3 Kontextanalyse

Für die Erklärung politischer Entwicklungen mithilfe des Advocacy Coalition Frameworks ist zunächst die Identifikation der wesentlichen politischen Rahmenbedingungen eines Policy-Subsystems erforderlich. Das Ziel der Kontextanalyse ist es, die relevanten (polit-historischen) Kontextbedingungen der EU-Datenschutzpolitik zu identifizieren, die in entscheidendem Maße Einfluss auf das Zustandekommen der DSGVO hatten.

Die Analyse folgt den Vorgaben des gewählten theoretischen Rahmens in Gestalt des ACF und hat zunächst zum Ziel, die Entwicklung der EU-Datenschutzpolitik von ihren Anfängen in den 1970er-Jahren bis zum Beginn des Aushandlungsprozesses der DSGVO im Hinblick auf das Variablenset relativ stabiler Parameter zu untersuchen, von denen im ACF angenommen wird, dass sie über längere Zeiträume (etwa zehn Jahre) stabil bleiben. Das Variablenset relativ stabiler Parameter umfasst (1) die grundlegenden Merkmale des betrachteten Problems, (2) die Verteilung natürlicher Ressourcen, (3) grundlegende soziokulturelle Wertvorstellungen und die Sozialstruktur sowie (4) die grundlegende verfassungsmäßige Struktur. Die Kontextanalyse hat darüber hinaus zum Ziel, die langfristig wichtigen politischen Gelegenheitsstrukturen insb. in Form des Grads der erforderlichen Zustimmung für wesentlichen Wandel sowie der relativen Offenheit des untersuchten politischen Systems herauszuarbeiten und zu untersuchen, inwiefern traditionelle Konfliktlinien in den untersuchten datenschutzpolitischen Auseinandersetzungen berührt werden. Schließlich soll im Rahmen der Kontextanalyse untersucht werden, inwiefern die Datenschutzpolitik durch externe, dynamische Systemereignisse beeinflusst wurde, von denen angenommen wird, dass sie sich innerhalb von weniger als zehn Jahren verändern können. Zum Variablenset der externen, dynamischen Systemereignisse zählt (1) der Wandel in den sozioökonomischen Bedingungen, (2) der Wandel in der öffentlichen Meinung, (3) der Wandel maßgeblicher (Regierungs-)Koalitionen und (4) Policy-Entscheidungen oder -Wirkungen aus anderen Subsystemen.

Anders als in der Akteurs- und Prozessanalyse des späteren DSGVO-Abschnitts (vgl. Unterabschnitt 4), wird bei der Kontextanalyse größerer Wert auf die Herausarbeitung von Entwicklungstendenzen gelegt und daher in geringerem und weniger systematischem Maße auf die Positionen der an

den Aushandlungsprozessen beteiligten Akteure eingegangen. Die Analyse fokussiert sich daher auf die zentralen und insb. institutionellen Akteure der entsprechenden Policy-Debatten.

Die Kontextanalyse umfasst die relevantesten datenschutzpolitischen Auseinandersetzungen bzw. Entwicklungen, die bis zur Verabschiedung der DSGVO insb. auf EU-Ebene geführt wurden bzw. sich ereigneten. Zu diesem Zweck teilt sich der Abschnitt in vier inhaltliche Unterabschnitte auf zweiter Ebene, plus einen fünften Unterabschnitt, in dem ein Zwischenfazit gezogen wird, auf. Zu Beginn werden in Unterabschnitt 3.1 die Frühphase der Datenverarbeitung und die Entstehung der OECD-Datenschutz-Richtlinien sowie der Datenschutz-Konvention des Europarats untersucht. Im zweiten Unterabschnitt (3.2) folgt die Analyse der Aushandlung der ersten Datenschutz-Instrumente, die auf Gemeinschaftsebene verabschiedet wurden, darunter insb. die DS-RL, aber auch das Safe Harbor-Abkommen, die ISDN-RL und die Datenschutz-VO. Der dritte Unterabschnitt (3.3) widmet sich der Analyse der Datenschutz-Politiken bzw. datenschutzrelevanten sicherheitspolitischen Maßnahmen, die unter veränderten politischen Rahmenbedingungen nach der Jahrtausendwende verhandelt wurden, darunter insb. die ePrivacy-RL, die Berichte der Kommission über die Durchführung der DS-RL, die Richtlinie zur Vorratsdatenspeicherung, die Gewährung des Zugriffs auf Fluggastdaten, der JI-Rahmenbeschluss sowie die Aushandlung der Cookie-RL.

Der vierte inhaltliche Unterabschnitt (3.4) widmet sich der Untersuchung des Wandels relevanter Kontextbedingungen, die für die Initiierung der Datenschutzreform von entscheidender Bedeutung waren. Zu diesem Zweck wird zunächst entlang der Analyse der Entstehung der EU-Grundrechtecharta, des Vertrags von Lissabon und des Stockholmer Programms der Wandel in der grundlegenden verfassungsmäßigen Struktur, des Grads der erforderlichen Zustimmung für wesentlichen Wandel sowie der relativen Offenheit des politischen Systems aufgezeigt. Daran schließt sich die Untersuchung der Veränderung sozioökonomischer Bedingungen und der öffentlichen Meinung in der EU an.

Im fünften Unterabschnitt (3.5) werden die Ergebnisse der Kontextanalyse schließlich zusammengefasst sowie auf Grundlage der Erkenntnisse aus der Kontextanalyse ein erster Überblick über die Advocacy-Koalitionen im Bereich der EU-Datenschutzpolitik geliefert.

3.1 Die Frühphase der Datenverarbeitung und die Divergenz nationaler Datenschutzgesetze

Am Anfang der Debatten über den gesetzlichen Schutz personenbezogener Daten stand die Diskussion staatlich-behördlicher Kontrollvorstellungen, die ihren Höhepunkt am Ende der 1960er-Jahre fanden. Mittels Verwaltungsautomation sollten Datenbestände automatisch zusammengeführt und ausgewertet werden können, um die Vereinfachung von Verwaltungsabläufen, Kostensenkungen und eine Optimierung staatlicher Planungsmaßnahmen zu erreichen. Zeitgleich warnten Kritiker vor den negativen Folgen dieser Pläne. So würde die grenzenlose Erhebung und Zusammenführung personenbezogener Daten nicht nur ein nie dagewesenes Maß an Durchleuchtung des Einzelnen ermöglichen, die computergestützte Auswertung der Daten könne zudem neues Wissen über Personen generieren, „das unter Umständen weit über das hinausgehe, was diese selbst über sich wissen." (Berlinghoff 2013a, 16) Schließlich würde der wachsende Informationsbestand auf Seiten der Exekutive die Informationsasymmetrie zwischen Regierung und parlamentarischer wie außerparlamentarischer Opposition verschärfen und somit zu einer Untergrabung des demokratischen Gemeinwesens führen (ebd.).

Als Reaktion auf diese Kritiken entstand das weltweit erste Datenschutzgesetz, das am 30. September 1970 im deutschen Bundesland Hessen verabschiedet wurde.[40] Weniger als drei Jahre später folgte das erste nationale Datenschutzgesetz, das am 11. Mai 1973 in Schweden verabschiedet wurde sowie zahlreiche weitere Datenschutzgesetze Staats- als auch Landesebene, wie der US Privacy Act (1974) oder das BDSG (1977) (Simitis u. a. 2019, 159 ff.).

Die Herausforderung, mit der alle frühen Datenschutzgesetze konfrontiert waren, lag darin, die mit der automatisierten Datenverarbeitung verbundenen Probleme in einer Zeit anzugehen, in der sich die potentiellen Probleme zwar noch nicht äußerten, jedoch auch nicht ignoriert werden konnten (ebd., 179, Rn. 72). In der Folge bildeten sich drei Regelungsmodelle heraus, in denen diese Herausforderung auf ganz unterschiedliche

40 Parallel zu Europa war auch in den Vereinigten Staaten eine Debatte über die automatisierte Datenverarbeitung entbrannt (Ware 1973; Westin 1967). Anders als in Europa beschränkte sich die politische Diskussion allerdings auf mögliche negative Folgen einzelner Verarbeitungsbereiche bzw. insb. auf den Kreditsektor. In der Folge wurde nur wenige Tage nach dem Hessischen Landesdatenschutzgesetz der US Fair Credit Reporting Act am 26. Oktober 1970 verabschiedet (Simitis u. a. 2019, 159 ff.).

Weise adressiert wurde. Das deutsche BDSG und das österreichische DSG hatten die Etablierung einer allumfassenden Regelung zum Ziel, die detaillierte Vorgaben zur Erhebung und dem Verarbeitungsverlauf machte und versuchten, einen Kompromiss zwischen einer möglichst umfassenden und einer möglichst flexiblen Regelung dadurch zu erreichen, dass eine Vielzahl von Generalklauseln weite Spielräume für die Datenverarbeiter offenließ (ebd., Rn. 73). Das schwedische Datenschutzgesetz (in ähnlicher Weise auch das norwegische Datenschutzgesetz) machte hingegen keinerlei Prozessvorgaben und setzte stattdessen auf die Genehmigung einer jeden automatisierten Verarbeitung personenbezogener Daten durch eine Kontrollinstanz (ebd., Rn. 74). Die USA wiederum stellten zwar einige Vorgaben zum Ablauf des Verarbeitungsprozesses auf, verzichteten aber auf eine allgemeine Datenschutzregelung zugunsten eines bereichsspezifischen Ansatzes, bei dem nur jene Bereiche reguliert wurden, in denen negative Folgen der Datenverarbeitung vermutet wurden (ebd., 75).

Die sowohl grundrechtliche Bedeutung, die der Verarbeitung von (personenbezogenen) Daten zugeschrieben wurde, als auch die wirtschaftliche bzw. politische Bedeutung in Kombination mit der Verabschiedung voneinander divergierender nationaler Datenschutzgesetze veranlasste gleich zwei internationale Organisationen dazu, internationale Instrumente zum Zwecke der Harmonisierung der divergierenden nationalen Datenschutzgesetze zu erarbeiten. Das erste dieser Instrumente sind die 1980 verabschiedeten *OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten*. Das andere und weitaus wirkungsvollere Instrument ist das Anfang 1981 verabschiedete *Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten* des Europarats, das besser unter dem Namen Datenschutz-Konvention Nr. 108 bekannt ist. Der folgende Unterabschnitt widmet sich der Entstehung und Aushandlung dieser beiden wegweisenden internationalen Datenschutz-Instrumente.

3.1.1 OECD-Datenschutz-Richtlinien

Die *Organisation für wirtschaftliche Zusammenarbeit und Entwicklung* bzw. OECD[41] ging aus der 1948 gegründeten *Organisation für europäische wirtschaftliche Zusammenarbeit* (OEEC - Organisation for European Economic Co-operation*)* hervor. Die OEEC diente der keynesianisch motivierten Verwaltung der im Rahmen des Marshallplans seitens der Vereinigten Staaten von Amerika gegenüber (west-)europäischen Staaten gewährten finanziellen Hilfen zum Zwecke des wirtschaftlichen Wiederaufbaus und der Zusammenarbeit in Europa nach Ende des Zweiten Weltkrieges (Woodward 2004, 114). Mit der Gründung der OECD im Jahre 1961 und der Überführung der OEEC in diese wurden die anfänglichen, stark am Wiederaufbau Europas orientierten politischen Ziele zunehmend in die Richtung allgemeiner marktwirtschaftlich motivierter wirtschaftspolitischer Kooperation der Mitgliedstaaten und des Abbaus von Handelshemmnissen geändert (ebd.).[42] Zur Erreichung ihrer Ziele kann die OECD auf verschiedene rechtliche Instrumente zurückgreifen. Zu unterscheiden ist vor allem zwischen rechtlich bindenden Instrumenten wie Entscheidungen oder internationalen Vereinbarungen und nicht-bindenden Instrumenten wie Empfehlungen und Deklarationen (OECD 2017).[43]

3.1.1.1 Erste Aktivitäten der OECD mit Datenschutzbezug

Der Beginn der Auseinandersetzung der OECD mit Fragen von Computer-Technologien lässt sich bis März 1968 zurückverfolgen, als auf einem Ministertreffen der OECD-Länder zum Thema Wissenschaft bestehende Technologiedifferenzen thematisiert wurden. Zur weiteren Untersuchung Computer-relevanter Themen richtete die OECD im Juni 1968 die sog. „Computer Utilisation Group" ein, die in den Folgejahren mehrere einschlägige Studi-

41 Ausnahmsweise wird hier auf die Verwendung der deutschen Abkürzung OWZE verzichtet, da sich auch im deutschen Sprachgebrauch die englische Abkürzung OECD (*Organisation for Economic Co-operation and Development*) weitgehend durchgesetzt hat.

42 Mit der Verallgemeinerung ihrer politischen Ziele ging auch eine gewisse Verbreiterung der mitgliedstaatlichen Basis einher: Italien (1962), Japan (1964), Finnland (1968), Australien (1971) und Neuseeland (1973) (Woodward 2004, 115).

43 Die überwiegende Mehrzahl der erlassenen Instrumente sind nicht-bindender Natur. Gemäß dem Stand des Jahres 2018 sind 25 Entscheidungen, 174 Empfehlungen und 27 Deklarationen in Kraft (OECD 2018).

en zur Nutzung von Datenbanken und den damit zusammenhängenden Datenschutzproblemen veröffentlichte.[44] Weil sich durch die Studien die Einschätzung, dass Datenschutz ein wirtschaftlich und gesellschaftlich relevantes Thema sei, bestätigte, setzte die „Computer Utilisation Group" 1972 zwei neue Gremien zur weiteren Untersuchung ein: Das „Data Bank Panel" sowie das „Panel on Policy Issues of Computer/Communications Interaction". Ersteres veranstaltete im Juni 1974 das „OECD Seminar on Policy Issues in data protection and privacy", auf dem verschiedene Datenschutzthemen und darunter erstmals auch die Frage nach grenzüberschreitenden Datenströmen thematisiert wurden, dem späteren Kernanliegen der OECD Privacy Guidelines.[45] Das Seminar brachte etwa 100 bedeutsame Entscheidungsträger aus den verschiedenen OECD-Mitgliedstaaten für einen Wissens- und Meinungsaustausch zusammen. Bedeutung und Notwendigkeit dieses Erfahrungsaustauschs rührten auch daher, dass in der Zwischenzeit mehrere OECD-Mitgliedstaaten – neben dem Bundesland Hessen (1970) auch Schweden (1973) und die Vereinigten Staaten (1974) – Datenschutzgesetze erlassen hatten, deren Regulierungsmodelle sich stark voneinander unterschieden (Gassmann 2010, 2). Das besonders restriktive schwedische Modell sah zum Beispiel die Genehmigung seitens der Datenschutzaufsichtsbehörde für jede einzelne grenzüberschreitende Datenübertragung vor, damit die Gefahr der Übertragung von (personenbezogenen) Daten zum Zwecke der Umgehung nationaler Regulierungen an sog. Datenoasen (*data havens*) – Staaten mit weniger strengen Datenschutzregelungen – möglichst vermieden wird. Diese Befürchtung teilten im Grundsatz auch weitere europäische Staaten, die in den Folgejahren Datenschutzgesetze erließen (Kirby 1980, 3 f.).

Die OECD wiederum, deren primäres Ziel in der Förderung wirtschaftlichen Wachstums durch internationale Kooperation auf dem Gebiet der Wirtschaftspolitik liegt, sah in der Verabschiedung voneinander divergierender nationaler Datenschutzbestimmungen die Gefahr der Erschwerung grenzüberschreitender Datenflüsse und daraus resultierender volkswirtschaftlicher Wachstumseinbuße. Schließlich organisierte das Data Bank

44 Die beiden 1971 veröffentlichen Studien widmeten sich den Themen „Computerised data banks in public administration", „Digital information and the privacy problem" sowie „Policy Issues in Data Protection and Privacy". Eine dritte Studie „Computer and Communications" wurde 1973 veröffentlicht (Gassmann 2010, 1 f.).

45 Neben dem Thema der grenzüberschreitenden Datenströme widmeten sich zwei weitere Panels den Themen „The Personal Identifier and Privacy" bzw. „Right of Citizen Access to their File" (WPISP 2011, 9).

Panel im Jahr 1977 das „Symposium on Transborder Data Flows and the Protection of Privacy", das sich dann auch explizit der Frage grenzüberschreitender Datenflüsse widmete. Auf dieser Veranstaltung trafen etwa 300 Persönlichkeiten aus den OECD-Mitgliedstaaten, der Privatwirtschaft und aus inter-gouvernementalen Organisationen aufeinander. Ein Kommentar des damaligen Präsidenten der französischen Datenschutzaufsichtsbehörde *Commission nationale de l'informatique et des libertés* (CNIL), Louis Joinet, der später eine entscheidende Rolle bei der Erarbeitung der OECD Privacy Guidelines einnehmen sollte, machte in besonderem Maße den gesellschaftlichen und politischen Wert deutlich, der grenzüberschreitenden Datenflüssen zugesprochen wurde:

> *„Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows." (WPISP 2011, 10)*

3.1.1.2 Die politischen Auseinandersetzungen während der Erarbeitung der OECD-Richtlinien

Im Ergebnis des Symposiums wurde das Data Bank Panel aufgelöst und stattdessen Anfang 1978 die *OECD Expert Group on Drafting Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data*[46] ins Leben gerufen. Die Gruppe wurde mit der Erarbeitung von Richtlinien zum Umgang mit personenbezogenen Daten bei grenzüberschreitenden Datenströmen beauftragt. Zur Lektüre der Expertengruppe zählten Texte von Westin, dessen früherem Forschungsassistenten David Flaherty, sowie verschiedene weitere Studien (González Fuster 2014, 78). Zudem stand die Expertengruppe im Austausch mit dem Europarat, der sich ebenfalls seit geraumer Zeit mit Fragen des Schutzes personenbezo-

46 Den Vorsitz der Expertengruppe übernahm der Australier und damalige Vorsitzende der australischen Kommission für Rechtsreformen, die zu dem Zeitpunkt ein Bundesdatenschutzgesetz für Australien vorbereitete, Michael Kirby. Den Vize-Vorsitz hatte der seinerzeitige CNIL-Präsident Louis Joinet inne. Daneben waren Jan Freese (Leiter der schwedischen Datenschutzaufsichtsbehörde), Jon Bing (Leiter der norwegischen Datenschutzaufsichtsbehörde), Stefano Rodotà aus Italien, Spiros Simitis aus Deutschland sowie William Fishman (US-Handelsministerium) und Lucy Hummer (US-Außenministerium) Teil der Expertengruppe (Kirby 2011, 7 f.).

gener Daten auseinandersetzte, sowie mit der Europäischen Kommission (Kirby 2011, 8).

Die Erarbeitung der Richtlinien gestaltete sich angesichts der Beteiligung zahlreicher Akteure aus europäischen Datenschutzaufsichtsbehörden und dem Feld der Menschenrechtspolitik als äußerst zäh. Der Grund dafür waren Meinungsverschiedenheiten zwischen europäischen und nicht-europäischen Vertretern. Während erstere Datenschutzregelungen als realen Schutz von Individuen unter Betonung der menschenrechtlichen Dimension und vor dem Hintergrund der zu diesem Zeitpunkt noch relativ frischen Erinnerungen an die durch den Missbrauch personenbezogener Daten ermöglichten Verbrechen des NS-Regimes befürworteten, sahen letztere datenschutzrechtliche Bestimmungen als Mittel für wirtschaftliche Zwecke. Die europäischen Vertreter waren mit dem Vorwurf konfrontiert, dass der europäische Ansatz zu bürokratisch sei, nicht ausreichend Rücksicht auf die wirtschaftlichen Erfordernisse grenzüberschreitender Datenflüsse nehme und möglicherweise auch protektionistisch motiviert sei, um europäischen Informationstechnologien einen künstlichen Vorteil gegenüber nicht-europäischen Wettbewerbern zu verschaffen. Die europäischen Vertreter sahen die Vorstellungen der nicht-europäischen Mitglieder hingegen als den Versuch der Erzielung einer Einigung zugunsten vereinfachter Datenverarbeitungen an, ohne dass zugleich praktische Verbesserungen auf dem Gebiet des Schutzes personenbezogener Daten erreicht würden (Kirby 2011, 4). So forderten die europäischen Vertreter eine Orientierung an der Sprache des Europarats, der zu diesem Zeitpunkt bereits zwei Europaratsempfehlungen ausgesprochen hatte (vgl. auch 3.1.2) und die darin befürworteten Datenschutzmaßnahmen ausschließlich auf den Schutz von Menschen bezog.

Nach langwierigen Debatten konnten sich schließlich die nicht-europäischen Vertreter mit ihren Forderungen weitgehend durchsetzen, sodass die Empfehlungen der Expertengruppe vorsahen, eine Balance zwischen den miteinander konkurrierenden Werten individueller Privatheit einerseits und dem Informationsbedarf einer informationsabhängigen Gesellschaft andererseits zu erzielen (González Fuster 2014, 78). Die Hoffnung der US-Delegation bestand darin, dass die Festlegung gemeinsamer Datenschutzstandards die OECD-Mitgliedstaaten dazu veranlassen würde, datenprotektionistische Maßnahmen zurückzufahren und dadurch grenzüberschreitende Datenflüsse zu erleichtern (WPISP 2011, 10). Allerdings war bereits der Versuch, eine Balance zu erzielen, hoch problematisch, wie die folgende

Abwägung unterstreichen soll: Wie viel Datenschutz darf zugunsten möglichst freier grenzüberschreitender Datenflüsse geopfert werden, sofern eine Diskrepanz im Datenschutzniveau der OECD-Mitgliedstaaten festzustellen ist?[47] Da allerdings beide Seiten tendenziell unzufrieden mit dem politischen Ergebnis waren, lief die Wahl des Instruments letztlich auf nicht-bindende OECD-Empfehlungen hinaus (Kirby 2011, 4). Die *OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten* wurden schließlich am 23. September 1980 vom obersten Rat der OECD in Form von OECD-Empfehlungen angenommen (OECD 1980b).

3.1.1.3 Inhalt der OECD-Richtlinien

Die Richtlinien sind in fünf Teile unterteilt, die sich je unterschiedlichen Aspekten widmen. Teil 1 „Allgemeines" beinhaltet Begriffsbestimmungen und den Anwendungsbereich der Richtlinien. So werden unter Nr. 1 „alle Informationen, die sich auf eine bestimmte oder bestimmbare Person […] beziehen", als personenbezogene Daten definiert und Nr. 2 sieht vor, dass die Richtlinien öffentliche wie nicht-öffentliche Stellen gleichermaßen einbeziehen. Zudem machen die OECD-Richtlinien keinen Unterschied zwischen automatisierter und manueller Verarbeitung personenbezogener Daten. Teil 2 widmet sich den Grundprinzipien der innerstaatlichen Anwendung. Darunter fallen die Verpflichtung zur Rechtmäßigkeit bei der Erhebung personenbezogener Daten ggf. mit Wissen bzw. Einwilligung des Betroffenen (Nr. 7), Vorgaben zur Zweckbindung (Nr. 8–10), zu Sicherheitsmaßnahmen (Nr. 11), Transparenzvorgaben (Nr. 12) Vorgaben zu Auskunftsrechten des Betroffenen (Nr. 13) sowie die Rechenschaftspflicht des Verantwortlichen zur Einhaltung der genannten Vorgaben (Nr. 14). Die Teile 3 und 4 widmen sich schließlich der Gewährleistung möglichst ungehinderter grenzüberschreitender Datenflüsse, indem Vorgaben zum freien Datenverkehr und zu legitimen Beschränkungen in den Nrn. 15–18 sowie zu internationaler Kooperation und Interoperabilität in den Nrn. 20–22 gemacht werden. Erwähnenswert ist zudem noch, dass die Vorgaben zur Umsetzung in nationales Recht in Teil 4 (Nr. 19) Maßnahmen zum Schutz

47 Diesem Problem wird sich auch in der Begründung der OECD-Richtlinien gewidmet, dort heißt es: „[…] There is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth." (OECD 1980a Explanatory Memorandum, Nr. 19 h)).

personenbezogener Daten auf Grundlage von Selbstregulierung, wie z. B. Verhaltenskodizes (Nr. 19 b.) auf dieselbe Stufe setzen wie gesetzliche Regelungen zum Schutz personenbezogener Daten (Nr. 19 a.) (ebd.).

3.1.1.4 Zwischenfazit und Bewertung

Da die Entscheidungen der OECD im Konsens getroffen werden, können die Ergebnisse in Form der OECD-Richtlinien als der größte gemeinsame Nenner zwischen allen beteiligten Mitgliedstaaten im Hinblick auf den Umgang mit der Materie des Schutzes personenbezogener Daten und grenzüberschreitenden Datentransfers interpretiert werden. Letztlich überbewertete die in den OECD-Richtlinien angestrebte Balance jedoch dem institutionellen Selbstinteresse der OECD entsprechend die Bedeutung der volkswirtschaftlichen Folgen reglementierter Datentransfers, während die Gewährleistung eines hohen Datenschutzniveaus nur so lange befürwortet wurde, wie dieser zu keiner Beschränkung des grenzüberschreitenden Transfers personenbezogener Daten führen würde. Entsprechend gering war letztlich der Einfluss der Richtlinien auf die nationalen Gesetzgebungen. Eine gewisse Harmonisierungswirkung konnten die Richtlinien allerdings trotz ihrer Unverbindlichkeit entfalten, sowohl was nationale Datenschutzgesetze (Schiedermair 2012, 150 f.), als auch weitere internationale Harmonisierungsbestrebungen angeht (Schiedermair 2012, 152 ff. WPISP 2011, 12–15). Zudem sind die in den OECD-Richtlinien vorgesehen Verarbeitungsgrundsätze – allerdings mit teils erheblichen Erweiterungen – noch heute Bestandteil vieler nationaler Datenschutzgesetze und insb. sowohl der DS-RL als auch der DSGVO.

Im Rückblick auf die Erarbeitung der OECD-Richtlinien kann festgehalten werden, dass bereits zu diesem vergleichsweise frühen Zeitpunkt zentrale Konfliktlinien der Datenschutzpolitik offen zu Tage traten, die bis hin zu den Verhandlungen zur Datenschutz-Grundverordnung auch weiterhin prägend für die Datenschutzdebatten sein sollten. Hierzu zählt insbesondere der Konflikt zwischen einer Grundrechtsorientierung einerseits und einer wirtschaftlichen Orientierung von Regelungen zum Schutz personenbezogener Daten andererseits. Der Kern dieses Spannungsfelds entfaltet sich entlang der Frage, wie die Balance im Detail auszusehen hat. Die OECD-Richtlinien versuchen, ein Mindestmaß an Ordnung in die internationale Verarbeitung personenbezogener Daten hineinzubringen, indem die Einschränkung grenzüberschreitender Datentransfers dann in Kauf genommen wird, wenn ein anderer Mitgliedstaat wesentliche Teile der

OECD-Richtlinien nicht einhält oder lediglich als Transit-Staat zur Umgehung von Datenschutzbestimmungen im eigenen Land fungiert (OECD 1980b Teil 3, Nr. 17). Problematisch dabei ist aber zugleich, dass die OECD-Richtlinien aufgrund ihres unverbindlichen Charakters und ihrer Vermeidung der Festlegung auf gesetzliche Vorgaben ohnehin nur bedingt wirksam sein konnten im Hinblick auf die Harmonisierung von nationalen Datenschutzregelungen. Letztlich zeigte sich anhand der Umsetzung der OECD-Richtlinien erstmals, wie der Versuch eine den Datenschutz wahrende Balance zwischen Datenschutz- und Wirtschaftsinteressen auf Basis von Selbstregulierung zu erzielen scheiterte. In den späten 1980er-Jahren wurde zunehmend klar, dass die OECD-Richtlinien eher national divergierenden und inhaltlich unzureichenden Selbstregulierungspraktiken zuträglich waren statt der Harmonisierung eines effektiven Schutzniveaus bzw. -regimes (C. J. Bennett und Raab 2006, 87 ff.).

3.1.2 Datenschutz-Konvention des Europarats

Der Europarat wurde mit der Unterzeichnung des Londoner Vertrags durch zehn westeuropäische Staaten[48] am 5. Mai 1949 ins Leben gerufen. Damit ist der Europarat die älteste europäische internationale Organisation. Wie die Gründung der OECD (3.1.1) und der Vorgänger-Organisationen der EU (3.2.1), ist auch die Entstehung des Europarats im zeithistorischen Kontext des zweiten Weltkrieges zu verstehen. Entscheidend waren dabei einerseits das politische Leitmotiv des „*Nie wieder*" und andererseits die Einschätzung der Sowjetunion als eine gegen Europa gerichtete militärische und gesellschaftspolitisch-ideologische Bedrohung, der entgegengetreten werden müsse. Mit der Gründung des Europarats sollte der Friede in Europa gewahrt werden, indem die Mitgliedstaaten durch politische Kooperation enger zusammenrücken. Jene Europaratsbefürworter (darunter insb. die Benelux-Länder und Frankreich), die für eine supranationale Organisationsform und damit für die Abtretung nationalstaatlicher Kompetenzen an eine übergeordnete Instanz eintraten, konnten sich allerdings gegenüber den Befürwortern eines Organisationsmodells auf Basis zwischenstaatlicher Kooperation (darunter insb. Großbritannien) nicht durchsetzen (Brummer

48 Neben den fünf Mitgliedern des Brüsseler Pakts (Frankreich, Großbritannien, Belgien, Luxemburg und die Niederlande) waren dies Dänemark, Norwegen, Schweden, Irland und Italien (Brummer 2008, 23).

2008, 21–23). Der Wunsch, den Europarat in Gestalt einer supranational verfassten Europäischen Union zu errichten, scheiterte also schon vor ihrer Gründung. Am Ende blieb ein politischer Kompromiss, den insbesondere die institutionelle Struktur der Organisation wiederspiegelt: Tonangebend sind die Regierungen der Mitgliedstaaten im Ministerkomitee (ebd., 33 ff.), während die Parlamentarische Versammlung vorrangig beratende Tätigkeiten wahrnimmt (ebd., 93 ff).

Anfangs noch vor dem Hintergrund des Ost-West-Konflikts deutlich schwächer ausgeprägt, war der Europarat vor allem seit den 1960er-Jahren darum bemüht, sich als möglichst offene Organisation zu verstehen, indem sie allen Staaten, die ihr noch nicht beitreten konnten oder wollten, die Möglichkeit des Beitritts niedrigschwellig offenhielt, sofern die Wertretrias des Europarats bestehend aus Demokratie, Menschenrechten und Rechtsstaatlichkeit grundsätzlich eingehalten wurde (Brummer 2008, 17). So zählte der Europarat Ende der 1970er-Jahre bereits 22 Mitgliedstaaten und umfasst heute nach mehreren größeren Erweiterungsrunden die mit dem Beitritt Montenegros 2007 ihr vorläufiges Ende fanden, mit 47 Mitgliedstaaten nunmehr beinahe alle europäischen Staaten (ebd., 28 f.). Zwar ging mit diesem enormen Mitgliederzuwachs auch eine Steigerung des Handlungsspielraums einher, doch leidet der Europarat seit einigen Jahrzehnten unter der Aufweichung seiner zentralen Prinzipien der Demokratie, Menschenrechte und Rechtsstaatlichkeit, da mehrere Mitgliedstaaten diese untergraben, während sie zugleich kaum nennenswerte Folgen zu befürchten haben (ebd., 31 f.).[49]

Zur Erfüllung seiner Aufgaben kann der Europarat auf verschiedene Instrumente zurückgreifen. Relevant für die Aktivitäten des Europarats auf dem Feld der Datenschutzpolitik sind vor allem zwei Instrumente: Konventionen und Empfehlungen. Sowohl die Ausarbeitung einer Konvention als auch ihre Annahme erfolgen seitens des Ministerkomitees. Damit Konventionen Bindungswirkung entfalten können, müssen Staaten der Konvention zunächst beitreten, d. h. diese ratifizieren (ebd., 62 ff.). Empfehlungen entfalten im Gegensatz zu Konventionen keine Bindungswirkung gegenüber den Mitgliedstaaten. Sie dienen vielmehr dem Versuch der allgemeinen Orientierung der Mitgliedstaaten auf neuen oder strittigen thematischen Feldern (Brummer 2008, 66).

Bereits achtzehn Monate nach Gründung des Europarats wurde am 4. November 1950 das wohl bekannteste Dokument des Europarats, die Eu-

49 Vgl. z. B. den Umgang mit den russischen Menschenrechtsverletzungen (Ackeret 2019).

ropäische Menschenrechtskonvention (EMRK), zur Zeichnung aufgelegt. Nach dem Erreichen der erforderlichen Zahl von zehn Staaten, die das Dokument ratifiziert hatten, trat die EMRK schließlich am 3. September 1953 in Kraft (143 f.). Die EMRK orientiert sich inhaltlich und terminologisch klar an der *Allgemeinen Erklärung der Menschenrechte* (AEMR) der Vereinten Nationen vom Dezember 1948. Zum einen wird in der EMRK der universelle Charakter der Menschenrechte, wie er in der AEMR festgeschrieben wurde, nachdrücklich unterstützt. Zum anderen aber bildet die EMRK den Versuch, „die ersten Schritte auf dem Weg zu einer kollektiven Garantie bestimmter in der Allgemeinen Erklärung aufgeführter Rechte zu unternehmen." (Europarat 2010 Präambel) Die Durchsetzbarkeit der in der EMRK dargelegten Menschenrechte wurde insbesondere über die Einführung des Individualbeschwerdeverfahrens möglich, mit der Einzelpersonen erstmals Rechte nach internationalem Recht erhielten, die unabhängig von den Rechten ihrer Heimatstaaten existierten. Den bedeutendsten Baustein des EMRK-Kontrollmechanismus bildet daher auch der Europäische Gerichtshof für Menschenrechte (EGMR), der seine Arbeit Anfang 1959 aufnahm (Brummer 2008, 143 ff.).

3.1.2.1 Erste Aktivitäten des Europarats mit Privatheits- und Datenschutzbezug

Datenschutz und Privatheit waren in den ersten Jahrzehnten seines Bestehens zunächst noch kein Thema für den Europarat (González Fuster 2014, 82). Dies änderte sich 1967. Auf einer Sitzung der Beratenden Versammlung des Europarats[50] wurde Art. 8 EMRK[51] dahingehend uminterpretiert, dass fortan nicht mehr nur das Privatleben (im Sinne räumlicher, häuslicher Privatheit)[52], sondern Privatheit im Allgemeinen als von dem Artikel umfasst verstanden wurde. Diese Neubestimmung des Begriffs fand im Kontext von Debatten über die Auswirkungen wissenschaftlicher und tech-

50 Die „Beratende Versammlung" wurde 1974 in „Parlamentarische Versammlung" umbenannt (Brummer 2008, 93).

51 „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz." (Europarat 2010 Art. 8 (1)).

52 An dieser Stelle sei auf Fusters Analyse der Sprachverwendung in AEMR und EMRK verwiesen. Dabei wird deutlich, dass der in der englischen Originalfassung der AEMR verwendete Term „privacy" kurz vor der Finalisierung der EMRK durch „private life" ersetzt wurde, aber in Anlehnung an das „vie priveé" im Französischen doch dasselbe meint (González Fuster 2014, 81 f.).

nologischer Entwicklungen auf den Schutz der Menschenrechte, statt. Im Anschluss beauftragte die Beratende Versammlung ihren Rechtsausschuss mit der Erstellung von zwei Anträgen: Einer Resolution zum Thema der Menschenrechte und moderner wissenschaftlicher Entwicklungen im Allgemeinen und einer weiteren Resolution, die sich mit der Problematik technischer Vorrichtungen zum Zwecke des Eindringens in und Abhörens von privaten Räumen auseinandersetzen und Regulierungsmöglichkeiten unterbreiten sollte (ebd., 83). Die vom Rechtsausschuss erarbeitete Antwort führte zu weiteren Diskussionen in der Beratenden Versammlung darüber, ob und inwiefern Art. 8 EMRK aber auch das nationale Recht der Mitgliedstaaten des Europarats dafür geeignet seien, den Schutz von Privatheit angesichts neuartiger wissenschaftlich und technologisch bedingter Risikoszenarien zu gewährleisten (ebd.).[53] Im Ergebnis dieser Debatten hielt die Beratende Versammlung im Rahmen der Empfehlung 509 (1968) fest, „that newly developed techniques […] are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights" (Parliamentary Assembly of the CoE 1968 Paragraph 3). Die Beratende Versammlung rief das Ministerkomitee schließlich dazu auf, das Expertenkomitee für Menschenrechte mit der Frage zu befassen, ob die mitgliedstaatliche Rechtslage einen ausreichenden Schutz vor Verletzungen des Rechts auf Privatheit bietet, die durch den Einsatz moderner wissenschaftlicher und technologischer Mittel entstehen können (ebd., Paragraph 8). Die Ministerkonferenz entsprach der Empfehlung der Beratenden Versammlung und beauftragte das Expertenkomitee mit der Erarbeitung einer Studie. In dieser 1970 fertiggestellten Studie wurde schließlich, entgegen den Erwartungen der Beratenden Versammlung, festgestellt, dass die in der Empfehlung genannten Risikogründe (das Abhören von Telefonen bzw. Abhöraktivitäten im Allgemeinen, versteckte Überwachung usw.) ausreichend unter Kontrolle seien. Allerdings wies das Expertenkomitee darauf hin, dass die Verbreitung von Rechnern ein Problem für die Privatheit darstelle, das womöglich nicht ausreichend von Art. 8 EMRK abgedeckt sei, da die Vorgaben des Art. 8 lediglich auf den öffentlichen aber nicht auch auf den nicht-öffentlichen Bereich anwendbar seien. Ein weiteres Unterkomitee, das sich ab 1971 mit derselben Materie auseinandersetze, grenzte das Problem schließlich auf

53 Der österreichische Wortführer des Rechtsausschusses (aber auch die übrigen Mitglieder) waren laut Fuster (2014, 83) besonders mit der Arbeit von Alan Westin vertraut.

die Nutzung elektronischer Datenbanken ein, sodass im Jahr 1973 zunächst die Empfehlung (73) 22 (Council of Europe 1973) und ein Jahr später die Empfehlung (74) 29 (Council of Europe 1974) durch den Europarat angenommen wurde. Ausgehend von der Auffassung, „the right to privacy, which is, by its very nature a matter belonging to the European public order" (Council of Europe 1974 Explanatory Report, Nr. 8), wurde mit ihnen das Ziel verfolgt, bis zur möglichen Ausarbeitung eines international verbindlichen Dokuments der Entstehung weiterer Divergenzen auf dem Gebiet nationaler Datenschutzregelungen entgegenzuwirken (Council of Europe 1973). In der Begründung der Empfehlung (73) 22 wurde ausgehend von der Feststellung, dass Art. 8 EMRK keinen ausreichenden Schutz der informationellen Privatheit („data privacy") vor technologisch bedingten Beeinträchtigungen biete, betont, dass der Privatsektor besonderen Anlass zur Sorge schaffe, weil dieser im Gegensatz zum öffentlichen Bereich einen eindeutig grenzüberschreitenden Fokus mit sich bringe und das Fehlen von Schutzregelungen in vielen Mitgliedstaaten die Position der Individuen schwäche (Council of Europe 1973 Explanatory Report, § 6). Inhaltlich orientierten sich die Empfehlungen an den miteinander übereinstimmenden Elementen bestehender nationaler Datenschutzgesetze, wie sich an den vorgeschlagenen Prinzipien zeigt: Vorgaben zur Rechtmäßigkeit bei der Erhebung (Nr. 1, 3)[54] und Verwendung (Nr. 9) personenbezogener Daten, Vorgaben zur Zweckbindung (Nr. 2, 5), Speicherfristen (Nr. 4), Transparenzvorgaben (Nr. 6), Datenqualität (Nr. 7), Sicherheits- (Nr. 8), Anonymisierungs- und Pseudonymisierungsmaßnahmen (Nr. 10).

3.1.2.2 Die Erarbeitung der Datenschutz-Konvention Nr. 108

Nach Verabschiedung der beiden Empfehlungen setzte der Europarat seine Tätigkeiten auf dem Gebiet des Datenschutzes fort, indem deren Implementierung in den Europaratsmitgliedstaaten im Hinblick auf die weitere Entwicklung der Divergenz nationaler Datenschutz-Bestimmungen verfolgt wurde. Zu diesem Zweck wurde im Jahr 1975 vom Sekretariat des Europarats eine Studie erarbeitet. In dieser wurde festgestellt, dass zwischen den

54 Da die Prinzipien beider Empfehlungen weitgehend übereinstimmend sind, beziehen sich die genannten Ziffern auf Empfehlung (73) 22. Erwähnenswert ist, dass Empfehlung (74) 29 zusätzlich (nationale) Ausnahmen von der Zweckbindung und bei den Speicherfristen für statistische, wissenschaftliche oder historische Zwecke unter Einhaltung von Garantien vorsieht (Nr. 4).

Datenschutzgesetzen der Mitgliedstaaten sowohl wesentliche Gemeinsamkeiten als auch entscheidende Diskrepanzen vorhanden waren (González Fuster 2014, 86). Die anhaltenden Diskrepanzen wurden 1976 schließlich seitens des Ministerkomitees zum Anlass für die Einrichtung eines Expertenkomitees[55] genommen, das mit der Erarbeitung einer Europaratskonvention *zum Schutze der Privatheit bei der Datenverarbeitung im Ausland und bei der grenzüberschreitenden Datenverarbeitung*[56] beauftragt wurde (Council of Europe 1981 Nr. 13).

Der Europarat war spätestens seit diesem Zeitpunkt an einer möglichst breiten Wirkung der auszuarbeitenden Europaratskonvention interessiert. So hatte bereits die erste Sitzung des Expertenkomitees einen Briefwechsel mit der OECD zur Folge, in dessen Rahmen sich die beiden Institutionen Zusammenarbeit und gegenseitige Unterstützung zusicherten. Einig waren sich beide Institutionen insbesondere dahingehend, dass eine künftige Europaratskonvention den von der OECD unterstützten Grundsatz des freien grenzüberschreitenden Informationsflusses respektieren und keine Hindernisse für den internationalen Handel mit personenbezogenen Daten errichten sollte (Council of Europe 1981 Nr. 14; González Fuster 2014, 87). Außerdem nahmen an den Sitzungen des Expertenkomitees Vertreter sowohl der OECD und vier ihrer nichteuropäischen Mitgliedstaaten (Australien, Kanada, Japan und die Vereinigten Staaten) als auch der Europäischen Kommission und damit der Europäischen Gemeinschaften teil. Im Laufe der Beratungen intensivierte sich die Kooperation zwischen dem Europarat und den Europäischen Gemeinschaften noch weiter. Während die Europäische Kommission sich jedoch später dazu entschied, das Ergebnis

55 Das *Commitee of Experts on Data Protection* war zwischen November 1976 und May 1979 tätig und wurde 1978 in *Project Group on Data Protection* (CJ-PD) umbenannt. Institutionell war es dem *Ausschuss für rechtliche Zusammenarbeit* (CDCJ – European Committee on Legal Co-operation) untergeordnet. Seit Ende 1974 war im Europarat zudem die Vorstellung vorherrschend geworden, dass sich in der Zwischenzeit die Verwendung des Begriffspaars „Data Protection" für die mit dem Schutz informationeller Privatheit bzw. dem Schutz personenbezogener Daten zusammenhängenden Problemstellungen in Europa durchgesetzt habe, sodass der Europarat eine allmähliche Umstellung des Europaratsvokabulars von *privacy* auf *data protection* vollzog (González Fuster 2014, 86 f.). Gemäß Frits W. Hondius (1975, 4), einem der wesentlichen Verantwortlichen bei der Erarbeitung der Datenschutz-Konvention, wurden Datenschutzrechte als ein Aspekt von Privatheit verstanden, nämlich der informationellen Privatheit.

