufl. 2005, Art. 2, Rn. 20 ff.; *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, 6. Aufl. 2016, S. 158 ff.; *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, Art. 51 GRCh, Rn. 18, 23 ff.; *Polakiewicz*, (Fn. 8), S. 507 f.; *Calliess*, Schutzpflichten, in: Merten/Papier (Hrsg.), HGR II, 2006, § 44; *von Arnauld*, (Fn. 8), S. 18 ff.; *Masing*, Herausforderungen des Datenschutzes, NJW 2012, S. 2305 ff.; *Di Fabio*, (Fn. 3), S. 90 ff.

15 Entgegenwirken bedeutet, dass solche Eingriffe nach Möglichkeit zu verhindern, zumindest aber zu ahnden und in ihren Folgen möglichst zu beseitigen sind.

16 Vgl. *Polakiewicz*, (Fn. 8), S. 506. Zum Schutz von Urheberrechten im Netz vgl. EuGH, Rs. C-314/12, *UPC Telekabel Wien*, EU:C:2014:192.

17 *Hesse*, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Aufl. 1999, Rn. 72.

ein Nullsummenspiel zu vermeiden und stattdessen eine Synthese herzustellen, in der die Rechte beider Seiten bestmöglich verwirklicht werden können.[18]

Die Kontrolle der Internet-Giganten übersteigt die Regelungs- und Durchsetzungsmacht der einzelnen Staaten aber bei weitem, nicht zuletzt, weil sie Daten auf Server in solchen Staaten verschieben können, die ihnen im internationalen Wettbewerb als Unternehmensstandort größtmögliche Freiheit lassen (Regulierungsoasen). Damit sind die Staaten je für sich kaum in der Lage, ihre grund- und menschenrechtliche Schutzpflicht zu erfüllen. Eine Lösung kann letztlich nur auf der globalen Ebene gefunden werden, doch erscheint eine weltweite Einigung derzeit als utopisch, denn die Auffassungen darüber, wie streng das Internet rechtlich kontrolliert werden sollte, gehen zu weit auseinander.[19] Für Europa bleibt als zweitbeste Lösung die regionale Bündelung der Kräfte, um gegenüber den Internet-Konzernen ein ausreichendes Maß an Regelungs- und Durchsetzungsmacht und gegenüber den USA sowie zukünftig auch China, Indien und anderen Mächten ein ausreichendes Maß an Verhandlungsmacht zu generieren.

Vor diesem Hintergrund erfährt der Daten-, Privatsphären- und Persönlichkeitsschutz im Sinne eines Rechts auf digitale Privatsphäre seit einiger Zeit auf UN-Ebene, auf der Ebene des regionalen Völkerrechts und im EU-Recht verstärkte Aufmerksamkeit.[20]

B. Datenschutzaktivitäten auf UN-Ebene

Die Vereinten Nationen sind in Reaktion auf die Snowden-Enthüllungen, die eine umfassende und weltumspannende Überwachung, Speicherung und Auswertung der digitalen Kommunikation durch die US-Geheimdienste offengelegt haben, zugunsten des Datenschutzes aktiv geworden.[21] Vor allem die UN-Generalversammlung,[22] der zum UN-Generalsekretariat gehörende Hochkommissar für Menschenrechte[23] und der UN-Menschenrechtsrat haben sich dem Daten-, Privatsphären- und Persönlichkeitsschutz gewidmet. Die International Law Commission[24] hatte das Thema „*Protection of personal data in transborder flow of information*“ schon 2006 in ihr Langzeitarbeitsprogramm aufgenommen, sich damit aber noch nicht befasst.[25] Der

18 Vgl. dazu *Polakiewicz*, (Fn. 8), S. 506 f. (mit Beispielen aus der EGMR-Rspr.).
19 Kritisch zur regulierungsfeindlichen Position der USA etwa der Menschenrechtskommissar des Europarats in CommDH/IssuePaper(2014)1, (Fn. 7), S. 48 ff., 54 ff., 91 f.
20 Vgl. *Weichert*, Globaler Kampf um digitale Grundrechte, KritJ 2014, S. 123 ff.
21 Zu früheren Aktivitäten der UNO vgl. *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012, S. 59 ff.
22 Resolution 68/167 v. 18.12.2013, The right to privacy in the digital age, A/RES/68/167, die im Konsensverfahren ohne Abstimmung angenommen wurde.
23 Bericht v. 30.6.2014, The right to privacy in the digital age, A/HRC/27/37.
24 Zu diesem Unterorgan der UN-Generalversammlung vgl. *Rao*, International Law Commission (ILC), in: Wolfrum, (Fn. 2).
25 Report of the International Law Commission on the work of its 58th session, GAOR, 61st Session, Supplement No. 10 (A/61/10), Annex IV, http://legal.un.org/docs/?symbol=A/61/10 (1.8.2016).

Menschenrechtsrat, ein Unterorgan der UN-Generalversammlung, hat 2015 sogar einen Sonderberichterstatter für das Recht auf Privatsphäre ernannt.[26]

Sonderberichterstatter *Joseph A. Cannataci* hat dem UN-Menschenrechtsrat inzwischen seinen ersten Bericht erstattet.[27] Darin heißt es, eine wesentliche Schwierigkeit bestehe im weltweiten Kontext darin, erst einmal ein die Kulturgrenzen überspannendes gemeinsames Verständnis von Privatsphäre und Persönlichkeitsrechten zu entwickeln.[28] Ungeachtet dessen hat die UN-Generalversammlung bestätigt, dass die Menschen online und offline dieselben Rechte hätten, einschließlich des in Art. 12 der Allgemeinen Erklärung der Menschenrechte[29] und in Art. 17 des Internationalen Paktes über bürgerliche und politische Rechte[30] festgelegten Rechts auf Privatsphäre.[31] Weiterhin fordert die Generalversammlung alle Staaten auf, das Recht auf Privatsphäre zu achten und gegen Eingriffe anderer staatlicher und nichtstaatlicher Akteure zu schützen, auch im Bereich der digitalen Kommunikation.[32] Diese Formulierungen lassen zugleich erkennen, dass es auf der Weltebene bisher kein geschriebenes spezielles Menschenrecht auf Datenschutz gibt. Die Auffassungen der Staaten über den Stellenwert von Daten- und Persönlichkeitsschutz im Verhältnis zu kommerziellen Interessen und Sicherheitsinteressen gehen so weit auseinander, dass eine weltweite effektive Durchsetzung eines Menschenrechts auf digitale Privatsphäre auf große Schwierigkeiten stößt.[33]

Inzwischen liegt auch der Bericht des *Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *David Kaye*, zur Rolle des privaten Sektors im digitalen Zeitalter an den UN-Menschenrechtsrat vor. Dieser nimmt die Gegenperspektive der Meinungsfreiheit ein und empfiehlt unter anderem, dass private Akteure im Informations- und Kommunikationstechnologiesektor transparente Verfahren zur Abschätzung der menschenrechtlichen Folgen ihrer (geschäftlichen) Entscheidungen einführen.[34] Dies muss auch für Entscheidungen zugunsten des Datenschutzes gelten.

C. Datenschutz durch Europarat und Europäischen Gerichtshof für Menschenrechte

Auf regionaler Ebene ist die Entwicklung weiter vorangeschritten. Eine Vorreiterrolle hat dabei der Europarat 1981 mit dem Übereinkommen zum Schutz des Menschen

26 Resolution 28/16, The right to privacy in the digital age, A/HRC/RES/28/16.
27 Cannataci-Bericht (A/HRC/31/64) v. 8.3.2016.
28 Vgl. ibid., S. 4.
29 Sartorius II Nr. 15.
30 BGBl. 1973 II, 1534 = Sartorius II Nr. 20.
31 Resolution 68/167, (Fn. 22), Ziffer 3; bestätigt in Ziffer 3 der Resolution 69/166 v. 18.12.2014, A/RES/69/166.
32 Resolution 68/167, (Fn. 22), Ziffern 1 und 4 (unter Einbeziehung der 4. Erwägung der Präambel); bestätigt in Ziffern 1 und 4 der Resolution 69/166, (Fn. 31).
33 *Von Arnauld*, (Fn. 8), S. 8 ff., spricht immerhin von einer realistischen Utopie.
34 Report v. 11.5.2016 (advance edited version), A/HRC/32/38, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/38 (1.8.2016).

bei der automatischen Verarbeitung personenbezogener Daten übernommen, das inzwischen von allen Europaratsmitgliedern ratifiziert worden ist.[35] Es handelt sich um den ersten und bisher auch einzigen in Kraft getretenen völkerrechtlichen Vertrag speziell zum Schutz personenbezogener Daten.[36] Er regelt die Datenverarbeitung im öffentlichen und privaten Sektor, und zwar auch in Fällen des grenzüberschreitenden Datenverkehrs. Dieses Übereinkommen steht nicht nur den Mitgliedern des Europarats zum Beitritt offen, sondern nach seinem Art. 23 kraft besonderer Einladung seitens des Ministerkomitees auch Nichtmitgliedstaaten. Im Laufe der Zeit ist es durch zahlreiche Empfehlungen des Ministerkomitees ergänzt worden,[37] die zwar als solche nicht rechtsverbindlich sind, aber vom EGMR regelmäßig als Hilfsmittel zur Interpretation von Art. 8 EMRK herangezogen werden.[38]

Das Übereinkommen wird weiterhin ergänzt durch das Zusatzprotokoll bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, das die Einrichtung unabhängiger Datenschutzinstanzen vorschreibt und die Datenübermittlung in Nichtparteien des Übereinkommens davon abhängig macht, dass dort ein angemessenes Datenschutzniveau gewährleistet ist.[39] Derzeit wird ein an die modernen Entwicklungen angepasstes neues Übereinkommen ausgehandelt, um das alte zu ersetzen.[40] Der Menschenrechtskommissar des Europarats hat hierzu im Februar 2015 ein einschlägiges Themenpapier mit einer Reihe von Empfehlungen vorgelegt.[41] Er schlägt unter anderem vor, dass die USA als Schritt zu einem umfassenderen globalen Ansatz zum Datenschutz dem Europarats-Übereinkommen beitreten sollten.[42]

Neben dem speziellen Datenschutz-Übereinkommen steht immer die EMRK, die in ihrem Art. 8 als Bestandteil des Rechts auf Privatsphäre ein Recht auf Datenschutz mitgarantiert. Dieses kann mit Hilfe der Individualbeschwerde nach Art. 34 EMRK vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) eingeklagt werden und ist deshalb wesentlich durchsetzungsstärker als die Regelungen in dem gegenwärtigen und auch dem zukünftigen Datenschutz-Übereinkommen. Indirekt trägt der EGMR aber auch zur Durchsetzung des Datenschutz-Übereinkommens bei, indem

35 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data v. 28.1.1981 (CETS No. 108).

36 Vgl. das gemeinsam von der EU-Grundrechteagentur, dem Europarat und dem EGMR 2014 veröffentlichte Handbook on European Data Protection Law, www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (1.8.2016), S. 15 f.

37 Abrufbar unter www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (1.8.2016).

38 *Polakiewicz*, (Fn. 8), S. 505.

39 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows v. 8.11.2001 (CETS No. 181), das von 36 Staaten ratifiziert worden ist.

40 *Polakiewicz*, (Fn. 8), S. 504, 507. In Afrika gibt es schon die allerdings noch nicht in Kraft getretene African Union Convention on Cyber Security and Personal Data Protection v. 27.6.2014, www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (1.8.2016).

41 CommDH/IssuePaper(2014)1, (Fn. 7).

42 Ibid., S. 91.

er dieses als Hilfsmittel zur Interpretation und Fortbildung des Art. 8 EMRK verwendet.[43]

In Europa wirken der Europarat und die Europäische Union beim Datenschutz eng zusammen.[44] Wenn vom europäischen Datenschutzrecht die Rede ist, sind damit die Europarats- und die EU-Komponenten gemeint. Dieses europäische Datenschutzrecht beruht auf einer Reihe von Grundprinzipien (Verarbeitung von Daten nur nach Treu und Glauben und auf rechtmäßige Weise, Konkretisierung und Begrenzung des Zwecks der Datenerhebung und -verarbeitung, Datensparsamkeit, Datenqualität und Datensicherheit) sowie von Rechten und Rechtsbehelfen der Datensubjekte und schließt eine Überwachung durch unabhängige Datenschutzbehörden ein.[45] Als besonders wichtig erscheint darüber hinaus, dass die europäischen Datenschutzregeln in gleicher Weise für alle Personen, ungeachtet ihrer Staatsangehörigkeit und ihres Wohnsitzes, gelten, die von einem Datenverarbeitungsvorgang seitens eines europäischen Verarbeitungsverantwortlichen betroffen sind.[46] Demgegenüber behandelt das US-amerikanische Recht Personen, die keine US-Bürger sind und in den USA keinen Wohnsitz haben, ausdrücklich schlechter.[47]

Die nachfolgenden Ausführungen konzentrieren sich auf aktuelle Maßnahmen der EU zur Verbesserung des Schutzes persönlicher Daten, der zugleich ein wichtiges Element des Schutzes der menschlichen Persönlichkeit (und nicht nur der Privatsphäre) darstellt,[48] die um eine digitale Dimension ergänzt wird.[49] Nicht zu Unrecht hat das Bundesverfassungsgericht (BVerfG) das Grundrecht auf informationelle Selbstbestimmung ebenso wie das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) abgeleitet.[50] Es hat darüber hinaus zu Recht betont, dass die einschüchternde Wirkung einer unbegrenzten Datensammlung auf die individuelle Grundrechtsausübung auch das demokratische System beeinträchtigen würde. Dies liegt daran, dass individuelle

„Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[51]

Demgegenüber hat der EGMR für die Zwecke des Datenschutzes das Recht auf Schutz der Privatsphäre (Art. 8 EMRK) als das am nächsten liegende Konventions-

43 *Polakiewicz*, (Fn. 8), S. 505.
44 Vgl. Handbook on European Data Protection Law, (Fn. 36).
45 CommDH/IssuePaper(2014)1, (Fn. 7), S. 16, 88 f.; Handbook an European Data Protection Law, (Fn. 36), S. 61 ff. Zum Erfordernis der Unabhängigkeit von Datenschutzbehörden vgl. EuGH, Rs. C-518/07, *Kommission/Deutschland*, EU:C:2010:125.
46 CommDH/IssuePaper(2014)1, (Fn. 7), S. 90.
47 Ibid., S. 92.
48 Ibid., S. 88.
49 *Luch/Schulz/Kuhlmann*, Ein Recht auf Vergessenwerden als Ausprägung einer selbstbestimmten digitalen Persönlichkeit, EuR 2014, S. 711 ff.
50 BVerfGE 65, 1; BVerfGE 120, 274; BVerfG, Urt. v. 20.4.2016, 1 BvR 966/09, 1 BvR 1140/09.
51 BVerfGE 65, 1 (43).

recht herangezogen.[52] Dieser Rückgriff auf allgemeine Regelungen ist jeweils notwendig, weil es weder im Grundgesetz noch in der EMRK ein besonderes Grund- oder Menschenrecht auf Datenschutz gibt. Denn als der Grundrechtskatalog des Grundgesetzes 1948/49 und der Menschenrechtskatalog der EMRK 1949/50 formuliert wurden, waren die technischen Möglichkeiten zur Datensammlung, -zusammenführung und -verarbeitung noch zu wenig entwickelt, um eine solche spezielle Gewährleistung zu erfordern.[53]

D. Datenschutz auf EU-Ebene

I. Primär- und sekundärrechtliche Maßnahmen

1. EU-Grundrechtecharta und AEUV

Angesichts der heutigen Gefährdungen ist die Festschreibung eines besonderen Grundrechts auf Datenschutz unerlässlich geworden. Ein solches findet sich im modernsten rechtsverbindlichen internationalen Grundrechtskatalog, nämlich der Charta der Grundrechte der Europäischen Union von 2007.[54] Neben dem Recht auf Achtung des Privat- und Familienlebens[55] ist der Schutz personenbezogener Daten in eine eigene Bestimmung (Art. 8 GRCh) aufgenommen worden, die zugleich die wesentlichen Grundsätze des europäischen Datenschutzrechts nachzeichnet und damit in den Grundrechtsschutz einbezieht.[56]

Nach Art. 6 Abs. 1 UAbs. 1 EUV hat die Charta der Grundrechte denselben Rang wie „die Verträge",[57] also Primärrechtsrang. Sie bindet sämtliche Einrichtungen der EU, die Mitgliedstaaten aber nur bei der Durchführung des EU-Rechts.[58] Art. 16 Abs. 1 AEUV wiederholt die grundrechtliche Gewährleistung des Art. 8 Abs. 1

52 Siehe vor allem EGMR (GK), Nrn. 20562/04, 30566/04, *S. and Marper v. UK*, Urt. v. 4.12.2008. Eine Zusammenfassung der einschlägigen Rechtsprechung auf dem Stand von April 2016 findet sich in folgenden von der Presseabteilung des EGMR verfassten Dokumenten: Factsheet – Personal Data Protection, www.echr.coe.int/Documents/FS_Data_ENG.pdf (1.8.2016); Factsheet – New technologies, www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf (1.8.2016).