56 Eigene Übersetzung. Im Original: „to prepare a convention for the protection of privacy in relation to data processing abroad and transfrontier data processing" (Council of Europe 1981 Nr. 13).

der Europaratsaktivitäten auf dem Felde der Harmonisierung nationaler Datenschutzbestimmungen abzuwarten, hielt das Europäische Parlament (EP) an der Erarbeitung von Gemeinschaftsregelungen zum Datenschutz in der EG fest (vgl. auch 3.2.2.1). In einem Brief an den Generalsekretär des Europarats signalisierte der Generalsekretär des Europäischen Parlaments allerdings auch das Interesse des Parlaments an den Arbeiten des Europarats. So wurde in der ebenfalls mitversendeten EP-Resolution aus dem Jahre 1979 nicht nur der Erlass eigener Gemeinschaftsstandards, sondern auch der Beitritt der EG zur Europaratskonvention gefordert (González Fuster 2014, 87). Die parlamentarische Versammlung des Europarats nahm Anfang 1980 zur Haltung des EP Stellung und lud dieses mittels einer Europaratsempfehlung dazu ein, die Harmonisierung mitgliedstaatlicher Datenschutzbestimmungen bzw. den Erlass harmonisierter Datenschutzbestimmungen entlang der – sich kurz vor ihrer Finalisierung befindenden – Europaratskonvention zu unterstützen (Parliamentary Assembly of the CoE 1980 Nr. 10). Eine möglichst breite Wirkung der Europaratskonvention sollte zudem auch dadurch erzielt werden, dass beschlossen wurde, dass auch nichteuropäische Staaten ihr beitreten können sollten. Dass die Datenschutz-Konvention nicht als Europaratskonvention, sondern schlicht als Konvention benannt wurde, spiegelt diesen Anspruch wider (Council of Europe 1981 Nr. 24).

Nachdem das zuständige Expertenkomitee 1979 eine erste Fassung der Datenschutz-Konvention vorbereitet hatte, wurde diese zunächst im Rahmen eines weiteren Expertenkomitees im April 1980 überarbeitet, finalisiert und schließlich am 17. September 1980 seitens des Ministerkomitees angenommen, aber erst am 28. Januar 1981 zur Unterzeichnung aufgelegt (Council of Europe 1981 Nr. 17; González Fuster 2014, 88).[57]

3.1.2.3 Inhalt der Datenschutz-Konvention 108

Im Gegensatz zu den OECD-Richtlinien, die zwei einander widerstrebende Ziele zu vereinen suchten, verfolgte die Datenschutz-Konvention des Europarats vielmehr das Ziel, „im Hoheitsgebiet jeder Vertragspartei für

57 Die Erstunterzeichner-Staaten sind: Dänemark, Deutschland, Frankreich, Luxemburg, Österreich, Schweden und die Türkei. Die Ratifizierung seitens einiger dieser Staaten erfolgte allerdings mit – teils erheblicher – Verzögerung. Im Extremfall der Türkei lagen 35 Jahre zwischen Unterzeichnung und Ratifizierung (Council of Europe 2019).

jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden (‚Datenschutz')" (Europarat 1981). Zwar sah auch die Europaratskonvention vor, dass *der bloße Hinweis* (Simitis u. a. 2019, 186, Rn. 103) auf den Schutz der Persönlichkeit des Betroffenen nicht dazu legitimiert, grenzüberschreitende Datenflüsse zu verbieten oder von einer besonderen Genehmigung abhängig zu machen (Europarat 1981, Art. 12 Abs. 2). Dennoch wurde nicht der ungehinderte Fluss von Informationen als Angelpunkt der Materie festgelegt: „Erst die Existenz einer von allen Vertragsstaaten akzeptierten Mindestregelung ebnet vielmehr den Weg zu einem grenzüberschreitenden Transfer der Daten" (Simitis u. a. 2019, 186, Rn. 103). Simitis zufolge ist Art. 12 Abs. 2 der Datenschutz-Konvention vielmehr als Kompromiss zu deuten, den der Europarat, insb. gegenüber den Nicht-Mitgliedstaaten, eingehen musste, um den erfolgreichen Abschluss der Konvention nicht zu gefährden (Simitis 2001, 102 f.).

Gonzáles-Fuster (2014, 89 f.) weist zudem darauf hin, dass eine herausragende Besonderheit der Datenschutz-Konvention ihre Verknüpfung der Forderung nach möglichst freien, grenzüberschreitenden Datenflüssen mit der Freiheit der Meinungsäußerung ist. Dazu verband die Präambel der Datenschutz-Konvention den „freien Informationsaustausch […] zwischen den Völkern" mit der Forderung nach „Informationsfreiheit ohne Rücksicht auf Staatsgrenzen" (Europarat 1981). Im erläuternden Bericht[58] zur Datenschutz-Konvention wurden die Vorgaben aus Art. 12 der Datenschutz-Konvention zum grenzüberschreitenden Verkehr personenbezogener Daten schließlich eindeutig in Bezug zu Art. 10 EMRK[59] gesetzt. Entsprechend wird konstatiert, dass der freie grenzüberschreitende Verkehr von Informationen nicht allein für Staaten von Bedeutung ist, sondern auch für Individuen (Council of Europe 1981 Nr. 9). Die von der OECD und insbesondere von ihren nichteuropäischen Mitgliedern vorgebrachte wirtschaftspolitisch motivierte Forderung nach möglichst freien grenzüberschreitenden Datenflüssen zur Vermeidung von Handelshemmnissen wird also in der Datenschutz-Konvention um eine menschenrechtspolitische Dimension ergänzt.

58 Vergleichbar einer Gesetzesbegründung, Erwägungsgründen, etc.

59 In diesem heißt es: „Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben." (Europarat 2010)

Davon abgesehen umfasst der Anwendungsbereich der Konvention ebenso wie die OECD-Richtlinien sowohl den öffentlichen als auch den nicht-öffentlichen Bereich, beschränkt sich aber im Gegensatz zu den OECD-Richtlinien nicht auf die automatisierte Verarbeitung personenbezogener Daten.[60] Die Definition personenbezogener Daten umfasst „jede Information über eine bestimmte oder bestimmbare natürliche Person" (Art. 2 a).[61] Art. 5 legt schließlich die Grundsätze dar, die den *harten* Kern des Datenschutzes ausmachen und die bis heute weitgehend intakt geblieben sind: Personenbezogene Daten müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden (Art. 5 a); sie dürfen nur für festgelegte und rechtmäßige Zwecke verarbeitet werden (Art. 5 b); sie müssen für den jeweiligen Verarbeitungszweck relevant und vom Umfang her angemessen sein (Art. 5 c); sie müssen sachlich richtig und auf dem neuesten Stand sein (Art. 5 d) und so aufbewahrt werden, dass ein Betroffener lediglich innerhalb der für den jeweiligen Zweck erforderlichen Verarbeitungszeit identifiziert werden kann (Art. 5 e).

Die Datenschutz-Konvention enthält in Art. 6 zudem Vorgaben zur Verarbeitung besonderer Arten personenbezogener Daten. Aufgelistet werden solche zur rassischen Herkunft, zu politischen, religiösen oder anderen Überzeugungen sowie Angaben zur Gesundheit, zum Sexualleben und zu Vorstrafen.[62]

Art. 8 schreibt schließlich die Betroffenenrechte fest. So müssen Betroffene im Rahmen ihres Auskunftsrechts die Möglichkeit haben, beim Verantwortlichen Informationen über die verwendeten personenbezogenen Daten, die Verarbeitungszwecke, aber auch über den gewöhnlichen Aufent-

60 Den Vertragsstaaten steht es allerdings gemäß Art. 3 Abs. 2 lit. c frei, darüber zu entscheiden, den Anwendungsbereich auf die manuelle Verarbeitung personenbezogener Daten auszudehnen.

61 Auch in diesem Bereich räumt die Konvention den Vertragsstaaten die Möglichkeit ein, den Anwendungsbereich auch auf Personengruppen, Vereinigungen, Stiftungen, Gesellschaften, Körperschaften oder andere Stellen mit oder ohne juristische Persönlichkeit auszudehnen (Art. 3 Abs. 2 lit. b).

62 Im erläuternden Bericht wurde allerdings unter Verweis auf die Bedeutung des Kontexts bei der Datenverarbeitung versucht klarzustellen, dass die Auflistung in der Konvention lediglich eine Orientierung zu bieten vermöge, Ergänzungen und Spezifizierungen im nationalen Recht also notwendig sein würden: "The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned. Information on trade union membership for example may be considered to entail as such a privacy risk in one country, whereas in other countries it is considered sensitive only in so far as it is closely connected with political or religious views." (Council of Europe 1981 Nr. 48)

haltsort oder den Sitz des Verantwortlichen zu erhalten (Art. 8 a). Art. 8 b schreibt zudem vor, dass diese Mitteilung in angemessenen Zeitabständen und ohne unzumutbare Verzögerung oder übermäßige Kosten sowie in verständlicher Form zu erfolgen hat. Art. 8 c schreibt die Rechte auf Berichtigung und Löschung fest und Art. 8 d sieht die Bereitstellung von Rechtsmitteln im nationalen Recht zum Zwecke der Durchsetzung der Betroffenenrechte vor.

Ein bedeutender Unterschied zu den OECD-Richtlinien liegt in Art. 10 vor, der die Schaffung von Sanktionsstrukturen und Rechtsmitteln im nationalen Recht für Verletzungen der Vorgaben der Datenschutz-Konvention vorsieht.

Zum Zwecke der verbesserten Anwendung der Konvention wurde sowohl die gegenseitige Unterstützung der Vertragsstaaten (Art. 13) als auch die Einrichtung eines Beratenden Ausschusses (Art. 18–20) vorgesehen. Der Ausschuss konnte unter anderem Änderungen vorschlagen und somit die Weiterentwicklung des Instruments sicherstellen.[63]

3.1.2.4 Zwischenfazit / Bewertung

Die Datenschutz-Konvention trat, nachdem sie durch fünf Mitgliedstaaten (Deutschland, Frankreich, Norwegen, Schweden, Spanien) ratifiziert wurde, am 1. November 1985 in Kraft. Stand Anfang 2019 wurde die Datenschutz-Konvention von insgesamt 54 Staaten, darunter 7 Nicht-Mitgliedstaaten, ratifiziert (Council of Europe 2019). Damit ist sie das erste und bis heute einzige verbindliche internationale Datenschutz-Instrument (P. de Hert und Papakonstantinou 2014, 635). Gegenüber den OECD-Richtlinien unterscheidet die Datenschutz-Konvention außerdem noch die vergleichsweise klare Adressierung von Datenschutz als zentralem Ziel und die Bevorzugung staatlicher Regulierung anstelle von Selbstregulierung zur Erreichung dieses Ziels. Viele der nach der Annahme der Datenschutz-Konvention erlassenen nationalen Datenschutzgesetze wurden von dieser geprägt. Die in der Konvention dargelegten Datenschutz-Grundsätze fungierten als Grundlage jeder weiteren europäischen Regelung auf dem Gebiet des Datenschutzrechts (Zerdick 1995, 81) bzw. als Grundlage auch im Hinblick

63 Aufgrund von mitgliedstaatlichen Meinungsverschiedenheiten enthält die Konvention keine Vorgaben zur Einrichtung unabhängiger Aufsichtsinstanzen (Simitis u. a. 2019, 186, Rn. 101).

auf die Überarbeitung der bestehenden nationalen Regelungen (González Fuster 2014, 93).[64]

Trotz dieser Vorzüge verfehlte die Konvention letzten Endes das Ziel der Schaffung eines ausreichend harmonisierten Datenschutzniveaus. Dies lag einerseits daran, dass die in den Artikeln 13 und 18–20 vorgesehen Maßnahmen bzw. der Beratende Ausschuss nur bedingt dazu geeignet waren, die einheitliche Anwendung der Konvention sicherzustellen. Während die Erarbeitung der Konvention noch seitens unabhängiger Sachverständiger erfolgte, gingen die Regierungen der Vertragsstaaten nach dem Beitritt zur Konvention dazu über, den Beratenden Ausschuss mit Regierungsvertretern zu besetzen, sodass die Chancen einer möglichst unabhängigen und wissenschaftlichen Beurteilung der Anwendung der Konvention verloren gingen, weil keine ernsthaften Änderungsvorschläge gemacht wurden (Simitis u. a. 2019, 187 f., Rn. 110). Schließlich verfehlte die Konvention das Harmonisierungsziel insbesondere in Bezug auf den Anwendungsbereich (Einbezug manueller Verarbeitung vs. ausschließlicher Einbezug automatisierter Verarbeitungen sowie Einbezug juristischer Personen vs. ausschließlicher Einbezug natürlicher Personen) sowie die konkrete Ausgestaltung der Verarbeitungsvoraussetzungen (Ausgestaltung der Auskunftsrechte bzw. genereller Verarbeitungstransparenz und die Verarbeitung besonderer Arten personenbezogener Daten) (Commission of the European Communities 1990, 2 f.).

Die Europäische Kommission, die bereits seit Jahren als Beobachterin an der Erarbeitung der Konvention beteiligt war, forderte die Mitgliedstaaten der Europäischen Gemeinschaften Mitte 1981 – und damit bereits kurz nach der Freigabe der Konvention zur Unterschrift – in einer Empfehlung dazu auf, die Datenschutz-Konvention noch im selben Jahr zu unterzeichnen und im Laufe des Jahres 1982 zu ratifizieren (Commission of the European Communities 1981). Die Nichtbefolgung dieser Kommissionsempfehlung sollte einige Jahre später schließlich ein ausschlaggebender Grund für die Erarbeitung der EU-DS-RL sein. Wie die Europäische Union mit der Herausforderung der zunehmenden Verarbeitung personenbezogener Daten umging und wie es zur Verabschiedung von EU-Maßnahmen zum Datenschutz kam, ist Gegenstand der folgenden Unterabschnitte.

64 Genannt werden das britische (1984), das irische (1988), das finnische (1987) sowie das niederländische Datenschutzgesetz (1989) (González Fuster 2014, 93 f.).

3.2 Die ersten Datenschutz-Instrumente auf Gemeinschaftsebene

Die Regulierung der Verarbeitung personenbezogener Daten durch die EU lässt sich bis in die 1970er-Jahre zurückverfolgen. Nachdem die Europäische Kommission zunächst nur wenig Interesse an einer Harmonisierung der nationalen Datenschutzregelungen hatte, änderte sie diese Einstellung mit dem Scheitern der OECD-Datenschutz-Richtlinien und der Datenschutz-Konvention des Europarats. In der Folge wurde zunächst die Datenschutz-Richtlinie 95/46/EG im Jahr 1995 und im Anschluss daran viele weitere Datenschutzbestimmungen verabschiedet und das Feld der Datenschutzpolitik zunehmend durch Europäische Regulierungen geprägt.

Die Verabschiedung der DS-RL markiert einen wichtigen Wendepunkt in der Geschichte des Datenschutzes, der in den Folgejahren nicht nur für die Mitgliedstaaten, sondern auch für viele Staaten weltweit von großer Bedeutung sein sollte. Die DSGVO stellt die Nachfolgerin der DS-RL dar. Das Ziel dieses Unterabschnitts ist die Erklärung des Zustandekommens der Richtlinie. Dazu wird zunächst ein Überblick über die frühesten Aktivitäten auf Gemeinschaftsebene geboten (vgl. 3.2.2.1 bis 3.2.2.2), der Aushandlungsprozess und die Rahmenbedingungen kurz skizziert sowie im Anschluss der Aushandlungsprozess inkl. der Konfliktlinien im Detail erörtert sowie eine Zusammenfassung der wichtigsten Inhalte der Richtlinie geliefert (vgl. 3.2.2.4 bis 3.2.2.8). Darauf folgt eine kurze Betrachtung ihrer Implementierung in den Mitgliedstaaten (vgl. 3.2.2.9).

Bevor jedoch der konfliktreiche Aushandlungsprozess der DS-RL beleuchtet wird, gibt der folgende Unterabschnitt 3.2.1 für ein besseres Verständnis der Aushandlungsprozesse und Konfliktkonstellationen auf EU-Ebene zunächst einen Überblick über die Struktur und Organe der Europäischen Union, die bis hin zum Aushandlungsprozess der DSGVO prägend für die datenschutzpolitischen Auseinandersetzungen auf EU-Ebene waren.

3.2.1 Struktur und Organe der Europäischen Union

Die Europäische Union in ihrer heutigen Form kann als staatsähnliches Gebilde charakterisiert werden, das wesentliche Bereiche des wirtschaftlichen, sozialen und politischen Lebens in den Mitgliedstaaten prägt (Wessels 2008, 20). Ein entscheidendes Merkmal der EU besteht allerdings in ihrem bis heute anhaltenden Fokus auf die Integration durch wirtschaftliche Kooperation, die erst allmählich und zuletzt vor allem durch das In-

krafttreten der EU-Grundrechtecharta eine andere Qualität angenommen hat, und die unter anderem für die Reform des EU-Datenschutzrechts entscheidend gewesen ist (Lelieveldt und Princen 2015; Tinnefeld 2009; Wessels 2008).

Der Fokus auf wirtschaftliche Integration hat seine Wurzeln in der Unterzeichnung des Pariser Vertrags zur Europäischen Gemeinschaft für Kohle und Stahl (EGKS) im Jahr 1951 sowie der Römischen Verträge im Frühjahr 1957. Ersterer fokussierte sich auf die Vergemeinschaftung der kriegswichtigen Güter Kohle und Stahl und letztere erweiterten die wirtschaftliche Zusammenarbeit in Richtung der Schaffung eines gemeinsamen Binnenmarktes vor dem Hintergrund der Idee europäischer Völkerverständigung, nachdem der weitergehende Vorstoß in Form der Europäischen Verteidigungsgemeinschaft (EVG), die eine Kooperation im militärischen und politischen Bereich vorgesehen hatte, von der französischen Nationalversammlung 1954 abgelehnt worden war (Wessels 2008, 66 ff.). Neben der Gründung der Europäischen Wirtschaftsgemeinschaft (EWG) sahen die Römischen Verträge auch die Gründung der Europäischen Atomgemeinschaft (EURATOM) zum Zwecke der Sicherstellung der friedlichen Verwendung der Atomenergie vor. Die sechs Unterzeichnerstaaten waren Belgien, Frankreich, die Bundesrepublik Deutschland, Italien, Luxemburg und die Niederlande. Mit dem Inkrafttreten des EG-Fusionsvertrags am 1. Juli 1967 wurden die drei bestehenden Gemeinschaften (EGKS, EWG und EURATOM) in den Europäischen Gemeinschaften zusammengeführt. Institutionell bedeutete dies, dass die bestehenden drei Ministerräte (der EGKS, der EWG und der EURATOM) zum Rat der Europäischen Union (bzw. geläufiger auch als Ministerrat[65] bekannt) sowie die bestehenden zwei Kommissionen (der EWG und des EURATOM) zur Kommission der Europäischen Gemeinschaften (die heutige Europäische Kommission) fusionierten.[66] Schon vor der Unterzeichnung des Fusionsvertrages teilten sich die drei Gemeinschaften eine parlamentarische Versammlung (das heutige Europäische Parlament), einen Gerichtshof (Europäischer Gerichtshof – EuGH) sowie einen Wirtschafts- und Sozialausschuss (WSA – heutiger Name: Europäischer Wirtschafts- und Sozialausschuss EWSA). In

65 Wenn im weiteren Verlauf des Textes die Rede vom *Rat* ist, ist stets der Ministerrat gemeint.

66 Um Verwirrungen aufgrund der Verwendung der unterschiedlichen Begrifflichkeiten zu vermeiden, werden im weiteren Verlauf durchgängig die aktuellen Bezeichnungen verwendet, also Ministerrat, Europäische Kommission, Europäisches Parlament usw.

mehreren Erweiterungsrunden wuchs die Zahl der Mitgliedstaaten von ursprünglich sechs auf bis zu 28 an.[67] Mit dem Inkrafttreten des Maastrichter Vertrags Ende 1993 wurde die intergouvernementale Zusammenarbeit der EG über die Wirtschaftskooperation (nunmehr als erste Säule bezeichnet) hinaus auf die teil-vergemeinschafteten Politikbereiche der gemeinsamen Außen- und Sicherheitspolitik (GASP) (zweite Säule) sowie der Justiz- und Innenpolitik (JI)[68] (dritte Säule) ausgeweitet. Nachdem der bislang weitest gehende Integrationsversuch in Form der EU-weiten Annahme des Europäischen Verfassungsvertrags an den Referenden in Frankreich und den Niederlanden 2005 scheiterte, wurden dessen wesentliche Elemente in Form des Vertrags von Lissabon umgesetzt. Dieser hob u. a. die zuvor geschaffene Säulenstruktur und damit auch die Unterscheidung zwischen supranationalem Gemeinschaftsrecht (Binnenmarkt) und intergouvernementalem Unionsrecht (PJZS – Polizeiliche und justizielle Zusammenarbeit) auf und weitete das für datenschutzpolitische Fragen bedeutsame, sog. Mitentscheidungsverfahren auf die PJZS aus. Bedeutsam war zudem, dass mit dem Inkrafttreten des Lissabon-Vertrags am 1. Dezember 2009 auch die bereits 2000 proklamierte EU-Grundrechtecharta Rechtskraft erlangte. In Folge des Inkrafttretens des Reformvertrages bilden nunmehr der EUV (Vertrag über die Europäische Union) sowie der AUEV (Vertrag über die Arbeitsweise der Union, ehemals EC Treaty) die primärrechtlichen Grundlagen der EU (Europäische Union 2010).

Im Folgenden werden kurz die zentralen Organe der EU und ihre Rolle im politischen Geflecht der Unionspolitiken vorgestellt.

3.2.1.1 Europäischer Rat

Der 1974 gegründete Europäische Rat versammelt neben dem Präsidenten des Europäischen Rates, dem Präsidenten der Europäischen Kommission

67 1973 traten das Vereinigten Königreich, Dänemark und Irland der Gemeinschaft bei, 1981 folgte Griechenland, 1986 Portugal und Spanien, 1995 Finnland, Österreich und Schweden, 2004 Estland, Lettland, Litauen, Polen, Tschechien, Slowenien, die Slowakei, Ungarn, Malta sowie Zypern, 2007 Rumänien und Bulgarien und schließlich 2013 Kroatien. Aktuell (Stand: Mitte 2020) steht der freiwillige Austritt Großbritanniens aus der EU bevor.

68 Nachdem die justizielle Zusammenarbeit in Zivilsachen und die flankierenden Maßnahmen zum freien Personenverkehr mit dem Vertrag von Amsterdam 1997 in die erste Säule verschoben worden waren, verblieben die polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS) in der dritten Säule, die fortan entsprechend bezeichnet wurde (Wessels 2008, 94).

und dem hohen Vertreter der Union für Außen- und Sicherheitspolitik außerdem die Staats- und Regierungschefs der Mitgliedstaaten. Er gilt als „oberstes" Gremium der EU (Wessels 2008, 155), da er der Union „die für ihre Entwicklung erforderlichen Impulse [gibt] und [...] die allgemeinen politischen Zielvorstellungen und Prioritäten hierfür fest[legt]" (Europäische Union 2010, Art. 15 (1)).

Dazu gehört sowohl die Befassung mit und die Setzung von Schwerpunkten im Hinblick auf eine enorm breite Themenpalette an Politikfeldern als auch die Initiierung neuer Tätigkeitsbereiche wie etwa im Bereich der Innen- und Justizpolitik seit Ende der 1990er sowie im Rahmen der Terrorismusbekämpfung seit 2001 (Wessels 2008, 163 f.). Besonders sichtbare und einflussreiche Eckpunkte dieser Politik sind die Mehrjahresprogramme, die von Kommission und Ministerrat erarbeitet und vom Europäischen Rat verabschiedet werden. Darunter fallen das Tampere Programm (Europäischer Rat 1999b), das Haager Programm (Europäischer Rat 2005a) sowie das Stockholmer Programm (Europäischer Rat 2010).

3.2.1.2 Europäische Kommission

In der institutionellen Architektur der EU kommt der Europäischen Kommission eine wesentliche Rolle bei der *Vorbereitung*, *Verabschiedung*, *Durchführung* und *Kontrolle* von verbindlichen Entscheidungen zu (Wessels 2008, 225). So hat die Kommission im Regelfall[69] das Initiativrecht zur Einbringung von Legislativvorschlägen inne, sodass sie im Rahmen der *Vorbereitung*sphase häufig als Agenda-Setterin fungiert (Fouilleux, Maillard, und Smith 2005, 617). Das Parlament und der Ministerrat können die Kommission lediglich dazu auffordern, gesetzgeberisch aktiv zu werden. Bei der Wahrnehmung ihrer Aufgaben ist die Kommission gemäß ihres vertraglich festgelegten Auftrags dazu verpflichtet, die „allgemeinen Interessen" der Union zu fördern (Europäische Union 2010, Art. 17) – womit die Kommission ein Gegengewicht zum Ministerrat bilden soll, in dem einzelstaatliche Partikularinteressen verfolgt werden (Wessels 2008, 228 f.). In der Phase der *Verabschiedung* eines Legislativvorschlags ist die Kommission in

69 Die einzige Ausnahme existiert im Bereich der justiziellen Zusammenarbeit in Strafsachen oder der polizeilichen Zusammenarbeit, wo neben der Kommission auch mind. ein Viertel der EU-Mitgliedsstaaten einen Legislativvorschlag unterbreiten können (Lelieveldt und Princen 2015, 86). Zudem können Parlament und Ministerrat die Kommission dazu auffordern, einen Legislativvorschlag für ein Themengebiet anzufertigen (EU-Ministerrat 2017; Europäisches Parlament 2020).

die Beratungen und Verhandlungen zwischen Ministerrat und Parlament als Mitgestalterin sowie im Rahmen von Vermittlungsausschüssen oder informellen Trilog-Verhandlungen als Vermittlerin eingebunden. Sobald eine verbindliche Entscheidung von Parlament und Ministerrat beschlossen wurde, kommt der Kommission die Gewährleistung der *Durchführung* derselben zu. Schließlich wacht die Kommission im Rahmen der *Kontrolle* über die Einhaltung des Vertragsrechts („Primärrecht") und der auf dieser Grundlage gefassten Beschlüsse („Sekundärrecht"), also Verordnungen, Richtlinien usw. (Wessels 2008, 229).

Im Zuge der Vertragsänderungen seit ihrer Gründung im Jahr 1951 hat sich das Aufgaben- und Kompetenzspektrum der Kommission stetig erweitert. Zuletzt wurden mit dem Inkrafttreten des Lissabon-Reformvertrages die Strukturen der EU sowie die Kompetenzen und Funktionsweisen ihrer Organe reformiert. Auf Grundlage dieser jüngsten Vertragsänderungen kann sich die Kommission bei der Auswahl ihrer Themen idealtypisch sowohl an den Vorgaben höherer politischer Ebenen (jährliches Arbeitsprogramm der Kommission, Vorschläge des Parlament oder der Mitgliedstaaten im Rahmen von Ministerrat oder Europäischem Rat) orientieren als auch eine Route *von unten* nehmen, indem die Kommission unter Bezugnahme auf bestehende Regelungen selbst zur Agenda-Setterin wird (Princen und Rhinard 2006a).

Dabei kann die Kommission auf verschiedene Legislativinstrumente zurückgreifen. Mittels einer Richtlinie kann die Kommission den Mitgliedstaaten verbindlich zu erreichende Ziele vorgeben, während das Wie, also Form und Mittel der Zielerreichung, den Mitgliedstaaten überlassen bleibt. Demgegenüber hat eine Verordnung unmittelbar geltende Wirkung in jedem Mitgliedstaat. Empfehlungen und Stellungnahmen der Kommission entfalten schließlich keinerlei bindende Wirkung (Wessels 2008, 196). Neben diesen vertraglich vorgesehenen Dokumenten veröffentlicht die Kommission zudem auch Grünbücher und Weißbücher, um Konsultationsprozesse anzustoßen bzw. einen Kommissionsstandpunkt darzulegen sowie Mitteilungen, in denen sich die Kommission zu verschiedenen Themen äußert (EU-Ministerrat 2017).

3.2.1.3 Der Rat der Europäischen Union – Ministerrat

Der Ministerrat war lange Zeit das zentrale Entscheidungsorgan der EU. Bis zur Gründung des Europäischen Rats war der Ministerrat das einzige Organ, in dem die Regierungen der Mitgliedstaaten – in Form von Minis-

tern oder Staatssekretären – repräsentiert waren. Trotz des allmählichen Aufstiegs des Parlaments zum Mitgesetzgeber, der mit dem Inkrafttreten des Lissabon-Vertrags seinen vorläufigen Höhepunkt erreichte, kommt dem Rat in der Hierarchie der EU-Organe, insbesondere aufgrund ihrer Nähe und des Einflusses auf den Europäischen Rat, immer noch eine zentrale Rolle zu (Naurin 2014). Denn obwohl die wegweisenden Entscheidungen der EU auf den Treffen des Europäischen Rats getroffen werden, erfolgt die meiste tatsächliche politische Arbeit der Mitgliedstaaten auf der Ebene des Ministerrats und der ihm unterstellten Vorbereitungsgremien (Hayes-Renshaw 2017; Naurin 2014). Dem Ministerrat kommen sowohl legislative als auch budgetäre sowie exekutive Aufgaben zu. Zudem fungiert der Ministerrat als Unterstützungs- und Umsetzungsgremium der Beschlüsse des Europäischen Rates (Europäische Union 2010, Art. 16). Der Ministerrat verabschiedet aber nicht nur Rechtsakte, wie es in den europarechtlichen Verträgen vorgesehen ist, sondern beispielsweise auch Schlussfolgerungen und Entschließungen. In diesen Dokumenten, die vertraglich nicht vorgesehen sind und die daher auch keine Rechtswirkung entfalten, äußert sich der Ministerrat zu unterschiedlichen Themen im Zusammenhang mit den Tätigkeitsbereichen der EU (EU-Ministerrat 2017).

3.2.1.4 Europäisches Parlament

Seit seinem Bestehen hat das Europäische Parlament zunehmend an Bedeutung gewonnen, sodass die ehemalige Dominanz von Kommission und Ministerrat immer mehr – und insbesondere seit dem Inkrafttreten des Lissabon-Vertrags – einem institutionellen Dreieck gewichen ist, in dem das Parlament zunehmend als Mitentscheider und Vetospieler, statt nur als Berater, auftritt (Wessels 2008, 119).

In den ersten Jahrzehnten, die auf seine Gründung folgten, war das EP zunächst (anfänglich unter dem Namen „Versammlung") als Diskussionsforum ohne Entscheidungsbefugnisse konzipiert, sodass ein Großteil seiner Tätigkeit im Bereich weniger bedeutsamer Prozesse verlief. Der Prozentsatz der politischen Entscheidungen, an denen das Parlament als Mitentscheider partizipiert, hat sich nach der erstmaligen Einführung des Mitentscheidungsverfahrens im Rahmen des Vertrags von Maastricht 1993 zunächst mit dem Inkrafttreten des Vertrags von Amsterdam 1999 und später den Verträgen von Nizza und Lissabon signifikant erhöht (Pittella, Vidal-Quadras, und Papastamkos 2014; Wessels 2008, 124).

Aufgrund seiner Macht-*Ferne* galt das Europäische Parlament über viele Jahre als ein im Vergleich zu Kommission und Rat offener Diskussionsort für umweltschutz-, verbraucherschutz- oder auch geschlechterpolitische Interessengruppen (sog. diffuse Interessen) aus der Zivilgesellschaft (Dür, Bernhagen, und Marshall 2013; Kluger Dionigi 2017; D. J. Marshall 2012). Mit dem Aufstieg zum Mitgesetzgeber hat sich diese Rolle des Parlaments allerdings deutlich gewandelt. So gilt das Parlament (bzw. die Ausschussvorsitzenden und zuständigen Rapporteure) inzwischen als einer der zentralen Adressaten für Interessengruppen jeglicher Couleur, sodass sich auch in den Entscheidungen des Parlaments immer weniger die Vertretung diffuser Interessen erkennen lässt. Sinnbildhaft im Bereich der Datenschutzpolitik war in diesem Zusammenhang das Abweichen des Parlaments von seiner früheren Position im Zusammenhang mit der EU-Richtlinie zum Zugriff auf Fluggastaten (Greis 2015) sowie zur Vorratsdatenspeicherung (Ripoll Servent 2013).[70]

In seiner Rolle als Mitgesetzgeber veröffentlicht das Parlament Berichte, in denen es seinen Standpunkt im Hinblick auf einen von der Kommission unterbreiteten Legislativvorschlag festlegt. Zudem kann auch das Parlament mittels Entschließungen/Resolutionen und Empfehlungen zu verschiedenen Fragen im Zuständigkeitsbereich der EU rechtsunverbindlich Stellung beziehen (Europäisches Parlament 2020).

3.2.2 Die EU-Datenschutz-Richtlinie 95/46/EG

3.2.2.1 Erste datenschutzpolitische Bestrebungen auf Gemeinschaftsebene[71]

Die ersten Aktivitäten auf Gemeinschaftsebene lassen sich bis in die frühen 1970er-Jahre zurückverfolgen. Vor dem Hintergrund der zunehmenden Verbreitung von Computern und der Zunahme der volkswirtschaftlichen Bedeutung der Datenverarbeitung setzten sich Kommission und Parlament mit der Frage auseinander, wie die EG auf diesem zukunftsträchtigen Wirtschaftsgebiet gemeinsam agieren könnte, um angesichts der drohenden Marktdominanz der Vereinigten Staaten bestehen zu können (Commission of the European Communities 1972). Zum Zwecke der Steigerung der

70 Vgl. auch die Unterabschnitte 3.3.4.3 bzw. 3.3.4.2 zum Thema der Fluggastdatenspeicherung bzw. zur Vorratsdatenspeicherung.

71 Die grundlegende Struktur dieses Abschnittes orientiert sich an der instruktiven Darstellung von Gloria Gonzáles-Fuster (2014), legt allerdings andere Schwerpunkte.

europäischen Wettbewerbsfähigkeit auf diesem Gebiet trat die Kommission schließlich Ende 1973 mit einem Entschließungsvorschlag für eine „gemeinschaftliche Politik auf dem Gebiet der Datenverarbeitung" mittels einer Kommissionskommunikation an den Ministerrat heran (Commission of the European Communities 1973). In diesem wirtschaftspolitisch motivierten Dokument, das sich der Schaffung möglichst günstiger Bedingungen für die weitere Verbreitung von Computern, Datenverarbeitungen, Datenbanken usw. widmete, setzte sich die Kommission in einem Punkt mit der Bedeutung der Frage auseinander, wie der Zugriff auf in zunehmendem Maße international verwaltete Datenbanken, die Informationen über Individuen enthalten, aussehen müsste. Einerseits forderte die Kommission darin die Durchführung öffentlicher Experten-Anhörungen und andererseits wurde vorgeschlagen, „to seek a genuine political consensus on this matter now with a view to establishing common ground rules, than to be obliged to harmonise conflicting national legislation later on." (Commission of the European Communities 1973, 13 Nr. 39) Der Ministerrat unterstützte im Anschluss an die Aufforderung der Kommission zwar die Schaffung einer *gemeinschaftlichen Politik auf dem Gebiet der Datenverarbeitung* und leitete entsprechende dahingehende Schritte im Rahmen einer Ministerratsentschließung vom 14. Juli 1974 ein, doch wurden die von der Kommission ebenfalls aufgeworfenen datenschutzpolitischen Fragen dabei vollständig ignoriert (Ministerrat 1974) und auch nicht anderweitig aufgegriffen (González Fuster 2014, 113).

Vor dem Hintergrund der öffentlich-medialen Debatte um die Zentralisierung von staatlichen Datenbanken in Frankreich[72] brachte der französische Europaparlamentsabgeordnete Pierre Bernard Cousté das Thema im März 1974 zudem im Europäischen Parlament ein und richtete eine mündliche Anfrage an den Ministerrat. Darin nahm Cousté Bezug auf die bereits erfolgte und noch laufende Einrichtung großer Datenbanken in verschiedenen EG-Mitgliedstaaten und erkundigte sich danach, ob der Ministerrat „zum Schutz der Bürger vor Eingriffen in ihre Privatsphäre im Rahmen der gemeinschaftlichen Informationspolitik geeignete Maßnahmen, wie insbesondere strenge gesetzliche Vorschriften über den Zugang zu solchen Informationen, zu treffen [gedenkt]." (Cousté 1974, 21)

Die Antwort auf Cousté kam seitens des amtierenden Präsidenten des Ministerrates, Hans Apel, dem seinerzeitigen von der SPD gestellten parlamentarischen Staatssekretär beim Bundesminister des Auswärtigen. Dieser

72 Das sog. *Projekt S.A.F.A.R.I.* (vgl. González Fuster 2014, 61 ff.).

teilte zunächst die geäußerten Bedenken und das Ziel des Schutzes personenbezogener Daten: „It is true that here we need strict provisions on access to this information, as you rightly say, Mr Cousté, to protect the private life of the individual." (European Communities 1974, 35) Apel stellte aber sodann die Notwendigkeit einer gemeinschaftlichen Politik, wie sie seitens der Kommission als möglicherweise erforderlich dargestellt worden war, infrage, da diese Frage zunächst im Ministerrat zu klären sei: „The prime aim is to protect private life. Whether this is to be achieved at national or Community level is a question of practical feasibility, not a matter for a European discussion of principle. […] Since it is not a matter of ideology, I think it should be quite easy to discuss." (ebd.) Am Ende der Parlamentsdebatte kündigte Cousté schließlich an, dass der Ausschuss für Wirtschaft und Währung des Europäischen Parlaments (ECON-Ausschuss - Committee on Economic and Monetary Affairs) bereits dabei war, einen einschlägigen Bericht zu erarbeiten (ebd., 37). Die Arbeiten an jenem Bericht waren tatsächlich bereits im Vorfeld der Plenardebatte am 13. Februar 1974 mit einem an den Rechtsausschuss (Legal Affairs Committee) gerichteten Brief des Parlamentspräsidenten initiiert worden. Der Parlamentspräsident forderte den Rechtsausschuss darin auf, eine Stellungnahme für den ECON-Ausschuss zu der Mitteilung der Kommission an den Rat über die Politik der Kommission im Bereich der Datenverarbeitung abzugeben (Legal Affairs Committee of the EP und Lord Mansfield 1975, 10).

Der Rechtsausschuss folgte der Aufforderung und überreichte seine Stellungnahme im Mai 1974 an den ECON-Ausschuss (ebd., 14). Vonseiten der Kommission war an dem Prozess der damalige Kommissar für das Ressort Industrie und Handel, Altiero Spinelli, beteiligt. In einem Brief an den Parlamentspräsidenten im März 1974 unterstrich Spinelli, selbst überzeugter Europäer, der Zeit seines Lebens für eine verstärkte Europäische Integration eintrat (Pinder 2007), die Bedeutung der Thematik und dass die „Commission realizes that the communication of data across frontiers will be a European problem likely to require harmonization" (Spinelli, zit. nach González Fuster 2014, 114). Allerdings sah es Spinelli aufgrund der verfassungsrechtlichen Bedeutung des Schutzes personenbezogener Daten als angemessener an, wenn sich das Parlament zunächst insb. in Gestalt öffentlicher Experten-Anhörungen tiefergehend mit der Thematik auseinandersetzt. Im Anhang des Briefes übersandte Spinelli zudem weitergehende Informationen der Kommission zu den Herausforderungen von Datenbanken für den Schutz der Freiheit der Individuen, konkrete Gestaltungsvorschläge für einen mit dem Thema befassten Parlamentsausschuss sowie

Angaben zu wesentlichen Aspekten des Themas, die einer tiefergehenden Untersuchung bzw. politischer Entscheidungen bedürften. Dass es sich bei dem Thema des Schutzes von Individuen im Kontext von Datenbanken um ein brisantes Thema handelte, bestätigte ein weiterer Brief, diesmal seitens des Vize-Präsidenten der Europäischen Kommission. Darin wurde dargelegt, dass, aufgrund des ausgesprochen politischen Charakters des Themas, die Befassung des Parlaments mit der Materie angemessener sei (González Fuster 2014, 114).

Diese Auffassung wurde allerdings auf Seiten des Parlaments nicht vollends geteilt. Dies hatte mehrere Gründe: Zum einen war das Parlament in den 1970er-Jahren eine noch weitgehend machtlose Diskussionsplattform. Ohne eigene Kompetenz hinsichtlich der Unterbreitung von Gesetzesvorschlägen konnte sie gegenüber der Kommission in Form von Parlamentsresolutionen lediglich ihren Wunsch äußern, gesetzgeberisch tätig zu werden, ohne dass die Kommission verpflichtet war, dem Wunsch nachzukommen. Gleichzeitig lag die Entscheidungsmacht in der EG in den 1970er-Jahren noch stärker als heute eindeutig bei den Mitgliedstaaten. Mit der 1974 erfolgten Gründung des Europäischen Rates, die seitens der Supranationalitätsbefürworter kritisiert wurde (Pinder 2007; Wessels 2008, 155 ff.), verfestigte sich diese Macht zudem noch weiter. Entsprechend wurde die Meinung vertreten, dass die Befassung des Parlaments mit der Materie lediglich als Vorbereitung dienen könne, während die *Sammlung von Fakten und Informationen, auf deren Grundlage die Kommission Gemeinschaftsvorschriften vorlegen könne, allerdings eine Aufgabe sei, die allein die Kommission zu erfüllen vermag*[73] (Legal Affairs Committee of the EP und Lord Mansfield 1975, 14). Zum anderen taten sich im Laufe der Auseinandersetzung des Parlaments mit der Materie Schwierigkeiten im Hinblick auf die Zuständigkeit auf. So war die Verwaltung von Datenbanken eine Frage, die in den Verantwortungsbereich der EG-Industriepolitik fiel. Das Interesse an der Befassung mit der Materie des Schutzes von Individuen beim für diesen Bereich zuständigen ECON-Ausschuss hielt sich dagegen in Grenzen, sodass der Ausschuss am 8. Juli 1974 alle weiteren Arbeiten einstellte. Erst als Kommissar Spinelli am 22. Juli 1974 den dahingehenden Wunsch der Kommission, dass das Parlament Stellung zu dem Thema nehme, bekräftigte, sicherte der Rechtsausschuss am 12. September 1974 schließlich die Erarbeitung eines entsprechenden Dokuments unter der Federführung

73 Eigene Übersetzung der entsprechenden Passage.

von Lord Mansfield[74] zu (ebd., 15). Das Verhalten des ECON-Ausschusses lässt sich wohl am ehesten mit dem verinnerlichten Selbstverständnis des Ausschusses erklären, der vielmehr als Vertreter bestimmter Interessen und nicht bloß als neutraler Austragungsort von Interessenkämpfen fungiert.[75] So zählt zum Kern-Themenportfolio des ECON-Ausschusses die Förderung der wirtschaftlichen Integration und des wirtschaftlichen Wachstums in der EU, jedoch nicht der Schutz von Verbraucherinteressen oder von Menschenrechten.[76] Dies darf aber nicht verwundern, da die Gründung der EG zu diesem Zeitpunkt erst sieben Jahre zurücklag und letztlich ohnehin nur deshalb Erfolg hatte, weil nach dem Scheitern weitergehender Integrationsbemühungen der Kompromiss die Fokussierung auf wirtschaftspolitische Kooperation vorsah (vgl. 3.2.1). Während es also nicht verwunderlich ist, dass der ECON-Ausschuss das Thema nicht aus der ihm vorgegebenen Menschenrechtsperspektive aufgegriffen hat, ist es dagegen durchaus verwunderlich, weshalb der Ausschuss das Thema nicht analog zur OECD aus einer wirtschaftspolitischen Perspektive heraus betrachtet hat. Die Antwort auf diese Frage mag darin liegen, dass der ECON-Ausschuss innerhalb seiner kurzen Tätigkeitsspanne (nur wenige Monate) nicht auf das für die Wirtschaftspolitik relevante Problem der grenzüberschreitenden Datenflüsse gestoßen war. Schließlich war selbst die – in ähnlichem Maße stark wirtschaftspolitisch motivierte – OECD, die sich zu diesem Zeitpunkt bereits seit Jahren mit dem Thema beschäftigte, erst im Juni 1974 auf den Themenkomplex grenzüberschreitender Datenflüsse aufmerksam geworden (vgl. 3.1.1).

Ende Februar 1975 wurde der vom Rechtsausschuss ausgearbeitete Vorschlag schließlich vom EP-Plenum in Form der *Entschließung über den Schutz der Rechte des Einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Datenverarbeitung* angenommen. Diese nahm Bezug auf die im Jahr 1973 an den Rat gerichtete Kommissionskommunikation, stellte allerdings zugleich zwei Ziele für

74 Lord Mansfield, mit bürgerlichem Namen William Murray, war zu dieser britischer Parlamentarier und Mitglied der britischen Delegation an das EP (Jackson 1993).

75 So zeigt die Forschung zum Ausschusswesen des Europäischen Parlaments, dass Ausschüsse im Allgemeinen dazu neigen, ihr eigenes Themenportfolio gegenüber den Themenportfolios anderer Ausschüsse zu begünstigen (Kluger Dionigi 2017, 156).

76 Diese Schwierigkeiten sollten später während des politischen Entscheidungsprozesses der DSGVO in Form der Torpedierung starker gesetzlicher Vorgaben in der DSGVO seitens der in erster Linie mit Wirtschaftsthemen beschäftigten Ausschüsse (insb. der ITRE-, aber auch der IMCO-Ausschuss) wiederkehren (vgl. Unterabschnitt 4.3).

eine künftige EG-Richtlinie auf, „nicht nur um sicherzustellen, daß die Bürger der Gemeinschaft einen maximalen Schutz vor Mißbrauch oder Defekten der Datenverarbeitungsverfahren genießen, sondern auch, um das Entstehen einander widerstreitender nationaler Rechtsvorschriften zu verhindern" (Europäisches Parlament 1975, 48 Nr. 1). Trotz der Empfehlung, dass eine Richtlinie *dringend notwendig* sei, bot die Resolution allerdings keine konkreten inhaltlichen Gestaltungsvorschläge für eine solche Richtlinie, sondern war vor allem darum bemüht, die Einsetzung eines Sonderausschusses in die Wege zu leiten, der sich mit dem Themenkomplex auseinandersetzen und Gestaltungsvorschläge erarbeiten sollte (ebd., Nr. 2 & 3). Nachdem die Einsetzung des Sonderausschusses doch nicht mehr erfolgte, beauftragte das Parlamentsplenum im Rahmen einer weiteren Entschließung Anfang April 1976 den Rechtsausschuss[77] mit der weiteren Berichterstattung zu laufenden und einzuleitenden Gemeinschaftsaktivitäten (Europäisches Parlament 1976, 27 Nr. 2). Daneben wurde die Europäische Kommission noch einmal darum ersucht, die Erarbeitung einer Gemeinschaftsregelung zum *Schutz der Rechte der einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Datenverarbeitung* voranzutreiben (ebd., Nr. 1).

Der Rechtsausschuss nominierte im Anschluss den sozialdemokratischen Europaabgeordneten Alfons Bayerl als Berichterstatter. Dieser veranlasste daraufhin die Einsetzung eines Sonderunterausschusses,[78] der sich zwischen Juni 1977 und März 1979 mit dem Themenkomplex auseinandersetzte. Bedeutende Eckpunkte dieser Auseinandersetzung waren eine seitens des Sonderunterausschusses organisierte öffentliche Experten-Anhörung im Jahr 1978, an der neben Kommissionsvertretern auch Beobachter der OECD und des Europarates teilnahmen, sowie die Veröffentlichung des sog. Bayerl-Berichts Mitte 1979, in dem die Ergebnisse des Unterausschusses zusammengetragen wurden (Bayerl 1979).

Der Bayerl-Bericht diente dem EP Mitte 1979 schließlich als Grundlage für die Verabschiedung einer dritten Entschließung (Europäisches Parlament 1979). Gegenüber den vorherigen Resolutionen stellt die 1979er Resolution eine deutliche inhaltliche Entwicklung dar. Erstens wurde darin gesetzgeberisches Handeln nicht mehr nur gefordert, sondern auch konkrete

77 Der Rechtsausschuss sollte dann auch bis zur deutlich später erfolgten Gründung des LIBE-Ausschusses (Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten) für Datenschutzfragen (darunter insbesondere die Verhandlungen zur DS-RL) auf Seiten des EP zuständig bleiben (Karaboga 2018, 151 ff.).

78 Das sog. *Data Processing and Individual Rights Sub-committee* (Bayerl 1979, 2).

Vorschläge hinsichtlich der Gestaltung der geforderten Rechtsvorschriften dargelegt. Zweitens hatte sich die Herangehensweise des Parlaments an das Thema von einer grundrechtsorientierten hin zu einer wirtschaftspolitisch motivierten verschoben. So wurde die Erforderlichkeit der in der Resolution geforderten Maßnahmen damit begründet, dass „eine harmonische Entwicklung der Wirtschaftstätigkeit im Rahmen des Gemeinsamen Marktes die Verwirklichung eines echten gemeinsamen Datenverarbeitungsmarktes voraussetzt, innerhalb dessen der freie Warenverkehr und der freie Dienstleistungsverkehr sichergestellt und der Wettbewerb nicht verzerrt ist" (ebd., 35 Nr. 1) und dass sich die Verabschiedung divergierender einzelstaatlicher Vorschriften „unmittelbar auf die Errichtung und das Funktionieren des Gemeinsamen Marktes auswirken" (ebd., 35 Nr. 2). Viele der Punkte, die in der Entschließung genannte wurden, sollten später Teil der DS-RL werden.

Noch im Begründungsteil wurde zum Zwecke der Überwachung der Anwendung der gewünschten Regelungen die Gründung eines Ausschusses von Vertretern der nationalen Organe der Mitgliedstaaten, also eine Art Datenschutzaufsichtsbehörde auf Gemeinschaftsebene vergleichbar der späteren Art. 29-Datenschutzgruppe bzw. dem heutigen Europäischen Datenschutzausschuss (EDSA) (ebd., S. 36 Nr. 13) – allerdings unter dem Vorsitz eines Parlamentsvertreters – vorgeschlagen (ebd., Nr. 14). Entsprechend wurde in der eigentlichen Entschließung dann auch die Einrichtung unabhängiger Aufsichtsbehörden zur Überwachung der Anwendung der vorgeschlagenen Regelungen auf mitgliedstaatlicher Ebene empfohlen (ebd., 37 Nr. 10–12).

Als Anwendungsbereich wurde sowohl die manuelle als auch die automatisierte Verarbeitung personenbezogener Daten vorgesehen sowie die Verarbeitung (ebd., 37 Nr. 1) und auch die Zusammenführung von Datenbanken (Nr. 6 und 7) einer vorgelagerten, generellen Melde- und Genehmigungspflicht unterlegt. Daneben betonte die Entschließung die Grundsätze der rechtmäßigen Erhebung personenbezogener Daten, der Zweckbindung (inkl. der Betonung der Notwendigkeit zur Einholung einer Einwilligung bei der Erhebung sensibler personenbezogener Daten), der Datenminimierung und -richtigkeit sowie Speicherbegrenzung (ebd., 37 Nr. 2). Regelugen zur Haftung (für materielle sowie immaterielle Schäden) (Nr. 3), zu Sanktionen (Nr. 16), zu den Informationspflichten des Verantwortlichen gegenüber dem Betroffenen (Nr. 4), zu Betroffenenrechten (Transparenz, Löschung, Berichtigung), sofern die Betroffenen ihren gewöhnlichen Aufenthalt im Hoheitsgebiet eines Mitgliedstaates haben (Nr. 8), inklusive der Garantie, diese Rechte *innerhalb einer angemessenen Frist und ohne Gebüh-*

ren und Kosten wahrnehmen zu können (Nr. 9), wurden ebenfalls vorgesehen. Interessanterweise sah der Vorschlag auch vor, dass die genannten Grundsätze sowohl für den Schutz von personenbezogenen Daten gelten sollten als auch für den Schutz von gruppenbezogenen Daten und für die Rechte von Gruppen (Nr. 17).

Für grenzüberschreitende Datenübertragungen innerhalb der Gemeinschaft (Nr. 13) wurde eine Meldepflicht und für Übertragungen in Drittstaaten (Nr. 14) eine Genehmigungspflicht seitens der Datenschutzaufsichtsbehörde auf Gemeinschaftsebene gefordert. Zudem drückte das Parlament seine Unterstützung für die Aktivitäten des Europarats aus und forderte die Kommission auf, zu überprüfen, ob die EG als solche (und nicht jeder Mitgliedstaat für sich) der künftigen Datenschutz-Konvention des Europarats beitreten könnte (EG Nr. 15).

In der Zwischenzeit hatte die Kommission auf die EP-Resolution aus dem Jahr 1976 hin, in der die Kommission erneut zur Erarbeitung einer Gemeinschaftsregelung zum Schutz der Rechte der Einzelnen aufgefordert worden war, einen Austausch mit Ministerratsvertretern zur Eruierung von Harmonisierungsmöglichkeiten initiiert (Commission of the European Communities 1976, 8 Nr. 2.4.4). Zugleich signalisierte die Kommission ihre Unterstützung für die in der Europaratsempfehlung (74) 29 vorgeschlagenen Prinzipien, die bereits seitens einzelner Mitgliedstaaten in nationales Recht umgesetzt worden waren (Commission of the European Communities 1976, 8 Nr. 2.4.4). Im April 1977 verabschiedeten Parlament, Rat und Kommission zudem eine gemeinsame Erklärung, in der sich alle drei Organe zur Wahrung der Grundrechte „wie sie insbesondere aus den Verfassungen der Mitgliedstaaten sowie aus der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten hervorgehen" (EG 1977) verpflichteten.

Zum Zwecke der verbesserten Entscheidungsfindung hinsichtlich der Erarbeitung einer EG-Richtlinie unterbreitete die Kommission dem Ministerrat schließlich einen Vorschlag zur Ausarbeitung einer Studie, in der „die wichtigsten Probleme der Harmonisierung der in der Gemeinschaft geltenden Rechtsvorschriften über den Schutz der Privatsphäre und die Ausarbeitung von Anwendungskodexen sowie entsprechenden Normen" (Ministerrat 1977, 26) untersucht werden sollten. In dieser vom Ministerrat im September 1977 (ebd.) genehmigten und zwischen 1978 und 1979 erstellten Studie (Commission of the European Communities 1982, 7) wurde festgestellt, dass trotz der Bestrebungen der Mitgliedstaaten, Divergenzen zu vermeiden, weiterhin mehrere Mitgliedstaaten gar keine Datenschutzrege-

lungen verabschiedet hatten. Während in Italien und Irland noch keinerlei gesetzgeberische Aktivitäten auf dem Gebiet des Datenschutzes festgestellt wurden, hatten Belgien, das Vereinigte Königreich und die Niederlande immerhin bereits Gesetzesvorschläge oder vorbereitende, einschlägige Studien eingebracht bzw. in Bearbeitung (González Fuster 2014, 118). Während einer parlamentarischen Fragerunde Ende 1979 unterrichtete der konservative Vizepräsident der Europäischen Kommission, Lorenzo Natali, schließlich das Parlament darüber, dass sich die Kommission der Notwendigkeit internationaler Regeln für den Schutz personenbezogener Daten zwar vollkommen bewusst sei, jedoch den Ausgang der Europaratsaktivitäten abzuwarten bevorzuge (ebd., 120).

Als die Datenschutz-Konvention 108 des Europarats schließlich Anfang 1981 verabschiedet wurde, teilte die Kommission Mitte 1981 in Form einer Empfehlung mit, dass sie die Konvention für ein geeignetes Instrument zur Herbeiführung eines einheitlichen Datenschutzniveaus auf europäischer Ebene halte und empfahl allen Mitgliedstaaten die Unterzeichnung der Konvention noch im laufenden Jahr und ihre Ratifikation vor Ende 1982. Für den Fall, dass die Mitgliedstaten die Konvention nicht binnen einer angemessenen Zeitspanne unterzeichnen und ratifizieren würden, behielt sich die Kommission zudem vor, einen eigenen Rechtsakt gemäß EWG-Vertrag vorzuschlagen (Europäische Kommission 1981). In der Folge finanzierte die Kommission weitere Studien zur Untersuchung der Entwicklungen auf dem Gebiet der Verarbeitung und des rechtlichen Schutzes personenbezogener Daten. Auf Grundlage der 1979er Studie verständigten sich die Kommission und der Ausschuss einzelstaatlicher Sachverständiger der Kommission auf die Fokussierung auf die folgenden sechs Unterthemen: (1) die Qualität und Quantität grenzüberschreitender Datenflüsse; (2) den organisatorischen Charakter und das technische Funktionieren von Datenschutzbehörden; (3) die Probleme hinsichtlich der Rechtspersönlichkeit (natürliche und juristische Personen); (4) die internationalen wirtschaftlichen Aspekte der Datensicherheit und Vertraulichkeit; (5) die technischen Aspekte des Rechts auf Zugang zu Datenbanken; sowie (6) die Kontrolle, Prüfung und Umsetzung der Anforderungen an die Vertraulichkeit und deren Umsetzung im Bereich der Datensicherheit (Commission of the European Communities 1982, 7 Nr. 1.2.2.). Das daraus resultierende Arbeitsprogramm, das 1981 initiiert wurde, hatte wiederum zum Ziel, die *Anforderungen an die Harmonisierung der Rechtsvorschriften sowie Empfehlungen und Normen zur Vertraulichkeit von Daten* zu prüfen und widmete sich der Untersuchung von:

- Datenschutz im Hinblick auf die neuen Informations- und Kommunikationstechnologien;
- Technologien für den Datenschutz und die Datensicherheit;
- personenbezogenen Daten und automatischen Entscheidungsprozessen;
- den Auswirkungen internationaler Datenschutzbestimmungen auf die Wirtschaftsbereiche, die am stärksten von der Informationsverarbeitung betroffen sind;
- Systemdesign und Datenschutz;
- freiem Zugang zu Informationen und Datenschutz;
- sowie von Datenbanken, verteilten Systemen und Datenschutz (Commission of the European Communities 1982, 29 f.)

Der an alle EG-Mitgliedstaaten gerichteten Kommissionsempfehlung, die Datenschutz-Konvention noch vor Ende 1981 zu unterzeichnen, kamen schließlich lediglich fünf der zehn EG-Mitgliedstaaten nach.[79] Das Europäische Parlament, das bereits seit 1975 für harmonisierte Gemeinschaftsregelungen zum Datenschutz eingetreten war und seitens Rat und Kommission mit dem Verweis auf intergouvernementale Harmonisierungbestrebungen insb. des Europarats vertröstet worden war, nahm die Verabschiedung der Konvention und die zögerliche Unterzeichnung bzw. Ratifikation dieser zum Anlass für eine weitere Resolution im März 1982. Trotz der Begrüßung der Verabschiedung der Datenschutz-Konvention des Europarats (Europäisches Parlament 1982, 40 Nr. 1) äußerte das Parlament seine Bedenken im Hinblick darauf, „daß nicht abzusehen ist, wann schließlich alle Mitgliedstaaten der Gemeinschaft dieses Europäische Übereinkommen unterzeichnet und ratifiziert haben werden" (ebd., Nr. 2) und drückte sein Bedauern darüber aus, dass die EG-Mitgliedstaaten der Kommissionsempfehlung nur teilweise nachgekommen waren (ebd., Nr. 13). Entsprechend bekräftigte das Parlament seine bereits 1979 geäußerte Meinung, dass die EG als solche der Datenschutz-Konvention beitreten sollte (Nr. 16). Mehr aber noch vertrat das Parlament – nunmehr auch unter Verweis auf Art. 100 des EWG-Vertrags, also im Hinblick auf die Errichtung oder das Funktionieren des Gemeinsamen Marktes[80] – die Position, dass der Erlass einer EG-Richtlinie

79 Diese waren: Dänemark, Deutschland, Frankreich, Luxemburg sowie das Vereinigte Königreich. Zu diesem Zeitpunkt noch nicht unterzeichnet wurde die Konvention dagegen von: Belgien, Italien, Irland, Griechenland und den Niederlanden (Council of Europe 2019).

80 „Der Rat erläßt einstimmig auf Vorschlag der Kommission und nach Anhörung des Europäischen Parlaments und des Wirtschafts- und Sozialausschusses Richtlinien für

trotz des Bestehens der Datenschutz-Konvention weiterhin nötig und erwägenswert sei (Nr. 3, 17). Als Eckpunkte einer künftigen Regelung wurden die Gleichbehandlung des öffentlichen und nicht-öffentlichen Bereichs, Zugangs- und Berichtigungsrechte, Regelungen zur Haftung sowie die Unterstellung des Betriebs von Datenbanken einer vorherigen Anmelde- und Genehmigungspflicht genannt (Nr. 17).

Allerdings hatte auch diese vierte Resolution des EP keine weiteren Auswirkungen auf die Datenschutzpolitik der EG. Kommission und Rat hielten daran fest, abzuwarten, inwieweit eine Harmonisierung mittels der Datenschutz-Konvention erreicht werden könne (Simitis 1995). Die Aktivitäten der EG auf dem Gebiet des Datenschutzes beschränkten sich in den Folgejahren auf die Erarbeitung von wissenschaftlichen Studien im Kontext der gemeinschaftlichen Politik auf dem Gebiet der Datenverarbeitung (González Fuster 2014, 121 f.). So genehmigte der Ministerrat zunächst im April 1984 die Ausschreibung weiterer Studien, u. a. mit dem für eine mögliche Harmonisierungspolitik relevanten Ziel der „Prüfung der in den Mitgliedstaaten geltenden oder in Ausarbeitung befindlichen Rechtsvorschriften und Erörterung der Angleichungsmöglichkeiten sowie der Instrumente, die auf Gemeinschaftsebene eingesetzt werden könnten" (Ministerrat 1984a, 31, Nr. 1.3.4). Aufgrund einer Ministerratsentschließung vom Juli 1984, in der die Gemeinschaftspolitik auf dem Gebiet der Datenverarbeitung dahingehend aktualisiert wurde, „mittelfristig ein systematisches Programm der Gemeinschaft zur Förderung der Forschung, industriellen Entwicklung und Anwendung der Datenverarbeitung aufzustellen" (Ministerrat 1984b, 49), wurde der Fokus der zu fördernden Studien allerdings erheblich verändert. Als alleiniges Ziel im Bereich des Datenschutzes wurde die „Fortsetzung der Untersuchungen über Datensicherung und Daten- und Softwareschutz, um die Entwicklung praktischer Werkzeuge für die Verwender zu fördern" (Ministerrat 1984b, 52, Nr. 1.3.3), festgelegt. In der folgenden Ausschreibung der Kommission ging es dann auch nicht mehr um die Arbeit an gemeinschaftsrechtlichen Grundlagen, sondern stattdessen vor allem um die Förderung praxisorientierter Projekte zum technischen (Selbst-)Datenschutz.[81]

---

die Angleichung derjenigen Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, die sich unmittelbar auf die Errichtung oder das Funktionieren des Gemeinsamen Marktes auswirken." (Europäische Gemeinschaften 1957, Artikel 100)

81 Lediglich im Bereich „Erfordernisse der Benutzer hinsichtlich der künftigen Gesetzgebung zu Fragen der Sicherheit und der Vertraulichkeit von Daten" fand sich auch

3.2.2.2 Parlament als Befürworter und Kommission als Bremserin von Gemeinschaftsregelungen?

Spiros Simitis, der an mehreren Stellen[82] in die politischen Beratungs- und Entscheidungsprozesse der damaligen Zeit involviert gewesen ist, lässt keinen Zweifel daran, dass die Kommission – aufgrund ihrer wirtschaftspolitischen Motivation – zu keinem Zeitpunkt tatsächliches Interesse an einer Harmonisierung von Datenschutzregelungen hatte. Simitis zufolge lässt sich der datenschutzpolitische Hauptkonflikt der 1970er und 1980er-Jahre dahingehend zusammenfassen, ob Datenschutzregelungen im Sinne des Schutzes fundamentaler Menschenrechte verstanden oder als wirtschaftspolitische Maßnahme aufgefasst wurden. Ein menschenrechtlich orientierter Regulierungsansatz – wie er seitens des EP verfolgte worden war – hätte daher notwendigerweise all jene Übertragungen personenbezogener Daten effektiv beschränken müssen, bei denen kein ausreichendes Schutzniveau vorhanden gewesen wäre. Die Kommission, und insbesondere die Binnenmarkt-Generaldirektion, habe daher, aufgrund ihrer Gebundenheit an die Gemeinschaftsverträge,[83] Datenschutz notwendigerweise einzig im Kontext der Wirtschaftspolitik bzw. insbesondere im Kontext der gemeinschaftlichen Politik auf dem Gebiet der Datenverarbeitung betrachten können. Diesem Verständnis gemäß waren personenbezogene Daten ein handelbares wirtschaftliches Gut wie jedes andere Gut auch – ohne besondere Schutzerfordernisse. Daher erschienen aus einer solchen wirtschaftspolitischen Perspektive heraus auch jegliche Datenschutzgesetze zunächst als Hindernisse beim Aufbau eines gemeinsamen, also grenzüberschreitenden europäischen Informations- bzw. Datenmarktes, da sie den grenzüberschreitenden Transfer personenbezogener Daten in Staaten ohne Datenschutzgesetze oder mit nur unzureichenden Datenschutzgesetzen er-

---

das Ziel „die Meinungen der Benutzer sowohl bezüglich der anzuwendenden Prinzipien als auch bezüglich der Verfahrensregeln, die in die künftige Gesetzgebung eingehen müßten, zusammenzustellen." (Europäische Kommission 1985, 4, Nr. 3.3.2)

82 Vor allem zu nennen sind hier: Datenschutzbeauftragter des Landes Hessen zwischen 1975 und 1991, Vorsitzender des Datenschutz-Experten-Komitees des Europarats zwischen 1982 und 1986, Berater der Europäischen Kommission in Datenschutzfragen seit 1988 bis ca. zur Jahrtausendwende, Berater des International Labour Office zur Erarbeitung von Beschäftigtendatenschutzregeln zwischen 1991 und 1994 (Simitis 2001, 99).

83 Gemäß EWG-Vertrag waren die Ziele der Gemeinschaft, die Gewährleistung des freien Warenverkehrs (Art. 9), die Freizügigkeit von Arbeitnehmern (Art. 48), von Dienstleistungen (Art. 59) sowie von Kapital (Art. 67).

schwert oder verhindert hätten. Dem seitens der Kommission verfolgten wirtschaftspolitischen Ansatz gemäß dienten Datenschutzregelungen somit allenfalls – und damit ganz im Gegenteil zum Parlamentsverständnis – dazu, einen möglichst ungehinderten Austausch von Informationen zu gewährleisten. Simitis zufolge war selbst die Unterstützung der Datenschutz-Konvention seitens der Kommission der Existenz von Art. 12 Abs. 2 der Datenschutz-Konvention geschuldet, mit dem die Blockierung von grenzüberschreitenden Datenflüssen auf Grundlage von Datenschutzgesetzen verhindert werden sollte (Simitis 1995, 446, 2001, 101; Simitis u. a. 2019, 193, Rn. 133).

Andere Autoren benennen hingegen die Anerkennung des Europarats als entscheidenden Faktor für die Zurückhaltung der Kommission. So hatte die Kommission ohnehin angekündigt, dass sie ein EG-Datenschutzinstrument vorschlagen würde, sofern die Mitgliedstaaten nicht von selbst der Konvention beitreten und harmonisierte Datenschutzgesetze erlassen. Dass die Kommission aber zunächst auf die Konvention setzte sei vor allem darauf zurückzuführen, dass der Europarat über mehr Mitglieder verfügte und die potentielle Harmonisierungswirkung einer Europaratskonvention größer sein könnte als die der EG (Burkert 1988, 756; Schmahl und Breuer 2017, 711).

Newman weist zudem darauf hin, dass bei der Kommission über lange Zeit das – seit der Verbreitung von Computern überholte – Verständnis vorherrschend gewesen sei, wonach die Verarbeitung personenbezogener Daten in erster Linie eine den öffentlichen Sektor betreffende Frage wäre, die folglich am besten auf mitgliedstaatlicher Ebene zu lösen sei, da die Gemeinschaft bei Fragen, die den öffentlichen Sektor betreffen, schlicht keine Kompetenz inne hatte (A. L. Newman 2008a, 110 f.).

Neben der Kommission opponierten aber auch die EG-Mitgliedstaaten gegen die Erarbeitung supranationaler Datenschutzregeln. Die drei großen Mitgliedstaaten Deutschland, Frankreich und insbesondere Großbritannien waren bis zuletzt Gegner jeglicher supranationalen Aktivität auf dem Gebiet des Datenschutzrechts (A. Newman 2007a, 131 f.). Ebenso wandten sich Vertreter der europäischen Wirtschaft klar gegen die Einführung einer gemeinschaftsweiten Harmonisierung der Datenschutzregelungen. Britische Unternehmen gingen – unter Verweis auf für die Wettbewerbsfähigkeit drohende, negative Konsequenzen – am intensivsten gegen europäische Regelungen vor. Aber auch deutsche Unternehmen, die aufgrund des in der Bundesrepublik herrschenden hohen Datenschutzniveaus am ehesten für die Unterstützung der Anhebung des Schutzniveaus in anderen

Ländern in Frage kamen, stellten sich gegen Harmonisierungsbestrebungen (Computerwoche 1990; A. L. Newman 2008a, 111 f.).

3.2.2.3 Der Meinungswandel der Europäischen Kommission

Mit der Veröffentlichung mehrerer Vorschläge im Hinblick auf den Schutz personenbezogener Daten im September 1990 wurde deutlich, dass sich die Haltung der Kommission schlagartig geändert hatte. Doch was waren die ausschlaggebenden Gründe für diesen bedeutungsschweren Meinungswandel, in dessen Folge die EU bis heute zur weltweiten Vorreiterin in Datenschutzfragen werden sollte?

Laut aktuellem Stand der Forschung zu den Gründen für die Erarbeitung der DS-RL waren vor dem Hintergrund der massiven Zunahme grenzüberschreitender Datenübertragungen am Ende der 1980er-Jahre vor allem zwei miteinander zusammenhängende und sich gegenseitig verstärkende Faktoren entscheidend. Die von dieser Zunahme am stärksten betroffenen Bereiche waren: Personalabteilungen; Banken, Versicherungen, Kreditkartenunternehmen und Kreditbüros; Direktmarketing; Fluggesellschaften, Reisebüros und andere am Tourismus beteiligte Unternehmen; Unternehmen, die Waren an internationale Kunden liefern oder anderweitig mit internationalen Kunden handeln wollen; und innerhalb der öffentlichen Verwaltung: Polizei, Zoll, Steuerbehörden und öffentliche Rentenversicherungsträger (Ellger 1990, 108–29).

Erstens war das Auftreten der Datenschutzaufsichtsbehörden als politischer Akteurinnen und Lobbyistinnen von entscheidender Bedeutung. Waren die Aufsichtsbehörden ursprünglich mit dem Ziel gegründet worden, einerseits die Einhaltung der Datenschutzregelungen bei den jeweiligen Verarbeitungen zu überwachen und andererseits Beratungsfunktionen im Hinblick auf den Umgang mit den oftmals auch für die Verantwortlichen selbst neuen Verarbeitungssystemen zu übernehmen, verschob sich ihre Rolle im Laufe der Zeit zunehmend hin zur Politikberatung. So kam mit steigender Erfahrung im Laufe der 1970er- und 1980er-Jahre zu der Überwachungs- und Beratungsrolle die kritische Hinterfragung bestehender gesetzlicher Regelungen und die proaktive Skizzierung von Fortentwicklungsmöglichkeiten des Datenschutzrechts hinzu (A. Newman 2007a, 132; Simitis 2001, 135 f.). Die auf die entsprechenden Aufsichtsbehörden-Positionen berufenen Individuen entstammten wiederum der epistemischen

Community Datenschutzregelungen befürwortender Privatheitsexperten, waren also überzeugungsgetriebene Akteure (A. Newman 2007a, 132).[84]

Als sich die Befürchtungen, dass Unternehmen ihre Datenverarbeitungen in jene Staaten ohne Datenschutzgesetze auslagern würden, seit Ende der 1970er-Jahre zunehmend bewahrheiteten, initiierten die nationalen Aufsichtsbehörden zunächst Formate zur internationalen Kooperation.[85] In der Folge kooperierten Vertreter der nationalen Aufsichtsbehörden im Rahmen von internationalen Arbeitsgruppen zu Themen wie Binnenmarkt- oder Telekommunikationspolitik und brachten abgestimmte Politikvorschläge in ihren jeweiligen Heimatländern ein. Im Vordergrund stand dabei die Befürwortung supranationaler Regelungen, um das EG-weit stark divergierende Datenschutzniveau zu vereinheitlichen und auf diese Weise die sog. Daten-Oasen trocken zu legen (A. L. Newman 2008a, 113). Schließlich war im Laufe der 1980er immer klarer geworden, dass die von der Kommission gewünschte und vom Parlament bezweifelte Harmonisierungswirkung der Datenschutz-Konvention, trotz aller Appelle an die EG-Mitgliedstaaten, nicht eintreten würde. Selbst im Jahr 1990 existierten in fünf[86] von zwölf EG-Mitgliedstaaten noch immer keine Datenschutzgesetze (Vgl. die Übersicht in Tabelle 3-1).

Als die Mitgliedstaaten und die Kommission trotz der anhaltenden offenkundigen Probleme weiterhin tatenlos blieben, begannen die Aufsichtsbehörden schließlich, Gebrauch von ihren neu erlangten Befugnissen zu machen, um den Datentransfer in Länder ohne Datenschutzgesetze zu stoppen. So verhinderte z. B. bereits die schwedische Datenschutzaufsichtsbehörde, das *Data Inspection Board*, im Jahre 1980 die Übertragung von Gesundheitsdaten über die schwedische Bevölkerung zum Zwecke der Herstellung von Gesundheitskarten aus Plastik in das Vereinigte Königreich, da dieses zu dem Zeitpunkt noch über keine Datenschutzregelungen verfügte (Bignami 2005, 844). Deutlich mehr Aufmerksamkeit erhielt hingegen die Entscheidung der französischen CNIL im Juli 1989, den

84 Entgegen etwa jenen primär im Dienste ihrer jeweiligen Regierungen stehenden Individuen, die in den beratenden Ausschuss berufen wurden, der im Zuge der Unterzeichnung der Datenschutz-Konvention des Europarats gegründet worden war (Simitis u. a. 2019, 187 f., Rn. 110).

85 Die erste der seither jährlich stattfindenden „Internationalen Konferenz der Datenschutzbeauftragten" fand 1979 in Bonn statt (ICDPPC 2017).

86 Belgien, Griechenland, Italien, Portugal und Spanien. Das Scheitern der Datenschutz-Konvention wurde besonders gut am Beispiel Spaniens deutlich: Trotz der Unterzeichnung der Konvention im Jahr 1982 sowie ihrer Ratifizierung im Jahr 1984 verfügte das Land 1990 noch immer über kein Datenschutzgesetz.

EG-Mitglieder (Stand: 1990)	DS-Gesetze vorhanden (Stand 1990)	Datenschutz-Konvention …		
		… unterzeichnet	… ratifiziert	… als Gesetz in Kraft getreten
Belgien	Nein	07.05.1982	28.05.1993	01.09.1993
BRD	Ja	28.01.1981	19.06.1985	01.10.1985
Dänemark	Ja	28.01.1981	23.10.1989	01.02.1990
Frankreich	Ja	28.01.1981	24.03.1983	01.10.1985
Griechenland	Nein	17.02.1983	11.08.1995	01.12.1995
Irland	Ja	18.12.1986	25.04.1990	01.08.1990
Italien	Nein	02.02.1983	29.03.1997	01.07.1997
Luxemburg	Ja	28.01.1981	10.02.1988	01.06.1988
Niederlande	Ja	21.01.1993	24.08.1993	01.12.1993
Portugal	Nein	14.05.1981	02.09.1993	01.01.1994
Spanien	Nein	28.01.1982	31.01.1984	01.10.1985
Verein. Kön.	Ja	14.05.1981	26.08.1987	01.12.1987
Neue EG-Mitglieder (seit 1.1. 1995)	**DS-Gesetze vorhanden (Stand 1990)**	**Datenschutz-Konvention …**		
		… unterzeichnet	**… ratifiziert**	**… als Gesetz in Kraft getreten**
Finnland	Nein	10.04.1991	02.12.1991	01.04.1992
Österreich	Ja	28.01.1981	30.03.1988	01.07.1988
Schweden	Ja	28.01.1981	29.09.1982	01.10.1985

Tabelle 3-1: Datenschutzgesetze und Umsetzung der der Datenschutz-Konvention in den EG-Mitgliedstaaten und Beitrittskandidaten im Jahr 1990 (eigene Zusammenstellung)

Datentransfer von Beschäftigtendaten der französischen Fiat-Tochter an das italienische Mutterunternehmen zu stoppen, weil Italien zu diesem Zeitpunkt noch immer über keine Datenschutzregelungen verfügte. Der Transfer durfte nach mehreren Wochen des Haderns letzten Endes erst dann stattfinden, als beide Fiat-Stellen einen Vertrag unterzeichnet hatten, in dem sie sich zur Einhaltung der französischen Datenschutzregelungen verpflichteten (Schwartz 1994, 491 f.). Zudem modifizierte das Netzwerk der Aufsichtsbehörden gegen Ende der 1980er-Jahre auch die Rahmung des Themas: Waren zuvor vor allem menschenrechtliche Erwägungsgründe in den Vordergrund gestellt worden, bemühte man sich fortan, die Existenz von Datenschutzregeln als eine Vorbedingung für die erfolgreiche administrative und Binnenmarktintegration in der Europäischen Gemeinschaft zu definieren (A. L. Newman 2008a, 113). So etwa in der Resolution der inter-

nationalen Konferenz der Datenschutzbeauftragten des Jahres 1989, in der die Kommission und Mitgliedstaaten zu supranationalem Handeln aufgefordert wurden (ICDPPC 1989). Angesichts der anhaltenden Untätigkeit von Kommission und Mitgliedstaaten drohten die Datenschutzbeauftragten bei einem weiteren Zusammentreffen im März 1990 schließlich damit, grenzüberschreitende Datentransfers in die fünf EG-Mitgliedsstaaten ohne Datenschutzgesetze vollständig zu unterbinden, sollten bis zur Vollendung des Binnenmarktes im Jahre 1992 keine gemeinschaftlichen und gleichwertigen Datenschutzstandards existieren. Der einige Monate zuvor gestoppte Datentransfer zwischen der französischen Fiat-Zweigstelle und dem italienischen Mutterkonzern – neben weiteren, vergleichbaren Transfer-Verboten – demonstrierte, dass die Behörden ihren Worten auch Taten folgen lassen würden (A. L. Newman 2008a, 114 f.).

Zweitens fanden, zusammenhängend mit dem ersten Grund, vertragsrechtliche Verschiebungen auf oberster EG-Ebene statt, die auch für den Datenschutz folgenreich sein sollten. Bereits seit den 1970er-Jahren wurde die intergouvernementale Kooperation im, zur damaligen Zeit noch nicht vergemeinschafteten Bereich Justiz und Inneres vorangetrieben (González Fuster 2014, 122 f.). Das wichtigste Ergebnis dieser Kooperation der Mitgliedstaaten war die Unterzeichnung der *Schengener Abkommen zur Abschaffung der stationären Grenzkontrollen* und weiterer Folgeabkommen zwischen den EG-Mitgliedstaaten[87] seit Mitte 1985. Zum Zwecke der darin angestrebten Abschaffung der Binnengrenzen wurden Ausgleichsmaßnahmen vorgesehen, mit denen die innere Sicherheit trotz offener Binnengrenzen gewährleistet werden sollte. Das zentrale Element dieser Sicherheitsmaßnahmen war der Aufbau des Schengener Informationssystems (SIS), mit dem die grenzüberschreitende Kooperation der fünf Vertragsstaaten hinsichtlich der automatisierten Personen- und Sachfahndung im Rahmen eines vernetzten Datenbestandes eingerichtet wurde. Im Kontext der Errichtung dieses für damalige Verhältnisse gigantischen Datenverarbeitungssystems wurde Datenschutzfragen allerdings zunächst keine Beachtung geschenkt. Besonders problematisch war, dass mit Belgien ein Staat am SIS teilnehmen sollte, der noch immer keinerlei Datenschutzgesetze verabschiedet hatte. Da die luxemburgische Datenschutzaufsichtsbehörde alleine nur wenig Handlungsmacht innehatte, setzte sie die Vertreter der

87 Zunächst zwischen der Bundesrepublik und Frankreich, gefolgt von Belgien, Luxemburg und den Niederlanden.

französischen und deutschen Aufsichtsbehörden auf der internationalen Konferenz der Datenschutzbeauftragten des Jahres 1988 schließlich über die Datenschutzgefahren des SIS im Zusammenhang mit der vertraglichen Einbindung Belgiens in Kenntnis. Gemeinsam traten die französischen, deutschen und luxemburgischen Vertreter in der Folge an die für das SIS zuständigen Stellen heran und teilten diesen mit, dass das SIS in seiner vorgesehenen Form gegen geltendes nationales Datenschutzrecht verstoße. Die Verhandlungen gerieten daraufhin ins Stocken, bis einige, am – verglichen mit den geltenden Datenschutzregelungen jener Staaten – niedrigen Schutzlevel der Datenschutz-Konvention des Europarats orientierte, Datenschutzvorkehrungen implementiert wurden.[88] Belgien musste sich zudem verpflichten, schnellstmöglich Datenschutzgesetze zu erlassen und eine Aufsichtsinstanz über das SIS ins Leben zu rufen (A. L. Newman 2008a, 115; Simitis 1995, 453).

Neben der intergouvernementalen Kooperation im Kontext der Schengener Abkommen intensivierte sich auch die Europäische Integration auf Gemeinschaftsebene seit Mitte der 1980er-Jahre. Mit der Unterzeichnung der Einheitlichen Europäischen Akte (EEA) Anfang 1986 wurde ein Prozess der verstärkten Europäischen Integration eingeleitet, der seinen Höhepunkt in der Unterzeichnung des Maastrichter Vertrags Anfang 1992 fand und die Europäische Gemeinschaft von einer Wirtschaftsunion hin zu einer politischen Union transformierte.[89] Das Ziel eines gemeinsamen Binnenmarktes wurde somit um die Abschaffung der Binnengrenzen, den Aufbau einer Wirtschafts- und Währungsunion, die Anerkennung der Unionsbürgerschaft, die Förderung einer gemeinsamen Außen- und Sicherheitspolitik sowie die Entwicklung einer engen Zusammenarbeit in den Bereichen Justiz und Inneres erweitert (Europäische Gemeinschaften 1992, Titel I, Art. B). Die vorherigen Verpflichtungen hinsichtlich der Gewährleistung des

88 Wie Simitis berichtet, sei das Fehlen jeglicher Datenschutzvorkehrungen damit gerechtfertigt worden, dass die Autoren diese schlicht vergessen hätten (Simitis 1995, 453).

89 So äußerten die Vertragsstaaten im Rahmen der EEA erstmals ihre Entschlossenheit, „gemeinsam für die Demokratie einzutreten, wobei sie sich auf die in den Verfassungen und Gesetzen der Mitgliedstaaten, in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und der Europäischen Sozialcharta anerkannten Grundrechte, insbesondere Freiheit, Gleichheit und soziale Gerechtigkeit, stützen“ (Europäische Gemeinschaften 1987, 2). In den vorangegangenen Verträgen äußerten sich die Vertragsstaaten tatsächlich an keiner Stelle zum Thema der Grundrechte.

freien Warenverkehrs, der Freizügigkeit von Arbeitnehmern, von Dienstleistungen sowie von Kapital galten somit zwar immer noch, doch die neuerliche, ausdrückliche Verpflichtung der Gemeinschaft, die Grundrechte ihrer Bürgerinnen und Bürger zu achten, trat fortan in gleichwertiger Weise neben diese.[90] Diese Verschiebung fand zudem vor dem Hintergrund der anhaltend rasanten technologischen Entwicklungen auf dem Gebiet der Datenverarbeitung und den daraus resultierenden individuellen und gesellschaftlichen Gefährdungen statt (Simitis 2001, 104). Wohin diese Entwicklungen führen könnten, falls keine angemessenen Gegenmaßnahmen getroffen würden, hatte das deutsche Bundesverfassungsgericht in seinem Volkszählungsurteil aus dem Jahre 1983 bereits unmissverständlich klargestellt:

> *„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist." (BVerfG 1983 C II 1 a))*

Schließlich ging auch die Kommission dazu über, die vom Europäischen Parlament seit mehr als einem Jahrzehnt und von Datenschutzexperten seit dem ersten hessischen Datenschutzgesetz vertretene Position zu übernehmen, dass die Förderung der EG-weiten wirtschaftlichen Kooperation und der Schutz von Grundrechten nicht als Widerspruch, sondern als zwei Seiten einer Medaille anzusehen seien (Simitis 1995, 447 f.). Daneben setzte selbst der Europäische Rat auf seinem Straßburger Treffen Ende 1989 im Hinblick auf die Verwirklichung der EEA und angesiedelt unter dem Punkt „Freizügigkeit und Europa der Bürger" erstmals die Zielmarke, dass bei der

90 „Die Union achtet die Grundrechte, wie sie in der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben." (Europäische Gemeinschaften 1992, Titel I, Artikel F (2))

intergouvernementalen „Zusammenarbeit zwischen den Verwaltungen der Persönlichkeitsschutz bei der Benutzung von Datenbanken mit personenbezogenen Angaben sichergestellt wird" (Europäischer Rat 1989, 6).

Zwei Gründe führten somit in Kombination dazu, dass das zuständige Datenschutz-Referat in der Generaldirektion Binnenmarkt und gewerbliche Wirtschaft unter der Aufsicht von Kommissionsvizepräsident und Binnenmarkt-Kommissar Martin Bangemann (FDP) die Arbeiten an Gemeinschaftsregelungen zum Datenschutz aufnahm (Karaboga 2018, 138): Das kontinuierliche Lobbying des Netzwerks nationaler Aufsichtsbehörden und insb. ihre Drohung, den Transfer personenbezogener Daten in jene fünf EG-Mitgliedstaaten zu unterbinden, womit das Binnenmarktprojekt als Ganzes hätte gefährdet werden können, sowie vertragsrechtliche Entwicklungen hin zu einer intensivierten Europäischen Integration auch auf politischen Themenfeldern vor dem Hintergrund der wachsenden Gefährdungslage, denen sich Grundrechte gegenübersahen.

Am 18. Juli 1990 legte die Kommission schließlich ein Bündel an Vorschlägen zum Schutz personenbezogener Daten vor.[91] Als Hauptelement des Schutzes personenbezogener Daten wurde der auch als Rahmenrichtlinie bezeichnete erste Richtlinienvorschlag[92] der Kommission (die spätere DS-RL 95/46/EG) vorgesehen, der sich insbesondere auf die Art. 100a[93]

91 Eine *Mitteilung zum Schutz von Personen im Hinblick auf die Verarbeitung personenbezogener Daten und die Informationssicherheit*, in der die Erwägungsgründe für das Legislativbündel dargelegt wurden, ein *Richtlinienvorschlag zum Schutz von Personen im Hinblick auf die Verarbeitung personenbezogener Daten* (die spätere DS-RL), ein *Richtlinienvorschlag zum Schutz personenbezogener Daten und der Privatheit im Telekommunikationsbereich* (die spätere ISDN-RL), einen *Entwurf einer Ministerratsentschließung zur Anwendung der für den Gemeinschaftsbereich vorgesehenen Verarbeitungsgrundsätze auch auf jene Bereiche mitgliedstaatlicher Datenverarbeitung im öffentlichen Bereich, die nicht vom Gemeinschaftsbereich abgedeckt sind* (also insb. im Feld Justiz und Inneres), eine *Erklärung zur Anwendung der für den Gemeinschaftsbereich vorgesehenen Verarbeitungsgrundsätze innerhalb der Gemeinschaftsorgane und –Einrichtungen*, eine *Empfehlung für einen Ministerratsbeschluss zur Aufnahme von Verhandlungen über den Beitritt der Europäischen Gemeinschaft zur Datenschutz-Konvention des Europarats* sowie ein *Vorschlag für einen Ministerratsbeschluss im Bereich der Informationssicherheit* (COM 1990).

92 Sofern im Folgenden vom Richtlinienvorschlag, Richtlinienentwurf oder Kommissionsentwurf die Rede ist, beziehe ich mich damit, sofern nicht anderweitig spezifiziert, auf diesen ersten Rahmenrichtlinienvorschlag der Kommission.