53 Eine solche spezielle Gewährleistung fehlt auch noch in der Amerikanischen Menschenrechtskonvention von 1969, der Afrikanischen Charta der Menschenrechte und Rechte der Völker von 1981 sowie der Arabischen Charta der Menschenrechte von 2004. Demgegenüber findet sich in Abschnitt 21 der ASEAN Human Rights Declaration von 2012 ein Verbot willkürlicher Eingriffe in die Privatsphäre „einschließlich personenbezogener Daten". Alle vorgenannten Dokumente finden sich in englischer Fassung in Europa-Institut (ed.), International Human Rights Law, 2015, S. 499 ff.

54 Vom 12.12.2007, ABl. C 202 v. 7.6.2016, S. 389.

55 Art. 7 GRCh.

56 Siehe auch Art. 39 EUV, Art. 16 AEUV.

57 Art. 1 Abs. 2 EUV.

58 Art. 51 Abs. 1 GRCh. Zur Reichweite der Bindung der Mitgliedstaaten EuGH, Rs. C-198/13, *Hernández*, EU:C:2014:2055, Rn. 33 ff.; *Jarass*, Charta der Grundrechte der EU, 2. Aufl. 2013, Art. 51, Rn. 11 ff.; *Bucher*, Die Bindung der Mitgliedstaaten an die EU-Grundrechtecharta bei Ermessensspielräumen, ZEuS 2016, S. 203 ff.

GRCh wörtlich. Das Verhältnis der beiden gleichzeitig primärrechtlich kodifizierten Garantien zueinander wird im Hinblick auf Art. 52 Abs. 2 GRCh problematisiert.[59] Tatsächlich spiegelt sich der in Art. 8 Abs. 2, Art. 52 Abs. 1 GRCh niedergelegte Gesetzesvorbehalt in Art. 16 Abs. 2 AEUV wider, so dass auch auf der Schrankenebene eine Parallelität der beiden Gewährleistungen besteht.

2. Datenschutzrichtlinien von 1995 und 2002 sowie Datenschutzverordnung von 2000

Daneben gibt es schon seit längerer Zeit[60] detaillierte sekundärrechtliche Bestimmungen vor allem in der Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.[61] Diese allgemeine Datenschutzrichtlinie soll in erster Linie die unterschiedlichen Datenschutzregelungen der Mitgliedstaaten harmonisieren, um Hindernisse für die Verwirklichung des Binnenmarktes zu beseitigen,[62] gleichzeitig aber auch die Grundrechte der betroffenen Personen schützen. Sie wird ergänzt durch die speziellere Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – ePrivacy-Richtlinie).[63] Da es sich um Richtlinien handelt, können sie ihre Schutzwirkungen erst nach ihrer Umsetzung in nationales (Gesetzes-)Recht voll entfalten.[64]

Während die vorgenannten Richtlinien den Mitgliedstaaten die Pflicht zur Gewährleistung des Datenschutzes gegenüber staatlichen Behörden sowie natürlichen und juristischen Personen auferlegen, wird der Datenschutz gegenüber der EU selbst durch die unmittelbar anwendbare Verordnung (EG) Nr. 45/2001 vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr gewährleistet.[65] Diese beruht auf einer anderen vertraglichen Ermächtigungs-

59 *Holznagel/Dietze*, Europäischer Datenschutz, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, 3. Aufl. 2015, § 37, Rn. 44; *Kingreen*, (Fn. 14), Art. 16 AEUV, Rn. 3 und Art. 8 GRCh, Rn. 2 f.

60 Der EGV enthielt schon seit dem Vertrag von Amsterdam von 1997 eine Ermächtigungsgrundlage zum Erlass von Datenschutzregelungen in Art. 286 Abs. 2.

61 ABl. L 281 v. 23.11.1995, S. 31. Konsolidierte Fassung mit späteren Änderungen abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:01995L0046-20031120&qid=1461923619194&from=DE (1.8.2016).

62 Sie beruht auf der Vorgängervorschrift von Art. 114 AEUV.

63 ABl. L 201 v. 31.7.2002, S. 37. Konsolidierte Fassung mit späteren Änderungen abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1461923376579&uri=CELEX:02002L0058-20091219 (1.8.2016). Diese RL ersetzt eine Vorgängerin von 1997.

64 Vgl. Art. 288 Abs. 3, Art. 291 Abs. 1 AEUV.

65 ABl. L 8 v. 12.1.2001, S. 1.

grundlage[66] und ist notwendig, weil die Richtlinien nur an die Mitgliedstaaten, nicht aber an EG/EU-Organe adressiert werden konnten.[67]

3. Datenschutz-Grundverordnung und Datenschutz-Richtlinie für die polizeiliche und justizielle Zusammenarbeit von 2016

Die Datenschutzrichtlinien und die Verordnung sind angesichts der rasanten technologischen Entwicklung und der fortschreitenden Globalisierung veraltet. Deshalb ist nach mehr als vier Jahre langen politischen Auseinandersetzungen vor kurzem eine neue Datenschutz-Grundverordnung verabschiedet worden, die die Richtlinie 95/46/EG durch nunmehr in sämtlichen Mitgliedstaaten unmittelbar wirksame Vorschriften[68] ersetzt.[69] Zur Ergänzung dieser auf Art. 16 AEUV gestützten Datenschutz-Grundverordnung (DSchGrVO)[70] ist aufgrund derselben Vertragsbestimmung gleichzeitig eine neue Datenschutz-Richtlinie für die polizeiliche und justizielle Zusammenarbeit (DSchRLPol) angenommen worden.[71]

Diese Aufspaltung in zwei Rechtsakte hat historische Gründe,[72] die durch die Erklärung Nr. 21 im Anhang der Schlussakte der Regierungskonferenz von Lissabon unter Berufung auf den spezifischen Charakter der polizeilichen und justiziellen Zusammenarbeit perpetuiert wurden. Die beiden vorgenannten Rechtsakte sehen eine zweijährige Übergangsphase vor: Die DSchGrVO gilt ab 25. Mai 2018;[73] die DSchRL-Pol ist bis 6. Mai 2018 in nationales Recht umzusetzen.[74] Auch die ePrivacy-Richtlinie

66 Art. 286 EGV (Vorgängervorschrift von Art. 16 Abs. 2 AEUV).
67 Vgl. jetzt Art. 288 Abs. 3 AEUV. Vgl. Handbook on European Data Protection Law, (Fn. 36), S. 19.
68 Art. 288 Abs. 2 AEUV.
69 VO (EU) 2016/679 v. 27.4.2016 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 v. 4.5.2016, S. 1. Vgl. *Schantz*, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841 ff.; *Kühling/Martini*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, S. 448 ff.
70 Diese gilt nach ihrem Art. 2 Abs. 2 lit. d nicht für die polizeilichen und justiziellen Aufgaben der Strafverfolgung, Strafvollstreckung und Gefahrenabwehr.
71 RL (EU) 2016/680 v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 v. 4.5.2016, S. 89. Diese ersetzt den Rahmenbeschluss 2008/977/JI des Rates v. 27.11.2008 (ABl. L 350 v. 30.12.2008, S. 60), der seinerseits die Datenschutzrichtlinie von 1995 ergänzte, die aus Kompetenzgründen auf binnenmarktrelevante Datenverarbeitungen beschränkt ist, vgl. Handbook on European Data Protection Law, (Fn. 36), S. 19.
72 Die allgemeine Datenschutzrichtlinie galt für die polizeiliche und justizielle Zusammenarbeit nicht, weil die Gemeinschaft zum Zeitpunkt ihres Erlasses im Jahre 1995 für diese Bereiche nicht zuständig war. Als ihr diese Zuständigkeit später übertragen wurde, erging dazu ein gesonderter Rahmenbeschluss.
73 Art. 99 Abs. 2; nach Art. 94 Abs. 1 DSchGrVO erfolgt die Aufhebung der RL 95/46/EG mit Wirkung vom selben Tag.
74 Art. 63 DSchRLPol.

soll demnächst überarbeitet werden. Die Kommission hat dazu im April 2016 ein öffentliches Konsultationsverfahren eingeleitet. Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die VO (EG) Nr. 45/2001 fort; diese soll indessen an die Grundsätze und Vorschriften der DSchGrVO angepasst werden.[75]

Die neue DSchRLPol erleichtert als Teil der Europäischen Sicherheitsagenda den Austausch ermittlungsrelevanter Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten, um die Verhinderung und Aufklärung von Terroranschlägen und anderen transnationalen Verbrechen zu verbessern. Trotzdem sollen personenbezogene Daten von Opfern, Straftätern und Zeugen besser geschützt sein als zuvor.[76] Die Richtlinie definiert nur Mindeststandards zum Datenschutz und behält es den Mitgliedstaaten in Art. 1 Abs. 3 vor, strengere Garantien festzulegen. Demgegenüber nimmt die DSchGrVO im Interesse des Binnenmarktes eine Vollharmonisierung vor, um ein unionsweit einheitliches Datenschutzniveau zu gewährleisten.[77] Die Mitgliedstaaten können im Anwendungsbereich der Verordnung von dieser abweichende Bestimmungen daher nur einführen, soweit diese sie dazu in Form von Öffnungsklauseln ausdrücklich ermächtigt, was recht häufig geschieht.[78]

Die DSchGrVO verbessert den Datenschutz allgemein, entlastet zugleich aber auch die Unternehmen (vor allem die kleinen und mittleren) durch bürokratische Erleichterungen. Sie soll dadurch, vor allem aber durch die Festlegung unionsweit geltender einheitlicher Regeln, die auch außereuropäische Anbieter von Dienstleistungen in der EU binden, zugleich den digitalen Binnenmarkt fördern.[79] Außerdem verfolgt sie einen differenzierten risikobasierten Ansatz, der die Verpflichtungen der Unternehmen nach den jeweiligen Risiken staffelt. Weiterhin sind die Regeln der Verordnung innovationsförderlich, weil sie Anreize dafür schaffen, dass datenschutzfreundliche Technik (z.B. Pseudonymisierung)[80] von der frühesten Entwicklungsphase an in Produkte und Dienstleistungen eingebaut wird.[81]

Zu den Kernpunkten der DSchGrVO gehören folgende: Die Datensubjekte sind klar und verständlich darüber zu informieren, wie ihre Daten verarbeitet werden, und erhalten erleichterten Zugang zu ihren Daten. Sie erhalten außerdem ein Recht auf erleichterte Übertragbarkeit ihrer Daten auf einen anderen Anbieter. Die Zulässigkeit der Datenverarbeitung wird von der ausdrücklichen Einwilligung der betroffenen Person abhängig gemacht. Damit hängt ein neu eingeführtes sogenanntes „Recht auf Vergessenwerden"[82] zusammen: Betroffene dürfen danach verlangen, dass ihre Daten gelöscht werden, wenn es keinen legitimen Grund für deren weitere Speicherung gibt.

75 Art. 2 Abs. 3, 98 DSchGrVO.
76 Vgl. Pressemitteilung des Europäischen Parlaments v. 14.4.2016, www.europarl.europa.eu/pdfs/news/expert/infopress/20160407IPR21776/20160407IPR21776_de.pdf (1.8.2016).
77 Art. 1 Abs. 3 DSchGrVO sowie Begründungserwägung 13.
78 *Kraska*, Auswirkungen der EU-Datenschutzgrundverordnung, ZD-Aktuell 2016, 04173 (beck-online).
79 Europäische Kommission, Pressemitteilung IP/15/6321 v. 15.12.2015.
80 Vgl. Definition in Art. 4 Ziffer 5 DSchGrVO.
81 Pressemitteilung der Kommission, (Fn. 79).
82 Vgl. dazu eingehend *Gstrein*, Das Recht auf Vergessenwerden als Menschenrecht, 2016.

Die Betroffenen erhalten überdies ein Recht auf Information darüber, ob ihre Daten gehackt wurden, damit sie geeignete Schutzmaßnahmen ergreifen können. Schließlich werden Verstöße schärfer sanktioniert: Bei Unternehmen können Geldbußen von bis zu 4 % des im vorangegangenen Jahr weltweit erzielten Umsatzes verhängt werden.[83]

Zum persönlichen, sachlichen und räumlichen Anwendungsbereich der DSchGrVO ist Folgendes festzuhalten: Die DSchGrVO schützt nur natürliche Personen bei der Verarbeitung personenbezogener Daten,[84] nicht hingegen juristische Personen.[85] Auch juristische Personen und Personenvereinigungen genießen indessen Grundrechtsschutz durch Art. 7 GRCh[86] und in eingeschränktem Maße auch durch Art. 8 GRCh.[87] Im Anschluss an die bisherige Rechtslage definiert Art. 4 Ziffer 2 DSchGrVO den Begriff „Verarbeitung" sehr weit. Sachlich ist die DSchGrVO anwendbar auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[88] Keine Anwendung findet die DSchGrVO jedoch insbesondere auf Datenverarbeitungen durch die Mitgliedstaaten im Rahmen einer Tätigkeit, die gar nicht in den Anwendungsbereich des Unionsrechts oder die in den Anwendungsbereich der Gemeinsamen Außen- und Sicherheitspolitik fällt.[89] Maßnahmen der Mitgliedstaaten im GASP-Bereich können freilich regelmäßig als Durchführung des Unionsrechts qualifiziert werden, soweit sie unionsrechtlich gebunden sind,[90] und unterliegen dann gemäß Art. 51 Abs. 1 GRCh den Unionsgrundrechten einschließlich der Art. 7 und 8 GRCh.

Räumlich anwendbar ist die DSchGrVO nach ihrem Art. 3 auf Datenverarbeitungen, soweit diese im Rahmen der Tätigkeit einer Niederlassung in der Union erfolgen, selbst wenn die Verarbeitung als solche außerhalb der Union stattfindet. Ist der Datenverarbeiter nicht in der Union niedergelassen, so findet die DSchGrVO gleichwohl Anwendung, wenn die Datensubjekte sich in der Union befinden und die Datenverarbeitung im Zusammenhang damit steht, ihnen in der Union Waren oder Dienstleistungen auch unentgeltlich anzubieten oder ihr in der Union erfolgendes Verhalten zu beobachten. In den letztgenannten Fällen muss der Datenverarbeiter nach Maßgabe des Art. 27 DSchGrVO einen Vertreter in der Union benennen.

83 Diese Zusammenfassung basiert auf der Pressemitteilung des Parlaments v. 14.4.2016, (Fn. 76) und der Pressemitteilung der Kommission v. 15.12.2015, (Fn. 79).
84 Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Ziffer 1 DSchGrVO).
85 Art. 1 DSchGrVO.
86 *Jarass*, (Fn. 58), Art. 7, Rn. 10.
87 Ibid., Art. 8, Rn. 7.
88 Art. 2 Abs. 1 DSchGrVO. Der Begriff „Dateisystem" wird in Art. 4 Ziffer 6 DSchGrVO definiert.
89 Art. 2 Abs. 2 lit. a und b DSchGrVO. Der Grund für die GASP-Ausnahme liegt in Art. 16 Abs. 2 UAbs. 2 AEUV i.V.m. Art. 39 EUV.
90 Art. 28 Abs. 2, Art. 29 EUV.

4. Richtlinie über Vorratsdatenspeicherung von 2006 und Richtlinie über Fluggastdatensätze von 2016

Zwei aus datenschutzrechtlicher Sicht problematische Sekundärrechtsakte sollen auch erwähnt werden: Die Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden,[91] und die ganz neue Richtlinie (EU) 2016/681 vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.[92] Die erstgenannte Richtlinie hat der EuGH wegen Verstoßes gegen Art. 7, 8 und 52 Abs. 1 GRCh in Verbindung mit dem Verhältnismäßigkeitsgrundsatz für ungültig erklärt.[93] Die PNR-Richtlinie wird mit Sicherheit aus demselben Grund dem Gerichtshof unterbreitet werden.[94]

II. Bahnbrechende Entscheidungen des EuGH seit 2014

Der EuGH, der bereits 1969 den grundrechtlichen Schutz personenbezogener Daten anerkannt hatte,[95] hat in den letzten beiden Jahren das europäische Datenschutzrecht vor allem durch drei bahnbrechende Entscheidungen in den Rechtssachen *Digital Rights Ireland*, *Google Spain* und *Schrems* wesentlich fortentwickelt. Im ersten Fall ging es um hoheitliche Eingriffe in das Grundrecht auf Datenschutz, im zweiten um die angemessene Ausbalancierung miteinander in Konflikt geratener Datennutzungsrechte von Unternehmen und Datenschutzrechte von Privatpersonen und im dritten um die Gewährleistung eines angemessenen Schutzniveaus bei der Übermittlung personenbezogener Daten durch ein privates Unternehmen in ein Drittland.