93 Abs. 1 des Art. 100a EWG-Vertrag (in der durch die EEA aktualisierten Fassung) besagt: „Soweit in diesem Vertrag nichts anderes bestimmt ist, gilt abweichend von Artikel 100 für die Verwirklichung der Ziele des Artikels 7a die nachstehende Regelung. Der Rat erläßt gemäß dem Verfahren des Artikels 189b und nach Anhörung

und 113 des EWG-Vertrags stützte und mit dem das allgemeine Datenschutzniveau festgelegt und im Rahmen der weiteren legislativen Aktivitäten befolgt werden sollte. Gemäß dem Kooperationsverfahren[94] sieht das Prozedere vor, dass der Kommissionsentwurf zunächst an das Europäische Parlament versendet wird. Der Parlamentspräsident überweist den Vorschlag an den federführenden Ausschuss, der (je nach Notwendigkeit unter Einbezug weiterer Ausschüsse) eine Entschließung erarbeitet und dem Plenum des Parlaments vorlegt. Im Falle der Annahme durch das Plenum wird die Entschließung des Parlaments an den Rat überwiesen. Die zuständigen Vorbereitungsgremien des Rats bereiten parallel zur Parlamentsentschließung eine gemeinsame Ratsposition vor. Das Parlament kann den Kommissionsvorschlag bzw. den Gemeinsamen Standpunkt des Rates billigen oder in Form eines aufschiebenden Vetos den Rat in zweiter Lesung zu einem einstimmigen Beschluss zwingen. Die Kommission kann jedoch – auch dann, wenn die Ratsmeinung noch nicht feststeht – unter Verweis auf die Parlamentsmeinung einen geänderten Vorschlag erarbeiten und veröffentlichen (Wessels 2008, 344), wie dies etwa bei der Erarbeitung der DS-RL der Fall sein sollte. Dem Fahrplan der Kommission nach sollten die Verhandlungen bis zur Vollendung des EG-Binnenmarktes am 31. Dezember 1992 abgeschlossen werden. Nach ersten Diskussionen nahm das Europäische Parlament im März 1992 zu dem Richtlinienvorschlag der Kommission Stellung, billigte diesen allerdings nur vorbehaltlich der von ihm vorgeschlagenen, sehr weitgehenden Änderungswünsche, womit sich zugleich abzeichnete, dass eine Verabschiedung bis zur Binnenmarkt-Vollendung nicht mehr möglich sein würde (Hoon 1992). Aufbauend auf der Stellungnahme des Parlaments und weiterer, zwischenzeitlich erfolgter Konsultationen stellte die Kommission Ende November 1992 ihren geänderten Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vor (KOM 1992). Nach einer längeren und hitzigen Verhandlungsphase

---

des Wirtschafts- und Sozialausschusses die Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben." (Europäische Gemeinschaften 1987, 8, Art. 18)

94 Bei dem Kooperationsverfahren, das im Zuge der EEA eingeführt wurde, handelt es sich um das erste Verfahren, in dessen Rahmen dem Europäischen Parlament ein eigenständiges Veto-Recht zugesprochen wurde. Insbesondere bot es dem Parlament in Form eines suspensiven Vetos die Möglichkeit, den Rat, sollte er der Position des Parlaments nicht entgegenkommen, in zweiter Lesung zu einem einstimmigen Beschluss zu zwingen (Wessels 2008, 123, 344).

im Ministerrat verabschiedete dieser seinen Gemeinsamen Standpunkt erst im April 1995 (Rat 1995). Das Parlament sprach dem Ministerrat seine Unterstützung zu und machte nur sieben kleinere Änderungsvorschläge (EP 1995), die alle vom Ministerrat angenommen wurden. Die Datenschutzrichtlinie 95/46/EG wurde schließlich am 24. Oktober 1995 von den Präsidenten des Parlaments und des Ministerrats unterzeichnet und damit erfolgreich verabschiedet (EU 1995).

Die folgende Analyse der DS-RL konzentriert sich – wie auch die vorangegangenen Ausführungen zu den OECD-Richtlinien, der Datenschutz-Konvention und den ersten Bestrebungen auf Gemeinschaftsebene – auf die zentralen datenschutzpolitischen Konfliktlinien. Auf Basis einer Durchsicht der Sekundärliteratur unter Hinzuziehung von Primärdokumenten werden die jeweiligen Konflikte, und, so gut es geht, auch die beteiligten Akteure inkl. ihrer jeweiligen Positionen dargestellt sowie das Zustandekommen der Policy-Ergebnisse erklärt.

3.2.2.4 EG-Richtlinienvorschlag von 1990

3.2.2.4.1 Kontext

In der dem Richtlinienvorschlag vorangestellten Kommissionsmitteilung wurde dargelegt, dass die Kommission die anhaltenden mitgliedstaatlichen Divergenzen im Hinblick auf das datenschutzrechtliche Schutzniveau zum Anlass für die Legislativvorschläge nimmt, weil die Divergenz die weitere Europäische Integration gefährde (Commission of the European Communities 1990, 2, Nr. 1). Damit nahm die Kommission einerseits Bezug auf das Fehlen von Datenschutzregelungen in den genannten fünf Mitgliedstaaten und andererseits auf die bestehenden Unterschiede im Schutzniveau in den sieben Mitgliedstaaten, die bereits Datenschutzregelungen verabschiedet hatten. Zu diesen zählten die aus Kommissionsperspektive weiterhin ungeklärten Fragen im Hinblick auf: Den Anwendungsbereich (1. ob dieser nur automatisierte oder auch manuelle Verarbeitungen umfassen sollte, 2. ob Datenschutzregelungen in gleichem Maße den privaten wie den öffentlichen Sektor umfassen sollten und 3. ob ausschließlich natürliche Personen oder auch juristische Personen umfasst sein sollten), die institutionelle Aufsicht (ob das Model des Datenschutzbeauftragten wie etwa in Deutschland oder das Modell einer Aufsichtsbehörde wie der CNIL in Frankreich praktiziert werden sollte), Informationspflichten bei der Erhebung personenbezogener Daten oder auch im Hinblick auf besondere Kategorien per-

sonenbezogener Daten (Commission of the European Communities 1990a, 2, Nr. 2; Prisclla M. Regan 1993, 259).

Zwar hatte die Kommission bei der Ausgestaltung ihrer Regelungsvorschläge grundsätzlich freie Hand, doch wurde ihr Handlungsspielraum von zwei Faktoren entscheidend eingeengt: Zum einen bedeutete die Verpflichtung der Gemeinschaft auf den Schutz der Grundrechte für die Kommission, dass sie bei der Gestaltung des Schutzniveaus nicht frei, sondern – auch auf Grundlage des Art. 100a Abs. 3 EWG-Vertrag – an die Gewährleistung eines hohen Schutzniveaus gebunden war (S. 5, Nr. 10 und 11). Diese Verpflichtung auf den Schutz der Grundrechte hatte zur Folge, dass der angestrebte Schutz vor dem Hintergrund der Zunahme grenzüberschreitender Datenübertragungen nicht an den Grenzen der Gemeinschaft Halt machen durfte. In anderen Worten musste das anvisierte hohe Schutzniveau nicht nur bei jedem Datentransfer zwischen EG-Mitgliedstaaten, sondern auch bei jedem grenzüberschreitenden Datentransfer in Drittstaaten gewährleistet sein.[95] Zum anderen musste die Kommission bei der Ausgestaltung ihres Richtlinienvorschlags eine ausgewogene Balance zwischen den Rechtselementen aus den existierenden Datenschutzgesetzen der EG-Mitgliedstaaten herstellen. Das mitgliedstaatliche Interesse galt dabei freilich nicht der Erarbeitung von neuen Gemeinschaftsregelungen, sondern dem Erhalt der eigenen Regelungen. D. h., ein Mitgliedstaat war grundsätzlich nur dann mit der Harmonisierung einverstanden, wenn diese das Heben seiner Datenschutzkonzepte auf Unionsebene bedeutete. Allerdings garantierte auch die Inkorporation zentraler Bestandteile der Datenschutzregelungen eines Mitgliedstaates alleine nicht die Unterstützung des jeweiligen Mitgliedstaats, sofern andere, von diesem als ebenso zentral betrachtete Elemente nicht im Richtlinienvorschlag vorzufinden waren.[96] Diese, im politischen Pro-

95 Martin Bangemann verteidigte dieses Vorgehen der Kommission später vor dem Europäischen Parlament gegen die Kritik, dass die Regelungen zu streng und damit impraktikabel seien, folgendermaßen: „Wir haben nicht die bestehenden Vorschriften auf einen gemeinsamen Nenner bringen wollen. […] Die Kommission hätte ganz einfach sagen können: Wir suchen uns ein mittleres Niveau heraus und machen einen Katalog von vielen Ausnahmen, dann haben wir keine Probleme. Wir haben diesen Ansatz bewußt nicht gewählt, sondern wollten zunächst einmal zeigen, was prinzipiell notwendig ist, um die Privatsphäre der einzelnen zu schützen. […] Aber wenn man nicht von klaren Prinzipien ausgegangen wäre, hätte man am Schluß einen ‚Flekkerlteppich' gehabt und im Prinzip gar nichts erreicht. Deswegen haben wir eine, wie ich zugebe, ambitiöse Vorlage gemacht […]." (EP 1992b, 23)

96 Obwohl die Kommission sich in ihrem 1990er-Richtlinienvorschlag stark am deutschen Datenschutzrecht orientierte (was freilich zu heftiger Kritik der anderen

zess der EU angelegte, inhärente Notwendigkeit zur Kompromissfindung erschwerte wiederum die Herstellung eines hohen Schutzniveaus – weil die Kommission auch jenen Staaten mit einem niedrigeren Datenschutzniveau entgegenkommen musste, indem Elemente ihrer Regelungsmodelle übernommen wurden, um sich ihrer Unterstützung sicher zu sein.

3.2.2.4.2 Grundsätzliche Konfliktlinien

Bei der Erarbeitung der Vorschläge hatte die Kommission eine technokratische Strategie verfolgt. Neben den jeweiligen Kommissionsverantwortlichen hatte sie ausschließlich einige wenige Vertreter nationaler – darunter offenbar vor allem deutscher – Aufsichtsbehörden konsultiert. Akteure aus der Zivilgesellschaft[97], der Wirtschaft oder den Regierungen der Mitgliedstaaten wurden dagegen gar nicht involviert. Entsprechend überrascht waren die meisten Beobachter über die Kommissionsvorschläge. Nachdem europäische Wirtschaftsvertreter bereits in der Vergangenheit ihr Desinteresse an harmonisierten Datenschutzregelungen zum Ausdruck gebracht hatten,[98] fühlten sie sich vom Kommissionsvorschlag in besonderem Maße

Mitgliedstaaten führte), wurde der Vorschlag seitens der deutschen Ratsdelegation nicht in besonderem Maße unterstützt. Stattdessen übte die Bundesrepublik Druck auf die Kommission aus, damit im Zuge der Überarbeitung des Vorschlags weitere Bestandteile des deutschen Datenschutzrechts, etwa das Konzept des betrieblichen Datenschutzbeauftragten, in die finale Richtlinie aufgenommen werden (Simitis 1995, 450).

97 Wobei anzumerken ist, dass die im Bereich der Datenschutzpolitik zu dieser Zeit bereits tätigen europäischen NGOs noch vergleichsweise jung waren. Die *Deutsche Vereinigung für Datenschutz e. V.* (DVD) sowie die *Gesellschaft für Datenschutz und Datensicherheit e. V.* (GDD) wurden beide 1977, der *Chaos Computer Club e. V.* (CCC) 1981, das *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.* (FIfF) 1984 und der *Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V. FoeBuD* (heute: Digitalcourage e. V.) 1987 gegründet. Andere Organisationen folgten teils deutlich später: das britische *Privacy International* (1990), das niederländische *Bits of Freedom* (2000), das französische *La Quadrature du Net* (2008), Die internationale Vereinigung der nationalen Organisationen *European Digital Rights* (EDRi) wurde 2002 gegründet (vgl. auch Unterabschnitt 3.4.2.3.1).

98 Vgl. diesbezüglich beispielsweise die von Newman zitierten Aussagen des Vorsitzenden des Bundesverbands der Deutschen Industrie (BDI), Friedrich Kretschmer, aus dem Jahr 1989, in denen dieser trotz der durch fehlende Harmonisierung entstehenden Wettbewerbsverzerrungen keine Notwendigkeit für eine Harmonisierung erkennt (A. L. Newman 2008a, 112).

überrumpelt (A. Newman 2007b, 4 f.). Zudem störten sich gerade Großbritannien und Frankreich am Richtlinienentwurf der Kommission, da sie darin zu wenige ihrer eigenen Datenschutz-Elemente vorfanden und die starke Anlehnung an deutsches Datenschutzrecht bemängelten (Bainbridge 1996, 25). Besonders dem Vereinigten Königreich, Irland, Dänemark und den Niederlanden (der sog. nördliche Block) widerstrebte der Gedanke der supranationalen Regulierung und Harmonisierung ihrer Datenschutzregelungen auf der Ebene der Europäischen Gemeinschaften grundsätzlich. Der nördliche Block vertrat die Auffassung, dass die Ratifizierung der Datenschutz-Konvention des Europarats ein ausreichendes Schutzniveau bieten würde, während es zugleich den Mitgliedstaaten größeren Freiraum bei der Gestaltung der Regelungen überlasse (Bignami 2005, 840 f. Pearce und Platten 1998, 533 f.). Der südliche Block, bestehend aus Italien, Belgien, Spanien, Luxemburg und Frankreich, war dagegen deutlich positiver gegenüber einer Gemeinschaftsregelung zum Datenschutz eingestellt (ebd.). Sie kritisierten einzelne Elemente des Richtlinienvorschlags, jedoch nicht die Notwendigkeit einer Regelung als solche (Bainbridge 1996, 25). Deutschland, das sich in den vorangegangenen Jahren ablehnend gegenüber europäischen Datenschutzregelungen gezeigt hatte (A. L. Newman 2008a, 111), konnte sich – trotz weiterhin geäußerter Kritik – aufgrund des starken Einbezugs deutscher Regelungen[99] mit dem Richtlinienvorschlag immerhin arrangieren (Pearce und Platten 1998, 534). Spanien hingegen schloss sich der Kritik des nördlichen Blocks am Einbezug der manuellen Verarbeitung an (Bignami 2005, 840 f.). Diese und viele weitere Fragen und Probleme waren Gegenstand zahlreicher Auseinandersetzungen, die sich Kommission, Parlament, Rat, Wirtschafts- sowie Aufsichtsbehördenvertreter in den folgenden Jahren liefern sollten. Das Parlament beauftragte den Ausschuss für Recht und Bürgerrechte mit der Erarbeitung einer Stellungnahme. Der Labour-stämmige britische Europaabgeordnete Geoffrey Hoon wurde zum Parlamentsrapporteur gewählt. Der fertige, sog. Hoon-Bericht lag Ende 1991 vor und wurde am 11. März 1992 vom Europäischen Parlament in erster Lesung nahezu einstimmig gebilligt (EP 1992a; Hoon 1992). Schon damals war die Rede von massivem Lobbying (Trubow 1992, 173) von mehr als einhundert Unternehmen und Verbänden (Priscilla M.

99 So etwa die Trennung der Regelungen für den öffentlichen und nicht-öffentlichen Bereich sowie die zentrale Stellung der Einwilligung, insb. dass ihre Einholung konkret und ausdrücklich zu erfolgen habe (Simitis 2001, 129).

Regan 1999, 207), das allerdings seitens Hoon selbst nicht problematisiert, sondern eher sogar positiv aufgenommen wurde (EP 1992b, 16 f.).

Schon bei der Aushandlung der DS-RL zeigte sich, wie stark umstritten das Thema Datenschutz war. Im folgenden Unterabschnitt werden die wichtigsten dieser Auseinandersetzungen und Konfliktlinien vorgestellt.

3.2.2.4.3 Konkrete Konflikte

Zu einer der zentralen Auseinandersetzungen während der Erarbeitung der DS-RL zählt der Konflikt um den Einbezug der manuellen Verarbeitung. Über die 1970er-Jahre hinweg[100] bis hin zur Datenschutz-Konvention des Europarats war die Vorstellung vorherrschend gewesen, dass eine Gefahr des Missbrauchs personenbezogener Daten vor allem im Kontext automatisierter Verarbeitungen bestand und dass automatisierte und manuelle Verarbeitungsweisen klar voneinander getrennt werden könnten. Wie die Verarbeitung personenbezogener Daten im Polizei- oder Beschäftigtenbereich jedoch im Laufe der Jahre verdeutlichten, trafen beide Annahmen nicht (mehr) zu. Manuell gelagerte Daten wurden digitalisiert und digital gespeicherte Daten zugleich auch manuell verarbeitet, sodass eine sinnvolle Grenzziehung zwischen beiden Bereichen zunehmend unrealistischer und schwieriger wurde (Simitis 2001, 125). Daher ging der Richtlinienvorschlag an diesem Punkt über die Datenschutz-Konvention des Europarats und die auf der Konvention basierenden nationalen Datenschutzgesetze der im nördlichen Block vereinigten Mitgliedstaaten hinaus und sah die Anwendung der Richtlinie sowohl auf automatisierte als auch auf manuelle Dateien mit personenbezogenen Daten vor. Die Staaten des nördlichen Blocks beharrten allerdings weiterhin auf der Position, dass Datenschutzregelungen im Kontext der aufkeimenden Informationstechnologien deshalb notwendig wurden, da die automatisierte Verarbeitung spezifische Risiken für die Privatheit von Betroffenen berge und die Regulierung auch der manuellen Verarbeitung die administrative wie wirtschaftliche Effizienz der Mitgliedstaaten zu behindern drohte (Council of the European Communities 1991). Der diesbezügliche Streit im Ministerrat stellte dann auch einen der Gründe dar, weshalb sich die Festlegung des Ministerrats auf

100 So etwa im Rahmen des Hessischen Landesdatenschutzgesetzes aus dem Jahr 1970 oder des schwedischen Datenschutzgesetzes aus dem Jahr 1973 (Simitis u. a. 2019, 161, Rn. 6 ff.).

eine gemeinsame Position enorm verzögerte (Simitis 1995, 465). Das Parlament unterstützte zwar den Vorschlag der Kommission, doch wurde am Richtlinienentwurf bemängelt, dass von Dateien und nicht von Daten die Rede war.[101] Entsprechend war eine der zwei zentralen Forderungen des Parlaments (EP 1992b, 16) die Ersetzung der Bezugnahme auf Dateien durch den schlichten Bezug auf die Verarbeitung personenbezogener Daten (Hoon 1992, siehe z. B. Änderung Nr. 10).

Darüber hinaus erstreckte sich der Richtlinienvorschlag, ebenso wie die OECD-Richtlinien und die Datenschutz-Konvention, zwar sowohl auf den nicht-öffentlichen als auch auf den vergemeinschafteten öffentlichen Bereich und überlies den Mitgliedstaaten in dieser Hinsicht keinen nationalen Freiraum. In Anlehnung an das damalige deutsche Recht wurden allerdings die für beide Bereiche vorgesehenen Regelungen nicht gemeinsam, sondern in unterschiedlichen Artikeln behandelt.[102] Auf Seiten der Mitgliedstaaten wurde die vorgesehene Aufspaltung der Regelungen insbesondere von Frankreich und Luxemburg kritisiert (Council of the European Communities 1991, 9, 16). Die Streichung der Unterscheidung von öffentlichem und privatem Sektor bildete sodann auch die zweite zentrale Forderung des Parlaments (EP 1992b, 16 f.).

Ein weiterer Konflikt entbrannte um die Ausweitung des Anwendungsbereichs der vorgeschlagenen DS-RL auf die nicht vom Gemeinschaftsrecht abgedeckten Bereiche mitgliedstaatlicher Datenverarbeitung im öffentlichen Bereich. Wie schon zuvor im Falle des SIS offenbarten die Mitgliedstaaten keinerlei Interesse an einem hohen Datenschutzniveau bei sicherheitsrelevanten Verarbeitungen (Simitis 2001, 115 f.). Insbesondere Frankreich und Großbritannien wehrten sich vehement gegen den Vorschlag der Kommission (Simitis 1995, 454), der lediglich auf Seiten der Datenschutzaufsichtsbehörden explizite Unterstützung fand (vgl. etwa Deutscher Bundestag 1991, 87 Nr. 28). In der Folge bewirkten die Mitgliedstaaten die Aufnahme von Art. 3 (2) Satz 1 in den Richtlinientext, mit dem die Ausklammerung aller Tätigkeiten aus dem Anwendungsbereich der Richtlinie unmissverständlich klargestellt wird, die nicht in den Anwendungsbe-

101 Diese Einschätzung wurde auch von den Datenschutzaufsichtsbehörden geteilt, da die Beschränkung auf Dateien sowohl „technisch überholt als auch Anlass zu einer Fülle von Interpretationsproblemen [sei]“ (Deutscher Bundestag 1991, 107 IV. Nr. 1).

102 So waren die entsprechenden Regelungen aufgeteilt in ein Kapitel II „Rechtmässigkeit der Verarbeitung im öffentlichen Bereich“ und ein Kapitel III „Zulässigkeit der Verarbeitung im privaten Bereich“ (KOM 1990).

reich des Gemeinschaftsrechts fallen, also „Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich“ (Art. 3 (2) DS-RL). Aus einer rein formellen Argumentation heraus, konnten die Mitgliedstaaten sich darauf beziehen, dass die DS-RL sich freilich nur auf jene Gemeinschaftsbereiche beziehen konnte, die von ihrer Rechtsgrundlage (Art. 100a und 113 des EWG-Vertrags) auch tatsächlich abgedeckt wurden. Dennoch war diese Ausklammerung höchst problematisch, waren die ersten Datenschutzgesetze doch vor allem ein Instrument zur Einhegung der wachsenden staatlichen Datenmacht. So hätten die Mitgliedstaaten durchaus die Möglichkeit gehabt, die Anwendbarkeit der Gemeinschaftsprinzipien zum Datenschutz auf die nicht-vergemeinschafteten Bereiche im Rahmen einer intergouvernementalen Vereinbarung zu gewährleisten. Später verabschiedete intergouvernementale Regelungen[103] offenbarten schließlich, dass die Mitgliedstaaten mehr Interesse an möglichst großen nationalen Spielräumen hatten als an einem gleichwertigen und hohen Schutz personenbezogener Daten in allen Rechtsbereichen (Simitis 2001, 117 f.). Entsprechend stellte Simitis fest: “In sum, what characterizes once more the Council's debates is not so much the readiness to engage in a racing to the top, in other words in a common effort to strive in the interest of the data subjects for the best possible protection, but rather to favor a racing to the bottom.” (Simitis 1995, 455)

Die Forderung nach mehr nationalen Freiräumen bei der Umsetzung war allerdings eine Forderung die sich nicht allein auf den nicht-vergemeinschafteten öffentlichen Bereich bezog, sondern im Hinblick auf verschiedene Elemente der DS-RL geäußert wurde. So plädierten einzelne Mitgliedstaaten, sofern sie mit einzelnen Regelungen nicht einverstanden waren, häufig für die Ausweitung der nationalen Freiräume bei der Umsetzung der unliebsamen Vorgaben, wie etwa im Falle des Einbezugs der manuellen Verarbeitung (Simitis 1995, 465). Weitere nationale Freiräume wurden allerdings aus unterschiedlichen Gründen auch seitens der Wirtschaft[104] und der nationalen Datenschutzaufsichtsbehörden gefordert. Während die Wirtschaft mittels der Befürwortung nationaler Freiräume

103 Vgl. hier etwa die im Juli 1995 unterzeichnete EUROPOL-Konvention, die u. a. elementare Betroffenenrechte nicht mit einschließt und somit nicht ansatzweise das in der DS-RL festgelegte Datenschutzniveau gewährleistet (H. Busch 1996).

104 Unter den Wirtschaftsvertretern, die sich zur Richtlinienentwurf äußerten, befanden sich bereits mehrere Akteure, die zu festen Größen des EU-Datenschutz-Sub-

die Umsetzungskosten der Richtlinie zu senken hoffte, indem der jeweilige Staat zuvor geltende Regelungen so weit wie möglich beibehält (A. L. Newman 2008b, 117), erhofften sich die Aufsichtsbehörden mehr Gestaltungsspielraum in Hinblick auf die Fortentwicklung der Datenschutzregelungen und damit auch die Möglichkeit der Anhebung des Schutzniveaus in ihrem Land (Deutscher Bundestag 1991, 107 II. A. L. Newman 2008b, 117).

Ein Vorschlag der Kommission hätte in dieser Hinsicht Vereinfachungen mit sich gebracht, war allerdings seinerseits hoch umstritten: So hatte die Kommission für sich weitgehende Rechtsetzungsbefugnisse im Hinblick auf die „für die Anwendung dieser Richtlinie auf die Besonderheiten bestimmter Bereiche erforderlichen Maßnahmen" vorgesehen (Art. 29 DS-RL-E). Dabei sollte die Kommission von einem beratenden Ausschuss bestehend aus Vertretern der Mitgliedstaaten unterstützt werden (Art. 30 DS-RL-E). Die Empfehlungen des Ausschusses sollten jedoch nicht bindend sein, sondern von der Kommission lediglich „soweit wie möglich" (ebd.) berücksichtigt werden. Wäre dieser Kommissionsvorschlag erfolgreich gewesen, hätte die Kommission die Befugnis gehabt, jegliche Details der Richtlinie unter Verweis auf ihre Anwendungsrelevanz, also etwa die Harmonisierung der Informations- und Meldepflichten usw. – unter weitgehender Übergehung nationaler Standpunkte – im Alleingang zu regulieren. Wie, angesichts der Zurückhaltung, die die Mitgliedstaaten im Hinblick auf die Harmonisierung ihrer Datenschutzregelungen in den vorangegangenen Jahrzehnten gezeigt hatten, zu erwarten war, zeigten sich die Mitgliedstaaten – in ansonsten ungewohnter Einigkeit – nicht mit dem Vorschlag der Kommission einverstanden. Insbesondere der beratende Charakter des Ausschusses stieß dabei auf Widerstand (Bignami 2005, 838 f.). Schließlich stand das Parlament auch in dieser Frage auf Seiten des Ministerrats und forderte im Hoon-Bericht die vollständige Streichung des betreffenden Artikels (Hoon 1992, 197, Änderung Nr. 94).

Zugleich traten Datenschutzaufsichtsbehörden wie auch das Parlament gemeinsam für eine Stärkung der europäischen Datenschutzinstanz (also der späteren Art. 29-Datenschutzgruppe). Während die Aufsichtsbehörden dafür warben, dass der Vorsitz nicht von einem Kommissionsvertreter,

systems werden sollten und die Jahre später bei den DSGVO-Verhandlungen mitwirkten. Diese sind: Die *Federation of European Direct Marketing* (FEDIM) und *European Direct Marketing Association* (EDMA), die 1997 zur *Federation of European Direct Marketing Association* (*FEDMA*) fusionierten, die *International Chamber of Commerce* (ICC), die *Union of Industrial and Employers' Confederations of Europe* (UNICE), die Im Jahr 2007 in *Businesseurope* umbenannt wurde).

sondern von einem gewählten Mitglied aus dem Kreis der Datenschutzaufsichtsbehörden übernommen wird (Deutscher Bundestag 1991, 108 Nr. 6), ging das Parlament mit seinem Vorschlag deutlich weiter und warb für die Ausstattung der Gruppe mit weitereichenden Vollmachten sowie die Aufnahme von Vertretern aus Gewerkschaften, Arbeitgeberverbänden und Bürgerrechtsgruppen in den Ausschuss (Hoon 1992, 90 und 93, Änderungen Nr. 88 und 128).

Schließlich stieß auch das von der Kommission vorgeschlagene hohe Schutzniveau auf einen breiten Widerstand. Sowohl Ministerrat als auch die Wirtschaft und selbst das Parlament empfanden den Richtlinienvorschlag als zu restriktiv (A. L. Newman 2008b; Pearce und Platten 1998; Priscilla M. Regan 1999; Simitis 2001).[105] Einzig die Aufsichtsbehörden begrüßten – unter Verweis auf die gleichzeitige Beibehaltung nationaler Freiräume – das angestrebte hohe Schutzniveau (Deutscher Bundestag 1991, 107 II.).

Im Zentrum der Kritik der Wirtschaftsvertreter standen die Mehrkosten, die sie bei der Umsetzung der Vorgaben des Richtlinienentwurfs befürchteten (Priscilla M. Regan 1999, 201). Diese Kritik umfasste im Detail insbesondere die Vorgaben betreffend die Weitergabe personenbezogener Daten in Drittländer einerseits und das Erfordernis der Einholung einer ausdrücklichen Einwilligung des Betroffenen andererseits. Bezüglich der Datentransfers in Drittländer wurden – vor allem seitens transnational agierender, darunter vieler US-amerikanischer Unternehmen – die von der Kommission vorgesehenen Bestimmungen als zu restriktiv kritisiert (ebd.).

Obwohl sich seit den 1970er-Jahren für Drittstaatentransfers die Regelung durchgesetzt hatte, dass diese nur in Drittländer erfolgen durften, die ein gleichwertiges Datenschutzniveau garantieren, wich die Kommission in ihrem 1990er-Richtlinienvorschlag von dem Gleichwertigkeitserfordernis ab. Stattdessen sollte bereits ein sog. *angemessenes* Datenschutzniveau im Zielland ausreichend sein. Dieser Wandel hatte laut Simitis zwei Ursachen: Zum einen wollte sich die Europäische Gemeinschaft damit gegen den Vorwurf wehren, man zwinge die eigenen Standards Drittstaaten auf. Zum anderen sollte das Angemessenheitserfordernis die neuerliche Flexibilität der Drittstaatentransfer-Regelungen hinsichtlich der Bewertung der Angemessenheit demonstrieren (Simitis 2001, 118 ff.). Trotz der Erleichterung auf Seiten der Wirtschaft, dass das Gleichwertigkeitserfordernis verworfen

105 Hoon interpretierte den Versuch der Kommission, ein *sehr hohes Schutzniveau* zu etablieren, sogar dahingehend, dass versucht werde, die Gesetze „in praktisch allen Mitgliedstaaten zu revolutionieren" (S. 16).

wurde, wurden die Kommissionsvorschläge – insbesondere seitens transnational agierender, darunter vieler US-amerikanischer Unternehmen – immer noch als zu restriktiv wahrgenommen (Priscilla M. Regan 1999, 201). So sah Art. 24 des Richtlinienvorschlags die rechtmäßige Weitergabe nur dann vor, sofern das Zielland ein *angemessenes* Datenschutzniveau, das diesem zuvor seitens der Kommission bescheinigt wurde, gewährleisten konnte. Während die Aufsichtsbehörden daran bemängelten, dass das Schutzniveau im Zielland gleichwertig und nicht nur angemessen sein sollte (Deutscher Bundestag 1991, 107 IV. Nr. 5), bemängelten Wirtschaftsvertreter das Fehlen von Sonder- bzw. Ausnahmeregelungen fernab der vorgesehenen Kommissionserlaubnis, die sie als zu starr interpretierten (Priscilla M. Regan 1999, 201). Tatsächlich sahen die Ausnahmebestimmungen des Art. 25 DS-RL-E vor, dass ein Mitgliedstaat von den Bestimmungen des Art. 24 abweichen konnte, nachdem dieser zuvor die Kommission und die übrigen Mitgliedstaaten über die geplante Ausnahmeregelung unterrichtet hatte und weder Kommission noch ein anderer Mitgliedstaat innerhalb von zehn Tagen Widerspruch eingelegt hatten, doch wurde auch diese Ausnahmeregelung als zu unflexibel kritisiert. Selbst das Parlament trat für die Erweiterung des Ermessensspielraums bei grenzüberschreitenden Datentransfers ein (EP 1992b, 17), insb. dafür, dass ein Transfer in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, auch mit der ausdrücklichen Einwilligung des Betroffenen erfolgen konnte (Hoon 1992, 193, Änderungen Nr. 78 und 127).

Schließlich wurde die Verpflichtung zur Einholung einer ausdrücklichen Einwilligung (gem. Art. 12 und 17 DS-RL-E) seitens der Wirtschaftsvertreter dahingehend kritisiert, dass diese zu bürokratischen Komplikationen, Verzögerungen und Erschwerungen bei vielen Formen der ihrer Meinung nach unproblematischen Verarbeitung personenbezogener Daten führe, für die keine ausdrückliche Einwilligung vonnöten sei (Priscilla M. Regan 1999, 201 f.). Wirtschaftsvertreter aus informationsverarbeitenden Bereichen, insb. dem Direktmarketing sowie der Kreditvergabe (ebd.) einerseits und gemeinnützige und politische Organisationen andererseits teilten dabei die Befürchtung, dass die Erstellung von Listen mit personenbezogenen Daten durch die Einwilligungsverpflichtung praktisch unmöglich würde (EP 1992b, 17 und 19 f.).[106] Gemeinnützige Organisationen befürch-

106 Der Streit drehte sich insbesondere darum, wie die Einholung der Einwilligung zu realisieren sei, wenn selbst das erste Anschreiben zur Einholung der Einwilligung

teten das Ende der Möglichkeit der Mittelakquise,[107] während beispielsweise der britische Direktmarketingverband auch mit der Verbesserung des Kundenwohls argumentierte, da trotz strengerer Datenschutzregelungen im Heimatland ein Deutscher durchschnittlich mehr Spam-Mails erhalten würde als ein Brite, in dessen Land weniger strenge Datenschutzvorgaben existierten (Priscilla M. Regan 1999, 209). Marktforschungs- und politische Meinungsforschungsunternehmen dagegen führten an, dass angesichts der strengen Vorgaben bezüglich der Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art 17 DS-RL-E selbst die Durchführung von Telefonumfragen nicht mehr möglich sein würde und das Opt-out-Modell daher gegenüber dem Opt-in-Modell zu bevorzugen sei (ebd.). In diesem Zusammenhang wurden auch die strengen Vorgaben hinsichtlich der Weiterverwendung bereits erhobener personenbezogener Daten zu anderen Zwecken als dem ursprünglichen Erhebungszweck, der gem. Art. 8 (2) DS-RL-E vorsah, dass jede Weitergabe mit dem Zweck der Datei vereinbar zu sein habe und andernfalls die ausdrückliche Einwilligung des Betroffenen einzuholen sei. Die Kommission bezweckte mit dieser Vorgabe den entstehenden Handel mit personenbezogenen Daten (vor allem bei Daten-Brokern) zu begrenzen bzw. zumindest eine verbesserte Kontrolle durch die Betroffenen zu gewährleisten. Unterstützt wurden diese Vorschläge der Kommission lediglich seitens der Datenschutzbehörden (Deutscher Bundestag 1991, 88).

Das Parlament (und insb. dessen britische Abgeordnete) vertrat hingegen auch bei dieser Frage die Position, dass eine bessere Balance zwischen den Datenverarbeitungsbedürfnissen öffentlicher und nicht öffentlicher Stellen und dem Schutzbedürfnis der Betroffenen herzustellen notwendig sei, indem vor allem das Opt-out-Modell an die Stelle des Opt-in-Modells tritt (EP 1992b). Vorschläge in Richtung einer Stärkung des Datenschutzes konnten sich im Parlament dagegen nicht durchsetzen. Die Forderung der deutschstämmigen Grünen Hiltrud Breyer etwa, dass der Betroffene das Recht auf den regelmäßigen Erhalt eines kostenlosen sog. Datenkontoauszugs erhalten sollte, in dem Auskunft über die bei einer verantwortlichen Stelle gespeicherten Daten gegeben wird, konnte sich nicht durchsetzen (EP 1992b, 22). Auch ihr Einwand, dass der Richtlinienentwurf nur indivi-

bereits gemäß dem Richtlinienvorschlag auf einer Einwilligung zu basieren habe (EP 1992b, 16 f.).

107 70 gemeinnützige britische Organisationen gründeten die gemeinsame Lobbying-Gruppe CHANGE (Charities and Non-profit Groups in Europe), mit der sie für flexiblere Regelungen eintraten (Priscilla M. Regan 1999, 210).

duelle Rechte thematisiere und dass auch kollektive Rechte, etwa in Form eines Arbeitnehmer-Datenschutzes, Gegenstand der Richtlinie sein sollten, fand keinen weiteren Zuspruch (ebd.). Daneben fand auch die Forderung des französischstämmigen gaullistisch-konservativen Europaabgeordneten Jacques Vernier, dass nicht nur darüber diskutiert werden müsse, dass „die Datei angelegt und kontrolliert wurde, sondern auch zu welchem Zweck sie genutzt wird" (Parl-Debatte S. 20) nur geringen Widerhall im Parlament, etwa hinsichtlich kosmetischer Verbesserungen der Regelungen zu rechnergestützten Entscheidungen (Hoon-Bericht, vgl. Änderung Nr. 46).

3.2.2.5 Überarbeiteter Richtlinienvorschlag von 1992

Nachdem das Parlament seine Position auf Grundlage des Hoon-Berichts verabschiedet hatte, machte die Kommission von der Möglichkeit Gebrauch, ihren Richtlinienvorschlag zu überarbeiten. Dazu nahm sie in erster Linie auf die Parlamentsposition (COM 1992, 2), daneben aber auch auf die seitens der Mitgliedstaaten, der Wirtschaft und Datenschutzaufsichtsbehörden geäußerten Kritikpunkte Bezug. Zu den angehörten Wirtschaftsvertretern zählten: UNICE (heute bekannt als Businesseurope), the banking federation, CELD, FEWITA, GEDIS, European Federation for Direct Marketing, EAT, CHANGE (non-profit-Organisation), European Society for Opinion and Marketing Research, ACT, EPC, ENPA, CAEJ, EBU und FAEP (ebd., 129). Mit dem Inkrafttreten der Änderungen des Vertrags von Maastricht am 1.11.1993 war die Beschlussfassung gemäß Art. 189 b nunmehr im „Mitentscheidungsverfahren" vorgesehen, was aus dem Parlament und dem Ministerrat gleichberechtigte Mitgesetzgeber machte (EP 1993, 31; Souhrada-Kirchmayer 2010, 509).

3.2.2.5.1 Kontext: Zugeständnisse und Zurückweisungen der Kommission

Mit ihrem überarbeiteten Richtlinienvorschlag verfolgte die Kommission das Ziel, die Anleihen aus französischem, niederländischem und britischem Datenschutzrecht deutlicher sichtbar zu machen, um sich der Unterstützung dieser Länder zu vergewissern.[108] Daneben ordnete die Kommissi-

108 Insbesondere die CNIL war sehr daran interessiert, mehr Einfluss auf die Gestaltung der Richtlinie zu nehmen. Zu diesem Zweck entsandte sie Personal in die

on die Textstruktur so um, dass die Bezüge auf die Datenschutz-Konvention des Europarats sichtbarer wurden (Pearce und Platten 1998, 533). Indem die Datenschutz-Prinzipien, die im ursprünglichen Richtlinienentwurf noch in der Mitte des Textes in Art. 16 untergebracht waren, nach Art. 6 vorgezogen wurden, machte die Kommission zunächst den Bezug auf die seit den 1970er-Jahren bestehenden und unverändert übernommenen Grundprinzipien des Datenschutzes deutlich (Bainbridge 1996, 25). In Bezug auf die Parlamentsposition wurden dessen zwei zentrale Forderungen erfüllt: Zum einen wurde die Aufspaltung der Regelungen in einen öffentlichen und einen nicht-öffentlichen Bereich aufgegeben und zum anderen wurde an die Stelle der Bezugnahme auf Dateien der Bezug auf die Verarbeitung personenbezogener Daten gesetzt (ebd.). Der französische Einfluss äußerte sich zum einen in der Einfügung der neuen Art. 15 DS-RL-ÜE (Betroffenenrecht auf Widerspruch) und Art. 16 (zu automatisierten Einzelentscheidungen).[109] Zudem erhielten die Aufsichtsbehörden in Art. 18 Abs. 4 die Befugnis, eine Verarbeitung, die hinsichtlich der Rechte und Freiheiten der Betroffenen besondere Risiken birgt, vor ihrer Durchführung prüfen zu können. Diese Verschärfung der Meldepflicht wurde wiederum in Art. 19 durch Vorgaben zur Vereinfachung und Befreiung von der Meldepflicht ergänzt, die seitens der Mitgliedstaaten für bestimmte Kategorien von Verarbeitungen, die die Rechte und Freiheiten der Betroffenen nicht beeinträchtigen, vorgesehen werden können.

Darüber hinaus wurden, in Anlehnung an das niederländische und britische Recht (Bainbridge 1996, 26) und wie zuvor seitens Großbritanniens und der Niederlande gefordert (Pearce und Platten 1998, 533), Elemente der Selbstregulierung in Form weitergehender Vorgaben zu Verhaltensregeln gestärkt. Während in Art. 20 des ursprünglichen Richtlinienentwurfs lediglich sehr abstrakte Aussagen zu europäischen Standes- oder Verhaltensregeln vorzufinden waren, widmete sich im überarbeiteten Entwurf je ein Artikel deutlich detaillierter nationalen (Art. 28) und gemeinschaftlichen Verhaltensregeln (Art. 29). Mit dem Entwurf von Verhaltensregeln durch Interessenverbände und durch deren Anerkennung seitens nationaler Aufsichtsbehörden im Falle mitgliedstaatlicher Verhaltensregeln oder durch die Kommission im Falle gemeinschaftlicher Verhaltensregeln sollte die

Kommission, um an der Überarbeitung des Richtlinienentwurfs unmittelbar mitzuarbeiten (Pearce und Platten 1998, 533).

109 Allerdings sei erwähnt, dass beide Artikel bereits weitgehend übereinstimmend in Art. 14 des ursprünglichen Richtlinienvorschlags unter „Ergänzende Rechte der betroffenen Person" enthalten waren (KOM 1990).

Spezifizierung der Vorgaben der Richtlinie im Hinblick auf die Besonderheiten bestimmter Wirtschaftsbereiche möglich werden, ohne dass weiteres staatliches Eingreifen nötig würde. Im Idealfall hätte die Erarbeitung branchenspezifischer Verhaltensregeln, so die Hoffnung der Kommission, bei neu auftretenden Gefahren für die Privatheit der Betroffenen, die nicht die Grundsätze des Datenschutzes tangieren, sondern lediglich branchenbezogene Spezifizierungen des in der Richtlinie festgelegten Schutzniveaus betreffen, weitere legislative Aktivitäten unnötig gemacht, weil die Unternehmen rechtzeitig freiwillige, angemessene Schutzstandards entwickelt hätten. Zudem wurde durch weitere Ergänzungen in Art. 18 DS-RL-ÜE versucht, dem vergleichsweise umfassenden Meldepflichtsystem des Vereinigten Königreichs mehr entgegenzukommen (Bainbridge 1996, 26).

Das Entgegenkommen gegenüber den Verarbeitern äußerte sich nicht zuletzt in der Änderung des Richtlinientitels. Spiegelte der Titel des ursprünglichen Richtlinienentwurfs noch die Intention der Kommission im Hinblick auf die Erreichung eines hohen Schutzniveaus wider, verdeutlichte der überarbeitete Titel den neuerlichen Drang auf die Bedürfnisse datenverarbeitender Stellen einzugehen und insbesondere deren Wunsch, Datenflüsse durch Datenschutzgesetzte nicht zu erschweren. So erhielt der ursprüngliche Titel, der schlicht den „Schutz bei der Verarbeitung personenbezogener Daten" vorsah, die Ergänzung „[…] Verarbeitung personenbezogener Daten *und zum freien Datenverkehr*" (Hervorhebung durch den Autor) (Simitis u. a. 2019, 194, Rn. 135).

Dem seitens der Aufsichtsbehörden geäußerten Wunsch nach der Erweiterung des aufsichtsbehördlichen Gestaltungsspielraums kam die Kommission nach, indem sowohl nationale Aufsichtsbehörden als auch die Datenschutzgruppe aufgewertet wurden. So wurde der die nationale Aufsichtsbehörde betreffende Art. 30 DS-RL-ÜE dahingehend geändert, dass in Abs. 1 die Unabhängigkeit der Behörde festgeschrieben wurde und in Abs. 2 Ts. 3 die Befugnisse der nationalen Behörden um die Befassung von Justizbehörden bei Verstößen gegen die Bestimmungen der Richtlinie erweitert wurden. Darüber hinaus wurde, dem Wunsch der Aufsichtsbehörden entsprechend, in Art. 31 Abs. 2 vorgesehen, dass der Vorsitz der Datenschutzgruppe nicht von einem Vertreter geführt, sondern mittels einer Wahl unter allen Gruppenmitgliedern ermittelt werden sollte. Außerdem wurde in Art. 32 Abs. 6 klargestellt, dass auch das Europäische Parlament in den Kreis der Adressaten des jährlichen Berichts der Datenschutzgruppe einbezogen sein sollte (Simitis u. a. 2019, 196, Rn. 144).

3.2.2.5.2 Weiterhin bestehende und ungelöste grundsätzliche Konfliktlinien

Insgesamt wurde der überarbeitete Entwurf deutlich positiver aufgenommen als der ursprüngliche Entwurf. Gleichwohl konnten aber auch die Zugeständnisse der Kommission in ihrem überarbeiteten Richtlinienvorschlag letztlich nichts an der britischen und irischen Blockadehaltung gegenüber einer Gemeinschaftsregelung zum Datenschutz ändern. Die Ministerratsdelegationen beider Länder vertraten weiterhin die Position, dass die Ratifikation der Europaratskonvention ausreichend sei, um den freien Fluss personenbezogener Daten innerhalb der Gemeinschaft zu gewährleisten. Ähnliche Bedenken wurden auch von Dänemark geäußert. Insbesondere Großbritannien war zudem einerseits grundsätzlich nicht an weiteren Gemeinschaftsmaßnahmen interessiert, die Kosten für die britische Wirtschaft zu verursachen drohten und andererseits teilte man auch nicht dieselben Sorgen über die durch den Missbrauch personenbezogener Daten drohenden Privatheitsgefährdungen wie sie in den übrigen Mitgliedstaaten geäußert wurden (Pearce und Platten 1998, 534). Zwar wurden die neuen Kommissionsvorschläge zum Ausbau der Bedeutung selbstregulatorischer Maßnahmen in Form von Verhaltensregeln begrüßt, doch konnten sie letztlich nur unzureichend sein angesichts der britischen und irischen Maximalforderung nach einer weitgehenden Substitution der meisten verbindlichen Vorschriften des Richtlinienvorschlags durch freiwillige Selbstregulierungsmaßnahmen (Simitis 2001, 120).[110]

In den Niederlanden stieß der überarbeitete Richtlinienvorschlag immerhin auf geteiltes Echo (Pearce und Platten 1998, 535). Die Bundesrepublik hingegen zeigte sich im Ministerrat nur wenig erfreut darüber, dass der überarbeitete Richtlinienvorschlag nicht mehr ganz so deutlich dem deutschen Datenschutzrecht nachempfunden war. Beanstanded wurde die unterschiedslose Anwendung derselben Vorgaben auf den öffentlichen und nicht-öffentlichen Bereich, aber auch das fortdauernde Fehlen der Möglichkeit, unternehmensinterne Datenschutzbeauftragte einberufen zu können und weitere Vorbehalte in Bezug auf die aus deutscher Sicht noch immer nicht ausreichend flexible Meldepflicht und Sonderbehandlung sensibler

110 Zum Teil waren auch absurde Gerüchte über die möglichen Folgen der Richtlinie im Umlauf: Michael Forsyth, britischer Staatsminister im Innenministerium, war beispielsweise selbst nach Vorlage des überarbeiteten Richtlinienvorschlags im Jahr 1994 davon überzeugt, dass die DS-RL verbiete, dass er seiner Großmutter einen Überraschungsblumenstrauß zusende (Battcock 1995, 162).

personenbezogener Daten sowie verfassungsrechtliche Bedenken im Hinblick auf die für die Aufsichtsbehörden vorgesehene Befugniserweiterung. Entsprechend befürwortete Deutschland weiterhin die Vorgaben des ursprünglichen Richtlinienvorschlags (Bainbridge 1996, 27). Deutschlands möglicher Wechsel in das Lager der Richtliniengegner war von entscheidender Bedeutung für die weiteren Verhandlungen, da das Gegner-Lager dadurch eine Sperrminorität erreicht hätte, mit der es den erfolgreichen Abschluss der Verhandlungen hätte verhindern können.[111]

Trotz des seitens der Kommission grundlegend überarbeiteten Richtlinienvorschlags waren die Staaten des südlichen Blocks, denen an einem erfolgreichen Abschluss der Verhandlungen gelegen war, somit gefordert, den Richtlinien-Gegnern weitere Konzessionen bei einer Reihe von Problemfeldern entgegenzubringen. Diese werden im Folgenden kurz umrissen.

3.2.2.5.3 Konkrete Konflikte und Pattsituation bedrohen erfolgreichen Abschluss der Verhandlungen

Durch die Richtlinie zu erwartende Mehrkosten

Die durch die Richtlinie befürchteten Mehrkosten bildeten einen zentralen, seitens Wirtschaftsvertretern geäußerten, Kritikpunkt. Entsprechend intensiv lobbyierten diese ihre eigenen Regierungen in Richtung der Ablehnung der Richtlinie oder zumindest flexiblerer Datenschutzregelungen, durch die sie sich geringere Implementierungskosten versprachen (vgl. z. B. Priscilla M. Regan 1999). So führte beispielsweise die Deutsche Gesellschaft für Datenschutz und Datensicherheit (GDD) im Jahr 1992 eine Befragung unter 255 Unternehmen (aus verschiedenen Branchen und unterschiedlicher Unternehmensgrößen) durch. Darin äußerten 91 Prozent der befragten Unternehmen ihre Ablehnung gegenüber dem Richtlinienvorschlag der Kommission mit der Begründung, dass dieser die Marktfragmentierung innerhalb Europas verschärfen würde (A. L. Newman 2008a, 112).

Eine vom britischen Innenministerium und eine vom Gesundheitsministerium initiierte Studie bekräftigten 1994 die Befürchtungen hinsichtlich drohender, überproportionaler Kosten. Auf Basis einer Umfrage unter

111 Ohne die 26 Stimmen der Richtlinien-Gegner kamen die Richtlinien-Befürworter nur noch auf 50 der benötigten 54 Stimmen für die Annahme von Legislativ-Vorschlägen der Kommission im Ministerrat, die gemäß dem qualifizierten Mehrheitswahlrecht zur damaligen Zeit nötig waren (vgl.: Tabelle 3-2).

625 öffentlichen Einrichtungen, Unternehmen und gemeinnützigen Organisationen wurden die Implementierungskosten auf 2 Milliarden britische Pfund geschätzt. Die Kosten für den staatlichen Gesundheitssektor wurden gleichzeitig auf 1 Milliarde britische Pfund geschätzt. Lediglich das britische Oberhaus war grundsätzlich positiv gegenüber der Richtlinie gestimmt, forderte aber dennoch, dass dem Ministerrat vor ihrer endgültigen Abstimmung eine gründliche Kosten-Folgenabschätzung vorgelegt wird (Pearce und Platten 1998, 534).

Während die niederländische Handelskammer die Implementierungskosten der Richtlinie für die heimische Wirtschaft als gering einschätzte und sogar Potential für langfristige Effizienzsteigerungen erkannte, rechnete die Wirtschaftsauskunftei Bureau Krediet Registratie, verantwortlich für die Verarbeitung personenbezogener Daten für Darlehen und Kredite, zu befürchtende, erhebliche administrative und Personal-Mehrkosten im Falle der Verabschiedung der DS-RL aus. Das niederländische Justizministerium schloss sich der gemäßigt positiven Position der Handelskammer an. Das Wirtschaftsministerium initiierte dagegen eine eigene Befragung der heimischen Wirtschaft, deren Ergebnisse die datenschutzkritische Position der Wirtschaftsauskunftei untermauerten (Pearce und Platten 1998, 535).

Zudem kritisierten sowohl der europäische Dachverband EUROCHAMBRES (The Association of European Chambers of Commerce), der zu diesem Zeitpunkt 24 nationale Handelskammern mit insgesamt mehr als 13 Millionen Unternehmen vertrat, als auch die ICC (International Chamber of Commerce – Internationale Handelskammer) beide Richtlinienfassungen im Hinblick auf die bei der Umsetzung befürchteten exzessiven Kosten für die Wirtschaft (Priscilla M. Regan 1999, 211).

Transparenzvorgaben und Informationspflichten des Verantwortlichen

Die Direktmarketingbranche zeigte sich zwar erfreut über die im neuen Vorschlag erfolgte Klarstellung, Werbeansprachen auch ohne die vorherige Einwilligung der Betroffenen gemäß dem Opt-out-Prinzip durchführen zu können, doch beklagte man die als zu restriktiv und umfassend wahrgenommenen Transparenz- und Informationspflichten in jenen Fällen, in denen die personenbezogenen Daten aus öffentlich zugänglichen Quellen stammten (Bainbridge 1996, 28). Der Kritik an den zu restriktiven Transparenz- und Informationspflichten schlossen sich Deutschland, Irland, die Niederlande und das Vereinigte Königreich an (Bignami 2005, 841).

Zweckbestimmung und ausdrückliche Einwilligung

Insbesondere die britische Direktmarketingbranche wandte sich sowohl gegen das Prinzip der Zweckbestimmung in Form der als zu eng kritisierten Bestimmungen hinsichtlich der Weiterverwendung zu anderen Zwecken als auch gegen die Verpflichtung, den Betroffenen die Möglichkeit zum Opt-out bieten zu müssen (Priscilla M. Regan 1999, 209). Vergleichbare Kritik kam auch aus dem Bereich der medizinischen, insbesondere der epidemiologischen Forschung. Deren Vertreter befürchteten, dass selbst die Vorgaben der überarbeiteten Richtlinienfassung die Weiterverwendung für andere Zwecke gesammelter personenbezogener Daten für medizinische Forschungszwecke unterbinden könnten. Kritisiert wurde insb. das Erfordernis, personenbezogene Daten nur bei Vorliegen der ausdrücklichen Einwilligung der Betroffenen für andere Zwecke weiterverwenden zu dürfen.[112] Vor allem die dänische Ministerratsdelegation war empfänglich für diese Kritik, sodass entsprechende Nachbesserungen des Richtlinientextes gefordert wurden (Bainbridge 1996, 28).

Vorgaben zum Datentransfer in Drittstaaten

In Reaktion auf die Kritik an den Drittstaatentransfer-Vorgaben des ursprünglichen Richtlinienvorschlags sah der überarbeitete Richtlinienentwurf in Art. 26 (1) nunmehr vor, dass ein Datentransfer in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, auch mit der Einwilligung des Betroffenen, bei Erforderlichkeit im Hinblick auf die Erfüllung eines Vertrags und für die Wahrung eines wichtigen öffentlichen Interesses oder lebenswichtiger Interessen des Betroffenen erfolgen können sollte. Zudem wurden die bei der Angemessenheitsprüfung zu berücksichtigenden Faktoren in Art. 26 (2) dahingehend flexibilisiert, dass nicht nur die in dem betreffenden Drittland „geltenden allgemeinen oder sektoriellen gesetzlichen Bestimmungen", sondern auch die „dort beachteten Standesregeln" in Betracht gezogen werden sollten. Weitgehend unverändert blieben die Bestimmungen hinsichtlich Genehmigung eines Transfers seitens eines einzelnen Mitgliedstaates. Diese hingen letztlich immer noch davon ab, dass

112 Die Kritik berief sich unter anderem auf die negativen Erfahrungen, die bei der Einholung der Einwilligung bei Krebspatienten in Deutschland für ein Krebspatientenregister gemacht worden waren. Selbst zwanzig Jahre nach der Verpflichtung zur Einholung der ausdrücklichen Einwilligung gelang dies nur in 70% der Fälle, obwohl ein immenser administrativ-personeller Aufwand betrieben wurde. Für valide Aussagen müsse ein Register dagegen 90–95% aller Fälle umfassen (Vanchieri 1993, 1023).

weder Kommission noch andere Mitgliedstaaten dem Transfer widersprachen. Im Streitfall wiederum sollte gemäß den ebenfalls weitgehend unveränderten Vorgaben zum beratenden Ausschuss in Art. 34 Abs. 2 DS-RL-ÜE immer noch die Kommission weitgehend autonom über geeignete Maßnahmen entscheiden. Entsprechend vehement wurden die Vorgaben zum Datentransfer in Drittstaaten von den Staaten des nördlichen Blocks (in diesem Fall das Vereinigte Königreich, Dänemark, Irland und Schweden, das aufgrund der bevorstehenden Aufnahme in die Gemeinschaft auch in die Verhandlungen zur DS-RL miteinbezogen wurde) abgelehnt (Bignami 2005, 841). Und auch seitens der Wirtschaft wurden die Konzessionen der Kommission als unzureichend kritisiert (Priscilla M. Regan 1999, 201). Die ICC vertrat zudem die Position, dass unternehmens- bzw. konzerninterne Datentransfers unabhängig vom Datenschutzniveau des Ziellandes möglich sein sollten (Priscilla M. Regan 1999, 211).

Gegen Harmonisierung – Für nationale Freiräume

Zeitgleich sprachen sich sowohl die Mitgliedstaaten als auch die Wirtschaft[113] und selbst die nationalen Datenschutzaufsichtsbehörden (Deutscher Bundestag 1993, 160 Nr. 33.5 b; A. L. Newman 2008b, 112) aus jeweils unterschiedlichen Gründen weiterhin gegen eine weitergehende Harmonisierung aus und traten gemeinsam für mehr nationale Freiräume ein. Die Datenschutzbehörden versprachen sich dadurch, „den Datenschutz auch künftig nicht nur zu erhalten, sondern ihn auch neuen technologischen und gesellschaften [sic] Anforderungen anpassen zu können. Besonders für Länder mit einem weitentwickelten bereichsspezifischen Datenschutz, wie die Bundesrepublik Deutschland, ist dies eine entscheidende Frage." (Deutscher Bundestag 1993, 160 Nr. 33.5 b)) Zudem traten die Aufsichtsbehörden mit der Verlagerung von mehr Macht auf die nationale Ebene dem allseits kritisierten Kompetenzzuwachs, den die Kommission für sich vorgesehen hatte, entgegen.

Die Mitgliedstaaten waren ohnehin der grundsätzlichen Ansicht, dass die Übertragung mitgliedstaatlicher Kompetenzen an die Gemeinschaft sich immer auf das Mindestmaß beschränken sollte und die Wirtschaft hoffte darauf, dass ihre Befürwortung nationaler Freiräume seitens der jeweiligen Mitgliedstaaten für eine möglichst wirtschaftsfreundliche Umsetzung der

113 Hier sei insbesondere EUROCHAMBRES genannt, der die Europäische Kommission im Jahr 1993 dazu aufforderte, den Mitgliedstaaten bei der Umsetzung der Richtlinie mehr Freiraum zu überlassen (Priscilla M. Regan 1999, 211).

Richtlinienvorgaben und der Senkung der Implementierungskosten der Richtlinie sorgen würde (A. L. Newman 2008a, 117 f.).

Ausweitung des Anwendungsbereichs auf manuelle Dateien

In jenen Ländern, in denen manuelle Verarbeitungen nicht vom Anwendungsbereich der nationalen Datenschutzgesetze umfasst waren, wehrten sich Wirtschaftsvertreter weiterhin dagegen, dass die Richtlinie auch diese umfassen sollte. Die Ausweitung des Anwendungsbereichs auch auf manuelle Verarbeitungen bedeutete für viele Unternehmen, dass viele ihrer laufenden und dem Datenschutzrecht nicht entsprechenden manuell geführten Datenbanken und manuellen Verarbeitungen nachträglich und kostenintensiv den Richtlinienvorgaben angepasst werden müssten. Entsprechend ablehnend standen Großbritannien, Irland und Dänemark auch weiterhin gegenüber der vorgesehenen Ausweitung des Anwendungsbereichs gegenüber (Battcock 1995, 164). Der nördliche Block konnte sich mit seinen Forderungen allerdings nicht durchsetzen. Statt der vollständigen Herausnahme der manuellen Verarbeitung aus dem Anwendungsbereich konnten sie im überarbeiteten Richtlinienentwurf allerdings immerhin eine deutliche Verlängerung der Anwendungsfrist auf manuelle Dateien erringen. Während die Umsetzung der übrigen Vorgaben der Richtlinie in nationales Recht binnen drei Jahren abgeschlossen sein sollte, wurde für die Anwendung der Richtlinienvorgaben auf manuelle Dateien zunächst eine Übergangsfrist von zehn Jahren ausgehandelt, um eine kosteneffiziente Durchführung zu ermöglichen (Simitis 1995, 465).

Daneben beschäftigte das vorgesehene Verbot automatisierter Einzelentscheidungen sowohl die Kredit-Scoring- und Werbeversandbranche, die Erschwerungen im Hinblick auf die Erstellung von Kundenprofilen befürchtete (Battcock 1995, 164 f. Priscilla M. Regan 1999, 209) als auch den Großteil des nördlichen Blocks (Dänemark, Irland und demVereinigten Königreich), der die Streichung des entsprechenden Artikels forderte (Bignami 2005, 841).

Ein weiterer Konflikt entbrannte um die Vorgaben zu besonderen Kategorien personenbezogener Daten. Während Belgien, Frankreich, Spanien und Portugal mit dem entsprechenden Artikel grundsätzlich zufrieden waren, beklagten die Staaten des nördlichen Blocks, aber auch die Bundesrepublik, dass nicht die Art eines Datums, sondern der spezifische Verarbeitungskontext im Hinblick auf besondere Schutzmaßnahmen relevant sein sollte. Doch fand diese Perspektive trotz aller Kritik an der mangelnden Flexibilität besonderer Kategorien personenbezogener Daten bei den Staa-

ten des südlichen Blocks keine Unterstützung (Bignami 2005, 841; Simitis 1995, 450).

Aufgrund der zahlreichen Konfliktfelder gerieten die Verhandlungen im Ministerrat im Laufe des Jahres 1993 zunehmend ins Stocken. Großbritannien, Irland, Dänemark und Deutschland legten schließlich im Oktober 1993 im Ministerrat ein gemeinsames Papier mit Änderungsanträgen für eine deutliche Ausweitung der nationalen Freiräume bei der Umsetzung vor, die das Harmonisierungsziel, aber auch das angestrebte Datenschutzniveau der Richtlinie vollends nichtig gemacht hätten.[114] Interessanterweise bezweckte Deutschland mittels der Forderung nach sehr weitreichenden nationalen Freiräumen die Aufrechterhaltung seiner als überlegen erachteten nationalen Datenschutz-Traditionen, während Großbritannien, Irland und Dänemark mittels der Freiräume vor allem die Absenkung des gemeinschaftlichen Schutzniveaus bei der nationalen Umsetzung anstrebten. An diesem Punkt wiederum war die rote Linie des südlichen Blocks sowie der Kommission erreicht.[115] Eher hätten die Richtlinienbefürworter den grenzüberschreitenden Verkehr personenbezogener Daten ganz gestoppt, als den Vorschlägen des nördlichen Blocks, die den Richtlinienentwurf und insbesondere das Harmonisierungsziel der Gemeinschaft bis zur Unkenntlichkeit verwässert hätten, nachzugeben. Somit lag Ende 1993 bzw. Anfang 1994 im Ministerrat eine Pattsituation vor und die Verhandlungen standen praktisch still (Bainbridge 1996, 28 f. Pearce und Platten 1998, 535 ff.).

Mitgliedstaat	Stimmen
Deutschland	10
Frankreich	10
Italien	10
Vereinigtes Königreich	10
Spanien	8
Belgien	5
Griechenland	5
Niederlande	5
Portugal	5

114 Durch Deutschlands Wechsel in das Lager der Richtliniengegner hatten diese Staaten eine Sperrminorität (26 Stimmen) inne. Die Richtlinienbefürworter verharrten hingegen bei 50 der benötigten 54 Stimmen (vgl. Tabelle 3-2).

115 Die datenschutzfeindliche Haltung des nördlichen Blocks wurde auch seitens der Datenschutzaufsichtsbehörden kritisiert (Der Spiegel 1993, 15).

Mitgliedstaat	Stimmen
Dänemark	3
Irland	3
Luxemburg	2
Insgesamt	76
Benötigt	54

Tabelle 3-2: Qualifiziertes Mehrheitswahlrecht bis Ende 1994, Richtliniengegner Ende 1993/Anfang 1994 in Rot (Council of the European Union 2013, 38)

3.2.2.6 Überwindung der politischen Pattsituation

Die politische Pattsituation auf der Ebene der Ratsarbeitsgruppe bzw. des AStV im Ministerrat konnte letztlich vor allem durch die Entwicklungen auf dem Gebiet der internationalen Informationspolitik und der neuerlichen Selbstverortung der Europäischen Gemeinschaft in diesem Kontext überwunden werden. Bereits 1992 hatte die erfolgreiche Wahlkampagne des zum US-Präsidenten gewählten Bill Clinton und seines Vize-Präsidenten Al Gore die Bedeutung der Informationspolitik für die wirtschaftliche Entwicklung vor Augen geführt und die Förderung von Informations- und Kommunikationstechnologien (IKT) zu einem zentralen Element des Regierungsprogramms ausgebaut. Jacques Delors, der langjährige sozialdemokratische Präsident der Europäischen Kommission, arbeitete zur selben Zeit an einer populären Neuausrichtung der Europäischen Gemeinschaft, die er nach den kritischen Maastrichter Referenden in Frankreich und Dänemark für notwendig erachtete.[116] Die Kommission veröffentlichte ihre neue Vision für die Gemeinschaft schließlich im Juni 1993 in Form des Weißbuchs „Wachstum, Wettbewerbsfähigkeit, Beschäftigung: Herausforderungen der Gegenwart und Wege ins 21. Jahrhundert", das den Wandel

116 Während Mitgliedstaaten wie Deutschland kein Referendum abhielten, fanden im Jahr 1992 in Frankreich, Irland und Dänemark Volksreferenden zum Maastrichter Vertrag statt. Das ablehnende Votum der Dänen im Juni 1992 und das knappe Ja der Franzosen markierten zugleich einen Wendepunkt in der Geschichte der Europäischen Integration. Die langsame, aber technokratische Fortsetzung der Europäischen Integration, die bis dahin als europaweiter gesellschaftlicher Konsens galt, gelangte an ihr Ende, die Politisierung der Europäischen Gemeinschaftspolitiken setzte ein und EU-skeptische Gruppierungen und Parteien erhielten erstmals ernsthaften Auftrieb (Harmsen und Spiering 2004).

der Gesellschaft hin zu einer Informationsgesellschaft als unaufhaltsam und die Schaffung eines „gemeinsamen Informationsraums" für die weitere Entwicklung der europäischen Wettbewerbsfähigkeit als zentral definierte (Europäische Kommission 1994b, 117, Nr. 5.2). Zur Erreichung dieser Ziele wurde eine Reihe von Maßnahmenvorschlägen formuliert. Einer der Vorschläge sah zur Realisierung des gemeinsamen Informationsraums die „Schaffung der rechtlichen, ordnungspolitischen, normativen und politischen Voraussetzungen" unter Wahrung der Interessen des einzelnen – zu denen Datenschutz hinzugezählt wurde – sowie der Interessen der Gemeinschaft (bestehende Universaldienste und künftige europäische Unternehmen) vor (ebd., 120 lit. b). Zur weiteren Ausarbeitung der erforderlichen Maßnahmen wurde die Gründung einer hochrangigen Arbeitsgruppe, der sog. *Task Force „Europäische Informationsinfrastruktur"* (ebd., 124, Nr. 5.4), bestehend aus einem Mitglied der Kommission, Regierungsangehörigen der Mitgliedstaaten, Vertretern des Europäischen Parlaments sowie hochrangigen Industrievertretern, vorgeschlagen. Von entscheidender Bedeutung war, dass die Task Force dem Europäischen Rat unmittelbar Bericht erstatten und Politik-Empfehlungen unterbreiten sollte (ebd.). Der Europäische Rat billigte die Einsetzung der Task Force auf seiner Sitzung im Dezember 1993, woraufhin diese umgehend mit der Erstellung eines ersten Berichts bis zur nächsten Sitzung des Europäischen Rates am 24. und 25. Juni in Korfu beauftragt wurde (Bangemann 1994, 6). Den Vorsitz der Gruppe übernahm Martin Bangemann, der bereits für die Initiative der Europäischen Kommission zur DS-RL mitverantwortlich gewesen war. Der Bericht der Task-Force, der als Bangemann-Report auch international über die Grenzen der EG hinaus Aufmerksamkeit erzeugen sollte, forderte dem neoliberalen Zeitgeist in der Politik entsprechend und viele der Elemente des Clinton/Gore-Aktionspapiers zur Schaffung einer Nationalen Informations-Infrastruktur übernehmend, die Deregulierung der europäischen IKT-Märkte mit dem Ziel der Stärkung marktbasierter Ansätze zur Erreichung der angestrebten Informationsgesellschaft (Krempl 1997). Der Erlass EG-weiter Datenschutz-Regeln wurde zudem erstmals mit dem Argument verbunden, dass diese ein notwendiges Element zur Herstellung von Vertrauen auf Seiten der Verbraucher für das erfolgreiche Gelingen der Informationsgesellschaft seien:

> *"The Group believes that without the legal security of a Union-wide approach, lack of consumer confidence will certainly undermine the rapid development of the information society. Given the importance and sensitiv-*

> *ity of the privacy issue, a fast decision from Member States is required on the Commission's proposed Directive setting out general principles of data protection." (Bangemann 1994, 22)*

Der Bangemann-Report wurde auf dem Treffen des Europäischen Rates in Korfu von den Regierungschefs der Mitgliedstaaten äußert positiv aufgenommen (Pearce und Platten 1998, 536). Entsprechend deutlich signalisierte der Europäische Rat dann auch seinen Wunsch hinsichtlich der Umsetzung der Kommissionsvorschläge zur Informationsgesellschaft:

> *„Der Europäische Rat ersucht den Rat und das Europäische Parlament, vor Jahresende Maßnahmen […] zu ergreifen, […] indem sie diese Entwicklung durch politische Impulse fördern, einen klaren und stabilen rechtlichen Rahmen (insbesondere in bezug [sic] auf den Marktzugang, die Kompatibilität zwischen Netzen, das geistige Eigentum, den Datenschutz und das Urheberrecht) schaffen und in Bereichen, die unter ihre Zuständigkeit fallen, beispielgebend vorangehen." (Europäischer Rat 1994b I Nr. 4)*

Sowie:

> *„Bei der Ausarbeitung der verschiedenen Rechtsakte zur Schaffung von Informatiksystemen muß dem Datenschutz, insbesondere folgenden Aspekten besondere Aufmerksamkeit gewidmet werden: Recht der Betroffenen auf Zugang zu dem System, Individualbeschwerderecht und Einrichtung einer gemeinsamen Aufsichtsstelle. Der Europäische Rat ersucht die zuständigen Gremien, diesen Fragen weiterhin Vorrang einzuräumen, und hofft, auf seiner Tagung im Dezember 1994 einen Zwischenbericht zu erhalten." (Europäischer Rat 1994b, III Nr. 2)*

Von diesem Zeitpunkt an erhielten die Verhandlungen zur DS-RL wieder Auftrieb. Entsprechend den Vorgaben des Europäischen Rates waren die mitgliedstaatlichen Delegationen, die sich im Ministerrat mit der DS-RL auseinandersetzten, in der Folgezeit gefordert, die politische Pattsituation zu überwinden und die Verhandlungen unter Erzielung eines politischen Kompromisses zu einem erfolgreichen und schnellen Ende zu bringen (Pearce und Platten 1998, 536).

Ein weiteres Schlüsselereignis, das zum erfolgreichen Abschluss der Verhandlungen beigetragen hat, war die Übernahme des Ministerratsvor-

sitzes[117] durch die Bundesrepublik im Juli 1994. Deutschland, das sich zuletzt auf die Seite der Richtliniengegner geschlagen hatte und damit den erfolgreichen Abschluss der Verhandlungen blockierte, auf ihre Seite zu ziehen, war ein zentrales Anliegen der Richtlinienbefürworter. Allerdings erwies sich dies als gar nicht notwendig, da Deutschland seine Haltung aus verschiedenen Gründen änderte. *Erstens* führte der verstärkte Dialog, der traditionell zwischen jedem Ratsvorsitz und der Kommission stattfindet, dazu, dass politische Missverständnisse überwunden werden konnten, indem die Kommission die Gelegenheit erhielt, die deutsche Ratsdelegation davon zu überzeugen, dass ihre nationalen Datenschutz-Traditionen von der Richtlinie nicht gefährdet würden. *Zweitens* war Deutschland, wie jeder andere Ratsvorsitz auch, grundsätzlich darum bemüht, während seines Vorsitzes potentiell prestige-trächtige Politik-Ergebnisse – insb. in Form gemeinsamer Ratspositionen – zu erzielen. Aus diesen taktischen Erwägungsgründen heraus machte die kurz zuvor in Korfu auf höchster europapolitischer Ebene geäußerte Forderung nach einem schnellen Abschluss der Verhandlungen zur DS-RL diese zu einem geeigneten Kandidaten zur Erzielung einer gemeinsamen Position. Schließlich und *drittens* war die Bundesrepublik, weil sie handfeste Fortschritte erzielen wollte, eher dazu geneigt, Konzessionen bei Themen einzugehen, wozu sie zuvor nicht bereit gewesen war (Bainbridge 1996, 30 f. Pearce und Platten 1998, 536 f.).

Zeitgleich wurde in den Mitgliedstaaten und insbesondere im Vereinigten Königreich sowie in den Niederlanden noch immer über die bei der Umsetzung der Richtlinie zu befürchtenden Kosten debattiert. Zur Überprüfung der Ergebnisse der vorherigen Studien und zum Zwecke der Erarbeitung einer eigenen, evidenzbasierten Position unternahm die

117 Der Rolle des Vorsitzes im Ministerrat kommt in der institutionellen Architektur sowohl des Ministerrats als auch der EU eine Schlüsselrolle zu. Der Vorsitz ist u. a. insbesondere verantwortlich für die Einberufung, Vorbereitung und Durchführung aller formellen und informellen Treffen des Ministerrats, für die Kompromisssuche bei Kontroversen und die Vertretung der Ministerratsposition gegenüber anderen EU-Institutionen wie auch Drittstaaten. Über viele Jahrzehnte rotierte der Vorsitz halbjährlich alphabetisch unter allen Mitgliedstaaten. Seit 2007 wurde die alphabetische Rotation zugunsten eines Dreiervorsitzes aufgegeben. Die dabei aufeinanderfolgenden drei Vorsitze setzen sich nach Möglichkeit aus einem größeren Mitgliedstaat, einem kleineren Altmitglied sowie einem neuen Mitgliedstaat zusammen und sollen zum Zwecke der Formulierung langfristigerer politischer Ziele ein gemeinsames Achtzehnmonatsprogramm formulieren, auf dem wiederum der jeweilige Vorsitz sein eigenes detailliertes Halbjahresprogramm aufbauen kann (EU-Ministerrat 2020; Wessels 2008, 214 ff.).

Kommission den für diese Zeit ungewöhnlichen Schritt der Beauftragung einer wissenschaftlichen Studie zur Untersuchung der bei der Umsetzung der Richtlinie in den Niederlanden und dem Vereinigten Königreich zu erwartenden Kosten (Pearce und Platten 1998, 537). Die Studie wurde im Zeitraum Juli 1994 bis Oktober 1994 von unabhängigen britischen und niederländischen Forscherinnen und Forschern durchgeführt. Im Gegensatz zur Mehrheit der anderen Studien verdeutlichten die Ergebnisse, dass die Mehrzahl der von der DS-RL betroffenen öffentlichen wie nicht-öffentlichen Organisationen nur mit sehr geringen finanziellen Mehrkosten während der Umsetzungsphase rechnen mussten, die laufenden Kosten nach Abschluss der Implementierungsphase jedoch wieder auf das Vor-Datenschutz-Richtlinien-Niveau sinken würden. Zwar wurde festgestellt, dass jene Wirtschaftsbereiche, die besonders viele Kundendaten verarbeiten (allen voran der Bankensektor sowie die Direktmarketingbranche) in besonderem Maße von gesteigerten Kosten betroffen sein würden, doch auch diese Zahlen waren deutlich niedriger als jene, die in den vorherigen Studien berechnet worden waren. Zudem stellte die Studie fest, dass die mit der DS-RL notwendig werdende Durchsicht datenverarbeitender Unternehmensprozesse auch zu Effizienzsteigerungen und zu Investitionen in datenverarbeitende Systeme führen könnte. Schließlich propagierte auch diese Studie das neue Argument, dass der angemessene Schutz personenbezogener Daten zu mehr Vertrauen in datenverarbeitende Dienste und zu deren gesteigerter gesellschaftlicher Akzeptanz führen und damit zu nachhaltigem wirtschaftlichen Erfolg beitragen würde (Bainbridge u. a. 1994). Parallel zu den Entwicklungen auf der Ebene des Europäischen Rates und den durch den deutschen Ministerratsvorsitz angestoßenen Entwicklungen, trugen die Ergebnisse dieser Studie ebenfalls dazu bei, dass der Widerstand gegen die Richtlinie in den Mitgliedstaaten zurückgefahren und die Kompromissbereitschaft gesteigert wurde (Pearce und Platten 1998, 537).

3.2.2.6.1 Politische Kompromisse

Aufgrund der genannten externen und internen Rahmenbedingungen wurden in der zweiten Hälfte des Jahres 1994 dann auch zügig Fortschritte im Hinblick auf die Erreichung einer gemeinsamen Position im Ministerrat erzielt.

So wurde die vorgesehene Übergangsfrist bezüglich der Anwendung der Richtlinienvorgaben auf manuelle Dateien von zehn Jahren auf zwölf Jahre

erhöht, sodass die irische Ratsdelegation ihren Widerstand gegen die Richtlinie zurückzog. Dänemarks Widerstand konnte aufgebrochen werden, indem eine Reihe von Ausnahmeregelungen bezüglich der Verarbeitung personenbezogener Daten zu wissenschaftlichen bzw. medizinischen Forschungszwecken in die Richtlinie eingebaut wurde. Auch bei dem Streitthema besonderer Kategorien personenbezogener Daten konnte eine Einigung erzielt werden. Die Bundesrepublik, Dänemark, Griechenland, Irland, die Niederlande, Portugal und Großbritannien konnten zur Aufgabe ihrer Ablehnung einer erschöpfenden Liste als sensibel eingestufter personenbezogener Daten bewegt werden, indem in den entsprechenden Artikel weitere Ausnahmebestimmungen hinzugefügt wurden (Bainbridge 1996, 28; Pearce und Platten 1998, 537 ff.).

Die dem deutschen Recht nachempfundene zentrale Stellung der Einwilligung wurde im Laufe der Verhandlungen ebenfalls abgeschwächt. Während im ursprünglichen Richtlinienentwurf noch von einer konkreten und ausdrücklichen Einwilligung und im überarbeiteten Richtlinienentwurf von einer ausdrücklichen Willensbekundung des Betroffenen für jede personenbezogene Datenverarbeitung die Rede war, was vor allem die Einwilligung in Schriftform erforderlich gemacht hätte, sah der finale Ratskompromiss nur noch eine Einwilligung *ohne jeden Zweifel* vor. Die ausdrückliche Einwilligung sollte nur im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten erforderlich sein (Simitis 2001, 129 f.).

Auch der Dauerstreit um die Meldepflicht konnte letztlich überwunden werden. Die Vorabkontrolle riskanter Verarbeitungen personenbezogener Daten wurde zur Ausnahme gemacht, während den Mitgliedstaaten die Möglichkeit eröffnet wurde, die Meldepflicht zu vereinfachen. Dazu bediente man sich in Art. 18 Abs. 2 DS-RL insbesondere des aus dem deutschen Datenschutzrecht stammenden und seitens der deutschen Ministerratsdelegation und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gewünschten (Deutscher Bundestag 1993, 160 Nr. 33.5 c)) Konzepts eines unabhängigen betrieblichen Datenschutzbeauftragten. Für die Bestellung eines betrieblichen Datenschutzbeauftragten, der die unabhängige Überwachung der jeweiligen Verarbeitungen und die Führung eines Verzeichnisses über diese gewährleistet, wurde die Vereinfachung der Meldepflicht bzw. die vollständige Befreiung eines Verantwortlichen von dieser Pflicht vorgesehen (Simitis 2001, 134 f.). Mittels derartiger Konzessionen konnte die Bundesrepublik schließlich dazu bewegt werden, einige ihrer zentralen Forderungen aufzugeben. Dies betraf zum einen

die fortwährend gestellte Forderung nach einer Mindestharmonisierung,[118] die von der Kommission und der Mehrheit der übrigen Mitgliedstaaten abgelehnt wurde und zum anderen die Ablehnung der vorgesehenen Regelungen zum Direktmarketing, das ohne die ausdrückliche Einwilligung der Betroffenen erfolgen dürfen sollte (Pearce und Platten 1998, 536 f.).

Kurz vor Abschluss der Verhandlungen wurden auf Druck Frankreichs hin schließlich auch die letzten verbliebenen Befugnisse der Europäischen Kommission im Hinblick auf die Harmonisierung des europäischen Datenschutzrechts gestrichen. Letztlich war die Kommission nur noch in die Genehmigung von Datentransfers in Drittstaaten eingebunden, verlor aber selbst dort die für sich vorgesehene herausgehobene Stellung (Bignami 2005, 839). Zudem wurde auf Druck Großbritanniens, Dänemarks, Irlands und Schwedens hin auch das Prozedere zur eigenständigen Genehmigung eines Datentransfers in einen Drittstaat seitens eines einzelnen Mitgliedstaates deutlich zugunsten der Mitgliedstaaten vereinfacht (Bignami 2005, 840).

Ende 1994 waren die Mitgliedstaaten schließlich soweit, eine gemeinsame Position zu verabschieden. Auf der Tagung des Binnenmarkt-Rates[119] am 8. Dezember 1994 konnte sodann eine informelle politische Einigung betreffend die DS-RL erzielt werden. Eine formelle Einigung war aus technischen Gründen nicht möglich, da der finale Kompromisstext bis zum Sitzungstermin nicht in allen EG-Sprachen vorlag. Einzig Großbritannien verharrte in Radikalopposition zur Richtlinie und war auch weiterhin gegen den vorgeschlagenen Kompromiss. Die britische Ablehnung ging so weit, dass Angehörige der britischen Ratsdelegation und selbst Minister aus der britischen Regierung noch in den ersten Wochen des Jahres 1995 die übrigen Mitgliedstaaten – letztlich ohne Erfolg – davon zu überzeugen

118 Das Prinzip der Mindestharmonisierung sieht vor, dass einzelne Länder bei der Richtlinienumsetzung höhere Standards festlegen dürfen, während die Maximal- oder Vollharmonisierung keine strengeren Vorschriften als in der Richtlinie erlaubt (EU 2018).

119 Zur Wahrnehmung seiner Aufgaben tagt der Ministerrat in unterschiedlichen Ratsformationen, deren Zuschnitt sich an Politikfeldern orientiert. Die Anzahl der Ratsformationen variierte im Laufe der Geschichte des Ministerrats teils erheblich. Von sieben Formationen im Jahr 1967 stieg ihre Anzahl auf bis zu 22 Formationen im Jahr 1990 und ist wieder auf aktuell zehn Formationen gesunken (EU-Ministerrat 2018b; Wessels 2008, 199). Einen Überblick über die Entwicklung der Zuständigkeitsstrukturen im Ministerrat bietet (Karaboga 2018, 143 ff.).

versuchten, die im Dezember erzielte politische Einigung zu widerrufen.[120] Die übrigen Mitgliedstaaten versuchten währenddessen umgekehrt die britische Ratsdelegation auf den AStV-Sitzungen im Januar und Februar 1995 davon zu überzeugen, ihre ablehnende Haltung zu überdenken. Zwar waren sie bereit, Zugeständnisse gegenüber dem Vereinigten Königreich zu machen, doch war der Spielraum für diese aufgrund der im Dezember bereits erzielten Einigung deutlich geringer als davor. Im Ergebnis führte die vom Vereinigten Königreich jahrelang vertretene Radikalopposition schließlich dazu, dass das Land selbst im Vergleich zu kleineren Staaten wie Dänemark einen nur äußert geringen Einfluss auf die Gestaltung der Richtlinie nehmen konnte, da es während der Verhandlungsphase keine kompromissorientierten Gestaltungsvorschläge machte, die von den Richtlinienbefürwortern ernsthaft hätten in Erwägung gezogen werden können. Zwar konnte Großbritannien trotz vielfacher Bemühungen[121] letztlich nicht zur Zustimmung zur Richtlinie bewegt werden, doch immerhin verwarf das Land seine Ablehnung und entschied sich aufgrund der vielen kleinen Konzessionen der anderen Mitgliedstaaten, die im Land immerhin anerkannt wurden, dazu, sich der Stimme zu enthalten (Bainbridge 1996, 31 f. Pearce und Platten 1998, 537 f. Simitis 1995, 445).

Am 1. Januar 1995 wurde die Europäische Gemeinschaft zudem um drei weitere Mitgliedstaaten – Finnland, Österreich und Schweden – erweitert. Alle drei Staaten waren in der entscheidenden Phase der Verhandlungen des vorangegangenen halben Jahres als Beobachter eingebunden. So waren alle drei Neumitglieder zum Zeitpunkt ihres Beitritts zur Gemeinschaft grundsätzlich mit den Inhalten der Richtlinie einverstanden. Der Gemeinsame Standpunkt des Ministerrates wurde schließlich unter dem neuen französischen Ratsvorsitz formell am 20. Februar 1995 auf der Tagung

120 Dies war auch deshalb unrealistisch, weil der Europäische Rat auf seinem Treffen am 9. und 10. Dezember in Essen sein Ersuchen aus dem Frühjahr an den Rat erneuert hatte, „die noch notwendigen rechtlichen Rahmenbedingungen – in Bereichen wie Marktzugang, Datenschutz und Schutz geistigen Eigentums – zügig zu schaffen." (Europäischer Rat 1994a, Nr. 6)

121 Die Kompromissbereitschaft der Richtlinienbefürworter wurde auch dadurch verstärkt, dass im Ministerrat, obwohl für Legislativvorschläge der Kommission das qualifizierte Mehrheitswahlrecht galt, eine Konsenslösung also technisch gesehen nicht notwendig war, für gewöhnlich die Erreichung eines Konsenses angestrebt wurde. Dementsprechend war es den Befürwortern nicht nur wichtig, die formal erforderliche Mehrheit zu erzielen, sondern möglichst alle Gegner durch weiteres Entgegenkommen zu einer Änderung ihrer Haltung zu bewegen (Bainbridge 1996, 31).

der Ratsformation „Allgemeine Angelegenheiten" (General Affairs Council) ohne Gegenstimmen[122] angenommen (Rat 1995). Trotz der Kritik an der vollständigen Streichung der Durchführungsbefugnisse der Kommission, zeigte sich diese einverstanden mit der gemeinsamen Position des Ministerrats (COM 1995, 8). Das Parlament bestätigte die Ministerratsposition in zweiter Lesung ebenfalls grundsätzlich und machte lediglich sieben kleinere Änderungsvorschläge[123] geltend (EP 1995), die sowohl von der Kommission (KOM 1995) als auch vom Ministerrat (Working Party on Economic Questions (Data Protection) 1995) akzeptiert und in der zweiten Lesung des Ministerrats am 24. Juli 1995 von diesem angenommen wurden. Die finale *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* wurde schließlich am 24. Oktober 1995 von den Präsidenten des Parlaments und des Ministerrats unterzeichnet (EU 1995).

122 Mit 77 von 87 Stimmen. Benötigt wurden mindestens 64 Stimmen (Council of the European Union 2013, 39). Vgl. auch Tabelle 3-3.

123 Es wurden zwar rund 60 Änderungsvorschläge eingebracht, doch der neue Rapporteur Medina Ortega (SPE, Spanien) im Parlamentsausschuss für Recht und Bürgerrechte (JURI) befürwortete lediglich die genannten sieben kleineren Änderungsvorschläge (Bainbridge 1996, 32).

Mitgliedstaat	Stimmen
Deutschland	10
Frankreich	10
Italien	10
Vereinigtes Königreich	10
Spanien	8
Belgien	5
Griechenland	5
Niederlande	5
Portugal	5
Österreich	4
Schweden	4
Dänemark	3
Irland	3
Finnland	2
Luxemburg	2
Insgesamt	*87*
Benötigt	*64*
Erhalten	*77*

Tabelle 3-3: Qualifiziertes Mehrheitswahlrecht nach der EU-Erweiterung im Jahr 1995 und Abstimmungsverhalten (Enthaltung des Vereinigten Königreichs) (Council of the European Union 2013, 39)

3.2.2.7 Inhalte der DS-RL

Im Ergebnis des politischen Kompromisses konnte sich in Bezug auf den sachlichen Anwendungsbereich (Art. 3 Abs. 1)[124] durchsetzen, dass kein Unterschied zwischen Regelungen für den öffentlichen und nicht-öffentlichen Bereich gemacht werden und dass allein das Vorhandensein einer Verarbeitung personenbezogener Daten den Ausschlag darüber gibt, ob sie in den Anwendungsbereich fällt oder nicht – unabhängig von der Art (manuell oder automatisiert) der Verarbeitung. Der von Großbritannien und Irland

124 Die Artikel-Angaben dieses Unterabschnitts beziehen sich grundsätzlich auf die finale DS-RL. Sofern der ursprüngliche Richtlinienentwurf von 1990 bzw. der überarbeitete Richtlinienentwurf von 1992 gemeint sind, wird die entsprechende Artikel-Angabe um „DS-RL-UE“ bzw. „DS-RL-ÜE“ ergänzt und spezifiziert.

favorisierte Versuch, die DS-RL auf den Standard der Datenschutz-Konvention des Europarats „zurückzuschrauben, die Automatisierung also nicht nur als Anlaß, sondern auch als Grenze der regulativen Intervention anzusehen" (Simitis 1997, 283) scheiterte somit endgültig. Allerdings wurde der Einbezug der manuellen Verarbeitung personenbezogener Daten unter den Vorbehalt des Vorhandenseins einer minimalen Organisationsstruktur gestellt. Zu diesem Zweck bedienten sich Kommission und Ministerrat der in deutschen Datenschutzgesetzen verwendeten Formulierung der *Speicherung der verarbeiteten Daten in einer Datei*. Die DS-RL fand, in anderen Worten, auf jede Verarbeitung personenbezogener Daten Anwendung – unabhängig davon, ob es sich dabei um eine automatisierte, teilautomatisierte oder vollständig manuelle Verarbeitung handelt, sofern die dabei verarbeiteten Daten in einer Datei gespeichert sind oder gespeichert werden sollen (Art. 3 Abs. 1) (Simitis 2001, 125 f.).[125] Damit wiederum nicht jede manuelle Verarbeitung personenbezogener Daten (so etwa das Führen eines Tagebuchs oder eines Notizbüchleins) in den Anwendungsbereich der Richtlinie fällt, bediente man sich des sog. Haushaltsprivilegs aus dem britischen und niederländischen Datenschutzrecht, wonach die Richtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten findet, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird (Art. 3 Abs. 2) (Simitis 2001, 126). Die Definition eines personenbezogenen Datums umfasste in der DS-RL „alle Informationen über eine bestimmte oder bestimmbare natürliche Person […], die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer [sic] oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind" (Art. 2 lit. a). Damit spezifizierte die DS-RL einerseits gegenüber den vorherigen internationalen Datenschutz-Instrumenten in deutlichem Maße, was konkret unter einer bestimmten oder bestimmbaren natürlichen Person zu verstehen ist. Andererseits wurde der Anwendungsbereich zugleich auf natürliche Personen eingeengt, während die Datenschutz-Konvention die

125 Etwa die Strukturierung einer manuellen Sammlung personenbezogener Daten nach Namen (Simitis 2001, 126).

Entscheidung darüber, ob auch juristische Personen umfasst sein sollten, noch den Vertragsparteien überlassen hatte.[126]

Der räumliche Anwendungsbereich der DS-RL (Art. 4) gab den Mitgliedstaaten die Anwendung ihres nationalen Datenschutzrechts in drei Fällen vor. Sobald eine Verarbeitung:[127]

- Gemäß Art. 4 Abs. 1 lit. a im Rahmen der Tätigkeiten einer Niederlassung im eigenen Hoheitsgebiet,
- gemäß Art. 4 Abs. 1 lit. b durch Verantwortliche mit Niederlassungen an Orten außerhalb dieses Gebiets, an denen aber das nationale Recht gemäß völkerrechtlichen Regelungen anwendbar ist, sowie
- gemäß Art. 4 Abs. 1 lit. c durch Verantwortliche in Drittländern, wenn diese zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreifen, die im Hoheitsgebiet des Mitgliedstaats belegen sind, es sei denn, dass dies nur zum Zweck der Durchfuhr erfolgt.