91 ABl. L 105 v. 13.4.2006, S. 54.

92 ABl. L 119 v. 4.5.2016, S. 132. Kritisch noch zum Entwurf der Kommission *Boehm/Cole*, Data Retention after the Judgement of the Court of Justice of the European Union, 2014, S. 81 ff. Siehe auch das Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security v. 14.12.2011, ABl. L 215 v. 11.8.2012, S. 4; sowie EuGH, verb. Rs. C-317/04 und C-318/04, *Parlament/Rat*, EU:C:2006:346, wo der Ratsbeschluss über den Abschluss eines Vorgängerabkommens für nichtig erklärt worden war. Vgl. *Boehm/Cole*, S. 73 ff.

93 Siehe unter D.II.1.b).

94 Der prozedurale Weg besteht darin, dass Klagen gegen nationale Umsetzungs- oder Ausführungsakte vor nationalen Gerichten erhoben werden und diese dann eine Vorabentscheidung des EuGH über die Gültigkeit der Richtlinie einholen (Art. 267 AEUV).

95 EuGH, Rs. 29/69, *Stauder*, EU:C:1969:57.

1. Das Urteil im Fall „Digital Rights Ireland" von 2014 gegen die Vorratsdatenspeicherung

a) Verzögerte EuGH-Entscheidung über Grundrechtsverletzungen

Dieses Urteil[96] betrifft die Vereinbarkeit der Richtlinie über die Vorratsdatenspeicherung[97] mit den Grundrechten der vielen Millionen betroffenen Kommunikationsteilnehmer. Der Gerichtshof hatte bereits mehr als fünf Jahre zuvor in einem Nichtigkeitsklageverfahren entschieden, dass die Richtlinie kompetenzgemäß erlassen worden war. Die Frage möglicher Grundrechtsverletzungen hatte er damals ausdrücklich offen gelassen, weil der klagende Mitgliedstaat allein die Kompetenzmäßigkeit der Richtlinie angegriffen hatte.[98] Deshalb prüfte er deren Vereinbarkeit mit den Grundrechten, die in der Öffentlichkeit von Anfang an bestritten worden war, erst 2014 – mehr als acht Jahre nach ihrem Inkrafttreten – und beendete damit endlich die jahrelange Rechtsunsicherheit.[99]

Die Richtlinie über die Vorratsdatenspeicherung verlangte von den Mitgliedstaaten, die vorsorgliche anlasslose Speicherung aller Telekommunikationsverkehrsdaten[100] durch die Anbieter entsprechender Dienste für die Dauer von mindestens sechs Monaten vorzuschreiben. Damit sollten die zuvor unterschiedlichen nationalen Regelungen im Interesse des grenzüberschreitenden Dienstleistungsverkehrs harmonisiert werden.[101] Die auf Vorrat gespeicherten Daten sollten den zuständigen mitgliedstaatlichen Stellen nach Maßgabe des nationalen Rechts zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten wie organisierter Kriminalität und Terrorismus zur Verfügung stehen. Die Richtlinie enthielt dazu keine Regelungen. Das BVerfG hatte bereits 2010 die deutschen gesetzlichen Bestimmungen zu ihrer Umsetzung wegen Verstoßes gegen das Grundrecht aus Art. 10 Abs. 1 GG, das als Bestandteil des Telekommunikationsgeheimnisses auch die Verkehrsdaten schützt, für nichtig erklärt.[102] Die Einholung einer Vorabentscheidung des EuGH zur Klärung der Frage, ob die Richtlinie ihrerseits wegen Verstoßes gegen europäische Grundrechte ungültig war, hatte es nicht für notwendig erachtet.[103]

96 EuGH, verb. Rs. C-293/12 und C-594/12, *Digital Rights Ireland*, EU:C:2014:238.
97 Siehe Fn. 91.
98 EuGH, Rs. C-301/06, *Irland/Parlament und Rat*, EU:C:2009:68, Rn. 57.
99 Kritik an dieser vermeidbaren Rechtsunsicherheit bei *Giegerich*, Spät kommt Ihr, doch Ihr kommt: Warum wird die Grundrechtskonformität der Vorratsdatenspeicherungs-Richtlinie erst nach acht Jahren geklärt?, ZEuS 2014, S. 3 ff.
100 Dazu gehören insbesondere die Rufnummern der beteiligten Telefonanschlüsse, die Namen und Anschriften der Teilnehmer, denen diese Rufnummern zugewiesen sind, die IP-Adressen beteiligter Computer, Datum und Uhrzeit des Beginns und Endes des Kommunikationsvorgangs und bei Mobiltelefonen die Standortkennung bei Beginn des Kommunikationsvorgangs. Ausdrücklich nicht zu speichern waren Daten, die Aufschluss über den Inhalt der Kommunikation geben.
101 Als vertragliche Ermächtigungsgrundlage diente Art. 95 EGV, die Vorgängervorschrift von Art. 114 AEUV. Diese hatte der EuGH 2009 in Rs. C-301/06, *Irland/Parlament und Rat*, EU:C:2009:68 als ausreichend anerkannt.
102 BVerfGE 125, 260.
103 BVerfGE 125, 260 (308 f.); kritisch *Giegerich*, (Fn. 99), S. 14 ff.

b) Nichtigerklärung der Richtlinie zur Vorratsdatenspeicherung durch den EuGH

Durch Vorabentscheidungsersuchen des irischen High Court und des österreichischen Verfassungsgerichtshofs wurde der EuGH dann im Fall *Digital Rights Ireland* endlich mit dem Problem der Grundrechtskonformität der Richtlinie befasst und erklärte diese daraufhin für ungültig. Dem Vorschlag des Generalanwalts, ihre Wirkungen analog zu Art. 264 Abs. 2 AEUV wegen der Dringlichkeit der mit ihr verfolgten sicherheitspolitischen Ziele vorübergehend aufrechtzuerhalten,[104] folgte der Gerichtshof nicht. Offensichtlich hielt er die Grundrechtsverstöße für irreparabel und wollte zugleich ein deutliches Zeichen dafür setzen, dass er das Grundrecht auf Datenschutz nicht weniger ernst nimmt als das BVerfG. Dies zeigt sich auch daran, dass der EuGH „angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens und des Ausmaßes und der Schwere des mit der Richtlinie 2006/24/EG verbundenen Eingriffs in dieses Recht" dem Unionsgesetzgeber nur einen eingeschränkten Gestaltungsspielraum zugestand und die Richtlinie daher einer strikten Kontrolle unterzog.[105] Diesen strengen Prüfungsmaßstab für anlasslose Massenüberwachungsmaßnahmen hat der EGMR inzwischen unter ausdrücklicher Berufung auf den EuGH übernommen.[106]

Der EuGH prüfte die Gültigkeit der Richtlinie anhand der Art. 7 und 8 GRCh, weil sie sowohl in das Recht auf Privatleben als auch das Recht auf Datenschutz eingreife.[107] Denn aus der Gesamtheit der auf Vorrat zu speichernden Daten könnten sehr genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden.[108] Der Eingriff sei geeignet, bei den Betroffenen das Gefühl ständigen Überwachtseins zu erzeugen, da er flächendeckend und anlasslos erfolge. Auf der Rechtfertigungsebene (Art. 52 Abs. 1 GRCh) lehnte der Gerichtshof zunächst eine Verletzung des Wesensgehalts der vorgenannten Grundrechte ab, weil die Richtlinie keinen Zugriff auf den Inhalt der Kommunikation gestatte, sondern nur auf die Verkehrsdaten, und die Diensteanbieter bestimmte Grundsätze des Datenschutzes und der Datensicherheit einhalten müssten.[109] Die dem Gemeinwohl dienende materielle Zielsetzung der Richtlinie, die ja vordergründig der Harmonisierung binnenmarktrelevanter nationaler Vorschriften diente, lag nach Ansicht des EuGH darin, „zur Bekämpfung schwerer Kriminalität und somit letztlich zur öffentlichen Sicherheit beizutragen."[110]

104 Schlussanträge GA *Cruz Villalón* zu EuGH, verb. Rs. C-293/12 und C-594/12, *Digital Rights Ireland*, EU:C:2013:845, Rn. 154 ff.
105 EuGH, verb. Rs. C-293/12 und C-594/12, *Digital Rights Ireland*, EU:C:2014:238, Rn. 48. *Granger/Irion*, The Court of Justice and the Data Retention Directive in Digital Rights Ireland, European Law Review 39 (2014), S. 845 f.
106 EGMR, Nr. 37138/14, *Szabó and Vissy v. Hungary*, Urt. v. 12.1.2016, Rn. 23, 68, 70 und 73 (noch nicht rechtskräftig). Vgl. auch *Cole/Vandendriessche*, From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg, EDPL 1/2016, S. 121 ff.
107 EuGH, verb. Rs. C-293/12 und C-594/12, *Digital Rights Ireland*, EU:C:2014:238, Rn. 32 ff.
108 Ibid., Rn. 27.
109 Ibid., Rn. 38 ff.
110 Ibid., Rn. 41 ff.

In der anschließenden Verhältnismäßigkeitskontrolle verneinte der Gerichthof jedoch die Erforderlichkeit der dazu vorgenommenen Grundrechtseingriffe. Denn in der Richtlinie fehlten klare, präzise und strikte Regelungen, um den wirksamen Schutz der auf Vorrat gespeicherten personenbezogenen Daten vor Missbrauchsrisiken sowie vor unberechtigtem Zugang und unberechtigter Nutzung zu gewährleisten. Diese unerlässlichen flankierenden Regelungen blieben zu weitgehend den Mitgliedstaaten überlassen. Außerdem schreibe die Richtlinie nicht vor, dass die Daten im Unionsgebiet gespeichert werden müssten. Deshalb sei die in Art. 8 Abs. 3 GRCh vorgeschriebene Überwachung durch eine unabhängige Stelle nicht vollumfänglich gewährleistet, obwohl sie ein wesentliches Element des Datenschutzes darstelle.[111] Während der EuGH also den Unionsgesetzgeber in der Pflicht sah, für ausreichende Datenschutzregelungen zu sorgen, hatte das BVerfG eine inhaltlich vergleichbare verfassungsrechtliche Verpflichtung dem Bundesgesetzgeber auferlegt.[112] Darin liegt jedoch kein Widerspruch, weil der nationale Ansatz des BVerfG darauf beruhte, dass das die Grundrechtseingriffe anordnende Unionsrecht selbst keine ausreichenden Schutzvorkehrungen enthielt.[113]

c) Vereinbarkeit nationaler Gesetze zur Vorratsdatenspeicherung mit den Unionsgrundrechten

(1) Autonome Wiedereinführung der Vorratsdatenspeicherung durch den deutschen Bundesgesetzgeber

Eine neue Richtlinie zur Vorratsdatenspeicherung hat der Unionsgesetzgeber bislang nicht erlassen. Vielmehr hat die Kommission erklärt, keinen entsprechenden Vorschlag machen zu wollen, und ohne einen solchen kann kein Unionsgesetzgebungsverfahren durchgeführt werden.[114] Demgegenüber hat der deutsche Bundesgesetzgeber die Vorratsdatenspeicherung in abgeschwächter Form autonom wiedereingeführt[115] und dabei versucht, den strengen verfassungsrechtlichen Vorgaben gerecht zu werden, die das BVerfG in seinem vorerwähnten Urteil von 2010 aufgestellt hatte.[116] Gegen dieses neue Gesetz sind wieder zahlreiche Verfassungsbeschwerden erhoben worden, deren Begründetheit das BVerfG erneut anhand von Art. 10 Abs. 1

111 Ibid., Rn. 51 ff.
112 BVerfGE 125, 260.
113 Kritisch zur Zentralisierungswirkung des EuGH-Ansatzes jedoch *Kühling*, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, S. 684.
114 Erklärung der Kommission zu nationalen Gesetzen zur Vorratsdatenspeicherung v. 16.9.2015, http://europa.eu/rapid/press-release_STATEMENT-15-5654_de.htm (1.8.2016). Vgl. Art. 17 Abs. 2 EUV, Art. 114 Abs. 1 AEUV.
115 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 10.12.2015, BGBl. 2015 I, 2218.
116 Siehe Fn. 112.

GG beurteilen muss.[117] Sollten die Beschwerdeführer erfolglos bleiben, so hätten sie die Möglichkeit, wegen Verletzung ihres Rechts auf Privatsphäre in Art. 8 EMRK beim EGMR Individualbeschwerden nach Art. 34 EMRK zu erheben. Es bestehen gute Aussichten darauf, dass die Beschwerden gegen das Gesetz entweder in Karlsruhe oder spätestens in Straßburg erfolgreich sein werden, weil die anlasslose und umfassende Vorratsdatenspeicherung mit dem Grundrecht auf Datenschutz kaum vereinbar ist.[118]

(2) Durchführung von Unionsrecht?

Ob das deutsche Gesetz nach Art. 51 Abs. 1 GRCh auch an den Unionsgrundrechten in Art. 7 und 8 GRCh, wie sie vom EuGH im Fall *Digital Rights Ireland* interpretiert wurden, gemessen werden kann, hängt davon ab, ob der Bundesgesetzgeber damit das Recht der Union durchgeführt hat. Eine umzusetzende EU-Richtlinie zur Vorratsdatenspeicherung existiert ja nicht mehr. Auch der Umstand, dass der Entwurf des Gesetzes gemäß der Richtlinie 98/34/EG[119] in der zum damaligen Zeitpunkt geltenden Fassung[120] der Kommission notifiziert wurde, genügt nicht, um es in den Anwendungsbereich der Grundrechtecharta zu bringen. Denn diese Notifikation dient lediglich dazu, der Kommission und den anderen Mitgliedstaaten eine vorbeugende Kontrolle darüber zu ermöglichen, ob geplante nationale technische Vorschriften mit dem Binnenmarktrecht der Union vereinbar sind.[121] Ihre Notifikation allein macht die mitgeteilten nationalen Vorschriften aber nicht zu einer Durchführung von Unionsrecht. Die Frage ist freilich, ob nationale Gesetze zur Vorratsdatenspeicherung aufgrund von Art. 15 Abs. 1 der ePrivacy-Richtlinie,[122] der seinerseits auf Art. 6 Abs. 1 EUV verweist, den Unionsgrundrechten unterliegen. Diese Frage ist derzeit Gegenstand zweier Vorabentscheidungsersuchen an den EuGH, welche die Vorratsdatenspeicherungsgesetze aus Schweden und dem Vereinigten Königreich betreffen.[123] Man kann auch argumentieren, dass die Vorratsdatenspeicherung, soweit

117 Das BVerfG hat durch zwei Beschlüsse v. 8.6.2016 Anträge auf Erlass einer einstweiligen Anordnung gegen das Gesetz abgelehnt (1 BvQ 42/15, 1 BvR 229/16). Die Frage, ob und in welcher Weise die Europäische Grundrechtecharta oder sonstiges Unionsrecht für die Beurteilung der angegriffenen Vorschriften Bedeutung entfalte, sei im Hauptsacheverfahren zu entscheiden.

118 Vgl. CommDH/IssuePaper(2014)1, (Fn. 7), S. 114 ff.

119 RL 98/34/EG v. 22.6.1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften über die Dienste der Kommunikationsgesellschaft, ABl. L 204 v. 21.7.1998, S. 37. Zu späteren Änderungen vgl. ABl. L 241 v. 17.9.2015, S. 12.

120 Die RL 98/34/EG wurde inzwischen ersetzt durch die RL (EU) 2015/1535 v. 9.9.2015, ABl. L 241 v. 17.9.2015, S. 1.

121 EuGH, Rs. C-194/94, *CIA Security International SA*, EU:C:1996:172, Rn. 36 ff.

122 Siehe Fn. 63.

123 Rs. C-203/15, *Tele2 Sverige*; Rs. C-698/15, *Secretary of State for the Home Department v. Davis and others*. In seinen Schlussanträgen v. 19.7.2016 in diesen verbundenen Rechtssachen hat der Generalanwalt die Anwendbarkeit der Unionsgrundrechte bejaht und sich dafür ausgesprochen, dass Mitgliedstaaten eine Vorratsdatenspeicherung unter strengen unionsrechtlichen Voraussetzungen einführen dürfen.