In Art. 6 wurden die Verarbeitungsgrundsätze einschließlich der Grundsätze der Rechtmäßigkeit sowie der Verarbeitung nach Treu und Glauben (lit. a), Zweckbindung (lit. b), Datenminimierung (lit. c), Richtigkeit (lit. d) und Speicherbegrenzung (lit. e) festgelegt. Bis auf eine Einschränkung blieben die Verarbeitungsgrundsätze gegenüber der Datenschutz-Konvention unverändert. So kam auch in der DS-RL, wie schon in den OECD-Richtlinien und der Datenschutz-Konvention zuvor, der Zweckbindung eine zentrale Rolle zu, wonach eine Verarbeitung personenbezogener Daten nur dann als rechtmäßig einzustufen ist, wenn diese einem konkreten und zuvor festgelegten Zweck dient: „Präventive Datensammlungen im Hinblick auf künftige, noch nicht feststehende Aktivitäten scheiden infolgedessen ebenso aus wie Datendepots, die sich jederzeit für neue Ziele reaktivieren lassen." (Simitis 1997, 285) Allerdings wurde der entsprechende Artikel im Ergebnis der Ratsverhandlungen dahingehend abgeändert, dass die Weiterverarbeitung von personenbezogenen Daten *zu historischen, statistischen oder wissenschaftlichen Zwecken im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen sind, sofern die Mitgliedstaaten geeignete Garantien vorsehen.*

126 Zumindest auf EU-Ebene sollte die Nichtanwendung der Datenschutzgesetze auf juristische Personen fortan zum Standard werden und zu keinen weiteren nennenswerten Kontroversen führen.

127 Die folgende Aufzählung ist in gekürzter Form übernommen aus: (Hornung 2019, 267 Rn. 5).

Art. 7 legte die Bedingungen für die Zulässigkeit einer Verarbeitung mit der Einwilligung gemäß Art. 7 lit. a als zentralem Bestandteil dar, die *ohne jeden Zweifel* zu erteilen war. Darüber hinaus konnte eine Verarbeitung auch dann als zulässig gelten, sofern sie gemäß Art. 7 lit. b für die Vertragserfüllung, gemäß lit. c für die Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen, gemäß lit. d für die Wahrung lebenswichtiger Interessen des Betroffenen, gemäß lit. e für die Wahrnehmung einer Aufgabe im öffentlichen Interesse bzw. in Ausübung öffentlicher Gewalt oder gemäß lit. f zur Verwirklichung des berechtigten Interesses des Verantwortlichen erfolgt, sofern dieses nicht das Interesse oder die Grundrechte und Grundfreiheiten des Betroffenen überwiegt. Gegenüber der Datenschutz-Konvention ist an dieser Stelle eine deutliche Spezifizierung der Zulässigkeitsbedingungen sowie eine relative Steigerung der Selbstbestimmungsfähigkeit der von einer Datenverarbeitung betroffenen Individuen festzustellen (Battcock 1995, 162 f.). Die von der Kommission beabsichtigte Einführung einer ausdrücklichen Einwilligung, die ein höheres Schutzniveau geboten hätte, hatte sich in den Verhandlungen allerdings nicht durchsetzen können.

In Art. 8 wurden die Vorgaben zu besonderen Kategorien personenbezogener Daten dargelegt. Demnach wird zunächst gemäß Art. 8 Abs. 1 die Verarbeitung jener personenbezogenen Daten untersagt, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über die Gesundheit oder das Sexualleben.[128] Abweichend von Abs. 1 kann eine Verarbeitung allerdings gemäß Art. 8 Abs. 2 in jenen Fällen erfolgen, in denen (lit. a) der Betroffene in eine Verarbeitung *ausdrücklich* einwilligt, (lit. b) die Verarbeitung erforderlich ist, um den arbeitsrechtlichen Pflichten des Verantwortlichen unter Vorsehung angemessener Garantien Rechnung zu tragen, (lit. c) die Verarbeitung zum Schutz lebenswichtiger Interesse des Betroffenen oder eines Dritten erforderlich ist, (lit. d) die Verarbeitung unter Wahrung angemessener Garantien seitens einer politisch, philosophisch oder gewerkschaftlich ausgerichteten nicht-kommerziellen Organisation erfolgt, oder (lit. e) die Verarbeitung auf Daten bezogen ist, die offenkundig seitens des Betroffenen öffentlich gemacht wurden. Grundsätzlich ausgenommen von den Vorga-

128 Die Auflistung entspricht im Wesentlichen jener der Datenschutz-Konvention. Abweichend ist in der DS-RL zusätzlich die Gewerkschaftszugehörigkeit benannt, während die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, in Art. 8 Abs. 5 DS-RL geregelt wird.

ben des Absatzes 1 waren zum einen (gemäß Art. 8 Abs. 3) Verarbeitungen, die zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erfolgen, und zum anderen (gemäß Art. 8 Abs. 4) Verarbeitungen, die aus Gründen eines wichtigen öffentlichen Interesses erfolgen.

Die Transparenzvorgaben im Falle der Erhebung beim Betroffenen selbst (Art. 10) und in jenen Fällen, in denen die Daten nicht bei dem Betroffenen erhoben wurden (Art. 11) spiegeln den Anspruch der DS-RL wider, die Kontrolle des Betroffenen über die Verarbeitung der ihn betreffenden Daten zu gewährleisten. Hinzu kommen die Betroffenenrechte in Form des Auskunftsrechts (Art. 12 lit. a), des Rechts auf Berichtigung, Löschung oder Sperrung (Art. 12 lit. b) und des Widerspruchsrechts (Art. 14). Das Auskunftsrecht sah vor, dass der Betroffene *in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten*[129] die Existenz einer sie betreffenden Datenverarbeitung, den Zweck der Verarbeitung, die Kategorien verarbeiteter Daten sowie die Empfänger oder Kategorien der Empfänger der Daten in Erfahrung bringen durfte. Art. 12 lit. c sah wiederum abweichend von den vorherigen internationalen Instrumenten vor, dass jede Berichtigung, Löschung oder Sperrung gemäß Art. 12 lit. b den Dritten, denen die Daten seitens des Verantwortlichen übermittelt wurden, mitzuteilen ist, *sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.* Art. 13 widmete sich den nationalen Freiräumen im Hinblick auf Ausnahmen und die Einschränkung der Transparenzvorgaben in den Artikeln 10 und 11 sowie die Betroffenenrechte in Art. 12.[130]

Art. 15 Abs. 1 sah schließlich das Verbot vollständig automatisierter Entscheidungen vor, die zum Zwecke der Bewertung einzelner Aspekte einer Person, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens erfolgen. Abweichend konnten Betroffene einer der in Art. 15 Abs. 1 genannten Entscheidungen gemäß Art. 15 Abs. 2 lit. a unterworfen werden, wenn diese der

129 Insofern entsprachen die Rahmenbedingungen betreffend die Dauer und Kosten des Auskunftsrechts jenen der Datenschutz-Konvention (vgl. Art. 8 lit. b).

130 Art. 13 Abs. 2 eröffnete den Mitgliedstaaten die Möglichkeit der Einschränkung der Betroffenenrechte sofern die Verarbeitung ausschließlich für Zwecke der wissenschaftlichen Forschung oder zur Erstellung von Statistiken erfolgt. Dieser Absatz war Ergebnis des zuvor genannten Kompromisses, der mit Dänemark erzielt wurde (González Fuster 2014, 138).

Vertragserfüllung dient und auf dem Ersuchen des Betroffenen basiert oder die berechtigten Interessen des Betroffenen, beispielsweise durch die Möglichkeit, seinen Standpunkt geltend zu machen, gewahrt werden. Art. 15 Abs. 2 lit. b sah die Zulässigkeit derartiger Entscheidungen zudem auch im Falle gesetzlicher Bestimmungen vor, sofern darin Garantien zur Wahrung der berechtigten Interessen des Betroffenen festgelegt wurden.

Die Art. 16 und 17 legten die Verarbeiterpflichten in Bezug auf die Vertraulichkeit bzw. die Sicherheit der Verarbeitung nieder. Art. 18 Abs. 1 regelte die Pflicht des Verarbeiters zur Meldung einer Verarbeitung bei der zuständigen Aufsichtsbehörde. Art. 18 Abs. 2 sah die Vereinfachung der bzw. die vollständige Ausnahme von der Meldepflicht seitens einzelner Mitgliedstaaten vor allem dann vor, wenn die verantwortliche Stelle einen unternehmensinternen Datenschutzbeauftragten einbestellt.

Für Verarbeitungen, die gemäß mitgliedstaatlicher Vorgaben spezifische Risiken für die Rechte und Freiheiten der Betroffenen beinhalten, sah Art. 20 die Möglichkeit der Vorabkontrolle seitens der Aufsichtsbehörde oder des unternehmensinternen Datenschutzbeauftragen zum Zwecke der Eindämmung der Risiken vor.

Rechtsbehelfe, Haftung und Sanktionen wurden in den Artikeln 22, 23 respektive 24 behandelt, machten den Mitgliedstaaten außer der Verpflichtung zur Schaffung der entsprechenden Strukturen allerdings keine weitergehenden Vorgaben zu den Details der Umsetzung.

In den Artikeln 25 und 26 wurden die bei der Übermittlung personenbezogener Daten in Drittländer zu beachtenden Grundsätze bzw. Ausnahmen dargelegt. Das im ursprünglichen Richtlinienvorschlag vorgesehene, vor allem auf einer durch die Kommission auszustellenden Genehmigung auf Basis der Evaluierung staatsrechtlicher Garantien basierende Übertragungsprinzip in Drittstaaten musste im Ergebnis des politischen Aushandlungsprozesses einem *flexibleren* Verfahren weichen. Die in den überarbeiteten Richtlinienvorschlag der Kommission integrierten Erleichterungen im Hinblick darauf, dass auch die in einem Drittland geltenden Standesregeln bei der Beurteilung der Angemessenheit berücksichtigt werden können und dass der Datentransfer in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, auch mit der Einwilligung des Betroffenen (nunmehr Art. 26 Abs. 1 lit. a), bei Erforderlichkeit im Hinblick auf die Erfüllung eines Vertrags und für die Wahrung eines wichtigen öffentlichen Interesses (nunmehr Art. 26 Abs. 1 lit. d) oder lebenswichtiger Interessen des Betroffenen (Art. 26 Abs. 1 lit. e) erfolgen kann, blieben in der Richtlinie enthalten, wurden allerdings teilweise ausgeweitet. So wurde der Punkt hinsichtlich

der Erfüllung eines Vertrags dahingehend erweitert, dass er gemäß Art. 26 Abs. 1 lit. b die Bedingungen für die Erfüllung eines Vertrags zwischen dem Betroffenen und dem Verantwortlichen und gemäß Art. 26 Abs. 1 lit. c die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags, der im Interesse des Betroffenen mit einem Dritten geschlossen wurde, vorsah. Schließlich kam als letzter Punkt hinzu, dass der Datentransfer auch dann stattfinden darf, wenn die Übermittlung aus einem Register erfolgt, dessen Inhalt ohnehin der Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, offen steht. Ebenso bedeutend waren die Entmachtung der Kommission im Rahmen des Ausschussverfahrens gemäß Art. 31 (der beratende Ausschuss gemäß Art. 30 DS-RL-UE) sowie die Ausweitung mitgliedstaatlicher Freiräume bei der Genehmigung eines Transfers seitens eines einzelnen Mitgliedstaates. Während in den nicht-finalen Richtlinienfassungen noch vorgesehen war, dass die Kommission relativ eigenständig und lediglich unter der optionalen Hinzuziehung der Meinung der Mitgliedstaaten über die Angemessenheit von Drittstaaten befinden können sollte, sah die finale DS-RL nunmehr vor, dass die Angemessenheit gemäß dem in Art. 31 geregelten Ausschussverfahren ausschließlich seitens mitgliedstaatlicher Vertreter entschieden werden sollte. In ähnlich radikaler Weise wurden auch die Vorgaben hinsichtlich der Genehmigung eines Transfers in einen Drittstaat seitens eines einzelnen Mitgliedstaates im Laufe des politischen Aushandlungsprozesses abgeändert. Während der ursprüngliche Richtlinienentwurf (Art. 25 DS-RL-UE) noch vorgesehen hatte, dass ein solcher Transfer nur nach Ablauf einer zehntägigen Frist ab dem Moment der Meldung des geplanten Transfers an Kommission und Mitgliedstaaten und sofern diese keinen Widerspruch erheben, erfolgen durfte, wurden die Vorgaben zunächst bereits im überarbeiteten Richtlinienentwurf flexibler gehandhabt. So wich die Zehntagesfrist im überarbeiteten Richtlinienentwurf (Art. 27 DS-RL-ÜE) der Vorgabe, dass die Unterrichtung lediglich *rechtzeitig* vor Wirksamwerden der Genehmigung erfolgen musste, damit die Kommission und Mitgliedstaaten noch vor Wirksamwerden Widerspruch einlegen können. In der DS-RL wurde schließlich nur noch vorgesehen, dass eine Unterrichtung überhaut erfolgen muss, der Zeitpunkt dieser wurde jedoch vollständig dem jeweiligen Mitgliedstaat überlassen, sodass die ursprünglich vorgesehene Interventionsmöglichkeit praktisch nicht mehr vorhanden war. Schließlich hatte auch die Abänderung des Ausschussverfahrens weitreichende Bedeutung für Drittstaatentransfers. Während gemäß den ersten beiden Fassungen der DS-RL (Art. 30 DS-RL-UE bzw. Art. 34 DS-RL-ÜE) auf einen Widerspruch

der Kommission oder der Mitgliedstaaten hin im beratenden Ausschuss die Kommission die Entscheidungsbefugnis innegehabt hätte, sah die finale DS-RL gemäß Art. 31 vor, dass bei strittigen Genehmigungen ausschließlich mitgliedstaatliche Vertreter in Entscheidungsverantwortung waren.

In Art. 27 wurde die Möglichkeit dargelegt, Verhaltensregeln auszuarbeiten. Die im ursprünglichen Entwurf (Art. 20 DS-RL-UE) noch sehr rudimentären und vor allem lediglich auf die Gemeinschaftsebene bezogenen Vorgaben waren bereits im überarbeiteten Richtlinienentwurf (Art. 28 und 29 DS-RL-ÜE) deutlich ausgeweitet worden. Nach Art. 28 sollten nationale Verhaltensregeln durch Interessenverbände ausgearbeitet, durch die zuständige nationale Aufsichtsbehörde auf ihre Verträglichkeit mit der DS-RL hin geprüft und gegebenenfalls genehmigt und durch die nächstzuständige mitgliedstaatliche Stelle amtlich veröffentlicht werden. Art. 29 DS-RL-ÜE sah allerdings abweichend von den vorgenannten Bestimmungen vor, dass die Kommission dazu befugt sein sollte, auch solche gemeinschaftlichen Verhaltensregeln zu veröffentlichen, die von der in Art. 31 DS-RL-ÜE genannten Gruppe (der späteren Art. 29-Datenschutzgruppe) nicht positiv bewertet wurden. In der finalen DS-RL wurde schließlich auch diese Befugnis der Kommission gestrichen und dem mitgliedstaatlichen Verfahren angeglichen. Nach Art. 27 Abs. 3 konnte die Kommission nämlich nur noch jene Verhaltensregeln veröffentlichen, zu denen die Art. 29-Datenschutzgruppe eine positive Stellungnahme abgegeben hatte. Am Ende des politischen Aushandlungsprozesses konnte sich der nördliche Block mit seiner Forderung, die gemeinschaftlichen Datenschutzregelungen grundsätzlich auf dem Prinzip der (regulierten) Selbtsregulierung fußen zu lassen, somit nicht durchsetzen. Verhaltensregeln stellten zwar ein zentrales Element von auf Selbstregulierung fußenden Gesetzen dar, doch kam ihnen in der DS-RL eine lediglich komplementäre und nicht die von den Richtliniengegnern gewünschte staatliche Regulierung substituierende Rolle zu (Simitis 2001, 109 f.).

Dem Regulierungsziel der Richtlinie, die Verarbeitung personenbezogener Daten an Bedingungen und Pflichten (so z. B. insbesondere die Zweckbindung) zu knüpfen und die Einhaltung dieser durch externe Kontrollinstanzen umfassend und konsequent kontrollieren zu lassen, entsprechend (Simitis u. a. 2019, 196 Rn. 142), legten die Art. 28–30 DS-RL jene die Einrichtung der Kontrollinstanzen betreffenden Spezifika nieder. Nachdem bereits der überarbeitete Richtlinienentwurf den Wünschen der Aufsichtsbehörden hinsichtlich der Erweiterung ihrer Befugnisse deutlich entgegengekommen war, wurden die entsprechenden Befugnisse in der finalen DS-

RL noch weiter ausgebaut. So sah Art. 28 die Überwachung der Umsetzung der DS-RL durch die Aufsichtsbehörden in völliger Unabhängigkeit vor und Art. 28 Abs. 2 sah darüber hinaus auch explizit die Anhörung der Datenschutzbehörden bei der Ausarbeitung datenschutzpolitischer Maßnahmen vor. Art. 28 Abs. 3 eröffnete den Aufsichtsbehörden zudem die Möglichkeit der Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen und ging damit über das beispielsweise in Deutschland geltende Recht, das die Weiterreichung identifizierter Probleme an den Bundestag oder die Landtage bzw. die Mitteilung gegenüber der Öffentlichkeit in Form jährlicher Berichte vorsah, deutlich hinaus. Zudem erhielten Aufsichtsbehörden im Rahmen von Art. 28 Abs. 3 auch das Klagerecht für Verstöße gegen die im nationalen Recht umgesetzten Vorgaben der DS-RL und Verantwortliche im Gegenzug die Möglichkeit des Rechtswegs gegen Entscheidungen der Aufsichtsbehörden.

Die Fähigkeit zur Auslegung der Datenschutzregelungen seitens der einzelnen Aufsichtsbehörden wurde allerdings zugleich durch das Ziel der Harmonisierung der europäischen Datenschutzgelungen beschränkt. Wichtigster Ausdruck dieses Ziels auf dem Gebiet des institutionellen Datenschutzes war die in Art. 29 festgeschriebene Entscheidung zur Gründung einer Datenschutzgruppe[131] – der sog. Art. 29-Datenschutzgruppe, die in den folgenden Jahrzehnten prägend für den europäischen Datenschutz werden sollte. Sie wurde insbesondere damit beauftragt, zu einer einheitlichen Anwendung der Richtlinie beizutragen (Art. 30 Abs. 1 lit. a), die Kommission hinsichtlich des Schutzniveaus in der EU und in Drittländern (Art. 30 Abs. 1 lit. b) sowie bei jedweder Erarbeitung datenschutzpolitischer Maßnahmen (Art. 30 Abs. 1 c) zu beraten. In Art. 30 Abs. 3 wurde zudem ausdrücklich anerkannt, dass die Datenschutzgruppe in eigener Initiative zu allen von ihr als wichtig bewerteten Fragen, die den Schutz personenbezogener Daten in der Gemeinschaft betreffen, Stellung nehmen können sollte.

Neben der Art. 29-Datenschutzgruppe, die sich der Harmonisierung der Datenschutzregeln widmen sollte, wurde im Rahmen von Art. 31 die Gründung eines weiteren Ausschusses zur Verteidigung der Interessen der Mit-

131 Bestehend aus je einem Vertreter der nationalen Aufsichtsbehörden, einem Vertreter der für die Datenschutzaufsicht über die Unionsorgane zuständigen Behörde und einem Vertreter der Europäischen Kommission (Art. 29 (2)).

gliedstaaten, bestehend aus je einem Vertreter eines jeden Mitgliedstaates und einem Vertreter der Europäischen Kommission, vorgesehen.[132]

Für die Umsetzung der Richtlinienvorgaben in nationales Recht wurde in Art. 32 eine Frist von drei Jahren nach ihrer Annahme vereinbart.

In Art. 33 wurde schließlich festgelegt, dass die Kommission dem Europäischen Parlament sowie dem Ministerrat regelmäßig, und erstmals sechs Jahre nach Annahme der Richtlinie einen Bericht über die Durchführung der Richtlinie und gegebenenfalls über notwendige Änderungsvorschläge vorzulegen hat.

3.2.2.8 Fazit: Bewertung der DS-RL

Gemessen an anderen damals in Kraft befindlichen Datenschutzgesetzen bzw. Datenschutz-Instrumenten können sowohl der 1990er-Richtlinienvorschlag als auch die letztendliche DS-RL sicherlich als innovativ gelten. Gemessen am Inhalt der damaligen europäischen Datenschutzgesetze stellten sie dagegen eher eine diffuse Konservierung bestehender Gesetze denn eine ernsthafte Weiterentwicklung dar (Simitis 1995, 451, 2001, 111). Dies hatte zwei Gründe. Zum *einen* war die Kommission sehr darum bemüht, für ihren Richtlinienvorschlag die Zustimmung möglichst vieler Mitgliedstaaten zu gewinnen. Folglich war der bestimmende Faktor der Richtliniengestaltung die Erhöhung der Wahrscheinlichkeit seiner Verabschiedung durch die eklektizistische Inkorporation möglichst vieler mitgliedstaatlicher Rechtselemente und nicht die Erarbeitung eines konsistenten und innovativen Datenschutzgesetzes (Simitis 1995, 2001). Viele unklare Formulierungen in der Richtlinien führten zudem bereits damals zu der Kritik, dass auf die Verabschiedung der Richtlinie *endlose Auslegungskontroversen* folgen würden (Simitis 2001, 130). Zum *anderen* führte aber auch die im politischen Prozess der EG angelegte Notwendigkeit der Erzielung von Kompromissen dazu, dass Möglichkeiten zur Weiterentwicklung und Harmonisierung der Richtlinie verspielt wurden. Letztlich versuchte die

132 Die Befürchtung, dass der Art. 31-Ausschuss die Gewährleistung des Schutzes personenbezogener Daten und die Weiterentwicklung bestehender Datenschutzregelungen in ähnlichem Maße behindern würde, wie der beratende Ausschuss der Datenschutz-Konvention, der seitens der Vertragsstaaten eher zur Rechtfertigung von Divergenzen und der Bekämpfung von Vorschlägen zur Weiterentwicklung der Datenschutzregelungen genutzt wurde, bewahrheitete sich immerhin nicht (Simitis 2001, 141).

Kommission, jeden Konflikt zu vermeiden, der aus ihrer Sicht die Verabschiedung der Richtlinie gefährdet hätte. Entsprechend wurden selbst in kritischen Fällen nationale Abweichungen von den Richtlinien-Vorgaben toleriert.[133] Die Unklarheit der Regelungen spiegelte somit den schwierigen Gesetzgebungsprozess aufgrund der unterschiedlichen Positionen der mitentscheidenden Instanzen, insb. im Rahmen des Ministerrats, wider (Simitis 2001, 112). Simitis attestierte daher: „Das mühsam zustandegekommene einheitliche Regelwerk droht wieder in seine nationalen Bestandteile zu zerfallen, die angestrebte ‚Harmonisierung' riskiert vollends zur Fiktion zu geraten." (Simitis 1997, 282 f.). Angesichts der sich anbahnenden Probleme hinsichtlich der Erreichung der angestrebten Harmonisierung legte die Kommission ihre Hoffnung schließlich in die Implementierung der Richtlinie (Simitis 2001, 111).

Das am Ende dominierende Verständnis zum Datenschutz war somit keines, das Datenschutz als Grundrecht betrachtete, sondern ein wirtschaftspolitischer Blick auf das Thema: Die DS-RL konnte nur verabschiedet werden, weil ansonsten der freie Verkehr personenbezogener Daten in der Gemeinschaft, oder besser, im gemeinsamen Binnenmarkt, gefährdet worden wäre (Simitis 1997, 282).

Die entscheidenden Akteure während der Aushandlung der Richtlinie waren die Mitgliedstaaten und letztlich waren es die unter den Mitgliedstaaten ausgefochtenen Konflikte, die entscheidenden Einfluss auf die Ausgestaltung der Richtlinie nehmen sollten. Unterstützt wurden die datenschutzkritischen Mitgliedstaaten sowohl von der europäischen als auch US-amerikanischen Wirtschaft. Während die Ablehnung auf Seiten von Mitgliedstaaten und Privatwirtschaft angesichts des Desinteresses, das diese Akteure in vorangegangenen Jahrzhenten an Gemeinschaftsregelungen zum Datenschutz gezeigt hatten, nicht verwunderte, tat es die Kritik am *zu hohen* Schutzniveau des ursprünglichen Richtlinienvorschlags, die von Seiten des Europäischen Parlaments kam, umso mehr. Als konsequente Vertreter eines hohen Datenschutzniveaus traten einzig die europäischen Datenschutzaufsichtsbehörden auf. Die Kommission war im Dilemma gefangen, einerseits ein hohes Schutzniveau zu befürworten und andererseits

133 Beispielhaft sei an dieser Stelle die Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 8 DS-RL genannt. Dieser verbietet im Rahmen des ersten Absatzes zunächst die Verarbeitung, schafft im zweiten Absatz allerdings dermaßen weitreichende nationale Ausnahmeregelungen, dass vom zuvor formulierten Verbot kaum etwas übrig bleibt (Simitis 2001, 112).

die Verabschiedung der Richtlinie durch Zugeständnisse gegenüber den Mitgliedstaaten und dem Parlament nicht zu gefährden.

Trotz der im Aushandlungsprozess vorgenommenen zahlreichen Senkungen des Schutzniveaus stellte die DS-RL 95/46/EG zum Zeitpunkt ihrer Verabschiedung das weitreichendste Datenschutzinstrument der Welt dar. Schließlich sollte die Richtlinie im Laufe der Jahre auch die Rolle der Datenschutz-Konvention ablösen und zum weltweit einflussreichsten Datenschutzinstrument aufsteigen (Greenleaf 2012; Raab und Bennett 2003).

Zu den markantesten Unterschieden der Richtlinie gegenüber der Konvention zählen die Stärkung der informationellen Selbstbestimmung der Betroffenen, die Einführung spezifischer Regelungen für Datentransfers in Drittstaaten, die Schaffung von Beschwerde- und Klagemöglichkeiten für Betroffene, die Einführung von Meldepflichten und gegebenenfalls der Vorabkontrolle von Verarbeitungen sowie die Beschränkung der automatisierten Verarbeitung personenbezogener Daten. Insbesondere mit der Verpflichtung der Mitgliedstaaten auf die Einrichtung einer Datenschutzaufsichtsbehörde und der Art. 29-Datenschutzgruppe ging der Richtlinienvorschlag weit über die Datenschutz-Konvention hinaus.

3.2.2.9 Implementierung der DS-RL in den Mitgliedstaaten

Der folgende Unterabschnitt widmet sich der Umsetzung der Vorgaben der Datenschutzrichtlinie 95/46/EG in nationales Recht. Fokussiert wird dabei vor allem die Einhaltung des zur Umsetzung vorgegebenen Zeitrahmens. Im Anschluss wird am Beispiel der Umsetzung in der BRD verdeutlicht, wie gering das Interesse an einer harmonisierten Umsetzung der DS-RL in einigen Mitgliedstaaten gewesen ist. Darauf, inwiefern sich diese Divergenz im Detail äußerte, wird an späterer Stelle (vgl. 3.3.3) eingegangen.

Die in der DS-RL vereinbarte Dreijahresfrist sah die Umsetzung der Richtlinienvorgaben in nationales Recht innerhalb von drei Jahren nach ihrer Annahme, also bis zum 24. Oktober 1998 vor. Doch sollte sich die EU-weite Implementierung der Richtlinie deutlich verzögern. Lediglich Italien, Griechenland, Großbritannien, Portugal und Schweden setzten die Richtlinienvorgaben innerhalb der vorgegebenen Frist um (vgl. grün markierte Mitgliedstaaten in Tabelle 3-4).[134] Belgien und Finnland folgten mit kurzer Verspätung im Dezember 1998 bzw. Mitte 1999. Österreich und Spanien

134 Von den fünf Mitgliedstaaten, die zu Beginn des politischen Aushandlungsprozesses der DS-RL noch über keine Datenschutzgesetze verfügten, hatten drei – Belgien,

setzten die Revision ihrer Datenschutzregelungen zum Jahresbeginn 2000 um, Dänemark Mitte 2000 (vgl. graumarkierte Mitgliedstaaten in Tabelle 3-4).

EG-Mitglieder (Stand: 2001)	Fristgemäße Umsetzung der Richtlinie	(Verabschiedung bzw.) Inkrafttreten der Implementierung	Notifikation an die Kommission
Belgien	Verzögert	11.12.1998	
BRD	Deutl. verzögert	23.05.2001	2001
Dänemark	Verzögert	01.07.2000	
Finnland	Verzögert	02.06.1999	
Frankreich	Deutl. verzögert	20.10.2005	2001
Griechenland	Fristgemäß	10.04.1997	
Irland	Deutl. verzögert	01.07.2003	2001
Italien	Fristgemäß	08.05.1997	
Luxemburg	Deutl. verzögert	01.12.2002	
Niederlande	Deutl. verzögert	01.09.2001	2001
Österreich	Verzögert	01.01.2000	
Portugal	Fristgemäß	27.10.1998	
Schweden	Fristgemäß	24.10.1998	
Spanien	Verzögert	14.01.2000	
Verein. Königreich	Fristgemäß	(16.07.1998) 01.03.2000[135]	

Tabelle 3-4: Implementierung der DS-RL in den Mitgliedstaaten (Commission of the European Communities 2003, 3; European Commission 2005; Korff 2002, 1)

Schwieriger gestaltete sich die Umsetzung hingegen in Deutschland, Frankreich, Irland, Luxemburg sowie in den Niederlanden (vgl. dunkelgraumarkierte Mitgliedstaaten in Tabelle 3-4). Nachdem diese fünf Mitgliedstaaten auf die von der Kommission zuvor versandte Aufforderung nicht reagiert

Portugal und Spanien – bereits im Laufe der Verhandlungszeit entsprechende Gesetze erlassen. Lediglich Italien und Griechenland hatten zum Zeitpunkt der Verabschiedung der DS-RL noch immer überhaupt keine Datenschutzgesetze in Kraft. Die zum 1. Januar 1995 der Gemeinschaft beigetretenen Mitgliedstaaten Österreich und Schweden hatten bereits lange vor ihrem Beitritt Datenschutzgesetze erlassen. Das dritte Neumitglied Finnland erlies 1992 ein Datenschutzgesetz (vgl. auch Tabelle 3-1).

135 Die Novelle des Data Protection Act wurde zwar Mitte 1998 verabschiedet, die meisten Änderungen traten allerdings zum 1. März 2000 in Kraft.

hatten, beschloss die Kommission Ende 1999 die Initiierung von Vertragsverletzungsverfahren vor dem EuGH gemäß Art. 226 EG-Vertrag (Europäische Kommission 2000a) und leitete diese schließlich am 1. Dezember 2000 ein (Europäische Union 2001). Als Deutschland, Frankreich, die Niederlande und Irland daraufhin schließlich konkrete Schritte zur Richtlinienumsetzung ankündigten, zog die Kommission ihre gegen diese Staaten gerichtete Klage wieder zurück (Commission of the European Communities 2003, 3). Einzig Luxemburg wurde am 4. Oktober 2001 vom EuGH aufgrund der Nichtumsetzung der DS-RL verurteilt (ECJ 2001).

Gerade der Implementierungsprozess in Deutschland und Frankreich war sinnbildlich für die Ablehnung harmonisierter Richtlinienvorgaben. Beide Länder hatten ein großes Interesse daran, den mitgliedstaatlichen Entscheidungsspielraum dahingehend zu nutzen, ihre nationalen Regelungen so weit es geht beizubehalten. Am Beispiel der Richtlinienumsetzung in Deutschland soll dies im Folgenden verdeutlicht werden: So hatte die Regierungskoalition aus CDU/CSU und der FDP (schwarz-gelbe Koalition) bereits die BDSG-Novelle des Jahres 1990 nicht dazu genutzt, ein effektives und modernes Datenschutzrecht zu entwickeln. Weder überzeugte die 1990er-Novelle im Hinblick auf die Harmonisierung von BDSG und den LDSG, noch nahm sie Rücksicht auf die informations- und kommunikationstechnologischen Veränderungen, die seit der vorherigen BDSG-Novelle im Jahr 1976 eine Anpassung der Regelungen erforderlich gemacht hatten (Simitis u. a. 2019, 173 ff.). Im Falle der Umsetzung der DS-RL wiederholte sich dieses Desinteresse. Nachdem die schwarz-gelbe Koalition weitgehend untätig geblieben war, beharrte das für die Novellierung des BDSG zuständige Bundesministerium des Innern (BMI) auch nach der im Jahr 1998 erfolgten Regierungsübernahme durch die rot-grüne Koalition bestehend aus SPD und Grünen auf der Position, dass geringfügige Änderungen des BDSG der Implementationsvorgabe bereits ausreichend Rechnung tragen würden. In der folgenden Debatte auf Grundlage des BDSG-Entwurfs vom 11. März 1999 waren vor allem sicherheitspolitische Bedenken im Hinblick auf die vorgesehenen Regelungen zur Videoüberwachung, die Kritik der Datenschutzbeauftragten am vorgeschlagenen Datenschutzaudit sowie die Kritik der Länder an der Übertragung der Überwachungsaufgaben an eine einzige, unabhängige Instanz dominant. Nachdem die Kommission das Vertragsverletzungsverfahren gegen Deutschland und die übrigen Staaten initiiert hatte, entschied sich das BMI für einen Strategiewechsel: „Auf eine erste mehr oder weniger ausschließlich der Anpassung an die EG-Vorga-

ben gewidmete Novellierungsstufe sollte möglichst bald eine zweite Phase folgen, deren Ziel eine konsequente Modernisierung des Datenschutzes sein müsste" (Simitis u. a. 2019, 177 Rn. 64). Dem in der Folge mit der Stimmenmehrheit von SPD und Grünen (CDU/CSU sowie FDP enthielten sich, während die PDS dagegen stimmte) unter Zeitdruck am 6. April 2001 verabschiedeten „Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze", das am 22. Mai 2001 in Kraft trat, fehlte es an einem Mindestmaß an Verständlichkeit, Lesbarkeit und Normenklarheit. Positiv gegenüber der 1990er-Novelle war lediglich etwa die Verbesserung der Rechte des BfDI hervorzuheben, doch wurde die Gewährleistung von dessen Unabhängigkeit entgegen den Richtlinienvorgaben nicht angegangen.[136]

3.2.3 Drittstaatentransfers und Safe Harbor-Vereinbarung

Nachdem die Datenschutzrichtlinie 95/46/EG verabschiedet worden war und während noch die ersten Umsetzungen in nationales Recht erfolgten, richtete sich das Augenmerk in der zweiten Hälfte der 1990er wieder auf das Thema der Drittstaatentransfers. Dieses war mit der Richtlinienverabschiedung der nationalen Datenschutzpolitik weitgehend enthoben worden. Stattdessen sollten Transfers in Drittstaaten fortan ausschließlich auf Basis der Art. 25 und 26 DS-RL erfolgen.

Ursprünglich hatten die Kommission und die Datenschutzbeauftragten intendiert, dass ein solcher Transfer grundsätzlich nur auf Basis eines Angemessenheitsbefundes der Kommission (Art. 25) erfolgen darf. Am Ende der Verhandlungen zur DS-RL erfuhr diese Regel jedoch eine Erweiterung um zahlreiche Alternativen, z. B. die Übertragung auf Basis der Einwilligung des Betroffenen, bei Erforderlichkeit im Hinblick auf die Erfüllung eines Vertrags, für die Wahrung eines wichtigen öffentlichen Interesses oder lebenswichtiger Interessen oder im Falle der Übermittlung aus einem öffentlichen Register (Art. 26 Abs. 1 lit. a bis f). Daneben sah Art. 26 Abs. 2 die Möglichkeit eines Datentransfers in einen Drittstaat, der kein angemessenes Schutzniveau im Sinne von Art. 25 gewährleistet, auf Basis der Genehmigung eines Mitgliedstaates vor, sofern der für eine Verarbeitung Verantwortliche, trotz des Fehlens staatlicher Datenschutzvorgaben, selbst ausreichende Datenschutzgarantien einräumt. Gerade die Datenschutzauf-

136 Für eine umfassendere Diskussion von Verbesserungen und Schwachstellen, siehe: (Simitis u. a. 2019, 177 Rn. 66)

sichtsbehörden bestanden bei der Umsetzung jedoch darauf, dass die *Ausnahme*regelungen tatsächlich als solche interpretiert und nicht zum Regelfall würden (Simitis 2001, 120). Der damalige stellvertretende Berliner Datenschutzbeauftragte Alexander Dix äußerte beispielsweise im Zusammenhang mit dem auf Basis einer Vertragslösung erfolgenden Datentransfer zwischen der Deutschen Bahn und der US-amerikanischen Citibank, dass die Festlegung vertraglicher Normen seitens privater Unternehmen die nationale Gesetzgebung in einem Drittstaat lediglich ergänzen und unterstützen, aber nicht ersetzen könnte (Dix 1996). Nach der Verabschiedung der DS-RL waren daher Drittstaaten, die ein Handelsinteresse mit der Europäischen Gemeinschaft hatten, das die Verarbeitung personenbezogener Daten tangierte, gefordert, ein angemessenes Datenschutzniveau zu garantieren oder in Kauf zu nehmen, dass die EG Datentransfers in diese Staaten blockierte. Verschiedene Staaten unternahmen in der Folge Anstrengungen, um ihre Datenschutzregelungen an die DS-RL anzupassen. Insofern wirkte die DS-RL, wie schon zuvor die Datenschutz-Konvention des Europarats, durchaus als internationale Normgeberin.[137]

Als besonders kompliziert sollte sich die Feststellung der Angemessenheit in Bezug auf die Vereinigten Staaten, den Haupthandelspartner der Europäischen Gemeinschaft bzw. seiner Mitgliedstaaten, erweisen. Die Regulierung des Schutzes personenbezogener Daten basierte in den Vereinigten Staaten Ende der 1990er-Jahre noch immer auf sektoralen Datenschutzgesetzen. Für die Mehrheit der Sektoren, in denen personenbezogene Daten verarbeitet werden, so insbesondere im Bereich des für grenzüberschreitende Datentransfers relevanten E-Commerce, galt hingegen ein auf Selbstregulierung gestützter Regulierungsansatz.[138] So sollte der individuelle Datenschutz vor allem durch das Vertrauen auf Zertifizierungsstellen

137 So passten sich etwa die im Jahr 2000 verabschiedeten Neufassungen der norwegischen und isländischen Datenschutzgesetze der DS-RL an. Auch der Europarat bemühte sich bei seinen Beratungen über neue Empfehlungen, der DS-RL Rechnung zu tragen. Schließlich trug auch die Prüfung und Feststellung der Angemessenheit des Datenschutzes in Drittstaaten zur internationalen Durchsetzung der europäischen Datenschutzstandards bei. Folgende Angemessenheitsbefunde stellte die Kommission aus: Schweiz 2000, Kanada 2002, Argentinien 2003, Israel 2011, Uruguay 2012, Neuseeland 2013 (Simitis u. a. 2019, 183 Rn. 89 und Fn. 231).

138 Zuletzt hatte das 1997 veröffentlichte *Framework for Global Electronic Commerce* der Clinton-Administration diesem Ansatz zusätzlich Nachdruck verliehen und dazu beigetragen, Privatheit als Sache des Individuums aufzufassen, die als vertrauensbildende Maßnahme den Erfolg von E-Commerce garantieren sollte (Clinton und Gore Jr. 1997).

gewährleistet werden, indem Webseiten-Betreiber die Zertifizierung ihrer Webseite beantragen und Gütesiegel-Agenturen wie TRUSTe oder BBBOnline diese dann ausstellten. In strittigen Fällen sollten, ebenfalls auf Selbstregulierung fußende, alternative Streitschlichtungsverfahren (alternative dispute resolution mechanism – ADR) Abhilfe schaffen (A. Busch 2012a, 413–15; Farrell 2003, 277). Klar war, dass das Fehlen eines US-weit einheitlichen Datenschutzgesetzes und die mangelnde Bereitschaft auf Seiten der zuständigen US-Stellen in Bezug auf die Verabschiedung einheitlicher Datenschutzregelungen zu einem Problem im Zusammenhang mit Datentransfers in die Vereinigten Staaten werden würden. Die Situation erinnerte an die Anfangszeit der Verhandlungen zur DS-RL. Zu Beginn der Verhandlungen hatten US-amerikanische Datenschutzbefürworter darauf gedrängt, ein einheitliches Datenschutzgesetz in den USA auszuarbeiten, damit der transatlantische Datenverkehr weiterhin reibungslos stattfinden könnte. Insbesondere bestand die Hoffnung, dass die US-amerikanische datenverarbeitende Wirtschaft die Verabschiedung von US-Datenschutzgesetzen aus ihrem wirtschaftlichen Eigeninteresse heraus fördern würde, damit Datentransfers aus der EG auch weiterhin erfolgen könnten (Prisclla M. Regan 1993). Anstatt bei der eigenen Regierung zu lobbyieren, übten US-amerikanische Wirtschaftsvertreter allerdings gemeinsam mit ihren europäischen Verbündeten Druck auf die Europäischen Entscheider aus, um eine Lockerung der europäischen Vorgaben zu Drittstaatentransfers zu erreichen. Ihre Strategie hatte Erfolg und statt des strengeren Gleichwertigkeitserfordernisses hatte sich in den Verhandlungen das flexiblere Angemessenheitserfordernis durchgesetzt (Priscilla M. Regan 1999). In ähnlicher Weise stand in der Zeit nach der Verabschiedung der DS-RL die Frage im Raum, ob die Vereinigten Staaten zum Zwecke ungehinderter Wirtschaftsflüsse einheitliche Datenschutzregelungen in Erwägung ziehen würden (C. J. Bennett und Raab 1997). Doch wieder sollten sich Wirtschaftsinteressen gegenüber Datenschutzinteressen durchsetzen. Die zuständigen US-Regierungsstellen gingen noch bis in die erste Hälfte des Jahres 1998 hinein zunächst wie selbstverständlich davon aus, dass transatlantische Datentransfers auf Basis der in Art. 26 DS-RL festgelegten Ausnahmebedingungen möglich und einheitliche, gesetzliche Datenschutzvorschriften nicht nötig sein würden (A. Busch 2012a, 414). Ira Magaziner, in der Clinton-Administration zuständig für den Bereich E-Commerce, ging sogar so weit, die drohende Blockade von Datentransfers in die Vereinigten Staaten vor die Welthandelsorganisation zu bringen, mit der Begründung, dass diese ein nichttarifäres Handelshemmnis darstellen würden (Farrell 2004, 5 f.).

Die Europäische Kommission hatte zur selben Zeit zunächst zwei mögliche Szenarien zur Hand, mit denen ihr Ziel einer möglichst geringfügigen Beeinträchtigung des transatlantischen Datenverkehrs erreicht werden könnte. Erstens stand die Frage im Raum, ob der sektorspezifische Datenschutz in der Vereinigten Staaten als angemessen nach Art. 25 DS-RL bewertet werden könnte. Eine von der Europäischen Kommission beauftragte und von den beiden US-amerikanischen Datenschutz-Professoren Paul Schwartz und Joel Reidenberg erstellte Studie lieferte zwar keine klaren Antworten auf diese Frage, doch bestanden die zuständigen Kommissionsstellen trotzdem darauf, dass formelle gesetzliche Regelungen im Rahmen eines allgemeinen Datenschutzgesetzes erforderlich seien (A. Busch 2012a, 415; Priscilla M. Regan 2003, 272). Zweitens bestand gemäß Art. 25 DS-RL grundsätzlich die Möglichkeit, bei der Berücksichtigung der Angemessenheit eines Drittstaates auch die im jeweiligen Staat geltenden Standesregeln, also auf Selbstregulierung fußende Maßnahmen, zu berücksichtigen. Doch auch diese Möglichkeit musste ausgeschlossen werden, da die Datenschutzbehörden diese Möglichkeit, wie bereits erwähnt, vehement ablehnten (vgl. Dix 1996). Insofern waren beide Seiten gefordert, Verhandlungen aufzunehmen.

Die ersten informellen Gespräche wurden Ende 1997, also etwa ein Jahr vor Inkrafttreten der DS-RL aufgenommen. Während die Zuständigkeit für die Verhandlungen auf europäischer Seite bereits klar war,[139] kristallisierte ssie ich für die US-Seite erst nach einiger Verzögerung heraus. Schließlich übernahm David Aaron, Staatssekretär für internationalen Handel im US-Handelsministerium, die Verhandlungsführung (Farrell 2004, 6 f.). Zu Beginn der eigentlichen Verhandlungen Anfang 1998 verhärteten sich die Fronten zunächst noch weiter. Die EG-Seite verwies auf die geltenden Gemeinschaftsgesetze und beharrte folglich auf der Position, dass die Vereinigten Staaten entsprechende staatliche Regulierungen erlassen müssten, um einen Angemessenheitsbefund ausgestellt bekommen zu können. Die US-Seite dagegen zeigte keinerlei Interesse am Erlass umfassender Datenschutzregulierungen. Einerseits widersprach dies dem US-amerikanischen (Selbst-)Regulierungsansatz und andererseits wurden die Forderungen der Europäischen Gemeinschaft in der US-Regierung im Sinne einer interna-

139 Geführt wurden die Beratungen von dem britisch-stämmigen Leiter der Generaldirektion Binnenmarkt und Dienstleistungen (GD Markt), John Mogg, unter Hinzuziehung weiterer GDs, insbesondere der Generaldirektion Auswärtige Beziehungen (González Fuster 2014, 139).

tionalen Machtfrage als ein *Herumschubsen* wahrgenommen, dem man keinesfalls nachgeben würde. Stattdessen verlangten die US-amerikanischen Verhandlungsführer, dass die in den Vereinigten Staaten geltenden sektoriellen Datenschutzregulierungen und Selbstregulierungsmaßnahmen als angemessen beurteilt würden. In der Folge gerieten die Verhandlungen schließlich in einen Stillstand (Farrell 2003, 292, 2004, 7). Die Verhandlungsposition der Vereinigten Staaten litt zeitgleich unter der nur sehr schleppend verlaufenden Umsetzung selbstregulierter Zertifizierungsmaßnahmen. Selbst das erste, von TRUSTe unter Beteiligung großer Unternehmen initiierte, Gütesiegel-Programm, das deutlich laxere Datenschutz-Vorgaben für Webseiten enthielt, zu denen sich teilnehmende Unternehmen freiwillig verpflichten sollten, als die DS-RL sie in der EG vorschrieb, wurde nur von wenigen Unternehmen in Anspruch genommen. Dies gab der europäischen Position Auftrieb und untermauerte den Anspruch der EG, dass für einen wirksamen Schutz personenbezogener Daten verbindliche Regelungen vonnöten waren. Zugleich übten Datenschutzbefürworter in den USA Druck auf Regierungsstellen aus, um den Datenschutz bei E-Commerce-Transaktionen zu gewährleisten. Die Drohkulisse der DS-RL wurde von diesen Datenschutzbefürwortern zur Untermauerung ihres Arguments genutzt. Erst als zu Beginn des Jahres 1998 zunehmend klarer wurde, dass mit dem Inkrafttreten der DS-RL ernsthafte Konsequenzen für die Geschäftspraktiken US-amerikanischer Unternehmen drohten, regte sich die zuständige US-Administration. Unter Androhung des Erlasses verbindlicher staatlicher Regulierungen erhöhten Politiker wie Ira Magaziner den Druck auf Unternehmen zur Inanspruchnahme von E-Commerce-Gütesiegeln. In der Folge nahm die Mitgliederzahl von TRUSTe bis Mitte 1998 rapide zu. Da die US-Administration befürchtete, dass diese Maßnahme nicht ausreichend sein würde, bewegte sie gemeinsam mit Unternehmensvertretern die anerkannte Selbstregulierungsorganisation Better Business Bureau (BBB) dazu, ein Datenschutz-Gütesiegel-Programm aufzusetzen. Nach anfänglichem Widerstand bei der BBB wurde nach der Zusicherung finanzieller Mittel das auf Online-Streitschlichtungen spezialisierte BBBOnline ins Leben gerufen (Farrell 2003, 291). Diese Fortschritte wirkten auf Seiten der EU nur wenig überzeugend. In der Folge blieben beide Seiten bei ihrer jeweiligen Maximalforderung der Anerkennung ihres Regulierungsmodells, sodass der Verhandlungsstillstand zunächst erhalten blieb (ebd.).

Eine Überwindung bahnte sich erst mit dem von David Aaron eingebrachten Vorschlag für einen sog. *Safe Harbor* an. Demnach sollten

zwischen der EG und den USA eine Reihe von Prinzipien ausgehandelt werden, zu deren Einhaltung sich US-Unternehmen, die ein Interesse an transatlantischen Datentransfers haben, verpflichten können sollten. Diese im Rahmen des Safe Harbor-Abkommens festgelegten Prinzipien sollten schließlich seitens der Europäischen Kommission als angemessen im Sinne der DS-RL anerkannt werden. Der grundlegenden Idee nach würden weder die Vereinigten Staaten ihr auf Selbstregulierung fußendes Regime ändern müssen, noch müsste die Europäische Gemeinschaft auf zentrale datenschutzrechtliche Bestandteile verzichten (A. Busch 2012a, 416 f. Farrell 2003, 291–93). Am 4. November 1998 legte Aaron schließlich einen ersten Entwurf für Safe Harbor-Prinzipien vor und rief US-Wirtschaftsvertreter dazu auf, diesen zu kommentieren. Die vorgeschlagenen Prinzipien waren Ausfluss der in den Vereinigten Staaten unter dem Namen *Fair Information Practices* bekannten Datenschutzprinzipien, die im Grundsatz auch in den von den Vereinigten Staaten angenommenen OECD-Richtlinien enthalten waren. Die sieben Prinzipien umfassten: Informationspflichten der Verarbeiter, Wahlmöglichkeiten der Betroffenen, Weitergabe verarbeiteter personenbezogener Daten, Datensicherheit, Datenintegrität/Zweckbindung, Auskunftsrechte der Betroffenen und schließlich das Thema der Durchsetzung. Der anderthalb Jahre andauernde und vier Phasen umfassende Konsultationsprozess auf US-Seite war insbesondere in den ersten zwei Phasen klar von Wirtschaftsinteressen dominiert, die für die Absenkung des in den Safe Harbor-Prinzipien vorgesehenen Schutzniveaus eintraten. Bürgerrechtliche Akteure brachten sich erst in den letzten beiden Phasen ein, konnten jedoch die Abschwächung der Vorgaben zu diesem späten Zeitpunkt nicht mehr verhindern (Priscilla M. Regan 2003, 273).

Während eine Einigung zwischen den Verhandlungsführern auf US- und EG-Seite im Hinblick auf die ersten sechs Themen im Laufe des Jahres 1999 noch vergleichsweise einfach möglich war, gestalteten sich die Diskussionen um das Thema der Durchsetzung als mühevoll. Insbesondere die mitgliedstaatlichen Vertreter der sozialdemokratischen Regierungen Deutschlands und Frankreichs lehnten die Idee eines Safe Harbor-Abkommens bzw. einer auf Selbstregulierung fußenden Lösung grundsätzlich ab. Ein Durchbruch bei den Verhandlungen konnte schließlich erst erzielt werden, als die europäische Verhandlungsdelegation im Januar 2000 nach Washington, D. C. eingeladen wurde und dort im Rahmen eines dreitägigen Workshops die Möglichkeit erhielt, mit den Vertretern der Selbstregulierungsstellen in einen direkten Dialog zu treten. Beobachtern zufolge habe dieser Diskurs

schließlich auch die letzten Skeptiker in den Mitgliedstaatsdelegationen davon überzeugen können, dass ein wirksamer Datenschutz auch auf Basis von Selbstregulierung gewährleistet werden könnte. In der Folge konnten die Verhandlungsparteien eine erste informelle Übereinkunft im März 2000 treffen. Am 9. Juni 2000 übermittelte das US-Handelsministerium schließlich die ausgehandelten Safe Harbor-Prinzipien an die Europäische Kommission. Wie üblich, begann das Europäische Parlament nach Erhalt des Kommissionsentwurfs eine Stellungnahme zu erarbeiten und überstellte den Entwurf des Safe Harbor-Abkommens zu diesem Zweck an den LIBE-Ausschuss. Der Bericht der italienisch-stämmigen sozialdemokratischen Europaabgeordneten Elena Ornella Paciotti (SPE, DS) wurde am 21. Juni zunächst vom Ausschuss mit 21 Stimmen (bei 0 Gegenstimmen und 16 Enthaltungen) angenommen und am darauffolgenden Tag schließlich auch vom Parlamentsplenum verabschiedet (Paciotti 2000, 4). Das Parlament bemängelte dabei jedoch nicht nur die konkreten Inhalte des Abkommens (etwa die unzureichende Ausgestaltung der Wahrnehmung von Betroffenenrechten) (ebd., 10, Nr. 7), sondern verwies auch auf folgende drei Aspekte: *Erstens* wurde in Bezug auf die Umsetzung des Safe Harbor-Abkommens in den Vereinigten Staaten grundsätzlich bemängelt, dass bislang lediglich Versprechungen gemacht worden seien, das im Safe Harbor-Abkommen versprochene System allerdings in der Realität nicht ansatzweise praktiziert werde. Insofern sei es fraglich, wie die EG-Verhandlungsführer realistischerweise davon ausgehen könnten, dass in einem Staat bzw. Unternehmen parallel zwei Datenschutzsysteme nebeneinander existieren könnten. Schließlich sollten sich US-amerikanische Unternehmen gemäß Safe Harbor dazu verpflichten, Bürgerinnen und Bürger der Europäischen Union anders zu behandeln als Menschen US-amerikanischer oder sonstiger Nationalität, was eine parallele Datenbankstruktur und viele weitere Maßnahmen erforderlich gemacht hätte (ebd., 9 f., Nr. 2 und 7). *Zweitens* wurde unter Verweis auf die in den Vereinigten Staaten geführten Konsultationen bemängelt, dass die Kommission während der Verhandlungen keine europäischen Unternehmen und Nichtregierungsorganisationen konsultiert hatte (ebd., 10, Nr. 4 und 5). Und *drittens* wurde in Bezug auf die europäischen Unternehmen festgestellt, dass der Abschluss des Safe Harbor-Abkommens zu einem offensichtlichen Wettbewerbsnachteil für diese führe, da somit US-amerikanische datenverarbeitende Unternehmen die Daten europäischer Bürgerinnen und Bürger auf Grundlage weniger

strenger Datenschutzregeln verarbeiten dürften als es den europäischen Unternehmen erlaubt war (ebd., 10, Nr. 4).[140]

Trotz der weitreichenden Kritik entschied die Art. 31-Gruppe letztlich einstimmig über die Angemessenheit des Safe Harbor-Abkommens (Farrell 2003, 294). Am 26. Juli 2000 befand die Kommission schließlich über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" gewährleisteten Schutzes, sodass das Safe Harbor-Abkommen am 1. November 2000 in Kraft trat (EU-Kommission 2000a).

Die Beurteilung des Abkommens war in den Folgejahren gespalten. So betonten einige Beobachter, dass die Safe Harbor-Einigung demonstriert hätte, dass auf Grundlage von Deliberation und geteilten sozialen Normen die Überwindung einer zwischenzeitlich als ausweglos geltenden Situation möglich geworden war, ohne dass eine Seite ihre Interessen einseitig durchsetzen konnte oder es zu einer Blockade oder einem Handelskonflikt kam. Darauf aufbauend wurde sogar gemutmaßt, dass Safe Harbor als neues Regulierungsmodell auf die in den USA und der EU geltenden Regulierungssysteme rückwirken, diese also verändern würde und dass Safe Harbor als Modelllösung für künftige transatlantische Dispute im Bereich des Datenaustausch dienen würde (Farrell 2003; vgl. Long und Quek 2002). Andere Autoren waren dagegen deutlich skeptischer und verwiesen einerseits darauf, dass Safe Harbor nicht einfach eine Kompromisslösung gewesen sei, die beiden Seiten in gleichem Maße entgegenkommt, sondern vor allem der Wirtschaft weiterhin weitgehend freien Handlungsraum überlasse und die US-Perspektive sich letztlich durchgesetzt habe. Zudem wurde selbst angesichts der schwachen Safe Harbor-Vorgaben infrage gestellt, in welchem Maße sich die US-amerikanische Datenwirtschaft an diese halten würde (vgl. insb. Priscilla M. Regan 2003).[141]

140 In den Vereinigten Staaten erntete das Abkommen sowohl vonseiten der Wirtschaft als auch vonseiten der Bürgerrechtler Kritik. Vor allem die National Business Coalition on E-Commerce and Privacy, zu deren Mitgliedern General Electric, Home Depot und VISA USA zählten, veröffentlichte eine vernichtende Kritik an den Inhalten des Abkommens auf Grundlage der im März 2000 erfolgten informellen Einigung (National Business Coalition 2000). Die bürgerrechtlichen Kritiker dagegen verwiesen auf das Scheitern das Selbstregulierungsmodells in den Vereinigten Staaten und vertraten konsequenterweise die Ansicht, dass es auch im Falle des Safe Harbor keinen wirksamen Datenschutz gewährleisten würde (TACD 2000).

141 Die letztgenannte Perspektive sollte Recht behalten: Das Abkommen wurde 2015 vom EuGH gekippt (vgl. auch Fn. 405).

3.2.4 ISDN-RL 97/66/EG

Gemeinsam mit dem Legislativvorschlag für die DS-RL hatte die Kommission 1990 auch einen *Richtlinienvorschlag zum Schutz personenbezogener Daten und der Privatheit im Telekommunikationsbereich* auf Grundlage des Kooperationsverfahrens veröffentlicht, der aufgrund der hitzigen Debatten um die DS-RL nur wenig Beachtung fand.

Die Erarbeitung der Richtlinie fand im Kontext der seit den 1980er-Jahren laufenden, gemeinschaftlichen Digitalisierungs- und Harmonisierungsbestrebungen sowie der Deregulierungspolitik im europäischen Telekommunikationsbereich statt, die zum 1. Januar 1998 wirksam wurde. Unter Bezugnahme auf die Hervorhebung der Bedeutung angemessener Maßnahmen zum Schutz personenbezogener Daten und der Privatheit im Lichte der technologischen Entwicklungen auf dem Gebiet der Telekommunikation seitens des Europäischen Parlaments und des Ministerrats sowie seitens der Datenschutzbehörden auf der Berliner Konferenz internationaler Datenschutzbeauftragter (Commission of the European Communities 1990, 8, Nr. 18), verfolgte der Richtlinienvorschlag zunächst das Ziel *der Harmonisierung der Vorschriften, die erforderlich sind, um einen gleichmäßigen Schutz der Privatsphäre in der gesamten Gemeinschaft zu gewährleisten und sowohl innerhalb der Mitgliedstaaten als auch grenzüberschreitend den freien Verkehr von Telekommunikationsgeräten und -diensten sicherzustellen* (Art. 1 Abs. 1 ISDN-RL UE). Mittels der Ausweitung bzw. Spezifizierung der in der Rahmenrichtlinie festzulegenden allgemeinen Datenschutz-Grundsätze im Sinne einer sektoralen Regulierung auf den Telekommunikationsbereich sollte auch im Zusammenhang mit der ISDN-RL „the fullest possible protection" (Commission of the European Communities 1990, 6, Nr. 13) erzielt werden. Dazu sollte in allen Mitgliedstaaten die Sicherheit[142] bzw. Vertraulichkeit von Telefongesprächen sichergestellt werden, das ungenehmigte Mithören bzw. die Speicherung von Telefongesprächen sowie neue

142 Die Regelung in Artikels 8 Abs. 1 des ursprünglichen Richtlinienentwurfs der Kommission sah die Gewährleistung eines dem Stand der Technik entsprechenden, angemessenen Schutzes personenbezogener Daten gegen unbefugten Zugriff und unbefugte Verwendung vor. Art. 8 Abs. 2 sah zudem die Benachrichtigung der Betroffenen seitens der Telekommunikationsorganisation im Falle eines besonderen Risikos der Verletzung der Netzsicherheit vor. Diese in Art. 4 der finalen ISDN-RL geregelte Vorschrift sollte später im Rahmen der Aushandlungen zur Novellierung der Nachfolgerrichtlinie der ISDN-RL, der ePrivacy-Richtlinie 2002/58/EG, zur Benachrichtigung im Falle einer Verletzung des Schutzes personenbezogener Daten ausgebaut werden (vgl. Unterabschnitt 3.3.2).

Techniken wie die Rufnummernübermittlung oder die Aufnahme in elektronische Verzeichnisse geregelt werden (Europäische Kommission 1990).

Gemeinsam mit seiner Stellungnahme zur DS-RL bewertete der Wirtschafts- und Sozialausschuss auch die für den Telekommunikationsbereich vorgesehene Richtlinie (WSA 1991, 45–47). Ebenso war auch die – ebenfalls unter Geoffrey Hoon ausgearbeitete – Parlamentsposition zur Telekommunikationsrichtlinie am 11. März 1992 gemeinsam mit Parlamentsposition zur DS-RL verabschiedet worden (Europäisches Parlament 1992).

Wie im Falle der DS-RL, unterbreitete die Kommission auch im Falle dieser Richtlinie bereits vor Beschluss des Gemeinsamen Standpunkts im Ministerrat einen geänderten Richtlinienvorschlag am 23. Juni 1994 *zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere in diensteintegrierenden digitalen Telekommunikationsnetzen (ISDN) und in digitalen Mobilfunknetzen* (Europäische Kommission 1994a).

Der Gemeinsame Standpunkt des Ministerrats in erster Lesung wurde am 12. September 1996 verabschiedet (Ministerrat 1996). Dem üblichen Mitentscheidungsverfahren gemäß verfolgten Ministerrat und Parlament das Ziel, am Ende der zweiten Lesung eine politische Übereinkunft zu erzielen. Zu dieser sollte es aber zunächst nicht kommen. Das Parlament bestätigte die Position des Ministerrats in seiner zweiten Lesung am 16. Januar 1997 nämlich nicht uneingeschränkt, sondern machte elf unter dem Rapporteur Medina Ortega ausgearbeitete Änderungsvorschläge geltend (Europäisches Parlament 1997a). Gefordert wurde zum einen eine bessere Gewährleistung der gemeinschaftsweiten Harmonisierung im Bereich der Telekommunikation bzw. störte sich das Parlament an den seitens des Ministerrats geforderten nationalen Freiräumen (vgl. Änd. 3 betreffend EG 7 des Gemeinsamen Standpunkts des Rats). Daneben plädierte das Parlament für die Wiedereinfügung des Rechts der Betroffenen, die Nichtaufnahme in ein Teilnehmerverzeichnis (z. B. Telefonbuch) kostenfrei beantragen zu können (vgl. Änd. 9 betreffend Art. 11 Abs. 2 des Gemeinsamen Standpunkts des Rats). Dieses war im überarbeiteten Entwurf der Kommission aus dem Jahr 1994 bereits enthalten gewesen, vom Ministerrat in seinem Gemeinsamen Standpunkt allerdings wieder gestrichen worden, indem den Betreibern von Telekommunikationsdiensten die Möglichkeit eröffnet wurde, dafür eine Gebühr zu verlangen. Zudem hatte das Parlament für die Ausweitung der Richtlinienregelungen auf juristische Personen plädiert, um „vor allem die KMU in bezug [sic] auf ihre Aufnahme

in öffentliche Verzeichnisse sowie in bezug [sic] auf unerbetene Anrufe" (Marlies Mosiek-Urbahn in: Europäisches Parlament 1997c, 236) zu schützen. Nachdem die Kommission zunächst ihrer weitgehenden Unterstützung für die Änderungen des Parlaments Ausdruck verliehen hatte (Europäische Kommission 1997), machte die Weigerung des Ministerrats, die Änderungswünsche des Parlaments anzunehmen, die Einsetzung eines Vermittlungsausschusses[143] erforderlich. Im Ergebnis konnte sich das Parlament vor allem mit seiner Forderung nach Einbezug auch juristischer Personen in den Anwendungsbereich der Richtlinie durchsetzen, während sich bezüglich der kostenfreien Nichtaufnahme in Verzeichnisse der Ministerrat – bis auf kleinere Konzessionen – weitgehend durchsetzen konnte und beim Thema Harmonisierung ein Kompromiss erzielt wurde (Europäisches Parlament 1997c).

Der vom Vermittlungsausschuss gebilligte gemeinsame Entwurf des Parlaments und des Rates wurde in dritter Lesung am 20. November 1997 vom Parlament (Europäisches Parlament 1997b) und am 1. Dezember 1997 vom Ministerrat angenommen. Die finale ISDN-RL wurde schließlich am 15. Dezember 1997 von den Präsidenten des Europäischen Parlaments und des Ministerrats unterzeichnet (Das Europäische Parlament und der Rat der Europäischen Union 1997).

Auch im Falle der ISDN-RL verzögerte sich die Umsetzung in den Mitgliedstaaten. Die Kommission leitete in der Folge Vertragsverletzungsverfahren gegen Frankreich, Irland und Luxemburg ein (EU-Kommission 2001a). Der EuGH sanktionierte schließlich Frankreich für die Versäumung der fristgemäßen Umsetzung der Richtlinie (EuGH 2001).

3.2.5 DS-VO 45/2001

Vom Anwendungsbereich der DS-RL ausgeschlossen war die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft. Bereits im Rahmen ihres 1990er-Legislativbündels hatte die

143 Für den Fall, dass der Rat die Vorschläge des Parlaments nicht annimmt, sehen die europäischen Verträge die Einberufung eines *Vermittlungsausschusses* binnen sechs Wochen vor. Dieser wird paritätisch aus Mitgliedern des Parlaments und des Ministerrats besetzt, während der Kommission die Moderationsrolle zukommt. Nach Einberufung muss der Vermittlungsausschuss innerhalb von sechs Wochen eine Einigung erzielen, da der Rechtsakt ansonsten als gescheitert gilt (Wessels 2008, 346).

Kommission daher auch eine Erklärung verabschiedet, in der für die Anwendung der für den Gemeinschaftsbereich vorgesehenen Verarbeitungsgrundsätze auf die Gemeinschaftsorgane und -einrichtungen geworben wurde. Zudem kündigte die Kommission an, zum frühestmöglichen Zeitpunkt (legislative) Maßnahmen folgen zu lassen, bis dahin allerdings zunächst die in der Rahmenrichtlinie festzulegenden Grundsätze auf die in ihrem Verantwortungsbereich erfolgende Verarbeitungen personenbezogener Daten anzuwenden. Daneben ermutigte die Kommission die übrigen Gemeinschaftsinstitutionen dazu, selbiges zu tun (Commission of the European Communities 1990, 74). Die Vorlage eines diesbezüglichen Rechtsaktes sollte allerdings noch einige Jahre auf sich warten lassen. Trotz fehlender Regulierung verarbeiteten die Gemeinschaftsorgane und -einrichtungen freilich weiterhin personenbezogene Daten, was wiederum zu Kritik vonseiten der Datenschutzaufsichtsbehörden führte (Deutscher Bundestag 1991, 60, 1993, 126–27; Simitis 1995, 468 f.). Allerdings konnte ein entsprechender Rechtsakt von der Kommission formell nicht vorgeschlagen werden, da der Schutz personenbezogener Daten bei der Verarbeitung durch die Gemeinschaftsorgane und -einrichtungen in den Europäischen Verträgen nicht vorgesehen war.

Die Situation änderte sich schließlich mit der Unterzeichnung des Vertrags von Amsterdam am 2. Oktober 1997.[144] Der neue Art. 286 im EWG-Vertrag besagte, dass ab dem 1. Januar 1999 „die Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und dem freien Verkehr solcher Daten auf die durch diesen Vertrag oder auf der Grundlage dieses Vertrags errichteten Organe und Einrichtungen der Gemeinschaft Anwendung [zu finden haben]" (Europäische Union 2002). Zudem forderte der zweite Absatz des entsprechenden EWG-Artikels (Art. 286 Abs. 2) die im Ministerrat versammelten Mitgliedstaaten dazu auf, unabhängig vom Erlass eines Rechtsaktes, die Errichtung einer unabhängigen Kontrollinstanz auf EU-Ebene noch vor dem 1. Januar 1999 zu fördern und gegebenenfalls entsprechende Bestimmungen zu verabschieden (ebd.).[145]

144 Mit dem am 1. Mai 1999 in Kraft getretenen Amsterdamer Vertrag wurden kleinere Ergänzungen und Anpassungen an der mit dem Maastrichter Vertrag grundlegend reformierten institutionellen Architektur vorgenommen (Wessels 2008, 94 f.).

145 Aufgrund des Widerstands der Kommission scheiterte dieses Anliegen jedoch. Offenbar war die Kommission über potentielle Überschneidungen des Tätigkeitsbereichs des Europäischen Ombudsmanns besorgt (González Fuster 2014, 144).

Zum Zwecke der Umsetzung der Bestimmungen des aktualisierten EWG-Vertrags legte die Kommission im Rahmen des Mitentscheidungsverfahrens dem Parlament sowie dem Ministerrat schließlich am 17. September 1999 ihren *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr* vor (Europäische Kommission 1999b). Der Wirtschafts- und Sozialausschuss gab seine Stellungnahme nur wenig später am 8. Dezember 1999 ab. Die Stellungnahme des Parlaments folgte mehr als ein Jahr später am 11. Oktober 2000 (Annahme des Rapporteur-Berichts im zuständigen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres) bzw. am 14. November 2000 (Annahme des Berichts im Parlamentsplenum). Der Ministerrat nahm den Standpunkt des Parlaments am 30. November an, sodass die Verordnung schließlich am 18. Dezember 2000 von den Präsidenten des Parlaments sowie des Rats unterzeichnet wurde und Ende Januar 2001 als *Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr* in Kraft getreten ist (Das Europäische Parlament und der Rat der Europäischen Union 2001).

Die auffälligste Änderung der finalen Verordnung gegenüber dem ursprünglichen Entwurf bestand in der Abänderung des Gegenstands der Verordnung in Art. 1. Der erste Satz des Artikels, der den *Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre* im Rahmen der Organe und Einrichtungen der Gemeinschaft als Gegenstand der Verordnung festlegt, wurde auf Vorschlag des Parlaments um die Aussage erweitert, dass die gemäß diesem Artikel erlassenen Bestimmungen *den freien Verkehr personenbezogener Daten untereinander oder mit Empfängern, die dem in Anwendung der Richtlinie 95/46/EG erlassenen einzelstaatlichen Recht der Mitgliedstaaten unterliegen, weder beschränken noch untersagen* dürfen. Da sich die Inhalte der Verordnung lediglich auf den Datenschutz bei der Datenverarbeitung in den Gemeinschaftsorganen und -einrichtungen bezogen, dabei zugleich das Schutzniveau der DS-RL wiederholten und keine umstrittenen neuen Elemente einbrachten, kam es zu keinen nennenswerten politischen Konflikten (Hijmans 2006).

3.3 Die Datenschutzpolitik der Europäischen Gemeinschaft nach der Jahrtausendwende

Mit der Jahrtausendwende ging die Datenschutzpolitik in der Europäischen Gemeinschaft in eine neue und konfliktreiche Phase über. Datenschützer, die für die Stärkung der datenschutzrechtlichen Regelungen im allgemeinen Datenschutzrecht wie auch im Sicherheitsbereich eintraten, konnten ihre Forderungen aufgrund der wirtschafts- und sicherheitspolitischen Bedeutungssteigerung, die die Datenverarbeitung erfahren hatte, nicht durchsetzen. In der Folge stagnierte die Entwicklung des Datenschutzrechts fast ein Jahrzehnt lang. Der vorliegende Unterabschnitt widmet sich der Analyse dieser Entwicklungen.

3.3.1 Hintergrund und Kontext: Wirtschafts- und sicherheitspolitisch bedingte Legitimationskrise des Datenschutzes

Das gesellschaftliche und politische Klima, das die Verabschiedung der Datenschutzgesetze der 1970er-Jahre bis hin zur DS-RL begünstigt hatte, wandelte sich im Laufe der 1990er-Jahre und stellte die Befürworter von Datenschutzregelungen zu Beginn der 2000er- bis insb. in die Mitte der 2000er-Jahre vor große neue Herausforderungen. Anders als zuvor waren nicht die strukturellen Regelungsdefizite deren Ursache, sondern eine sich in dieser Zeit zunehmend verschärfende, Subsystem-extern bedingte Legitimationskrise. Zwei Entwicklungen trugen dazu entscheidend bei: Zum einen wirtschaftspolitische und zum anderen sicherheitspolitische Effekte. Diese Faktoren werden in den folgenden Unterabschnitten herausgearbeitet.

3.3.1.1 Kommerzialisierung von (personenbezogenen) Daten und IuK-Technologien als Wirtschaftsmotor

Bereits in der ersten Hälfte der 1980er-Jahre versuchte die Europäische Kommission auf die im Jahr 1982 erfolgte Entflechtung des US-amerikanischen Telefonmonopolisten AT&T und die stärker wettbewerbliche Neuorganisation des dortigen Telekommunikationssektors mit dem Versuch zu reagieren, die Mitgliedstaaten von einer engeren Kooperation auf Gemeinschaftsebene im Hinblick auf die Telekommunikationspolitik und

von begleitenden Deregulierungsmaßnahmen nach US-amerikanischem Vorbild zu überzeugen. Allerdings konnte sich die Kommission anfangs nur teilweise durchsetzen. Während europaweit die ersten Deregulierungsmaßnahmen umgesetzt wurden, nahmen die Mitgliedstaaten auch weiterhin Rücksicht auf die Interessen der nationalen Telekommunikationsriesen (vor allem Deutschland und Frankreich), indem als Kerntechnologie auf ISDN und auf europäische Netz-Standards gesetzt wurde (vgl. z. B. die Empfehlungen des Bangemann-Berichts: Bangemann 1994).[146] Nachdem ab der zweiten Hälfte der 1990er endgültig klar geworden war, dass sich das Internet weltweit als Netzwerktechnologie durchgesetzt hatte und die nationalen Computernetz-Politiken gescheitert waren (Werle 2005), konnte sich die Europäische Kommission schließlich Ende der 1990er-Jahre als die führende europäische Institution auf dem Gebiet der europäischen Telekommunikationspolitik etablieren und eine Reihe von Gemeinschaftsmaßnahmen auf diesem Gebiet durchsetzen, die das Ziel der wirtschaftlichen Stärkung der Europäischen Gemeinschaft hatten (V. Schneider und Werle 2007, 271 ff.). Aufbauend auf der Unterteilung des Internets in eine Infrastrukturebene und eine Dienstleistungsebene sowie auf der Einsicht, dass die Gemeinschaft bei der Auseinandersetzung um die Infrastrukturebene bereits in einen uneinholbaren Rückstand geraten war, wurde der Fokus seit Anfang der 2000er-Jahre auf die Förderung der europäischen Industrie auf der Dienstleistungsebene in Gestalt von E-Commerce-Anwendungen gelegt. In der Zwischenzeit hatte sich wiederum die Verarbeitung personenbezogener Daten bereits zu einem Kernelement der Wertschöpfung auf der Dienstleistungsebene des Internets entwickelt. Die zunehmende Konzentration aller Kommunikationsmittel auf der Ebene des Computers bot dieser Kommerzialisierung von Daten Vorschub: „Mit steigendem Um-

146 Angesichts der sich ankündigenden Liberalisierung der Telekommunikationsmärkte bauten die staatlichen Telekommunikationsunternehmen, die ihre eigenen Standards durchsetzen wollten, auf die OSI-nahen ISDN-Standards mit dem Ziel, verschiedene Sprach- und Datendienste auf digitaler Basis in integrierter Form in einem Netz anbieten zu können und damit auch ihre Monopole zu verteidigen. Noch 1994 hieß es in den Empfehlungen „Europa und die globale Informationsgesellschaft" der Bangemann-Kommission für den Europäischen Rat, dass ISDN als Baustein der Informationsgesellschaft gefördert werden müsse, während das Internet nur am Rande erwähnt wurde (Werle 2005, 25). Demgegenüber hatten die skandinavischen Länder, die Niederlande und bis zu einem gewissen Grade auch das Vereinigte Königreich ihre Telekommunikationsmärkte früher liberalisiert bzw. nicht auf ISDN gesetzt, weshalb sich das Internet und entsprechende wirtschaftliche Gewinne in diesen Ländern früher und effizienter durchsetzen konnten (ebd.).

fang und fortschreitender Differenzierung wächst auch der Eigenwert der Datenbestände. Die Daten lösen sich mehr und mehr aus ihrem ursprünglichen Verarbeitungszusammenhang und fügen sich zu einem Informationskapital zusammen. Die Verwertungsmöglichkeiten reichen von einer weit reichenden Revision der Absatzstrategien bis hin zu einer konsequenten Vermarktung. Der Datenberg wandelt sich so zur Datenmine. Je tiefer die Stollen getrieben werden, desto größer der Nutzen." (Simitis 2000, 312) Dabei wurde zugleich in zunehmendem Maße auf die Kooperation der Betroffenen gesetzt: Indem diesen Dienste im Austausch für ihre personenbezogenen Daten angeboten wurden, konnten Datenverarbeiter ganz legitim auf Basis der individuellen Einwilligung Zugriff auf enorme personenbezogene Datenmengen erhalten und diese zu Zwecken des Data Mining und der personalisierten Werbung nutzen (ebd., 312). Die Vereinigten Staaten, die noch bis in die Mitte der 1990er-Jahre in einer Rezession steckten, konnten ihrer Wirtschaft mittels der gezielten Unterstützung der Verbreitung von IuK-Technologien zu massiven Wachstumsgewinnen verhelfen, sodass IuK-Technologien als *bahnbrechende Basis- und Schlüsseltechnologie* bezeichnet wurden (vgl. Grupp, Legler, und Breitschopf 2003).[147] So wurde 1999 ein enormes Wachstum des elektronischen Handels allein in Deutschland von 3 Milliarden D-Mark auf über 25 Milliarden D-Mark bis 2002 prognostiziert (Persson 1999). Letztlich konnte beispielsweise im ersten Quartal 2004 eine Wachstumsrate von 28,1 Prozent verzeichnet werden, während der konventionelle Handel lediglich mit 8,8 Prozent gewachsen war. Der elektronische Handel in Europa betrug 86 Mrd. Dollar im Jahr 2001 und in den Vereinigten Staaten wurde 2004 ein E-Commerce-Handelsvolumen von 120 Mrd. Dollar erzielt. Unter Einbezug des B2B-Bereichs betrug das E-Commerce-Handelsvolumen im Jahr 2001 in der Europäischen Gemeinschaft 430. Mrd. Dollar und in den Vereinigten Staaten bereits 1,08 Bio Dollar (The Economist 2004; UNCTAD 2004).

Waren in Zeiten der Großcomputer nur wenige private Akteure imstande gewesen, die entsprechende Infrastruktur zu finanzieren, konnten seit den 1980er-Jahren auch kleinere Betriebe Daten mittels der einfacher finanzierbaren Personal Computer verarbeiten und für Produktionssteige-

147 „Nicht unbedingt einzelne etablierte Firmen der Branche, sondern insgesamt die amerikanische informationstechnische Industrie und die Anbieter Internet basierter Dienstleistungen profitierten von dem ‚First Mover Advantage' der USA, der gegenüber Deutschland wegen der einseitigen Technologiepolitik besonders groß war." (Werle 2005, 29)

rungen nutzen. Ende der 1990er war der Personal Computer schließlich zu einem Haushaltsprodukt avanciert, das als Terminal zur Nutzung des Internets diente (Bendrath 2007b, 17). Damit durchlebte die Datenverarbeitung einen grundlegenden Bedeutungswandel: Waren Datenschutzvorkehrungen in den 1970er- und 1980er-Jahren noch vor allem aus der Angst vor einem Big-Brother-Szenario heraus gerechtfertigt worden, das den Staat als Hauptgefahr in den Mittelpunkt der Betrachtung rückte, war seit den 1980er-Jahren in zunehmendem Maße die Privatwirtschaft an die Stelle staatlicher Stellen als Hauptakteur der Datenverarbeitung getreten. Wurde zuvor befürchtet, dass die massenhafte Verarbeitung personenbezogener Daten die Kommunikations- und Partizipationsfähigkeit des Einzelnen einschränken würde, so schien sich mit dem Zugriff auf das Internet trotz der gleichzeitig zunehmenden Verarbeitung personenbezogener Daten eben jener Kommunikations- und Partizipationsraum des Einzelnen in ungekanntem Maße auszuweiten (Simitis 2000, 314 f.). Verstärkt wurde dieser Effekt durch die später als Netzeuphorie bezeichneten Hoffnungen, dass mit der Verbreitung des Internets die unausweichliche Lösung beliebiger Menschheitsprobleme, allen voran die Erreichung einer echten, globalen, demokratischen Öffentlichkeit, möglich werde.[148] Dass dieses Erfolgsmedium, das Internet, das massives wirtschaftliches Wachstum und gesellschaftliche Entwicklung versprach, in weiten Teilen der Gesellschaft und Politik als weitgehend unregulierter Ort[149] wahrgenommen wurde,

148 Sinnbildlich für diese Perspektive sei auf John Perry Barlows „A Declaration of the Independence of Cyberspace" (1996) verwiesen. Für frühe Kritiken, siehe: (Horvath 1996; Lovink und Schultz 1996). Für eine spätere, umfassende Kritik, siehe: (Morozov 2011).

149 In Bezug auf die Selbstverwaltung des technischen Internets (etwa die Verwaltung der technischen Standards und Protokolle) ist dies zwar eine durchaus treffende Feststellung. So hatte das US-Verteidigungsministerium in der Frühphase der Entwicklung des Internets einen sehr weitgehenden Einfluss auf die Gestaltung des Internets, der jedoch mit der Abkoppelung des zivilen Internets vom militärischen MILNET im Jahr 1983 ein Ende fand. Fortan erfolgte die Weiterentwicklung des Internet auf Basis der sog. Multi-Stakeholder-Governance (Abbate 1999, 43 ff. Warnke 2011, 45 f.). In Bezug auf den wirtschaftlichen Erfolg US-amerikanischer Unternehmen auf der Dienstleistungsebene des Internets kann dieser Perspektive jedoch entgegnet werden, dass die Clinton-Administration Mitte der 1990er, angesichts der wirtschaftlichen Wachstumspotentiale dieses Sektors, enorme Anstrengungen unternommen hatte, den Erfolg US-amerikanischer Unternehmen durch regulative Maßnahmen (Stichwort: *Regulierte Selbstregulierung*, so etwa mit den 1997 verabschiedeten E-Commerce-Gesetzen) abzusichern (Holznagel und Werle 2004, 27; U.S. Government Working Group on Electronic Commerce 1998).

verstärkte in Verbindung mit dem zu dieser Zeit große Anziehungskraft ausstrahlenden politischen Fokus auf Soft-Governance-Maßnahmen (EU-Kommission 2001c; vgl. z. B. Tömmel 2008), die Bereitschaft auf Seiten der politischen Entscheider, zum einen grundsätzlich weniger intensiv – sei es auch im Hinblick auf die Verhinderung negativer Effekte neuer Technologien mittels Datenschutzmaßnahmen – regulieren zu wollen, und zum anderen Regulierung noch stärker als zuvor eher als Katalysator für wirtschaftliches Wachstum zu nutzen. Die Verabschiedung der Signaturrichtlinie 1999/93/EG sowie der E-Commerce-Richtlinie 2000/31/EG sind in diesem Zusammenhang als derartige Katalysator-Maßnahmen zu bewerten, die den unbedingt notwendigen rechtlichen Rahmen abstecken, innerhalb dessen sich der E-Commerce-Markt ansonsten weitgehend unreguliert ausbreiten können sollte (Holznagel und Werle 2004, 26 f.). Mahnungen zur Wahrung des Datenschutzes konnten sich in diesem gesellschaftlichen und politischen Klima kaum mehr Gehör verschaffen (Simitis 2000, 312).

Stattdessen wurde seit Mitte der 1990er-Jahre eine andere – im Kontext des Bangemann-Reports bereits kurz angesprochene (vgl. Unterkapitel 3.2.2.6) – Perspektive auf den Umgang mit personenbezogenen Daten dominant. Datenschutzmaßnahmen sollten nicht mehr nur Individuum und Gesellschaft vor staatlichen Übergriffen schützen, sie sollten vielmehr im Sinne einer vertrauensbildenden Maßnahme zwischen Anbietern und Kunden in der virtuellen Welt, in der es keinen physischen Kontakt der Kunden mit Verkäufern oder Produkten gibt, wirken und somit zu einer gesteigerten gesellschaftlichen Akzeptanz neuer Technologien beisteuern und das auf neuen IuK-Technologien basierende Gelingen wirtschaftlichen Wachstums flankieren (Priscilla M. Regan 1999). Während einige Unternehmen bereits die Existenz von staatlichen Datenschutzregelungen als Behinderung des wirtschaftlichen Potentials des neuen E-Commerce-Marktes kritisierten, gingen andere Unternehmen erfolgreich dazu über, nationale und europäische Entscheider von der Notwendigkeit einer zu schaffenden Balance zwischen dem rechtlichen Schutz personenbezogener Daten und der wirtschaftlichen Verwendung ebenjener Daten zu überzeugen. Datenschutz galt, diesem aktualisierten Verständnis nach, zunehmend als individualistisch verstandener Verbraucherschutz, während das angestrebte Wirtschaftswachstum als gesellschaftliches Ziel bzw. Förderung des Allgemeinwohls definiert wurde. Der technologische Rückstand der Europäischen Gemeinschaft erhöhte dabei die Bereitschaft der Politik, Konzessionen zugunsten wirtschaftspolitischer Versprechungen einzugehen. In anderen Worten setzt sich zu dieser Zeit in zunehmendem Maße die Perspektive

durch, dass der Schutz personenbezogener Daten in erster Linie nur insoweit aufrechterhalten werden sollte als dieser zu mehr Vertrauen in digitale Technologien und dadurch zu mehr Wirtschaftswachstum führte (Bendrath 2007a).

Diese wirtschaftspolitisch ausgelöste Legitimationskrise des Datenschutzes wurde sodann um eine sicherheitspolitisch motivierte Legitimationskrise ergänzt, die deren Effekte verstärken sollte. Die nähere Betrachtung dieser zweiten Legitimationskrise ist Gegenstand des folgenden Kapitels.