EU-ausländische Diensteanbieter betroffen sind, einen Eingriff in den grenzüberschreitenden Dienstleistungsverkehr darstelle und aus diesem Grunde an die Art. 7 und 8 GRCh gebunden sei.[124]

Sollte der EuGH die Vorlagefrage bejahen, müssten die mitgliedstaatlichen Gerichte nationale Vorschriften zur Vorratsdatenspeicherung – neben den nationalen Grundrechten und Art. 8 EMRK – auch an Art. 7 und 8 GRCh messen. Art. 8 EMRK gibt in seiner Auslegung durch den EGMR dabei den Mindeststandard vor, hinter dem Art. 7 und 8 GRCh nicht zurückbleiben dürfen, den sie aber durchaus übertreffen können,[125] worüber letztlich ebenfalls der EuGH zu entscheiden hätte.[126] Aufgrund ihres unionsrechtlich angeordneten Anwendungsvorrangs vor unvereinbarem nationalem Recht[127] haben die Unionsgrundrechte eine größere Durchschlagskraft als Art. 8 EMRK. Sie überlagern auch nationale Grundrechte mit geringerer Schutzwirkung, doch können die letzteren ein höheres Schutzniveau vorsehen und zusätzliche Rechtsbehelfe (z.B. Verfassungsbeschwerde) eröffnen.[128]

(3) Bereichsausnahme „nationale Sicherheit"?

Die Vorratsdatenspeicherung wird zumeist unter Hinweis auf die öffentliche Sicherheit und/oder nationale Sicherheit gerechtfertigt. Da sie nach dem EuGH-Urteil im Fall *Digital Rights Ireland* den Wesensgehalt der Art. 7 und 8 GrCh nicht verletzt,[129] hängt ihre Zulässigkeit davon ab, ob sie die Grenzen des Verhältnismäßigkeitsgrundsatzes wahrt.[130] Zweifelsohne stellt die Wahrung sowohl der öffentlichen Sicherheit als auch der nationalen Sicherheit eine von der Union anerkannte dem Gemeinwohl dienende Zielsetzung dar, zu deren Gunsten die Grundrechte eingeschränkt werden können. Zu prüfen bleibt jedoch die Erforderlichkeit des Eingriffs und seine Verhältnismäßigkeit im engeren Sinne, was eine Abwägung zwischen den Sicherheitserfordernissen und den entgegenstehenden Grundrechten erfordert, um ein angemessenes Gleichgewicht (d.h. eine praktische Konkordanz) zwischen ihnen herzustellen.[131]

Gleichgültig, ob der EuGH oder ein nationales Gericht eine solche Abwägung vornehmen – sie kann dazu führen, dass das mitgliedstaatliche Interesse an der Wahrung der öffentlichen Sicherheit und/oder der nationalen Sicherheit ganz oder teilweise hinter die Unionsgrundrechte zurückgesetzt wird. Während das in Bezug auf die öf-

124 So *Boehm/Cole*, (Fn. 92), S. 56 f.; kritisch hingegen *Schiedermair/Mrozek*, Die Vorratsdatenspeicherung im Zahnräderwerk des europäischen Mehrebenensystems, DÖV 2016, S. 94 f.
125 Art. 52 Abs. 3 GRCh.
126 Art. 267 Abs. 3 AEUV.
127 Vgl. die Erklärung (Nr. 17) zum Vorrang im Anhang zur Schlussakte der Regierungskonferenz von Lissabon, ABl. C 306 v. 17.12.2007, S. 256.
128 Art. 53 GRCh.
129 Siehe unter D.II.1.b).
130 Art. 52 Abs. 1 GRCh.
131 Vgl. EuGH, Rs. C-547/14, *Philip Morris u.a.*, EU:C:2016:325, Rn. 154.

fentliche Sicherheit keineswegs ungewöhnlich ist,[132] kommt in Bezug auf die nationale Sicherheit der erst durch den Vertrag von Lissabon eingefügte Art. 4 Abs. 2 Satz 3 EUV ins Spiel, wonach die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt.[133] Das könnte man so verstehen, dass Maßnahmen eines Mitgliedstaats zugunsten seiner nationalen Sicherheit an keinem (auch keinem grundrechtlichen) Maßstab des Unionsrechts gemessen werden dürfen, weil sie von vornherein außerhalb von dessen Anwendungsbereich liegen.[134] Gegen eine solche ganz dem nationalen Belieben anheimgegebene Bereichsausnahme[135] spricht jedoch die konkrete Regelung in Art. 347, 348 AEUV, welche die Mitgliedstaaten selbst im Kriegsfall grundsätzlich an ihren unionsrechtlichen Pflichten festhält und deren Einhaltung auch durch Kommission und Gerichtshof überwachen lässt. Es ist daher zu erwarten, dass der EuGH den Art. 4 Abs. 2 Satz 3 EUV in ähnlicher Weise anwenden wird wie Art. 345 AEUV.[136] Dies entspräche seiner bisherigen Rechtsprechung zur primärrechtlichen Lage vor dem Inkrafttreten des Vertrags von Lissabon. Trotz der auch damals schon vorbehaltenen Zuständigkeit der Mitgliedstaaten für die Wahrung ihrer inneren und äußeren Sicherheit hatte es der Gerichtshof abgelehnt, eine entsprechende Ausnahme vom Anwendungsbereich des Gemeinschaftsrechts anzuerkennen, weil sonst dessen Verbindlichkeit und einheitliche Anwendung beeinträchtigt werden könnte.[137]

2. Das Urteil im Fall „Google Spain" von 2014: Begründung eines „Rechts auf Vergessenwerden" zweiten Grades

a) Einleitung und Ausgangsverfahren

Während das Urteil zum Fall *Digital Rights Ireland* einen hoheitlichen Eingriff in die Grundrechte auf Privatleben und Datenschutz betraf, ging es im Urteil *Google*

132 Seit langem wird z.B. im Rahmen von Art. 45 Abs. 3 und Art. 52 AEUV die öffentliche Sicherheit mit den Grundfreiheiten abgewogen, wenn ein Mitgliedstaat diese aus Sicherheitsgründen beschränkt.

133 Vgl. auch die Erklärung Nr. 20 zu Art. 16 AEUV im Anhang der Schlussakte der Regierungskonferenz von Lissabon von 2007, ABl. C 326 v. 26.10.2012, S. 347.

134 Vgl. in diesem Sinne die Begründungserwägung 16 der DSchGrVO und die Begründungserwägung 14 der RL (EU) 2016/680. Art. 23 DSchGrVO erlaubt den Mitgliedstaaten, bestimmte in der VO gewährleistete Rechte und Pflichten aus Gründen der nationalen Sicherheit zu beschränken, bindet die Mitgliedstaaten dabei jedoch an unionsrechtliche Vorgaben und macht damit deutlich, dass die nationale Sicherheit keine Bereichsausnahme bildet.

135 Abschnitt C, Ziffer 5 des Beschlusses der im Europäischen Rat vereinigten Staats- und Regierungschefs über eine neue Regelung für das Vereinigte Königreich innerhalb der EU (Anlage I zu den Schlussfolgerungen des Europäischen Rats v. 19.2.2016) deutet in diese Richtung. Nachdem das Brexit-Referendum eine Mehrheit für den Austritt des Vereinigten Königreichs aus der EU ergeben hat, ist der vorgenannte Beschluss seinen eigenen Bestimmungen (Abschnitt E, Ziffer 2) entsprechend obsolet geworden.

136 Zu Art. 345 AEUV vgl. *Kühling*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl. 2012, Art. 345 AEUV, Rn. 6 ff.

137 EuGH, Rs. C-372/05, *Kommission/Deutschland*, EU:C:2009:780, Rn. 68 ff.

Spain, das die anders zusammengesetzte Große Kammer des EuGH nur einen guten Monat später erließ,[138] um das Verhältnis der Datensubjekte zu privaten Verarbeitern ihrer personenbezogenen Daten nach Maßgabe der allgemeinen Datenschutzrichtlinie 95/46/EG[139] und der hinter dieser stehenden Grundrechte aus Art. 7 und 8 GRCh. Die nachfolgenden Ausführungen übergehen die Detailregelungen der Richtlinie und konzentrieren sich auf die grundrechtliche Situation. Der Gerichtshof hat die Richtlinienbestimmungen nämlich nicht nur – im Einklang mit seiner bisherigen Rechtsprechung – im Lichte der Grundrechte ausgelegt, sondern hat sie darüber hinaus geradezu als Regelungen zur Durchführung der grundrechtlichen Schutzerfordernisse behandelt.[140] Dementsprechend hat er zum einen den Anwendungsbereich der Richtlinienbestimmungen weit definiert und diese zum anderen so interpretiert, dass sie den Schutz der Privatsphäre effektiv und auf einem hohen Niveau gewährleisten können.[141]

Ein Spanier war 1998 als Schuldner von Forderungen der Sozialversicherung einem Zwangsversteigerungsverfahren ausgesetzt gewesen, in dem sein Grundstück gepfändet und versteigert wurde. Die bevorstehende Zwangsversteigerung war in einer auflagenstarken spanischen Tageszeitung zweimal unter Nennung seines Namens angezeigt worden. Die Anzeigenveröffentlichung war auf Anordnung des Arbeits- und Sozialministeriums in rechtmäßiger Weise erfolgt, um Informationen über den Versteigerungstermin möglichst weit zu verbreiten und dadurch für eine höchstmögliche Zahl an Bietern zu sorgen.[142] Vor diesem Hintergrund entschied die spanische Datenschutzagentur AEPD im Jahre 2010 auf die Beschwerde des Betroffenen, dass dieser gegen den Herausgeber der Tageszeitung keinen Anspruch auf Löschung dieser Informationen habe, die weiterhin online abrufbar waren.[143] Seiner gleichzeitigen Beschwerde gegen Google Spain SL und Google Inc. gab AEPD jedoch statt. Bei Eingabe seines Namens in die Suchmaschine des Google-Konzerns (Google Search) wurden den Internetnutzern nämlich weiterhin auch Links zu den beiden vorgenannten Annoncen angezeigt. Die AEPD hielt dies für unzulässig und ordnete an, die Informationen aus den Indexen von Google Search zu entfernen. Gegen diese Anordnung erhoben Google Spain und Google Inc. beim zuständigen spanischen Gericht Klage, das seinerseits dem EuGH eine Reihe von Fragen zur Auslegung der allgemeinen Datenschutzrichtlinie vorlegte. Das EuGH-Verfahren ist nicht zuletzt deswegen interessant, weil der Generalanwalt und die Große Kammer ganz unterschiedliche rechtliche Ansätze verfolgten.[144]

138 EuGH, Rs. C-131/12, *Google Spain*, EU:C:2014:317.
139 Siehe Fn. 61.
140 EuGH, Rs. C-131/12, *Google Spain*, EU:C:2014:317, Rn. 68 f.
141 Ibid., Rn. 34, 38, 53, 58, 66 und 84.
142 Ibid., Rn. 14, 16.
143 Ibid., Rn. 16.
144 Vgl. *Allen*, Remembering and Forgetting – Protecting Privacy Rights in the Digital Age, EDPL 3/2015, S. 164 ff.

b) Extensive Anwendung des EU-Datenschutzrechts durch den EuGH

(1) Suchmaschinenbetrieb als Datenverarbeitung

Der EuGH entschied erstens, dass die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellt Informationen, die personenbezogene Daten enthalten, zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Reihenfolge zur Verfügung zu stellen, eine Verarbeitung personenbezogener Daten im Sinne der Richtlinie darstelle, für die der Suchmaschinenbetreiber als Verantwortlicher im Sinne der Richtlinie einzustufen sei.[145] Dies begründete der Gerichthof unter anderem damit, dass die Richtlinienbestimmungen im Interesse eines wirksamen und umfassenden Schutzes der Datensubjekte weit auszulegen seien. Die Suchmaschinen hätten maßgeblichen Anteil an der weltweiten Verbreitung personenbezogener Daten, die ohne sie nicht gefunden würden, obwohl sie bereits im Internet veröffentlicht worden seien. Zudem erhielten die Nutzer von Suchmaschinen mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen und könnten damit ein mehr oder weniger detailliertes Profil der Person erstellen. Deshalb würden die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten durch Suchmaschinen über die Veröffentlichung der Daten auf den nachgewiesenen Websites hinaus erheblich beeinträchtigt.[146] Demgegenüber hatte der Generalanwalt in seinen Schlussanträgen dargelegt, dass Suchmaschinenbetreiber in der Regel keine für die Datenverarbeitung Verantwortliche im Sinne der Richtlinie seien, weil sie keine Kontrolle über die auf den Webseiten Dritter vorhandenen personenbezogenen Daten ausübten und die rechtlichen Verpflichtungen von Verantwortlichen nicht erfüllen könnten.[147]

(2) Werbung durch europäische Tochter erstreckt EU-Datenschutzrecht auf US-Muttergesellschaft

Zweitens erklärte der Gerichtshof im Einklang mit den Schlussanträgen des Generalanwalts die Richtlinie und die nationalen Bestimmungen zu ihrer Umsetzung auf den vorliegenden Fall für anwendbar, obwohl Google Search allein von der US-amerikanischen Muttergesellschaft Google Inc. ohne Mitwirkung ihrer spanischen Tochtergesellschaft Google Spain betrieben werde.[148] Denn die Tätigkeiten von Google Spain – Vermarktung von Produkten und Diensten der Onlinewerbung in Spanien – seien untrennbar mit den Tätigkeiten von Google Search verbunden: Die Suchmaschine werde erst mit der Vermarktung von Werbeflächen, die gleichzeitig mit den Such-

145 Der Sache nach entsprechend hat der BGH persönlichkeitsrechtsverletzende Suchwortergänzungsvorschläge bei der Eingabe eines Namens durch die Autocomplete-Funktion einer Suchmaschine dem Betreiber (Google Inc.) zugerechnet (BGHZ 197, 213).

146 EuGH, Rs. C-131/12, *Google Spain*, EU:C:2014:317, Rn. 21 ff., 36 ff.

147 Schlussanträge GA *Jääskinen* zu EuGH, Rs. C-131/12, *Google Spain*, EU:C:2013:424. So im Ergebnis auch *Sartor*, Search Engines as Controllers, 21 MJ 3 (2014), S. 564 ff.

148 Entsprechend hat der BGH, (Fn. 145), die Anwendbarkeit deutschen Deliktsrechts bejaht.

ergebnissen eingeblendet würden, wirtschaftlich rentabel gemacht und sei ihrerseits das Mittel, um die Vermarktung der Werbeflächen zu ermöglichen. Im Interesse eines wirksamen Grundrechtsschutzes müssten die Verpflichtungen und Garantien der Richtlinie auf eine derartige Konstellation erstreckt werden. Dass der Standort der Server, auf denen die mit Hilfe der Suchmaschine indexierten Informationen vorübergehend gespeichert werden und der aus Wettbewerbsgründen von Google geheim gehalten wird, möglicherweise außerhalb Europas liegt, spielte für den EuGH keine Rolle.[149]

Art. 3 Abs. 2 lit. a DSchGrVO kodifiziert nunmehr das vom Gerichtshof vorweggenommene Marktortprinzip sogar noch in schärferer Form.[150] Dieser Ansatz kann zu Regelungskonflikten führen, wenn der Datenverarbeiter in einem Drittland sitzt und dort abweichenden Datenschutzregeln unterliegt.[151] Andererseits kann die EU nur durch Anwendung des Marktortprinzips die Grundrechte ihrer Bürger schützen.[152]

(3) Grundsätzlicher Vorrang der Grundrechte des Datensubjekts – eigenständiger Löschungsanspruch gegen Suchmaschinenbetreiber

Drittens wurde der EuGH gefragt, ob ein Suchmaschinenbetreiber verpflichtet sei, zur Wahrung der Grundrechte einer Person von der Ergebnisliste, die im Anschluss an eine anhand des Namens dieser Person durchgeführte Suche angezeigt werde, Links zu von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person auch dann zu entfernen, wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht würden und ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig sei.[153]

Der Gerichtshof wies zunächst darauf hin, dass die Richtlinie 95/46/EG ihrerseits darauf abzielte, „ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten, insbesondere der Privatsphäre, natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten".[154] Überdies seien Richtlinienbestimmungen ohnehin stets im Lichte der einschlägigen Grundrechte auszulegen, im vorliegenden Fall der Art. 7 und 8 GRCh.[155] Andererseits müssten die berechtigten Interessen, einschließlich der Grundrechte, des für die Datenverarbeitung Verantwortlichen und gegebenenfalls von Dritten in Rechnung gestellt werden. Dies erfordere eine Abwägung der einander gegenüberstehenden Rechte und Interessen.[156]

149 BGHZ 197, 213, Rn. 43, 45 ff. Zustimmend *von Arnauld*, (Fn. 8), S. 21 ff.
150 *Kühling*, Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz, EuZW 2014, S. 529.
151 *Kuner*, Google Spain in the EU and International Context, Maastricht Journal of European and Comparative Law 22 (2015), S. 159 ff.
152 *Hijmans*, Right to Have Links Removed, 21 MJ 3 (2014), S. 560.
153 EuGH, Rs. C-131/12, *Google Spain*, EU:C:2014:317, Rn. 62.
154 Ibid., Rn. 66.
155 Ibid., Rn. 68 f.
156 Ibid., Rn. 74.

Die danach auch im vorliegenden Fall notwendige Abwägung ergab für den Gerichtshof – anders als für den Generalanwalt[157] – einen Vorrang der Grundrechte auf Achtung des Privatlebens und Datenschutz der betroffenen Person.[158] Denn die Verarbeitung personenbezogener Daten durch den Suchmaschinenbetreiber könne die vorgenannten Grundrechte erheblich beeinträchtigen, weil sie einen strukturierten Überblick über alle im Internet vorhandenen Informationen zu einer bestimmten Person und damit die Erstellung eines Persönlichkeitsprofils ermögliche und zudem den in der Ergebnisliste enthaltenen Informationen Allgegenwart (Ubiquität) verleihe. Im Hinblick auf die potenzielle Schwere des Eingriffs könne dieser nicht allein durch das wirtschaftliche Interesse des Suchmaschinenbetreibers gerechtfertigt werden; vielmehr müsse das Informationsinteresse der Internetbenutzer einbezogen werden.[159] In der Regel überwögen die Grundrechte der betroffenen Person aus Art. 7 und 8 GRCh auch die Interessen der Internetbenutzer, doch könne dies in besonders gelagerten Fällen anders sein. Das Abwägungsergebnis hänge ab von der Art der betreffenden Information, deren Sensibilität für das Privatleben der betroffenen Person und dem Interesse der Öffentlichkeit am Zugang zu dieser Information, das seinerseits je nach der Rolle der Person im öffentlichen Leben variiere.

Der EuGH unterstrich, dass der sich aus dieser Abwägung üblicherweise ergebende Anspruch der betroffenen Person auf Entfernung des betreffenden Links aus der Ergebnisliste der Suchmaschine unabhängig davon bestehe, ob die Primärinformation, zu der dieser Link führe, vorher oder gleichzeitig von dem Herausgeber der Internetseite gelöscht werde. Denn ein wirksamer und umfassender Schutz der betroffenen Person könne nicht erreicht werden, wenn diese vorher oder parallel gegen den Verwalter der Primärinformation vorgehen müsse. Auch sei nicht auszuschließen, dass sie gegen diesen keinen Löschungsanspruch habe, etwa weil die Abwägung der kollidierenden Rechtspositionen in diesem Verhältnis zu einem anderen Ergebnis führe. Denn die Listung einer Primärinformation als Ergebnis einer Suche mit einem Personennamen könne deren Zugänglichkeit erheblich erleichtern und eine entscheidende Rolle bei deren Verbreitung spielen, so dass sie einen stärkeren Eingriff in das Grundrecht auf Achtung des Privatlebens der betroffenen Person darstelle als die Veröffentlichung der Primärinformation.

Der Gerichtshof bejahte schließlich die dritte Vorlagefrage, ob die betroffene Person vom Suchmaschinenbetreiber die Entfernung von Links von der Ergebnisliste auch dann verlangen kann, wenn die Primärinformation wahrheitsgemäß ist und von dem Betreiber der Internetseite rechtmäßig veröffentlicht wurde. Denn die personenbezogenen Primärdaten entsprächen möglicherweise den Zwecken, für die sie ursprünglich erhoben oder verarbeitet worden seien, angesichts der verstrichenen Zeit nicht mehr, seien dafür nicht mehr erheblich oder gingen darüber hinaus. Ihre Wei-

157 Schlussanträge GA *Jääskinen* zu EuGH, Rs. C-131/12, *Google Spain*, EU:C:2013:424, Rn. 126 ff.

158 Ibid., Rn. 80 ff. Die Abwägung des BGH, (Fn. 145), ging auch zugunsten des Klägers aus, weil die Suchwortergänzungsvorschläge unwahre Tatsachenbehauptungen enthielten.

159 Einzubeziehen ist auch die Meinungsäußerungsfreiheit des Informationsurhebers, so zu Recht *Kühling*, (Fn. 150), S. 529.

terverarbeitung durch den Suchmaschinenbetreiber wäre dann rechtswidrig, selbst wenn der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste kein Schaden entstehe.[160] Dies in Anbetracht aller Umstände des Einzelfalls festzustellen und die Abwägung der kollidierenden Rechte und Interessen vorzunehmen, sei Sache des vorlegenden Gerichts. Dennoch ließ der Gerichtshof erkennen, dass im Ausgangsfall, in dem es um sensible Daten einer Privatperson über ein lange zurückliegendes Ereignis ohne erkennbare aktuelle Bedeutung ging, die betroffene Person einen Anspruch darauf haben dürfte, dass die betreffenden Links aus der Ergebnisliste, die bei der Suche mit dem Namen dieser Person erscheint, entfernt werden.[161]

c) Bewertung: Sieg des Datenschutzes durch Zensur des Internets?

Das EuGH-Urteil gegen Google ist als Sieg der Souveränität des Rechts gegen die Umgehungsmechanismen der Internet-Giganten gefeiert worden.[162] Unzweifelhaft hat der Gerichtshof im vorliegenden Fall entgegen den Schlussanträgen des Generalanwalts die Grundrechte der Einzelnen auf Persönlichkeits- und Datenschutz gegenüber den Internet-Giganten entscheidend gestärkt. Diese wirken zwar nicht direkt im Horizontalverhältnis, sondern nur auf dem Umweg über eine grundrechtskonforme Interpretation der allgemeinen Datenschutzrichtlinie, gewähren aber dennoch effektiven Schutz. Auch die neue DSchGrVO ist grundrechtskonform zu interpretieren. Da diese Interpretation sich im Dreieck zwischen Datensubjekt, Datenverarbeiter (Internet-Gigant) und Öffentlichkeit abspielt, sind neben den Persönlichkeits- und Datenschutzgrundrechten der betroffenen Person die unternehmerische Freiheit und Meinungsfreiheit des Datenverarbeiters[163] und die Informationsfreiheit der Mitglieder der Öffentlichkeit in einen Abwägungsprozess einzustellen, der zur Bildung einer praktischen Konkordanz führt. Auch die Meinungsfreiheit desjenigen ist einzubeziehen, der die Primärinformation auf seiner Internetseite veröffentlicht hat, die durch

160 Vgl. ibid. Demgegenüber ist in den USA ein Betroffener, der den Betreiber einer Suchmaschine (*people search engine*) auf Berichtigung falscher Angaben zu seiner Person im Suchergebnis auf der Grundlage des Fair Credit Reporting Act von 1970 verklagen will, nur klagebefugt, wenn er eine tatsächliche Verletzung eines rechtlich geschützten Interesses belegen kann. Die Unrichtigkeit der Angaben allein genügt dafür nicht, vgl. US Supreme Court, *Spokeo Inc. v. Robins*, No. 13-339, Entscheidung v. 16.5.2016, www.supremecourt.gov/opinions/15pdf/13-1339_f2q3.pdf (1.8.2016).

161 EuGH, Rs. C-131/12, *Google Spain*, EU:C:2014:317, Rn. 94, 96, 98.

162 Vgl. *Kühling*, (Fn. 150), S. 527, 532.

163 Die Meinungsfreiheit der Suchmaschinenbetreiber bleibt regelmäßig im Hintergrund, wenn die Suchmaschine die aufgelisteten Links nicht nach inhaltlichen Kriterien filtert, ist aber involviert, vgl. Schlussanträge GA *Jääskinen* zu EuGH, Rs. C-131/12, *Google Spain*, EU:C:2013:424, Rn. 132. Bei Internet-Nachrichtenportalen spielt sie hingegen die zentrale Rolle, siehe EGMR [GK], Nr. 64569/09, *Delfi AS v. Estonia*, Urt. v. 16.6.2015; EGMR, Nr. 22947/13, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, Urt. v. 2.2.2016.

die Indexierung eine wesentlich weitere Verbreitung erfährt.[164] Es handelt sich also regelmäßig um ein Rechteck von widerstreitenden Grundrechten.[165]

In diesem Abwägungsprozess kommt nach Ansicht des EuGH den Persönlichkeits- und Datenschutzgrundrechten der betroffenen Person ein besonderes Gewicht zu, jedenfalls wenn es sich um keine Person der Zeitgeschichte (*public figure*) handelt. Demgegenüber hatte der Generalanwalt die Rechte der Suchmaschinen- und Webseitenbetreiber auf Meinungsfreiheit sowie die Informationsfreiheit der Allgemeinheit für vorrangig gehalten und dabei die Informationsfreiheit im Unionsrecht für besonders schutzwürdig angesehen, „vor allem angesichts der anderenorts immer ausgeprägteren Neigung autoritärer Regimes, den Zugang zum Internet zu beschränken oder die im Internet zugänglichen Inhalte zu zensieren".[166] Während der Gerichtshof also im Zweifel für den Persönlichkeits- und Datenschutz der betroffenen Person entscheiden will, hatte der Generalanwalt sich im Zweifel für die Informationsfreiheit ausgesprochen, immer bezogen auf Fälle, in denen die personenbezogene Information der Wahrheit entspricht und rechtmäßig im Internet veröffentlicht wurde.[167] Für jeden der beiden Ansätze sprechen gute Gründe, doch hat der EuGH im Verhältnis zum Generalanwalt das letzte Wort. Es bleibt abzuwarten, ob dieser oder ein ähnlich gelagerter Fall dem Europäischen Gerichtshof für Menschenrechte unterbreitet wird[168] und dieser dann die Kollision zwischen Art. 8 und 10 EMRK in der gleichen Weise auflöst wie der EuGH.[169]

Das EuGH-Urteil im Fall *Google Spain* gilt als Grundlage eines „Rechts auf Vergessenwerden".[170] Der Gerichtshof verwendet diesen Begriff allerdings lediglich bei der Wiedergabe der dritten Frage des vorlegenden Gerichts.[171] Dieses wollte wissen, ob ein Anspruch eines Datensubjekts gegen den Suchmaschinenbetreiber auf Entfer-

164 Dieser Aspekt spielte im Ausgangsverfahren einer amtlichen Bekanntmachung keine Rolle und wird vom EuGH daher nicht behandelt. Vgl. jedoch die Schlussanträge GA *Jääskinen* zu EuGH, Rs. C-131/12, *Google Spain*, EU:C:2013:424, Rn. 122, 134.

165 Eingehend *Spiecker genannt Döhmann*, A new framework for information markets: Google Spain, CMLR 52 (2015), S. 1045 ff.

166 Schlussanträge GA *Jääskinen* zu EuGH, Rs. C-131/12, *Google Spain*, EU:C:2013:424, Rn. 121, 126 ff.

167 Kritiker aus Nordamerika werfen dem EuGH vor, er habe das Recht auf Datenschutz zum Recht auf Zensur umgefälscht: *Wolf*, Impact of the CJEU's Right to be Forgotten, 21 MJ 3 (2014), S. 551 ff.

168 Wenn Google Spain im spanischen Ausgangsverfahren letztlich unterliegt, könnte es nach Art. 34 EMRK eine Individualbeschwerde gegen Spanien einlegen. Da die spanischen Gerichtsentscheidungen vom EU-Recht determiniert werden, würde der EGMR nach Maßgabe seiner „Bosphorus"-Rechtsprechung – EGMR, Nr. 45036/98, *Bosphorus*, Urt. v. 30.6.2005 – vermuten, dass Spanien die Konventionsrechte von Google Spain nicht verletzt habe, und diese Vermutung auch nicht als im Einzelfall widerlegt ansehen. Eine strikte Prüfung anhand der EMRK würde der EGMR hingegen vornehmen, wenn der Eingriff in die Rechte des Suchmaschinenbetreibers (Art. 10 EMRK, Art. 1 ZP) von einem Gericht eines Konventionsstaats vorgenommen würde, der kein EU-Mitglied ist.

169 Kritisch zur Ausblendung der EMRK-Dimension durch den EuGH *Frantziou*, Further Developments in the Right to be Forgotten, Human Rights Law Review 2014, S. 772 ff.

170 *Boehme-Neßler*, Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, NVwZ 2014, S. 825 ff.

171 EuGH, Rs. C-131/12, *Google Spain*, EU:C:2014:317, Rn. 20, 89.

nung von Links zu von Dritten rechtmäßig veröffentlichten Internetseiten mit wahrheitsgemäßen personenbezogenen Informationen nur besteht, wenn diese Informationen dem Datensubjekt schaden können, oder bereits dann, wenn es nur möchte, dass sie nach einer gewissen Zeit vergessen werden. Der EuGH antwortete im Sinne der zweiten Alternative und bejahte damit der Sache nach ein Recht auf Vergessenwerden zweiten Grades im Sinne eines Rechts auf Nichtindexierung von in einem Internet-Archiv weiterhin vorhanden bleibender Primärinformation. Ein echtes Recht auf Vergessenwerden müsste hingegen auch die Entfernung der Primärinformation selbst umfassen.[172] Angesichts der globalen Informationsvernetzung wäre deren restlose Eliminierung aber schon faktisch kaum durchsetzbar, selbst wenn die Primärinformation unwahr ist, zu Unrecht verarbeitet wurde oder kein berechtigtes Interesse an ihrer Erhaltung besteht.[173] Ihre Tilgung aus dem betreffenden Internet-Archiv würde überdies auf einen mit dem von Art. 10 EMRK geschützten Informationsinteresse der Öffentlichkeit unvereinbaren Versuch zur Umschreibung der Geschichte durch „Bereinigung" der Internet-Archive der Medien hinauslaufen. Daher können in ihren Grundrechten verletzte Datensubjekte in aller Regel nur einen Anspruch darauf haben, dass der weiterhin verfügbar bleibenden Primärinformation ein Hinweis auf ihr Obsiegen in einem Zivilprozess hinzugefügt wird.[174]

Zur Umsetzung der Anforderungen des EuGH-Urteils in Europa musste Google inzwischen mehrere hunderttausend Anträge betroffener Personen auf Entfernung von Suchergebnissen bearbeiten. In der Praxis funktioniert dies weitgehend, doch gehen bei den Datenschutzbeauftragten auch zahlreiche Beschwerden ein.[175] Streitig ist insbesondere noch, ob ein weltweit operierender Suchmaschinenbetreiber die Entfernung von Suchergebnissen auf seine europäischen Suchmaschinenseiten beschränken darf oder weltweit durchführen muss.[176]

d) Kodifikation der Entscheidung in Art. 17 DSchGrVO

Das EuGH-Urteil in *Google Spain* hat zu einer umfassenden Kodifikation eines Rechts auf Löschung („Recht auf Vergessenwerden") in Art. 17 DSchGrVO geführt. Danach können Datensubjekte die unverzügliche Löschung ihrer personenbezogenen Daten von allen für die Bearbeitung Verantwortlichen verlangen, also sowohl von dem Betreiber der Internet-Seite mit der Primärinformation als auch von dem Suchmaschinenbetreiber, der die Verknüpfung zu dieser Seite herstellt,[177] soweit zumindest einer der abschließend aufgelisteten Löschungsgründe auf den jeweiligen Verant-

172 *Nolte*, Das Recht auf Vergessenwerden – mehr als nur ein Hype?, NJW 2014, S. 2240.
173 Siehe dazu im Einzelnen *Gstrein*, (Fn. 82), S. 21, 231 ff.
174 Vgl. EGMR, Nr. 33846/07, *Węgrzynowski and Smolczewski v. Poland*, Urt. v. 16.7.2013, Rn. 65 ff.
175 Dazu näher *Tomik*, Gefiltert, FAZ Nr. 35 v. 11.2.2016, S. 8.
176 Vgl. http://rsw.beck.de/aktuell/meldung/recht-auf-vergessen-werden-google-zieht-gegen-franzoesische-datenschutz-aufsicht-vor-gericht (1.8.2016).
177 Vgl. die weite Definition von „Verarbeitung" und „Verantwortlicher" in Art. 4 Ziffern 2 und 7 DSchGrVO.

wortlichen zutrifft. Kurzgefasst erkennt Art. 17 Abs. 1 DSchGrVO folgende sechs Löschungsgründe an: Die personenbezogenen Daten sind für den Zweck, für den sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig. Die betroffene Person widerruft ihre Einwilligung, auf der die Verarbeitung beruhte, und es gibt keine andere Rechtsgrundlage für diese. Die betroffene Person legt Widerspruch gegen die Verarbeitung ein. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet. Die Löschung ist zur Erfüllung einer unionsrechtlichen oder nationalrechtlichen Verpflichtung erforderlich. Die personenbezogenen Daten wurden von einem Kind im Zusammenhang mit einem Angebot von Diensten der Informationsgesellschaft[178] erhoben.

Art. 17 Abs. 2 DSchGrVO enthält eine weitergehende Regelung für Fälle, in denen ein löschungspflichtiger Verantwortlicher die personenbezogenen Daten öffentlich gemacht und damit die Grundrechte des Datensubjekts in besonders schwerwiegender Weise beeinträchtigt hat. In einer Konstellation wie im Fall *Google Spain* würde der Betreiber der Internetseite von dieser Regelung erfasst, nicht jedoch der Suchmaschinenbetreiber, der bereits veröffentlichte Daten nur indexiert. Den Veröffentlicher trifft über die Löschungspflicht hinaus die weitere Pflicht,

> „unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art [zu treffen], um [andere] für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat."

Demzufolge müsste der Betreiber der Internetseite unter anderem die Betreiber von Suchmaschinen entsprechend informieren. Diese Ausweitung des Rechts auf Löschung, die dem „Recht auf Vergessenwerden" im Netz mehr Geltung verschaffen soll,[179] wird mit ihrer Anknüpfung an die verfügbare Technologie, die Implementierungskosten und die Angemessenheit der Maßnahmen zu zahlreichen Streitfällen führen. Deren Entscheidung durch die nationalen Gerichte in Kooperation mit dem EuGH wird im Laufe der Zeit die notwendigen richterrechtlichen Klarstellungen bringen.

Art. 17 Abs. 3 DSchGrVO schränkt sowohl das einfache Recht auf Löschung nach Art. 17 Abs. 1 DSchGrVO als auch das erweiterte Recht auf Löschung nach Art. 17 Abs. 2 DSchGrVO ein. Diese Rechte sollen nicht bestehen, wenn die Verarbeitung aus mindestens einem von fünf abschließend aufgelisteten Gründen erforderlich ist: zur Ausübung des Rechts auf freie Meinungsäußerung und Information; zur Erfüllung einer unions- oder nationalrechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse; in bestimmten Fällen aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit; für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke

178 Vgl. Art. 4 Ziff. 25 DSchGrVO i.V.m. Art. 1 Ziffer 1 lit. b der RL (EU) 2015/1535 v. 9.9.2015, ABl. L 241 v. 17.9.2015, S. 1.

179 Vgl. die Begründungserwägung 66 der DSchGrVO.

oder statistische Zwecke; schließlich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Bei Anwendung des Art. 17 Abs. 3 DSchGrVO, der eine gesetzliche Grundlage im Sinne des Art. 52 Abs. 1 GRCh für Einschränkungen der Grundrechte in Art. 7 und 8 GRCh bildet, ist regelmäßig eine Abwägung zwischen diesen Grundrechten und den in Art. 17 Abs. 3 DSchGrVO kodifizierten entgegenstehenden Rechten und Interessen erforderlich. Diese erfolgt im Kontext der nach Art. 52 Abs. 1 Satz 2 GRCh vorgeschriebenen Verhältnismäßigkeitsprüfung. Ob die Grundrechte des betroffenen Datensubjekts in dieser Abwägung typischerweise vorrangig sind, wie der EuGH in *Google Spain* entschieden hat, oder das Informationsinteresse der Allgemeinheit, wie es der Generalanwalt vorgeschlagen hatte, kann man dem Text der Bestimmung nicht entnehmen. Es ist zu erwarten, dass die Anwendung des Art. 17 Abs. 3 DSchGrVO die nationalen Gerichte und den EuGH häufig beschäftigen wird.

3. Das Urteil im Fall „Schrems" von 2015: Schutz gegen die Übermittlung personenbezogener Daten in unsichere Drittländer

Etwa eineinhalb Jahre nach den beiden vorstehend analysierten Urteilen traf die Große Kammer des EuGH eine weitere Grundsatzentscheidung zum Datenschutz im Fall *Schrems*. Es ging dort um die Gewährleistung eines angemessenen Datenschutzniveaus bei Übermittlung personenbezogener Daten durch ein privates Unternehmen (Facebook Ireland Ltd., eine Tochtergesellschaft der in den USA ansässigen Facebook Inc.) in das Drittland USA, wo sie auf Servern von Facebook Inc. gespeichert wurden.[180]

a) Hintergrund: Die Grundsätze des „sicheren Hafens" zum Datenschutz

Während die EU- und die EWR-Staaten einen datenschutzrechtlichen Binnenraum bilden, in dem ein unbehinderter grenzüberschreitender Datenverkehr gewährleistet werden kann, weil überall dieselben datenschutzrechtlichen Mindeststandards gelten,[181] sind Drittländer in dieser Hinsicht unsicheres Terrain. Die allgemeine Datenschutzrichtlinie 95/46/EG stellt daher in Art. 25 besondere Anforderungen an die Übermittlung personenbezogener Daten in Drittländer, um die Umgehung der europäischen Datenschutzstandards durch Verlagerung der Datenverarbeitung aus Europa heraus zu verhindern.[182] Eine solche Übermittlung ist nur zulässig, wenn im Drittland ein „angemessenes Schutzniveau" für die Daten gewährleistet ist, was unter Berücksichtigung aller Umstände beurteilt werden muss. Die Aufgabe, dieses sicherzustellen, teilen sich die Mitgliedstaaten und die Kommission. Letztere kann nach

180 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650.
181 *Kühling/Heberlein*, EuGH „reloaded": „unsafe harbor" USA vs. „Datenfestung" EU, NVwZ 2016, S. 7. Vgl. Art. 1 Abs. 2 RL 95/46/EG und Art. 1 Abs. 3 DSchGrVO.
182 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 73.

Art. 25 Abs. 6 der Richtlinie allgemein feststellen, dass ein bestimmtes Drittland ein angemessenes Schutzniveau gewährleistet.

Mit ihrer Entscheidung 2000/520 stellte die Kommission fest, dass die USA ein angemessenes Schutzniveau gewährleisteten, obwohl es dort kein allgemeines Datenschutzgesetz gab.[183] Sie stützte sich unter anderem auf die der Entscheidung angehängten „Grundsätze des ‚sicheren Hafens' zum Datenschutz" und die als „Häufig gestellte Fragen" betitelten Leitlinien zu deren Umsetzung, die beide vom US-Handelsministerium stammten, sowie auf weitere Anlagen. Aus diesen ergab sich, dass die Empfänger der Daten in den USA („US-Organisationen") sich eindeutig und öffentlich verpflichtet haben mussten, diese Grundsätze nach Maßgabe der Leitlinien einzuhalten (System der Selbstzertifizierung). Weiterhin war festgelegt, dass die Geltung der Grundsätze begrenzt werden konnte

> „a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen [...]".

In der Variante b) mussten die Datenempfänger nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das notwendige Ausmaß beschränkte. Zur Durchsetzung waren private Schiedsverfahren sowie Beschwerden an die Federal Trade Commission wegen unlauterer oder irreführender Geschäftspraktiken vorgesehen.

Nachdem durch die Snowden-Enthüllungen öffentlich bekanntgeworden war, dass die US-Nachrichtendienste im Rahmen des sogenannten PRISM-Programms in umfassender und beliebiger Weise auf in den USA gespeicherte personenbezogene Daten auch von Unionsbürgern zugriffen, stellte die Kommission selbst im November 2013 in zwei Mitteilungen fest, dass das Safe-Harbor-System erhebliche Schwachstellen aufweise, und zwar sowohl hinsichtlich der tatsächlichen Zugriffe der US-Nachrichtendienste auf die Daten mehrerer hundert Millionen europäischer Kunden als auch hinsichtlich der nur sehr eingeschränkten Rechtsschutzmöglichkeiten. Safe Harbor sei zu einem Informationskanal geworden, über den die amerikanischen Nachrichtendienste auf ursprünglich in Europa verarbeitete personenbezogene Daten zugreifen könnten.[184] Die Aufhebung dieses Systems würde freilich den Interessen der beteiligen Unternehmen in der EU und den USA schaden, doch werde sie mit den US-Behörden unverzüglich Gespräche über die festgestellten Mängel aufnehmen.[185]

b) Ausgangsverfahren in Irland

Herr *Schrems*, der Kläger des Ausgangsverfahrens, ein in Österreich wohnhafter österreichischer Staatsangehöriger, musste, um Facebook nutzen zu können, 2008 einen Vertrag mit Facebook Ireland abschließen. Auf dessen Grundlage wurden seine per-

183 Europäische Kommission, Entscheidung v. 26.7.2000, ABl. L 215 v. 25.8.2000, S. 7.
184 Schlussanträge GA *Bot* zu EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:627, Rn. 157.
185 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 11 ff.

sönlichen Daten an in den USA befindliche Server von Facebook Inc. übermittelt und dort verarbeitet. Im Juni 2013 legte er Beschwerde beim irischen Datenschutzbeauftragten ein, um diesen zu veranlassen, Facebook Ireland die Übermittlung seiner personenbezogenen Daten in die USA zu verbieten. Zur Begründung verwies er auf die vorgenannten Enthüllungen von *Edward Snowden*. Daraus ergebe sich, dass das Recht und die Praxis der USA keinen ausreichenden Datenschutz gewährleisteten.

Der irische Datenschutzbeauftragte wies die Beschwerde als unbegründet zurück, weil nicht bewiesen sei, dass die US-Nachrichtendienste auf die persönlichen Daten gerade des Beschwerdeführers zugegriffen hätten,[186] und die Kommission überdies bindend festgestellt habe, dass in den USA ein angemessenes Datenschutzniveau besteht. Daraufhin erhob Herr *Schrems* Klage beim High Court, der dem EuGH die Frage zur Vorabentscheidung vorlegte, ob ein unabhängiger nationaler Datenschutzbeauftragter an eine Kommissionsentscheidung nach Art. 25 Abs. 6 der allgemeinen Datenschutzrichtlinie absolut gebunden sei oder das Datenschutzniveau in dem betreffenden Drittland selbstständig prüfen dürfe.

c) EuGH erkennt Verletzung grundrechtlicher Wesensgehalte durch die Kommission

Das EuGH-Urteil wurde ganz ungewöhnlich schnell nur dreizehn Tage nach den Schlussanträgen des Generalanwalts verkündet, denen es sich in allen wesentlichen Punkten anschloss.[187] Einwände, welche die U.S. Mission bei der EU gegen die Schlussanträge erhoben hatte, insbesondere was die Darstellung der Rechtslage in den USA betraf, fanden bei den Richtern kein Gehör.[188] Diese sahen von einer detaillierten Prüfung des Inhalts der Safe-Harbor-Grundsätze ab und beschränkten sich darauf, eklatante und offenkundige Schutzlücken festzustellen.[189] Damit identifizierte sich der EuGH erneut als Protagonist des Grundrechtsschutzes in Europa im Allgemeinen und des Datenschutzes im Besonderen.[190]

186 Auf dieses Argument ging der EuGH in seinem Urteil nicht ein; der GA *Bot* zu EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:627, Rn. 59 ff., hatte es zu Recht zurückgewiesen. Denn allein der Umstand, dass die Daten aller Facebook-Benutzer dem unbegrenzten Zugriff von US-Behörden ausgesetzt sind, belegt, dass in den USA kein angemessenes Datenschutzniveau existiert. Auch der EGMR verlangt für die Beschwerdebefugnis gegenüber geheimen Überwachungsmaßnahmen, gegen die es keinen effektiven nationalen Rechtsschutz gibt, keinen Nachweis der persönlichen Betroffenheit, vgl. EGMR [GK], Nr. 47143/06, *Zakharov v. Russia*, Urt. v. 4.12.2015, Rn. 171.

187 Vgl. *Gstrein*, Regulation of Technology in the EU and beyond – The state of play in autumn 2015, Saar Blueprint 03/2015 EN, http://jean-monnet-saar.eu/wp-content/uploads/2013/12/The-regulation-of-Technology-in-the-European-Union-and-beyond_EN.pdf (1.8.2016), S. 9 f. Zu einer Abweichung des Urteils von den Schlussanträgen siehe jedoch Fn. 192.

188 Stellungnahme v. 28.9.2015, http://useu.usmission.gov/st-09282015.html (1.8.2016).

189 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 98. Vgl. *Coudert*, Schrems vs. Data Protection Commissioner, European Law Blog v. 15.10.2015, http://europeanlawblog.eu/?p=2931 (1.8.2016); *Kühling/Heberlein*, (Fn. 181), S. 9 f.

190 *Gstrein*, (Fn. 187), S. 10; *Eichenhofer*, „e-Privacy" im europäischen Grundrechtsschutz: Das „Schrems"-Urteil des EuGH, EuR 2016, S. 86.

Der Gerichtshof betonte eingangs unter Bezugnahme auf seine frühere Rechtsprechung die Bedeutung der in Art. 7 und 8 GRCh gewährleisteten Grundrechte sowie die Notwendigkeit, die Richtlinie 95/46/EG grundrechtskonform zu interpretieren. Wesentliches Element des europäischen Datenschutzes sei die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten mit weitreichenden Befugnissen. Die in der Richtlinie vorgesehene Feststellung, ob ein Drittland ein angemessenes Datenschutzniveau gewährleiste, werde sowohl von den Mitgliedstaaten als auch von der Kommission getroffen. Eine entsprechende Entscheidung der Kommission nach Art. 25 Abs. 6 der Richtlinie richte sich an die Mitgliedstaaten und binde diese und alle ihre Organe gemäß Art. 288 Abs. 4 AEUV, solange sie nicht vom Gerichtshof für ungültig erklärt worden sei.[191] Nationale Datenschutzbeauftragte könnten daher keine dieser Entscheidung zuwiderlaufenden Maßnahmen treffen.[192] Sie seien aber nicht gehindert, sondern nicht zuletzt im Hinblick auf Art. 8 Abs. 3 GRCh sogar verpflichtet, ihrerseits in völliger Unabhängigkeit zu prüfen, ob die Anforderungen des Art. 25 der Richtlinie – angemessenes Datenschutzniveau im Drittland – erfüllt seien. Sollte dies ihrer Auffassung nach nicht der Fall sein, so müsse ihnen nach dem jeweiligen nationalen Recht eine Klagemöglichkeit zustehen, um die nationalen Gerichte zu einer inzidenten Überprüfung der gegenteiligen Kommissionsentscheidung veranlassen zu können.[193] Wenn die nationalen Gerichte die Bedenken der Datenschutzbeauftragten an der Gültigkeit der Kommissionsentscheidung teilten, müssten sie dazu eine Vorabentscheidung des EuGH einholen.

Obwohl der irische High Court danach nicht ausdrücklich gefragt, sondern nur entsprechende Zweifel angemeldet hatte, prüfte der EuGH die Gültigkeit der Kommissionsentscheidung 2000/520, um dem vorlegenden Gericht sogleich eine vollständige Antwort geben zu können. Der von der Richtlinie 95/46/EG vorgegebene Prüfungsmaßstab – „Gewährleistung eines angemessenen Schutzniveaus" in einem Drittland – bedeutet für den EuGH wie schon für den Generalanwalt, dass dort rechtlich und tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet wird, das dem in der Union durch die Richtlinie 95/46/EG im Lichte der Grundrechtecharta garantierten Niveau der Sache nach gleichwertig ist. Die Kommission sei verpflichtet, auch nach Erlass einer entsprechenden positiven Entscheidung die Angemessenheit des Schutzniveaus im Drittland in regelmäßigen Abständen zu prüfen, jedenfalls wenn Anhaltspunkte für diesbezügliche Zweifel bestünden. Angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung der Privatsphäre und der großen Zahl von möglicherweise

191 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 51 ff.

192 Dementgegen hatte der GA *Bot* zu EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:627, Rn. 117 ff., 227, 237, die nationalen Datenschutzbeauftragten für befugt gehalten, die Datenübermittlung in das Drittland ggf. auszusetzen, noch bevor der EuGH die Entscheidung der Kommission für ungültig erklärt.

193 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 65. Der Bundesrat hat inzwischen verlangt, zur Umsetzung der Safe-Harbor-Entscheidung des EuGH ein ausdrückliches Klagerecht der Datenschutzaufsichtsbehörden von Bund und Ländern in Gestalt einer „objektiven Feststellungsklage" im BDSG zu verankern, vgl. Entschließung des Bundesrates v. 13.5.2016, BR-Drs. 171/16 (Beschluss).

in ihren Grundrechten verletzten Personen unterlägen Kommissionsentscheidungen nach Art. 25 Abs. 6 der Richtlinie einer strikten Kontrolle durch den Gerichtshof.[194] Damit ist gemeint, dass der Kommission kein eigener Beurteilungsspielraum zusteht, den der EuGH zu achten hätte.

Der EuGH stellte fest, dass die Entscheidung 2000/520 gegen den Wesensgehalt sowohl des Grundrechts auf Achtung des Privatlebens (Art. 7 GRCh) als auch des Grundrechts auf wirksamen gerichtlichen Rechtsschutz (Art. 47 GRCh) verstieß, und erklärte sie deshalb für ungültig. Der Unterschied zum Fall *Digital Rights Ireland*, in dem er eine Wesensgehaltsverletzung in Bezug auf Art. 7 GRCh abgelehnt hatte, lag darin, dass die US-Behörden im vorliegenden Fall generell auf den Inhalt elektronischer Kommunikation und nicht nur die Verkehrsdaten zugreifen konnten.[195] Der Verstoß gegen den Wesensgehalt des Art. 47 GRCh ergab sich für den EuGH daraus, dass die Datensubjekte keinerlei Rechtsbehelf hatten.

Der Gerichtshof kritisierte, dass nur selbstzertifizierte US-Organisationen, nicht aber US-Behörden an die Safe-Harbor-Grundsätze gebunden seien und dass ein genereller und unbestimmter Vorrang der nationalen Sicherheit, des öffentlichen Interesses und unvereinbarer gesetzlicher Anordnungen vorbehalten werde. Er beanstandete weiterhin, dass die Kommission keine Feststellung zu in den USA eventuell bestehenden rechtlichen Schranken für Eingriffe in die Grundrechte der Datensubjekte oder zu dem für diese eventuell verfügbaren wirksamen gerichtlichen Rechtsschutz getroffen habe. Ob die dem unbegrenzten Zugriff der US-Behörden ausgesetzten Informationen über die Privatsphäre der Datensubjekte sensiblen Charakter hätten oder die Betroffenen durch solche Eingriffe Nachteile erlitten haben könnten, sei unerheblich.[196] Nachdem der EuGH bereits Verstöße gegen die Wesensgehaltssperre feststellt hatte (Art. 52 Abs. 1 Satz 1 GRCh), brauchte er keine detaillierte Verhältnismäßigkeitsprüfung mehr vorzunehmen (Art. 52 Abs. 1 Satz 2 GRCh).[197] Deswegen konnte er sich auch eine Abwägung der Grundrechte der Datensubjekte mit den gegenläufigen Rechten und Interessen (z.B. nationale Sicherheit der USA sowie wirtschaftliche Rechte und Interessen der beteiligten Unternehmen im Hinblick auf eine möglichst freie Datenübermittlung) ersparen.

d) Bewertung: Dogmatik und Folgen des „Schrems"-Urteils

(1) Datenexport bedingt Grundrechtsexport unter strikter gerichtlicher Kontrolle

Dogmatisch betrifft das „Schrems"-Urteil, wie das „Google Spain"-Urteil, das Verhältnis der Datensubjekte zu privaten Verarbeitern ihrer personenbezogenen Daten, nimmt aber auch Grundrechtsgefährdungen seitens dritter Staaten in den Blick und thematisiert überdies wesentlich deutlicher als jenes die Schutzpflicht sowohl der EU als auch der Mitgliedstaaten. Diese bilden gemeinsam die Spitze eines gleichschenk-

194 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 70 ff.
195 *Eichenhofer*, (Fn. 190), S. 84 f.
196 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 79 ff.
197 Vgl. *Eichenhofer*, (Fn. 190), S. 84 f. zur Abwägungsfähigkeit des Wesensgehalts.

ligen Dreiecks, an dessen Basis sich das Datensubjekt und der private Datenverarbeiter in der EU auf gleicher Höhe gegenüberstehen. Durch Übertragung der personenbezogenen Daten an einen zweiten Datenverarbeiter in einem Drittland setzt der (EU-)Datenverarbeiter das Datensubjekt weiteren Grundrechtseingriffen durch jenen und die Behörden des Drittlandes aus.

Der Übertragungsakt als solcher stellt eine in der EU stattfindende und deshalb ohne weiteres den europäischen Datenschutzregeln und Grundrechten unterworfene Maßnahme dar, so dass keine völkerrechtlich möglicherweise problematische extraterritoriale Anwendung europäischen Rechts vorliegt.[198] In die Beurteilung der Angemessenheit des Datenschutzniveaus im Drittland werden auch Zugriffsrechte von Drittlandsbehörden einbezogen, die zur Wahrung der dortigen öffentlichen oder nationalen Sicherheit erfolgen. Entsprechende Zugriffsrechte von mitgliedstaatlichen Behörden liegen demgegenüber außerhalb des Anwendungsbereichs der Datenschutzbestimmungen des EU-Sekundärrechts[199] – nicht jedoch des Art. 8 GRCh.[200]

Die Aufgabe der EU und des betreffenden Mitgliedstaats (hier Irland) besteht in diesen Drittlandskonstellationen darin, die Grundrechte des Datensubjekts und des Datenverarbeiters sowie das öffentliche Interesse (z.B. am Datenverkehr mit dem Drittland)[201] in ein ausgewogenes Verhältnis (d.h. eine praktische Konkordanz) zu bringen. Dazu sind die Gesetzgeber, die in den Gesetzesvollzug eingebundenen Exekutivstellen und bei der Auslegung der entsprechenden Gesetze die Gerichte der europäischen und nationalen Ebene verpflichtet. In Erfüllung seiner Schutzpflicht hat der europäische Gesetzgeber unter anderem die Richtlinie 95/46/EG erlassen. Die Kommission hat bei der Anwendung des Art. 25 Abs. 6 dieser Richtlinie ihre Schutzpflicht im vorliegenden Fall aber vernachlässigt, so dass der irische High Court und der EuGH eingreifen mussten, um eine angemessene praktische Konkordanz wiederherzustellen. Dass der EuGH der Kommission in einem derart grundrechtssensiblen Bereich keinen Beurteilungsspielraum einräumt, ist nicht zu beanstanden. Im Übrigen hätte die Kommission die Grenzen eines solchen Spielraums im vorliegenden Fall zweifellos überschritten. Die ausdrückliche Klarstellung des Gerichtshofs in Bezug auf seine Kontrolldichte ist daher offensichtlich für zukünftige Fälle gedacht.

Nach Art. 25 Richtlinie 95/46/EG ist die Übermittlung von personenbezogenen Daten in Drittländer nur zulässig, wenn diese ein „angemessenes Schutzniveau" gewährleisten. Eine eindeutige Definition dieses unbestimmten Rechtsbegriffs enthält

198 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 44 f. Vgl. auch die entsprechende ständige Rspr. des EGMR seit dem „Soering"-Fall, dazu *Grabenwarter/Pabel*, (Fn. 14), S. 212 ff.

199 Art. 3 Abs. 2 RL 95/46/EG, Art. 2 Abs. 2 lit. a DSchGrVO. Kritisch deshalb *Kühling/Heberlein*, (Fn. 181), S. 10, 12.

200 Siehe unter D.II.1.c)(3).

201 Vgl. die Mitteilung der Europäischen Kommission, COM (2016) 117 final, S. 2: „Der Transfer und der Austausch personenbezogener Daten sind ein zentraler Bestandteil der engen Verbindungen zwischen der Europäischen Union (EU) und den Vereinigten Staaten (USA) – im kommerziellen Bereich ebenso wie bei der Durchsetzung von Rechtsvorschriften."

die Richtlinie nicht, so dass sich ein Interpretationsspielraum eröffnet.[202] Im Anschluss an die Schlussanträge des Generalanwalts hat der EuGH das erforderliche Niveau indessen aufgrund einer teleologischen Interpretation hoch angesetzt: Zwar brauche das Drittland kein dem in der Unionsrechtsordnung garantierten Niveau identisches Schutzniveau gewährleisten; dieses müsse jedoch der Sache nach gleichwertig sein. Denn Art. 25 solle verhindern, dass durch eine Verlagerung der Datenverarbeitung in Drittländer die Datenschutzregeln des Unionsrechts umgangen werden. Diesem Zweck wird in der Tat nur eine Interpretation gerecht, die entsprechend hohe Anforderungen an das dortige Schutzniveau stellt. Andererseits lässt die Richtlinie erkennen, dass sie den für die Entwicklung des internationalen Handels wichtigen grenzüberschreitenden Verkehr von personenbezogenen Daten grundsätzlich positiv beurteilt.[203] Außerdem verlangt Art. 25 Abs. 2 Richtlinie 95/46/EG, dass die Angemessenheit des Schutzniveaus in einem Drittland unter Berücksichtigung aller Umstände beurteilt wird, wozu nach Art. 16 GRCh auch die Grundrechte der beteiligten Wirtschaftsunternehmen und die Freiheiten derjenigen Nutzer gehören, die größeren Wert auf kostenlosen Zugang zu Diensten als auf Datenschutz legen.[204] Diese bezieht der EuGH jedoch in seine Begründung nicht ein.

Zum angemessenen Schutzniveau in Drittländern zählt der EuGH im Lichte des Art. 47 GRCh auch wirksamen gerichtlichen Rechtsschutz, mit dessen Hilfe Einzelne Zugang zu den sie betreffenden personenbezogenen Daten erlangen oder deren Berichtigung oder Löschung erwirken können.[205] Ob schiedsgerichtlicher Rechtsschutz ausreicht, erscheint danach zumindest sehr zweifelhaft.[206]

(2) Rückwirkende Ungültigkeit der Kommissionsentscheidung

Die Ungültigerklärung der Kommissionsentscheidung durch den EuGH wirkt auf den Zeitpunkt ihres Erlasses zurück, denn der Gerichtshof hat sein Urteil in dieser Hinsicht nicht beschränkt, und seine Begründung macht deutlich, dass die Entscheidung von Anfang an mit Art. 25 Abs. 2, 6 Richtlinie 95/46/EG unvereinbar war, weil das Datenschutzniveau in den USA zu keiner Zeit angemessen war, nicht erst seit dem Beginn des PRISM-Programms. Damit stellte der Gerichtshof zugleich der Sache nach fest, dass sämtliche Datenübertragungen in die USA in den letzten fünfzehn Jahren mit den Vorgaben der Richtlinie 95/46/EG und der Grundrechte aus Art. 7 und 8 GRCh unvereinbar waren. Die sich aus diesen unzulässigen Datenverarbeitungen an sich ergebenden Löschungsansprüche der Betroffenen[207] richten sich aber nicht gegen US-amerikanische Zweitverarbeiter und könnten diesen gegenüber ohnehin nicht durchgesetzt werden. Gegenüber den EU-Erstverarbeitern, die die Daten unzulässi-

202 Näher *Kühling/Heberlein*, (Fn. 181), S. 9.
203 Begründungserwägung 56 der RL 95/46/EG.
204 *Kühling/Heberlein*, (Fn. 181), S. 9, 12.
205 EuGH, Rs. C-362/14, *Schrems*, EU:C:2015:650, Rn. 95.
206 *Ukrow*, Privatsphäre und Rechtsstaat – Gefällt mir, www.emr-sb.de/tl_files/EMR-SB/content/PDF/Publikationen/EMR_Das%20aktuelle%20Stichwort_Safe%20Harbour_20151006.pdf (1.8.2016). Vgl. auch *Jarass*, (Fn. 58), Art. 47, Rn. 17 ff.
207 Vgl. Art. 12 lit. b RL 95/46/EG.

gerweise übermittelt hatten, bestehen jedoch Löschungsansprüche sowie Ansprüche auf Information der US-Zweitverarbeiter über die erfolgte Löschung.[208]

Das „Schrems"-Urteil hat eine sehr große praktische Tragweite, verursacht es doch politisch und wirtschaftlich relevante Störungen im außerordentlich großen transatlantischen Datenverkehr. Immerhin nahmen daran im Oktober 2015 unter dem Safe-Harbor-System ungefähr 4000 Unternehmen teil.[209] Aus diesem Grund ist die Entscheidung vor allem von Kommentatoren aus den USA heftig kritisiert worden, die ein Grundrecht auf Datenschutz nicht anerkennen.[210] Andere haben eingewandt, der EuGH hätte die Abwägung zwischen den Erfordernissen der nationalen Sicherheit und der Freiheit der Einzelnen demokratisch besser legitimierten politischen Organen überlassen sollen.[211] Indessen hat der demokratisch legitimierte europäische Gesetzgeber aus Europäischem Parlament und Rat in Art. 25 Richtlinie 95/46/EG die Anforderungen an Datenübermittlungen an Drittländer festgelegt und die Kommission diese offensichtlich verkannt. Eventuelle Ermächtigungen zum Datenzugriff seitens des Gesetzgebers oder der Exekutive der USA sind den Unionsbürgern gegenüber nicht demokratisch legitimiert.[212]

Durch die Ungültigerklärung der Kommissionsentscheidung liegt die Verantwortung dafür, dass die USA ein angemessenes Schutzniveau gewährleisten, nach Art. 25 Abs. 1 Richtlinie 95/46/EG derzeit wieder vollumfänglich bei den Mitgliedstaaten. Diese können jedoch das dortige Schutzniveau nach den deutlichen Feststellungen des EuGH gegenwärtig schlechterdings nicht als angemessen einstufen. Deshalb kann der Datenverkehr mit den USA derzeit nur mit Hilfe der Ausnahmebestimmung des Art. 26 Richtlinie 95/46/EG und ihren nationalen Umsetzungsvorschriften aufrechterhalten werden.[213] Diese Situation ist offensichtlich unbefriedigend, zumal bestritten wird, dass die Anforderungen von Art. 26 Richtlinie 95/46/EG erfüllt sind.[214] Die Artikel-29-Datenschutzgruppe[215] hatte deswegen kurz nach dem „Schrems"-Urteil die beschleunigte Aushandlung einer zufriedenstellenden Ersatzlösung mit den USA

208 Vgl. Art. 12 lit. c RL 95/46/EG.

209 *Gstrein*, (Fn. 187), S. 9.

210 Vgl. z.B. *Epstein*, Europe's top court goes off the rails, Politico v. 8.10.2015, www.politico.eu/article/ecj-off-the-rails-safe-harbor-eu-us-data-protection/ (1.8.2016). Kritisch wegen der verursachten Rechtsunsicherheit aber auch *Schwartmann*, Datentransfer in die Vereinigten Staaten ohne Rechtsgrundlage, EuZW 2015, S. 868.

211 *Miller*, Schrems v. Commissioner: A Biblical Parable of Judicial Power, VerfBlog v. 7.10.2015.

212 *Antpöhler*, Schrems – Towards a High Standard of Data Protection for European Citizens, Völkerrechtsblog v. 18.11.2015.

213 Siehe dazu eingehend die Mitteilung der Kommission an das Europäische Parlament und den Rat zu der Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika auf der Grundlage der Richtlinie 95/46/EG nach dem Urteil des Gerichtshofs in der Rechtssache C-362/14 (Schrems), COM (2015) 566 final v. 6.11.2015.

214 *Antpöhler*, (Fn. 212); *Schwartmann*, (Fn. 210), S. 866 ff.; *Kühling/Heberlein*, (Fn. 181), S. 11 f.

215 Diese beruht auf Art. 29 RL 95/46/EG und besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen, einem Vertreter der für die EU eingerichteten Stelle und einem Kommissionsvertreter. Sie ist unabhängig und hat eine beratende Funktion.

ultimativ angemahnt und damit gedroht, dass die Datenschutzbehörden in Europa ansonsten konzertierte Schritte einleiten würden, um die Einhaltung der europäischen Datenschutzstandards im Datenverkehr mit den USA sicherzustellen.[216] Der von einigen befürchtete „Alptraum" in den transatlantischen Beziehungen ist freilich ausgeblieben.

(3) Ausreichende Reparatur durch den neuen EU-US Datenschutzschild?

Die Kommission hatte schon im Januar 2014 mit den USA Gespräche über eine Verbesserung des transatlantischen Datenschutzregimes aufgenommen, die aber kaum Fortschritte brachten, bis das „Schrems"-Urteil den notwendigen Druck erzeugte. Bereits im Februar 2016 teilte die Kommission dann mit, dass eine politische Einigung mit den USA über einen neuen Rahmen für den transatlantischen Datenverkehr unter dem Namen „EU-US Datenschutzschild (*EU-US Privacy Shield*)" gefunden worden sei.[217] Daneben hatte man, was nur kurz erwähnt werden soll, am 8. September 2015 ein EU-US-Rahmenabkommen paraphiert, das für transatlantische Datentransfers zu Zwecken der Strafverfolgung hohe Datenschutzstandards festschreibt.[218]

Der neue EU-US Datenschutzschild besteht derzeit aus einem auf Art. 25 Abs. 6 Richtlinie 95/46/EG gestützten neuen Beschluss der Kommission vom 12. Juli 2016 über die Angemessenheit des Datenschutzniveaus in den USA mit insgesamt sieben Anhängen.[219] In diesen Anhängen finden sich Erklärungen und Erläuterungen verschiedener US-Behörden, die an die Justizkommissarin der EU adressiert sind bzw. an sie weitergeleitet werden und in ihrer Gesamtheit das Datenschutzniveau in den USA widerspiegeln. Diese Erklärungen und Erläuterungen sollen im Federal Register (Amtsblatt der USA) veröffentlicht werden, um die darin enthaltenen Zusagen auch in den USA öffentlichkeitswirksam bekannt zu machen. Die US-Garantien sind zwar mit der Kommission ausgehandelt und am 2. Februar 2016 vereinbart worden, haben jedoch nicht die Qualität eines verbindlichen völkerrechtlichen Vertrags zwischen der EU und den USA, sondern allenfalls von politisch bindenden Versprechen. Dementsprechend wurden die detaillierten Verfahrensvorgaben des Art. 218 AEUV für den Abschluss von völkerrechtlichen Übereinkünften mit Drittstaaten nicht eingehalten.

Die Kommission hält den EU-US Datenschutzschild für eine „konsequente und effektive Antwort auf [...] das Schrems-Urteil."[220] Als Verbesserungen gegenüber der

216 Statement of the Article 29 Working Party v. 16.10.2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (1.8.2016).

217 Europäische Kommission, Pressemitteilung IP/16/216 v. 2.2.2016.

218 Vgl. Europäische Kommission, Fact Sheet MEMO/15/5612 v. 8.9.2015. Der Judicial Redress Act von 2016, der bisher den US-Bürgern und dauerhaft in den USA wohnhaften Ausländern vorbehaltene Rechtsschutzmöglichkeiten auf Unionsbürger ausdehnt, dient nur der Erfüllung von Vorgaben dieses Rahmenabkommens, vgl. Mitteilung der Kommission, Transatlantischer Datenaustausch: Wiederherstellung des Vertrauens durch starke Schutzvorkehrungen, COM (2016) 117 final v. 29.2.2016, S. 3, 14 ff.

219 C(2016) 4176 final. Das gesamte Paket ist als Anhang der Pressemitteilung IP/16/2461 v. 12.7.2016 abrufbar und wird demnächst im ABl. veröffentlicht.

220 COM (2016) 117 final, S. 10.

früheren Situation hebt die Kommission Folgendes hervor: US-Firmen, die Daten aus Europa importieren, unterlägen strengeren rechtlichen Auflagen, die konsequenter durchgesetzt würden. Die Zugriffsmöglichkeiten von US-Behörden auf die importierten Daten seien klar begrenzt, und die Einhaltung dieser Grenzen werde effektiv überwacht. Die Grundrechte der Unionsbürger würden durch verschiedene Rechtsbehelfe wirksam geschützt. Eine jährliche gemeinsam von der Kommission und vom US-Handelsministerium vorgenommene Überprüfung stelle sicher, dass alle Aspekte der Vereinbarung zuverlässig funktionierten; anderenfalls werde die Kommission das Verfahren zur Aussetzung des Datenschutzschilds aktivieren.[221] Kritiker wenden ein, dass der neue Datenschutzschild den Anforderungen der europäischen Grundrechte nach Maßgabe des „Schrems"-Urteils weder in Bezug auf die kommerzielle Datenverarbeitung in den USA noch in Bezug auf Zugriffsmöglichkeiten der US-Behörden auch nur annähernd entspreche.[222]

In ihrer Stellungnahme zum Beschlussentwurf der Kommission vom 29. Februar 2016 erkannte die Artikel-29-Datenschutzgruppe[223] zwar wesentliche Verbesserungen gegenüber der Safe-Harbor-Situation an, machte aber auch etliche Bedenken geltend und forderte die Kommission zur Abhilfe auf.[224] Die Gruppe wies in diesem Zusammenhang darauf hin, dass der EuGH der Kommission im Hinblick auf die Angemessenheit des Datenschutzniveaus im Zielland der Datentransfers keinen Beurteilungsspielraum zubilligt. Zunächst kritisierte sie die Unübersichtlichkeit, die sich aus der Aufspaltung der Information in den Angemessenheitsbeschluss selbst und zahlreiche, teils unklar formulierte und nicht völlig konsistente Anhänge ergebe. Dies erschwere den Datensubjekten, Organisationen und Datenschutzbeauftragten den Zugang.[225]

In Bezug auf die kommerzielle Datenverarbeitung, wo für die beteiligten Unternehmen weiterhin ein Verfahren der Selbstzertifizierung gilt, vermisste die Gruppe eine klare Bezugnahme auf das Prinzip, dass Daten nur für einen bestimmten Zweck verarbeitet werden dürfen und ihre Speicherung mit der Erfüllung des ursprünglichen Verarbeitungszwecks enden muss. Es werde auch nicht eindeutig festgelegt, dass jeder Weitertransfer von Daten aus den USA in ein anderes Drittland nur erfolgen dürfe, wenn die dortigen Datenschutzstandards ebenfalls angemessen seien. Die verbesserten Rechtsschutzmöglichkeiten für betroffene Unionsbürger seien zu undurchsichtig, schwierig zu nutzen und deshalb nicht wirksam genug.[226]

Hinsichtlich der staatlichen Zugriffsmöglichkeiten im Interesse der nationalen Sicherheit erkannte die Gruppe zwar wesentliche Fortschritte gegenüber der vorherigen Rechtslage. Sie bemängelte jedoch, dass die Stellungnahme des *U.S. Office of the Di-*

221 Ibid., S. 11 ff.
222 *Weichert*, EU-US-Privacy-Shield – Ist der transatlantische Datentransfer nun grundrechtskonform?, ZD 2016, S. 214 ff.
223 Siehe Fn. 215.
224 Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (16/EN WP238), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (1.8.2016).
225 Ibid., S. 12 ff.
226 Ibid., S. 15 ff.

rector of National Intelligence in Anhang VI die massive und unterschiedslose Sammlung von aus der EU transferierten personenbezogenen Daten nicht ausschlössen, die nach ihrer Auffassung niemals verhältnismäßig und grundrechtskonform sein könne. Hinsichtlich des Rechtsschutzes erkannte die Gruppe an, dass die Einrichtung der Ombudsperson die Situation von Unionsbürgern wesentlich verbessere. Sie bezweifelte jedoch, dass die Ombudsperson hinreichend unabhängig sei, angemessene Befugnisse besitze und zufriedenstellende Abhilfe gewährleiste, falls ein Geheimdienst nicht kooperationswillig sei.[227]

Die Kommission hat daraufhin nach eigenen Angaben eine Reihe von Verbesserungen an ihrem ursprünglichen Entwurf vorgenommen. Sie hat insbesondere mit den USA

> „weitere Klarstellungen zur Sammelerhebung von Daten, die Stärkung der Ombudsstelle und präzisere Verpflichtungen für Unternehmen in Bezug auf Beschränkungen für die Speicherung und die Weitergabe von Daten vereinbart."[228]

Bei alledem darf nicht außer Acht gelassen werden, dass die Ansätze zum Schutz der Privatsphäre in den USA und Europa sehr verschieden sind. Denn während in Europa ein ganzheitlicher Ansatz verfolgt wird, der sich erneut in der DSchGrVO manifestiert, bevorzugen die USA einen sektoralen Ansatz mit einer Mischung von gesetzlichen und untergesetzlichen Vorgaben sowie Selbstregulierungsmechanismen in jeweils unterschiedlichen Anteilen.[229] Es erscheint unrealistisch anzunehmen, dass die USA das europäische Datenschutzmodell einfach rezipieren werden.[230] Daher sind Kompromisse unausweichlich, und diese setzen Spielräume für die politischen Organe voraus, die durch gerichtliche Vorgaben nicht übermäßig beschränkt werden dürfen.[231] Außer Zweifel steht jedoch, dass der neue Angemessenheitsbeschluss der Kommission dem EuGH alsbald zur Überprüfung unterbreitet werden wird. Es ist keineswegs sicher, dass der EuGH sich angesichts seiner im „Schrems"-Urteil festgelegten hohen Anforderungen mit den im EU-US Datenschutzschild gegenüber dem Safe-Harbor-System erzielten Verbesserungen zufrieden geben wird.[232]

e) Die Regelungen der DSchGrVO zur Datenübermittlung in Drittländer

Die neue DSchGrVO enthält im Gefolge des „Schrems"-Urteils im Vergleich zur derzeitigen Richtlinie 95/46/EG sehr viel ausführlichere und strengere Bestimmungen zur Übermittlung personenbezogener Daten an Drittländer oder an erstmals miter-

227 Ibid., S. 33 ff.
228 Europäische Kommission, Pressemitteilung IP/16/2461 v. 12.7.2016.
229 Entwurf des Angemessenheitsbeschlusses der Kommission, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf (1.8.2016), Annex II, I.1.
230 Vgl. *Schwartmann*, (Fn. 210), S. 868.
231 *Kühling/Heberlein*, (Fn. 181), S. 12.
232 Skeptisch z.B. *Gryffroy*, The EU-US Privacy Shield: An Effective New Framework for Transatlantic Data Flows or A Weak Compromise Doomed to Fail?, Saar Brief v. 18.2.2016, http://jean-monnet-saar.eu/?p=1211#_ftn23 (1.8.2016).

wähnte internationale Organisationen[233] im Kapitel V (Art. 44-50). Die erwähnte Stellungnahme der Artikel-29-Datenschutzgruppe weist deshalb in zutreffender Weise darauf hin, dass ein Angemessenheitsbeschluss der Kommission auf der Grundlage des EU-US Datenschutzschildes mit dem Geltungsbeginn der DSchGrVO am 25. Mai 2018 auf jeden Fall einer Überprüfung bedarf.[234] Insbesondere schreibt Art. 44 DSchGrVO ausdrücklich vor, dass alle Bestimmungen von Kapitel V in einer Weise anzuwenden sind, die sicherstellt, „dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird." Anders als bisher, wird jetzt auch die Zulässigkeit der Weiterübermittlung von Daten an ein anderes Drittland oder eine andere internationale Organisation denselben strikten Anforderungen unterworfen wie die Erstübermittlung.[235]

Die DSchGrVO bewertet den Datenverkehr mit Drittländern zwar weiterhin als wirtschaftlich und politisch grundsätzlich positiv,[236] lässt aber für die Einbeziehung der Grundrechte der betroffenen Wirtschaftsunternehmen in die Angemessenheitsbeurteilung eher weniger Raum als die Richtlinie 95/46/EG, die in Art. 25 Abs. 2 immerhin ausdrücklich die Berücksichtigung aller Umstände verlangt.[237] Die DSchGrVO erhebt auch noch stärker als die Richtlinie 95/46/EG den Anspruch, mit europäischen Daten auch europäische Datenschutzstandards zu exportieren. Ob dies ohne weiteres gelingen wird und ob die EU sich anderenfalls vom weltweiten Datenaustausch abschotten kann, erscheint als fraglich.

Die Prüfung der Kommission, ob das Drittland[238] oder die internationale Organisation ein angemessenes Schutzniveau bietet, wird durch die in Art. 45 Abs. 2 DSchGrVO festgelegten Kriterien vorstrukturiert. Mit zu berücksichtigende, wenngleich nicht allein ausschlaggebende Kriterien sind die Existenz und wirksame Funktionsweise unabhängiger Datenschutzbehörden in dem betreffenden Drittland bzw. der betreffenden internationalen Organisation (lit. b) sowie die von diesen eingegangenen internationalen Verpflichtungen und sonstige Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten oder aus der Teilnahme an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben (lit. c),[239] sowie die Umsetzung dieser Verpflichtun-

233 Vgl. die Definition in Art. 4 Ziffer 26 DSchGrVO.
234 Article 29 Data Protection Working Party, (Fn. 224), S. 15.
235 Art. 44 DSchGrVO.
236 Begründungserwägung 101 der DSchGrVO.
237 Art. 45 Abs. 2 DSchGrVO listet demgegenüber nurmehr Kriterien auf, die die Kommission „insbesondere" zu berücksichtigen hat und die allesamt auf den Datenschutz fokussiert sind.
238 Der Angemessenheitsbeschluss der Kommission kann sich jetzt auch auf ein Gebiet eines Drittlandes oder ein oder mehrere spezifische Sektoren in diesem Drittland beschränken.
239 Art. 45 Abs. 2 lit. c DSchGrVO unterscheidet zwischen eingegangenen internationalen Verpflichtungen (*commitments*) – damit sind anscheinend spezifische Verpflichtungen auf Datenschutz gemeint – und anderen Verpflichtungen (*obligations*) eher allgemeiner Art aus rechtsverbindlichen Übereinkünften oder Instrumenten bzw. der Teilnahme an multilateralen oder regionalen Schutzsystemen. Die Begründungserwägung 105 der DSchGrVO lässt erkennen, dass der Beitritt eines Drittlandes zum Europarats-Übereinkommen von 1981 und Zusatzprotokoll von 2001 positiv zu berücksichtigen ist.

gen.[240] In Bezug auf lit. b und c ist bei den USA Fehlanzeige zu vermerken. Die Kommission wird ausdrücklich verpflichtet, die Entwicklungen in Drittländern und bei internationalen Organisationen fortlaufend zu überwachen und ihre Angemessenheitsbeschlüsse gegebenenfalls für die Zukunft zu widerrufen, zu ändern oder auszusetzen.[241]

Art. 48 DSchGrVO enthält eine Abwehrvorschrift gegen extraterritoriale Maßnahmen von Drittländern, mit denen in die Verarbeitungstätigkeit von natürlichen und juristischen Personen eingegriffen werden soll, die der Hoheitsgewalt der Mitgliedstaaten unterliegen.[242] Dazu gehören insbesondere Tochtergesellschaften von Gesellschaften mit Drittstaatszugehörigkeit (wie etwa Google Spain und Facebook Ireland).[243] Um derartige Eingriffe auszuschließen, insbesondere (aber nicht nur) wenn sie völkerrechtswidrig sind, ordnet Art. 48 DSchGrVO an, dass Gerichtsurteile und Verwaltungsentscheidungen aus Drittländern, mit denen von einem EU-Datenverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, nur anerkannt oder für vollstreckbar erklärt werden dürfen, wenn sie auf eine in Kraft befindliche Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Erlaubt bleibt jedoch die Übermittlung aus sonstigen im Kapitel V anerkannten Gründen, beispielsweise nach Art. 49 Abs. 1 lit. d DSchGrVO, falls sie aus (im Unions- oder mitgliedstaatlichen Recht anerkannten) wichtigen Gründen des öffentlichen Interesses notwendig ist. Eine an sich unzulässige Datenübermittlung an ein Drittland oder eine internationale Organisation darf ausnahmsweise dann vorgenommen werden, wenn sie nicht wiederholt erfolgt, nur eine begrenzte Zahl von Personen betrifft, für die zwingenden Interessen des Datenverarbeiters erforderlich ist, die Interessen oder die Rechte und Freiheiten der Datensubjekte nicht überwiegen und der Datenverarbeiter aufgrund eigener Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Datenverarbeiter muss die Aufsichtsbehörde und die betroffenen Personen von der Übermittlung unterrichten und den letztgenannten auch seine zwingenden berechtigten Interessen offenlegen.[244]

E. Fazit: Europäische Datenschutzanliegen in einer vernetzten Welt

Im Daten- und Persönlichkeitsrechtsschutz hat Europa, jüngst vor allem in Gestalt der EU, durch Gesetzgebung, Rechtsprechung und internationale Praxis eine Vorreiterrolle in der Welt übernommen. Zu nennen sind hier vor allem die neue Datenschutz-Grundverordnung der EU vom 27. April 2016 und die EuGH-Urteile in den Rechtssachen *Digital Rights Ireland* (2014), *Google Spain* (2014) und *Schrems* (2015). Damit ist die Union einerseits Vorbild, läuft aber andererseits Gefahr, sich durch übergroßen Ehrgeiz zu isolieren. Denn wenn die übrigen Weltteile nicht davon über-

240 Letzteres ergibt sich ausdrücklich nur aus der Begründungserwägung 105 der DSchGrVO.
241 Art. 45 Abs. 4, 5 DSchGrVO.
242 Vgl. die zugehörigen Erläuterungen in der Begründungserwägung 115 der DSchGrVO.
243 Zu einem konkreten Microsoft betreffenden Fall vgl. *Gstrein*, (Fn. 187), S. 11.
244 Art. 49 Abs. 1 UAbs. 2 DSchGrVO.

zeugt oder durch die Ausübung von (Wirtschafts-)Macht dazu gedrängt werden können, die hohen europäischen Schutzstandards zu übernehmen, steht Europa vor der Wahl, seinen Ehrgeiz zu mäßigen und Kompromisse einzugehen oder den Datenverkehr mit Drittländern zu unterbrechen. Da die zweite Option mit erheblichen wirtschaftlichen und politischen Nachteilen verbunden ist, spricht mehr für Kompromissbereitschaft. Diese lässt sich leichter rechtfertigen, wenn man einkalkuliert, dass der ungehinderte grenzüberschreitende Datenverkehr nicht nur wirtschaftliche Interessen und Rechte – Eigentum, Berufs- und unternehmerische Freiheit – bedient, sondern auch die weltweite Meinungsäußerungs- und Informationsfreiheit fördert. Er liegt deshalb im objektiven Interesse der internationalen Gemeinschaft als ganzer. Den Testfall für die europäische Kompromissbereitschaft liefert der neue EU-US-Datenschutzschild, den die Kommission zur Sicherstellung des freien transatlantischen Datenverkehrs nach den Vorgaben des „Schrems"-Urteils gerade ausgehandelt hat und der mit Sicherheit alsbald dem EuGH zur Kontrolle am Maßstab der europäischen Grundrechte unterbreitet wird.