3.3.1.2 Von 9/11 bis London 2005: Der Einfluss von Terroranschlägen

Am 11. September 2001 entführten mehrere, dem islamistischen Terrornetzwerk al-Qaida zugehörige, Selbstmordattentäter zeitgleich vier Passagierflugzeuge und verursachten mittels der auf das World Trade Center in New York sowie auf das Pentagon in Arlington verübten Selbstmordanschläge den Tod von knapp 3.000 Menschen. Dieser historisch beispiellose Angriff auf die Vereinigten Staaten hatte nicht nur weitreichende außenpolitische, sondern auch innenpolitische Folgen, von denen viele gesellschaftliche und staatliche Bereiche betroffen waren. Von enormer politischer Bedeutung war insbesondere die zunehmende Versicherheitlichung der Innenpolitik. Diese betraf nicht nur die Vereinigten Staaten, sondern auch ihre Verbündeten, von denen die größtmögliche Kooperation im Hinblick auf die Eindämmung als terroristisch eingestufter Gefahren abverlangt wurde (Fey 2012, 38). Von Bedeutung für die vorliegende Arbeit ist insbesondere die im Nachgang der Anschläge erfolgte massive Ausweitung von geheim- und nachrichtendienstlichen[150] Überwachungsmaßnahmen – zunächst in den Vereinigten Staaten und in der Folgezeit auch in der EU und ihren Mitgliedstaaten. Angetrieben vom Übergang „vom Rechtsstaat zum Präventionsstaat“ (Denninger 2002) war bzw. ist das Leitziel jener sich mit diesem Staatstypus identifizierenden sicherheitspolitischen Akteure die Ab-

150 Die begriffliche Differenzierung sei wie folgt zu verstehen: „Geheimdienste bezeichnen in den meisten Staaten eigene, von den regulären Polizeibehörden mehr oder weniger verselbstständigte Dienststellen zur Aufklärung und Bekämpfung vergangener oder zukünftiger Bestrebungen gegen Bestand, Sicherheit oder Grundelemente der politischen Ordnung eines Staates. Nachrichtendienste hingegen beschränken sich darauf, solche Bestrebungen aufzuklären, überlassen deren Bekämpfung aber anderen Stellen. Sie sind also ausschließlich auf Beschaffung und Verarbeitung von Informationen gerichtet.“ (Gusy 2014, 9)

wehr und Verhinderung von Anschlägen sowie die Gewährleistung von Sicherheit als oberstem Ziel: „Während der Rechtsstaat normenverletzendes Verhalten lediglich sanktioniert, ist der Präventionsstaat bemüht, die Normenverletzung an sich zu verhindern. Zu diesem Zweck muss er umfangreiches Wissen über jeden einzelnen Bürger sammeln und in der Exekutive Kapazitäten aufbauen, um jeder plausiblen Art von aus Normverletzung erwachsender Bedrohung wirksam entgegentreten zu können." (A. Busch 2012b, 865) In anderen Worten setzte sich zu Beginn der 2000er-Jahre die Überzeugung durch, dass eine möglichst große Informationsbasis eine Schlüsselvoraussetzung für die erfolgreiche Bekämpfung des Terrorismus darstelle. Meinungsverschiedenheiten existierten lediglich hinsichtlich der für eine wirksame Bekämpfung benötigten konkreten Datenmenge, der Speicherdauer erhobener Daten, der Betroffenenrechte sowie der Spezifika des Zugriffs auf die Daten seitens Sicherheitsbehörden. So forderten sicherheitspolitisch motivierte Akteure im Nachgang der Anschläge vom 11. September auch innerhalb der EU die Ausweitung des Informationsaustauschs zwischen den zuständigen Behörden der Mitgliedstaaten sowie den entsprechenden europäischen Institutionen. Datenschutzrechtliche Vorgaben wurden von diesen Akteuren dabei regelmäßig als Behinderung der behördlichen Pflichten wahrgenommen und gegenüber der Öffentlichkeit auch in dieser Weise kommuniziert. Eine beliebte wiederkehrende Rhetorik in diesem Kontext war die Gleichstellung von Datenschutz mit „Täterschutz" (Wetzel 2012, 559 f.).[151] Bürgerrechtlich motivierte Akteure erwiderten, dass Datenschutz die Verarbeitung personenbezogener Daten nicht verhindere und auch „keine Marotte von Gespenstersehern [sei], sondern […] den Staat, und nicht nur ihn [dazu zwinge], bestimmte Regeln bei der Verarbeitung personenbezogener Informationen einzuhalten – [sic] und zwar zum Schutz der Bürger." (Simitis, zit. nach: Klingst 2001)

Den Höhepunkt erreichte die innereuropäische Debatte mit den Anschlägen von Madrid am 11. März 2004 und London am 7. Juli 2005. Die bis dahin auf dem Felde der Terrorismusbekämpfung vor allem auf

151 So hatte sich etwa der damalige von der SPD gestellte Bundesinnenminister Otto Schily im Nachgang von 9/11 dahingehend geäußert, dass ein überzogenes Maß an Datenschutz zu den Anschlägen beigetragen habe. Belege lieferte Schily keine (Sanders 2001). Wie sich später herausstellen sollte, war das Problem nicht das Fehlen einer ausreichend großen Datenbasis, sondern im Gegenteil der Mangel an zielführenden Auswertungsmethoden der bestehenden, enormen Datenbestände (Matheou 2015).

Solidarität gegenüber den Vereinigten Staaten gerichteten EU-Aktivitäten[152] kondensierten sich erst im Nachgang der Madrider Anschläge, zunächst im Rahmen der *Erklärung zum Kampf gegen Terrorismus* der Staatschefs der EU (Europäischer Rat 2004) und der darin beschlossenen Einrichtung der Position einer unionsweiten Koordination für die Terrorismusbekämpfung und schließlich in Folge der Londoner Anschläge zu einer *EU-Strategie zur Terrorismusbekämpfung* (EU-Ministerrat 2005b; MacKenzie, Kaunert, und Léonard 2015, 96 f.). Die Folge war eine massive Versicherheitlichungspolitik (Buzan, Waever, und Wilde 1998, 24 ff.), die zum Erlass dutzender weitreichender Regelungen führte, die den Handlungsspielraum von Überwachungs- und Polizeibehörden ausdehnten. So wurden zwischen 2001 und 2013 allein seitens der EU insgesamt 238 Maßnahmen – darunter 88 rechtsverbindliche Maßnahmen wie Verordnungen, Richtlinien und Beschlüsse – zur Bekämpfung von Terrorismus verabschiedet (Hayes und Jones 2013, 25).

Die folgenden Unterabschnitte beschreiben, wie es den Befürwortern von Datenschutzregelungen unter diesen veränderten Kontextbedingungen zunehmend schwerer fiel, öffentliches Gehör zu finden und sich in den datenschutzpolitischen Aushandlungsprozessen durchzusetzen.

3.3.2 ePrivacy-Richtlinie 2002/58/EG

Der erste datenschutzpolitische Aushandlungsprozess, bei dem Wirtschafts- und Sicherheitsinteressen sich in relevantem Maße gegenüber Datenschutzinteressen durchsetzen konnten, stellt die Aushandlung der ePrivacy-Richtlinie dar. Die Analyse des Aushandlungsprozesses zeigt insbesondere, wie in der Anfangsphase der Verhandlungen im Vorfeld von 9/11 zunächst noch wirtschaftspolitische Argumente dominant waren und wie diese nach den Terroranschlägen von sicherheitspolitischen Argumenten abgelöst wurden.

3.3.2.1 Vorgeschichte zur ePrivacy-Richtlinie

Noch vor Inkrafttreten der Bestimmungen des Rechtsrahmens für Telekommunikation zum 1. Januar 1998, initiierte die Kommission mit der

152 So etwa die Ende 2003 angenommene EU-außenpolitisch motivierte *Europäische Sicherheitsstrategie* (Europäischer Rat 2003).

Veröffentlichung eines Grünbuchs Anfang Dezember 1997 einen ersten öffentlichen Evaluations- und Konsultationsprozess[153] zur Identifikation und zum Abbau weiterer Barrieren auf dem Weg zu einer wettbewerbsfähigeren Europäischen Gemeinschaft auf dem Gebiet der Telekommunikation. Das Grünbuch der Kommission rahmte das Thema Datenschutz lediglich als nebensächliche Maßnahme, die im Hinblick auf das übergeordnete Ziel der Förderung der Systemkonvergenz und der Förderung eines EU-weiten Telekommunikationssektors nur insofern bedeutsam sei, dass durch Datenschutz das für die erfolgreiche Verbreitung und Nutzung konvergenter Systeme benötigte Vertrauen aufgebaut werde (European Commission 1997, 29). Die Grundrechtsperspektive auf Datenschutz fand erst später in den Konsultationsergebnissen Erwähnung. Interessanterweise ordnete die Kommission das Thema Datenschutz und Privatheit dabei einerseits dem Themenfeld Verbraucherschutz bzw. -Interessen (European Commission 1998, 30) und andererseits dem Themenfeld „Securing Public Interest Objectives in the Light of Convergence" zu und rahmte es somit auch als ein öffentliches Interesse (ebd., 31). Die Mehrheit der am Konsultationsprozess teilnehmenden Akteure befürworteten zwar die regulatorische Festlegung eines Mindest-Datenschutzniveaus (ebd., 32). Allerdings stellten einige Akteure aus der Wirtschaft die Notwendigkeit weiterer Verbraucherschutzmaßnahmen auch grundsätzlich infrage (ebd., 31).[154]

Nachdem die Kommission ihre Strategie zur weiteren Entwicklung elektronischer Kommunikationsinfrastrukturen und zugehöriger Dienste ausgearbeitet hatte, veröffentlichte sie Anfang November 1999 den sog.

153 Der Konsultationsprozess fand zwischen Dezember 1997 und Mai 1998 statt. In einer ersten Runde gingen schriftliche Stellungnahmen von insgesamt 270 Akteuren bei der Kommission ein. In einem weiteren Schritt setzten sich die Ratsformationen *Verkehr und Telekommunikation* sowie *Kultur und Audiovisuelle Medien* mit der Materie auseinander. Außerdem gab der WSA eine Stellungnahme ab. Schließlich wurden im dritten Schritt zwischen März und April 1998 Anhörungen mit ausgewählten Akteuren durchgeführt. Folgende Akteure, die an diesem Konsultationsprozess partizipierten, nahmen später auch am politischen Aushandlungsprozess der DSGVO teil: ACT. AmCham EU, BEUC, ENPA, EPC, ETNO, FAEP, FEDMA, ICC, UNICE (später umbenannt in: Businesseurope), VDZ, WFA, Intel, Nokia, Telefónica (European Commission 1998, 1 und 42 ff.).

154 Mit der Veröffentlichung der Konsultationsergebnisse folgte auf den ersten öffentlichen Konsultationsprozess ein zweiter, weniger umfangreicher, der zwischen Ende Juli und November 1998 lief, doch wurden im Rahmen dieser Konsultation keine datenschutzpolitisch relevanten Themen diskutiert, weswegen diese nicht näher betrachtet wird (European Commission 1999).

Kommunikationsbericht 1999, mit dem ein weiterer Konsultationsprozess[155] initiiert wurde (Europäische Kommission 1999a). Darin wurde zum einen über die bis dahin umgesetzten Liberalisierungsbestrebungen im Telekommunikationsbereich reflektiert und zum anderen *Vorschläge für die Hauptkomponenten eines neuen Rahmens für Kommunikationsinfrastrukturen und zugehörige Dienste* unterbreitet (ebd., ii). Die auf dem Europäischen Ratstreffen vom März 2000 verabschiedete Lissabonner Strategie bettete die geplanten Maßnahmen schließlich in den Gesamtkontext gemeinschaftlicher Deregulierungsmaßnahmen im Telekommunikationssektor ein, deren übergeordnetes Ziel im Aufbau eines wettbewerbsfähigen europäischen Binnenmarktes lag. Die Strategie betonte das Potential für Wachstum, Wettbewerbsfähigkeit und die Schaffung von Arbeitsplätzen durch den Übergang zu einer digitalen und wissensbasierten Gesellschaft, indem eine günstige und qualitativ hochwertige Kommunikationsinfrastruktur aufgebaut wird (Europäischer Rat 2000b). Dazu sah die Kommission die Verabschiedung einer Rahmenrichtlinie vor, mit der die allgemeinen und spezifischen politischen Ziele festgelegt werden sollten, sowie vier spezifischer Richtlinien zu den Themenbereichen *Erteilung von Genehmigungen*, *Zugang und Zusammenschaltung*, *Universaldienst*, und eine Richtlinie zum *Schutz der Privatsphäre und Datenschutz* (ebd.).[156] Da bereits die ISDN-RL 97/66/EG einige Aspekte des Themas abdeckte, sollte diese im Rahmen des Gesetzesbündels aktualisiert werden. Dabei verwies die Kommission einerseits auf die unzureichende Harmonisierung aufgrund von Unterschieden bei der Umsetzung der Richtlinie und andererseits auf die Notwendigkeit der Überarbeitung der – bereits zum Zeitpunkt ihrer Verabschiedung als veraltet bewerteten (Debusseré 2005, 72) – Richtlinienvorgaben, damit sichergestellt würde, dass die Regelungen für einen konvergierenden Telekommunikationsmarkt, der neben der Festnetztelefonie auch jegliche mobile, satelliten- oder kabelbasierte Technologie umfasst, geeignet wären (Europäische Kommission 1999a, 54 und 73). Im Rahmen des öffentlichen Konsultati-

155 Hauptverantwortlich für diesen Konsultationsprozess war die Generaldirektion Informationsgesellschaft bzw. deren Referat Rechtsrahmen A/1 (Europäische Kommission 1999a, xii).

156 Das Gesetzesbündel hatte neben der Aktualisierung bestehender Regelungen insb. die Vereinfachung der geltenden Regelungen zum Ziel, indem die geltenden zwanzig Rechtsvorschriften auf sechs reduziert werden sollten (Europäische Kommission 1999a, 21).

onsprozesses gingen mehr als 200 Antworten bei der Kommission ein.[157] In ihrer Mitteilung zu den Ergebnissen der Konsultation resümierte die Kommission, dass sich die Mehrheit der Einsendungen und vor allem die partizipierenden Regulierungsbehörden wie die Art. 29-Datenschutzgruppe für die Überarbeitung der ISDN-RL aussprachen, damit die Technologieneutralität der Regelungen und damit ihre Wirksamkeit weiterhin gewährleistet werden könnten. Allerdings vertraten Wirtschaftsvertreter – ähnlich zu ihrer während der ersten Konsultation zur Konvergenz vertretenen Position – auch während dieser Konsultation die Position, dass die Notwendigkeit einer sektorspezifischen Regulierung grundsätzlich infrage zu stellen sei. Seitens der Wirtschaftsvertreter wurden die bestehenden horizontalen Rechtsvorschriften in Gestalt der DS-RL 95/46/EG als ausreichend bewertet. Sektorspezifische Präzisierung der Richtlinienvorgaben seien erforderlichenfalls mit einem flexiblen Instrument wie Verhaltensregeln besser zu erreichen statt mit staatlicher Regulierung (Europäische Kommission 2000b, 5 und 18).

3.3.2.2 Veröffentlichung des Kommissionsvorschlags

Die Europäische Kommission veröffentlichte schließlich am 12. Juli 2000 im Rahmen des Mitentscheidungsverfahrens ihren *Vorschlag für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation* (EU-Kommission 2000b). Der Vorschlag sah überwiegend kleinere Anpassungen an den Stand der Technik sowie die Aufrechterhaltung des in der Vorgängerrichtlinie festgelegten Datenschutzniveaus vor. Lediglich im Zusammenhang mit zwei Richtlinienelementen sollte es zu Konflikten kommen. In Bezug auf die Debatte, ob an Betroffene gerichtete Werbung nur nach der vorherigen Einwilligung dieser erfolgen dürfte (Opt-in) oder Betroffene nach dem Erhalt der Werbung das Recht auf Widerruf (Opt-out) erhalten sollten, vertrat

157 Der Konsultationsprozess fand zwischen Mitte November 1999 und Mitte Februar 2000 statt. Neben schriftlichen Einsendungen berücksichtigte die Kommission dabei auch die Beiträge von mehr als 500 Personen, die bei einem zweitägigen öffentlichen Hearing am 25. und 26. Januar 2000 teilnahmen. Auch an diesem Konsultationsprozess waren viele Akteure beteiligt, die später während des Aushandlungsprozesses der DSGVO eine wichtige Rolle spielen sollten: AmCham EU, Association of Commercial Television in Europe ACT, BEUC, ENPA, Euro-ISPA, European Public Telecommunications Network Operators' Association (ETNO), GSM Europe, Intel, Microsoft, Nokia, Telefónica, UNICE/Businesseurope (Europäische Kommission 2000b, 32 ff.).

die Kommission zwar die Position, dass ein Opt-in-Verfahren zu bevorzugen sei. Aus Rücksichtnahme auf die diesbezüglichen unterschiedlichen Positionen in den Mitgliedstaaten und anhaltende Kritik aus der Wirtschaft hin, schlug die Kommission allerdings die Regelung dieser Materie im mitgliedstaatlichen Recht statt auf Gemeinschaftsebene vor (Art. 13 Abs. 2). In einem weiteren zentralen Aspekt, nämlich der seitens einiger Mitgliedstaaten geforderten anlasslosen Aufbewahrung von Verkehrsdaten für einen längeren Zeitraum und der Zurverfügungstellung dieser Daten an staatliche Exekutivbehörden, hatte sich die Kommission unnachgiebig gezeigt und war bei der bereits in der ISDN-RL verwendeten Formulierung geblieben. Demnach sollten Verkehrsdaten gelöscht werden, sobald sie nicht länger für die Erbringung des Dienstes bzw. für die Gebührenabrechnung benötigt würden (EG 15). Art. 15 Abs. 1 wiederum sah mitgliedstaatliche Ausnahmen im Zusammenhang mit der Sicherheit des Staates, der Landesverteidigung und der Ermittlung und Verfolgung von Straftaten vor. Da diese Regelung lediglich anlassbezogene Speicherungen erlaubte, stieß sie auf Seiten der mitgliedstaatlichen Exekutivbehörden auf vehemente Ablehnung, da die Regelung als eine inakzeptable Einschränkung der Ermittlungstätigkeiten bewertet wurde. Spätestens seit dem Jahr 1997 forderten europaweit zahlreiche Exekutivbehörden den Aufbau der Möglichkeit einer Vorratsdatenspeicherung, mittels derer sie sich Erleichterungen in ihrer Ermittlungstätigkeit erhofften (Bunyan 2002; Statewatch 2001).

3.3.2.3 Formierung des Gemeinsamen Standpunktes im Ministerrat

Nachdem die Kommission den Gesetzgebungsprozess initiiert hatte und der Legislativvorschlag an den Ministerrat übersandt worden war, erhielt nicht die Ratsarbeitsgruppe *Datenschutz*,[158] die bereits für die Beratungen zur DS-RL, zur ISDN-RL sowie zur DS-VO die Zuständigkeit inne hatte, sondern die Arbeitsgruppe *Telekommunikation* unter der Leitung der Ratskonfiguration „Verkehr/Telekommunikation" (Karaboga 2018, 145–48). Auf der Sitzung der Arbeitsgruppe am 29 Mai 2001 brachte die schwedische Ratspräsidentschaft gemeinsam mit der belgischen und britischen Delegation den Vorschlag ein, die in Art. 6 Abs. 1 des Richtlinienentwurfs enthal-

158 Bis zu ihrer Umbenennung im Sinne einer klareren Zuordnung im Jahr 1999 firmierte die Arbeitsgruppe unter dem Namen „Wirtschaftsfragen (Datenschutz)" bzw. „Economic Questions – Data Protection" (Presidency of the Council of the European Union 2006, 1).

tene Löschungspflicht für Verkehrsdaten herauszunehmen, da diese den Erfordernissen der Exekutivbehörden nicht entspräche. Die griechische, italienische sowie die niederländische Ratsdelegation gemeinsam mit der Kommission lehnten den Vorschlag unter Verweis auf die menschen- und grundrechtliche Bedeutung der Thematik allerdings ab. Ausgehend von einem britischen Vorschlag, schlug die schwedische Ratspräsidentschaft zudem eine Änderung von Art. 15 vor. Demnach sollte in Art. 15 Abs. 1 eine Ausnahme für die Mitgliedstaaten vorgesehen werden, Verkehrsdaten für eine bestimmte Zeit speichern zu dürfen. In der letzten Version des Diskussionsstandes der Arbeitsgruppe setzte sich schließlich ein Vorschlag Belgiens (der folgenden Ratspräsidentschaft) durch, wonach Art. 6 Abs. 1 dahingehend abgeändert werden sollte, dass die zu löschenden Daten gemäß dem nationalen Recht für rechtmäßige Zwecke weiterverarbeitet werden dürfen sollten. Die Art. 29-Datenschutzgruppe bzw. dessen Vorsitzender Stefano Rodotà wandte sich daraufhin am 7. Juni 2001 mit einem Brief an Göran Persson, den amtierenden schwedischen, sozialdemokratischen Vorsitzenden des Ministerrates, und forderte diesen dazu auf, den *bestehenden, ausgewogenen Ansatz* beizubehalten und den Vorschlag der Kommission zu unterstützen (Article 29 WP 2001).

Die am 27. Juni 2001 auf der Tagung des Ministerrats (Telekommunikation) erzielte Einigung zwischen den Mitgliedstaaten blendete diese und weitere bürgerrechtliche Zwischenrufe allerdings aus, indem die vom AStV erfolgte Ergänzung von Art. 15 Abs. 1 gestrichen bzw. in den Erwägungsgrund 10 verschoben wurde (Statewatch 2001).

Währenddessen übten die Ministerratsvertreter nicht nur Druck auf die Gegner der Vorratsdatenspeicherung im Ministerrat aus, sondern auch auf das Parlament und die Kommission. Diese blieben jedoch zunächst bei ihrer ursprünglichen Position und traten für eine Beibehaltung des Datenschutzniveaus (Kommisison) der Vorgängerrichtlinie (97/66/EG) bzw. eine Erhöhung (Parlament) ein. Erst die Terroranschläge vom 11. September sollten die Kommissions- und Parlamentsmeinung nachhaltig verändern.

3.3.2.4 Formierung der Parlamentsposition in erster Lesung: Erster Cappato-Bericht

Die Parlamentspräsidentin beauftragte am 8. September 2000 zunächst den LIBE-Ausschuss[159] damit, die Stellungnahme des Parlaments vorzubereiten. Dieser wählte den italienisch-stämmigen, linksliberalen Marco Cappato (zu dieser Zeit: Technische Fraktion der Unabhängigen Abgeordneten – TGI / Lista Emma Bonino)[160] zum Berichterstatter. Bald darauf, am 6. Oktober 2000, legte die Parlamentspräsidentin gemäß Hughes-Verfahren (heute: Verfahren mit assoziierten Ausschüssen)[161] fest, dass der Parlamentsbericht vom LIBE-Ausschuss gemeinsam mit dem ITRE-Ausschuss (Berichterstatterin: Ilka Schröder von den Grünen bzw. der Europäischen Freien Allianz/EFA) ausgearbeitet werden sollte (Cappato und Schröder 2001, 4). Am 2. November 2000 verabschiedete zunächst die Art. 29-Datenschutzgruppe ihre Stellungnahme, in der sie die mit dem Legislativvorschlag verfolgte Absicht der Kommission, ein hohes Datenschutzniveau aufrechtzuerhalten, ausdrücklich unterstützte (Artikel 29-Datenschutzgruppe 2000). Anfang 2001 gab auch der Wirtschafts- und Sozialausschuss seine den Kommissionsvorschlag unterstützende Stellungnahme ab (WSA 2001). Der letztlich aufgrund von Komplikationen doch nicht im Hughes-Verfahren verfasste LIBE-Bericht wurde schließlich am 5. September 2001 im Plenum des Europäischen Parlament debattiert. Berichterstatter Cappato unterstützte die Kommission darin, enge Grenzen für die Speicherung von Verkehrsdaten vorzusehen, mit der klassisch liberalen Begründung, dass „die größte Gefahr für die Privatsphäre der Bürger gerade in der Allmacht des Staates beim Zugang zu personenbezogenen Daten besteht“ (Vgl. Cappato, in: Europäisches Parlament 2001b). Der Parlamentsbericht ging in diesem Bereich daher viel weiter als die Kommission und trat für eine weitere Be-

159 Als mitberatende Ausschüsse waren der Ausschuss für Industrie, Außenhandel, Forschung und Energie (ITRE), JURI, der Ausschuss für Umweltfragen, Volksgesundheit und Verbraucherpolitik (ENVI) sowie der Haushaltsausschuss beteiligt. Der Haushaltsausschuss entschied sich allerdings dazu, keine Stellungnahme abzugeben (Karaboga 2018, 152).

160 Zwischen 2001 und 2004 hatte Cappato keine Fraktionszugehörigkeit im EU-Parlament. In der sechsten Wahlperiode gehörte er der ALDE-Fraktion an (EP 2020b).

161 Da Ausschüsse dazu neigen ihr Kern-Themenportfolio zu begünstigen, findet dieses Verfahren gem. Art. 47 der Geschäftsordnung des EP Anwendung, um die Gefahr der Erarbeitung einseitiger Ergebnisse zu vermeiden, sofern die Zuordnung eines zu beratenden Legislativvorschlags nicht klar zugunsten eines einzelnen Ausschusses möglich ist (Kluger Dionigi 2017, 156 ff.).

schränkung der Speicherung von Verkehrsdaten ein: Diese sollte nur dann zulässig sein, soweit sie „in einer demokratischen Gesellschaft angemessen, verhältnismäßig und zeitlich begrenzt ist. Diese Maßnahmen müssen ganz und gar die Ausnahme darstellen, sich auf eine allgemein verständliche spezifische Rechtsvorschrift stützen und von gerichtlichen oder zuständigen Behörden für Einzelfälle genehmigt sein. Im Rahmen der Europäischen Menschenrechtskonvention und gemäß den Entscheidungen des Menschrechtsgerichtshofs ist jede Form einer großangelegten elektronischen Überwachung verboten." (vgl. Änderungsantrag 50, in: Cappato und Schröder 2001, 37) Bezüglich der Opt-in/Opt-out-Thematik schlug Cappato jedoch im Gegensatz zum Kommissionsvorschlag eine einheitliche Kompromissregelung vor, die aufgrund der von Cappato bemängelten Unwirksamkeit des Opt-in-Prinzips bei der Bekämpfung von Spam auf das Opt-out-Prinzip unter Einbeziehung der betroffenen Wirtschaftssektoren setzen und auf Selbstregulierungsmechanismen (Filter und Technologien) basieren sollte (vgl. bspw. die Änderungsanträge 38 und 43, in: Cappato und Schröder 2001).[162]

Den Cappato-Bericht nahm zunächst der LIBE-Ausschuss am 11. Juli 2001 mit 22 Stimmen (bei 12 Gegenstimmen und 5 Enthaltungen) an (Cappato und Schröder 2001, 4). Daraufhin wurde der Entwurf am 5. September 2001 im Europäischen Parlament debattiert und darüber am darauffolgenden Tag abgestimmt. Nachdem zuvor im Plenum vor allem länger über die Opt-in/Opt-out-Frage gestritten worden war (Europäisches Parlament 2001b, 2001c), lehnte eine aus PSE, Grünen und Linken bestehende Mehrheit den Bericht mit 204 Stimmen ab, während lediglich 129 Abgeordnete (aus der liberalen Fraktion (ELDR) sowie TDI (Technische Fraktion der Unabhängigen Abgeordneten) gemeinsam mit etwas mehr als 40 Abgeordneten der EVP-ED) dafür stimmten. 155 vor allem der EVP-ED zugehörige Abgeordnete enthielten sich (Europäisches Parlament 2002a, 261 f.). Um ein Scheitern des Legislativvorschlags zu verhindern, beantragte Cappato schließlich die Rücküberweisung des Berichts an den LIBE-Ausschuss. Das Parlament gab dem statt und der LIBE-Ausschuss setzte sich in zwei weiteren Sitzungen (am 10. und 22. Oktober) mit der Überarbeitung des Berichts auseinander (Cappato 2001, 5).

162 Diese Haltung Cappatos, einerseits Datenschutz im Hinblick auf Sicherheitsfragen den Vorzug zu geben und andererseits Einschränkungen des Schutzniveaus dann in Kauf zu nehmen, wenn dieses mit wirtschaftspolitischen Zielen konfligiert, deckt sich mit der Analyse der Haltung liberaler Parteien zum Datenschutz (Baumann 2013; Schütz und Karaboga 2015, 18).

3.3.2.5 Post 9/11: Formierung der Parlamentsposition in erster Lesung: Zweiter Cappato-Bericht

Wenige Tage nach den Terroranschlägen vom 11. September traten die EU-Justiz- und Innenminister zusammen, um „die erforderlichen Maßnahmen zur Wahrung eines höchstmöglichen Sicherheitsniveaus sowie jede andere angezeigte Maßnahme zur Bekämpfung des Terrorismus zu ergreifen." (EU-Ministerrat 2001, 1) Zudem ersuchte der Ministerrat die EU-Kommission, „Vorschläge zu unterbreiten, mit denen dafür Sorge getragen wird, dass die Strafverfolgungsbehörden die Möglichkeit erhalten, im Zusammenhang mit kriminellen Handlungen zu ermitteln, die unter Anwendung elektronischer Kommunikationssysteme begangen wurden, und Maßnahmen gegen die Urheber zu ergreifen." (EU-Ministerrat 2001, 3, Nr. 4) Ergänzt wurde diese Forderung um den Hinweis, dass der Rat besonders darauf achten werde, „dass ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Notwendigkeit des Zugangs der Strafverfolgungsbehörden zu Daten *für strafrechtliche Ermittlungszwecke* gewährleistet wird." (ebd., Hervorhebung durch den Autor) Doch machte dieser wohl aus Rücksicht auf Datenschutzbedenken integrierte Passus zugleich die sehr weitgehende Intention des Ministerrats deutlich: Die anfallenden Daten sollten eben nicht nur für Zwecke der Terrorismusbekämpfung, sondern für jedweden strafrechtlichen Ermittlungszweck verwendet werden können (ebd.).

Zusätzlicher Druck auf die EU-Organe wurde auch aus dem EU-Ausland geübt. Nachdem die Europäischen Institutionen und Mitgliedstaaten im unmittelbaren Nachgang der Anschläge ihre Solidarität und Hilfsbereitschaft gegenüber den Vereinigten Staaten bekundet hatten, sandte die US-Regierung im Namen von Präsident George W. Bush einen Brief an die EU-Kommission bzw. Kommissionspräsident Romano Prodi, in dem die Organe der EU zur Verabschiedung einer Reihe von Sicherheitsmaßnahmen aufgefordert wurden. So wurde die EU u. a. dazu aufgerufen, Datenschutzfragen im Zusammenhang mit den Erfordernissen der Strafverfolgung und der Terrorismusbekämpfung zu berücksichtigen und die bestehenden Rechtsvorschriften im Datenschutzbereich dahingehend zu lockern, dass die *Speicherung kritischer Daten für einen angemessenen Zeitraum* ermöglicht würde (US Mission to the EU 2001). Interessanterweise verfügten nicht einmal die Vereinigten Staaten unter dem PATRIOT Act

zu diesem Zeitpunkt selbst über eine der Öffentlichkeit bekannte Vorratsdatenspeicherung (Bunyan 2002).[163]

Nach Abschluss der Diskussionen im Ausschuss wurde der Entwurf für den zweiten Cappato-Bericht nur kurze Zeit nach dem Anschlägen in den USA am 22. Oktober 2001 vom LIBE-Ausschuss mit 23 Stimmen (bei 14 Gegenstimmen) angenommen und an das Parlamentsplenum überwiesen (Cappato 2001, 5). Dieses setzte sich am 12. November 2001 mit dem Bericht auseinander. Darin bestätigte der Ausschuss – entgegen den Forderungen des Ministerrats und der US-Administration – seine bereits zuvor festgelegte und das Datenschutzniveau stärkende Position hinsichtlich des Umgangs mit Verkehrsdaten. Außerdem kam Berichterstatter Cappato den Bedenken der Sozialdemokraten insofern entgegen, als für SMS-Werbung die Opt-in-Regel festgelegt werden sollte. Dagegen sah der zweite Bericht die Ausweitung der Opt-out-Regel – entgegen dem Parlamentsstandpunkt im ersten Bericht – auf öffentliche Verzeichnisse (also Telefonbücher) vor und auch in Bezug auf den Erhalt von unerbetenen Mails wurde am Opt-out-Prinzip festgehalten. Die Gründe dafür lassen sich besonders gut dem Redebeitrag des LIBE-Ausschussmitglieds Ulrik von Boetticher (EVP-ED, CDU) entnehmen: „Sollte das Parlament Werbung im Bereich business to customer zunächst generell verbieten, wie es der Vorschlag von Frau Paciotti nun vorsieht, werden Unternehmen eben ihre Werbung von den USA oder anderen Drittstaaten aus in die Europäische Union versenden. Nichts, aber auch gar nichts wäre damit für den europäischen Verbraucher gewonnen, einzig der europäische Markt im elektronischen Handel wäre geschwächt. Wir wollen darum den Staaten, die heute ein Opt out-System haben, dieses auch belassen, die Entwicklung beobachten und nach zwei Jahren neu entscheiden. […] Einzig dieser Vorschlag unterstützt die Interessen der Verbraucher, ohne massiv Arbeitsplätze in Europa zu vernichten." (Europäisches Parlament 2001d) Cappato verwies zudem darauf, dass nicht der Versand von E-Mail-Werbung die größte Gefahr für den Datenschutz darstellte, sondern der staatliche Zugriff: „Ich möchte jedoch nicht, dass, nachdem wir unsere große und verständliche Sorge wegen der durch unerbetene Werbe-E-Mails verursachten Belästigung bewiesen haben, wir ande-

163 So hatten nicht nur die Snowden-Enthüllungen die auf Basis des PATRIOT Act erfolgte massenhafte Speicherung von Verbindungsdaten im Rahmen des Überwachungsprogramms PRISMS zu Tage gebracht (Appelbaum und Poitras 2013). Schon vor der NSA praktizierte bereits die Drug Enforcement Agency (DEA) zwischen 1992 und 2013 eine umfassende geheime und keiner demokratischen Kontrolle unterworfene Vorratsdatenspeicherung (Beuth 2015b).

rerseits den nationalen Polizeibehörden demnächst die uneingeschränkte Befugnis erteilen, nach Gutdünken über unsere personenbezogenen Daten zu verfügen. Das ist kein Problem, das einzig und im engeren Sinne nur diese Richtlinie betrifft, sondern ein allgemeineres politisches Problem, dessen bin ich mir bewusst. Ich fürchte, dass wir genau diese Richtung einschlagen; ich fürchte, die größten Gefahren für den Schutz der Privatsphäre gehen nicht von einer mehr oder weniger erbetenen E-Mail-Werbung aus." (ebd.) Zudem verwies Cappato, dem liberalen Verständnis nach individueller Selbstbestimmung entsprechend, darauf, dass es bereits technische Möglichkeiten gäbe, die Absender-Adressen von Spam oder unerbetener Werbung zu blockieren, um fortan keine E-Mails mehr von diesen zu erhalten (ebd.).

Gekontert wurde dieses Argument seitens der sozialdemokratischen Paciotti damit, dass es „neben Leuten wie unserem Berichterstatter, der sich mit der Benutzung elektronischer Instrumente sehr gut auskennt, […] es noch viele [gibt], sehr viele Bürgerinnen und Bürger wie mich, denen der Umgang damit noch wenig vertraut ist und die sich deshalb Sorgen machen." (ebd.) Zudem verknüpfte Paciotti ihre Kritik am Opt-out-Prinzip schließlich mit der Frage nach Nutzer-Vertrauen: „Solange ich also nicht geschützt werde - [sic] und ich spreche für mich persönlich, obwohl es viele andere, vorwiegend ältere Bürgerinnen und Bürger wie mich gibt, die sich weniger auskennen als viele junge Leute - [sic], werde ich keinen Gebrauch vom elektronischen Geschäftsverkehr machen, weil ich kein Vertrauen dazu habe. Die Vorstellung, in einem durch das ganze Internet geisternden Verzeichnis zu stehen, Nachrichten zu erhalten, dann ihre Löschung zu verlangen, sie vorher öffnen zu müssen und zu versuchen, diese Instrumente zu verstehen, ist wenig vertrauenerweckend. Es kann ja sein, dass die Entwicklung der Elektronik einen besseren Schutz ermöglicht, doch zunächst einmal muss diese Entwicklung stattfinden; vorher müssen wir die Möglichkeiten für die Entwicklung des e-Commerce schaffen, wofür es Vertrauen braucht, was mit diesem Vorschlag nicht geschaffen wird." (ebd.)

Der finisch-stämmige sozialdemokratische EU-Kommissar für Industrie und Informationsgesellschaft Erkki Antero Liikanen lehnte die Vorschläge des Berichterstatters mit derselben Begründung ab[164] und ergänzte dies

164 „Wenn wir also positive Rahmenbedingungen für die Entwicklung des elektronischen Geschäftsverkehrs und der Mobildienste der dritten Generation schaffen wollen, müssen wir jetzt dafür zu sorgen, dass die Akzeptanz der drahtlosen Internetdienste nicht durch riesige Mengen von ‚Müll' in der elektronischen Post, für die

mit dem wirtschaftspolitischen Argument, dass das „Ausfiltern dieser unerwünschten Massenwerbung […] schätzungsweise über 8,2 Mio. US-Dollar kosten [werde]." (ebd.)

Lediglich die Abgeordnete und Verfasserin der Stellungnahme des mitberatenden ITRE-Ausschusses, Ilka Schröder (GUE/NGL)[165], vertrat unter Absehung wirtschaftspolitischer Argumente die Position, dass es bei der bevorstehenden Entscheidung um die Selbstbestimmung des Individuums ginge und dem Cappato-Bericht deshalb nicht zugestimmt werden sollte (ebd.).

Der Cappato-Bericht wurde schließlich am 13. November 2001 mit einer großen Mehrheit von 339 Stimmen angenommen. Vor allem die EDD, ELDR (ALDE), EVP-ED, UEN sowie die parteilosen Abgeordneten stimmten weitgehend geschlossen für den Cappato-Bericht. Unterstützung erhielten die Befürworter zudem von etwas weniger als der Hälfte der SPE-Abgeordneten. Die 92 Gegenstimmen setzen sich vor allem aus den Stimmen der Grünen/EFA und der GUE/NGL zusammen.[166] Hinzukamen einige sozialdemokratische und liberale Abweichler. Die 89 Enthaltungen setzten sich hingegen vor allem aus Sozialdemokraten zusammen. Etwa die halbe Fraktion enthielt sich und fand Unterstützung von einem liberalen, vier parteilosen, zwei konservativen, zwei nationalkonservativen/europaskeptischen (UEN) sowie einem grünen Abgeordneten (Europäisches Parlament 2002b, 38 f.).

3.3.2.6 Interinstitutionelle Auseinandersetzungen und ein schaler Kompromiss

Kurz nach Verabschiedung der Parlamentsposition trat der Ministerrat (Telekommunikation) am 6. und 7. Dezember 2001 zusammen und nahm in Art. 15 Abs. 1 erneut die Formulierung auf, dass Verbindungsdaten „während einer begrenzten Zeit gemäß den allgemeinen Grundsätzen des Gemeinschaftsrechts aufbewahrt werden" dürfen sollen. Zugleich demons-

der Verbraucher gegen seinen Willen zahlen soll, erschwert wird." (vgl. Liikanen, in: Europäisches Parlament 2001d)

165 Schröder war Abgeordnete der Grünen auf Bundes- und Europaebene, verließ jedoch aufgrund ihrer Unzufriedenheit mit dem flüchtlings- und militärpolitischen Kurs der Partei (Schröder 2001) die grüne Europafraktion am 27. September 2001 und schloss sich am 28. September 2001 der GUE/NGL an (EP 2020a).

166 Je ein Abgeordneter der Grünen/EFA stimmte für den Vorschlag bzw. enthielt sich. Die GUE/NGL war die einzige Fraktion die ausnahmslos dagegen stimmte (ebd.).

trierte der Ministerrat auf dieser Sitzung seine Enschlossenheit, keine Kompromisse bei der Frage der Speicherung von Verkehrsdaten elektronischer Kommunikation eingehen zu wollen und intensivierte auf diese Weise den Druck auf Kommission und Parlament. Seine Änderungen begründete der Ministerrat später mit den „erheblichen Gefahren, die durch die Ereignisse am 11. September 2001 sichtbar geworden sind," (vgl. Begründung des Rates, Nr. III, in: EU-Ministerrat 2002, 51) Die Kommission signalisierte daraufhin erstmals auf der Ratstagung am 6. Dezember die Bereitschaft, ihren Widerstand gegen die Änderungen in Art. 6 und Art. 15 Abs. 1 aufzugeben, woraufhin die Art. 29-Datenschutzgruppe gegen die Reduktion demokratischer Standards zugunsten von Anti-Terror-Maßnahmen Einspruch erhob und die „zunehmende Tendenz, den Schutz der Privatsphäre als Hindernis eines effizienten Kampfs gegen den Terrorismus darzustellen" mit Nachdruck kritisierte (Bunyan 2002).

Schließlich verabschiedete der Ministerrat seinen zuvor festgelegten Gemeinsamen Standpunkt am 28. Januar 2002 unter der konservativen spanischen Ratspräsidentschaft offiziell (EU-Ministerrat 2002), sodass gemäß dem Mitentscheidungsverfahren das Parlament an der Reihe war, eine zweite Lesung abzuhalten, in der es auf die Ministerratsposition reagiert. Bereits zwei Tage nach Bekanntgabe der Ministerratsposition wandte sich die Kommission in einer Mitteilung an das Parlament, in der sie ihre Unterstützung der Ministerratsposition zum Ausdruck brachte und dem Parlament die Annahme der Ministerratsposition empfiehl (EU-Kommission 2002). Ihren Meinungswechsel begründete die Kommission mit dem Argument, dass die Änderungen des Ministerrats hinsichtlich Art. 15 Abs. 1 aus datenschutzrechtlicher Perspektive unbedenklich seien, da mit ihnen keine generelle Verpflichtung der Mitgliedstaaten zur Speicherung von Verkehrsdaten bzw. zur Abweichung vom Grundsatz der Löschung vorgesehen würde und somit „der erste Satz des Artikels 15 dem Wesen nach rechtlich nicht verändert und [„] ihm nichts hinzugefügt" (ebd.) werde. Dabei handelte es sich freilich um den Versuch der Kommission, angesichts ihres bedingungslosen Einknickens gegenüber den Forderungen der Mitgliedstaaten mithilfe eines rhetorischen Tricks den Anschein von Integrität zu wahren. Denn dass eine Reihe von Mitgliedstaaten bereits spätestens seit dem Jahr 1998 die Einführung einer gemeinschaftsweiten Vorratsdatenspeicherung befürwortete, wird den Kommissionsverantwortlichen hinlänglich bekannt gewesen sein (Statewatch 2001). Insofern konnte der Änderungsvorschlag des Ministerrats – entgegen der Interpretation der Kommission – nur so gedeutet werden, dass mit ihm Tür und Tor für

eine generelle Aufbewahrung von Verkehrsdaten geöffnet würde. Fraglich ist, ob die Kommission zu diesem Zeitpunkt überhaupt noch ernsthaft gegen die Einführung einer unionsweiten Vorratsdatenspeicherung war, oder ob der als Gegnerschaft interpretierte Passus nicht lediglich ein Verweis auf einen primärrechtlichen und zu diesem Zeitpunkt noch ungeklärten Zuständigkeitskonflikt hinsichtlich der Speicherung von Verkehrsdaten zu Zwecken der Strafverfolgung gewesen ist (Bunyan 2002). So begründete die Kommission ihre Ablehnung damit, dass die ePrivacy-Richtlinie, „die sich auf Artikel 95 EG-Vertrag stützt, keine wesentlichen Bestimmungen über Maßnahmen des Gesetzesvollzugs enthalten" dürfe. Dementsprechend sollte sie „keinerlei konkrete Maßnahmen, die die Mitgliedstaaten für notwendig halten mögen, verbieten oder billigen." (ebd.). Die Gegnerschaft der Kommission lässt sich auf Basis dieser Zitate m. E. daher lediglich als ein Verweis auf die ungeklärte Frage, ob derartige Maßnahmen Gegenstand einer Regulierung im Rahmen der ersten oder der dritten Säule zu sein hätten, verstehen.

Am 6. Februar 2002 überwies der Parlamentspräsident den Gemeinsamen Standpunkt des Rates schließlich erneut an den LIBE-Ausschuss. Auf Grundlage des LIBE-Beschlusses vom 29. August 2000 war weiterhin Marco Cappato der zuständige Berichterstatter. Auf drei weiteren LIBE-Sitzungen im Februar, März und April wurde über die Änderungsanträge des Ministerrats beraten und schließlich am 18. April 2002 der Entwurf für eine Stellungnahme des Parlaments für die zweite Lesung mit 36 Stimmen bei 6 Gegenstimmen und 0 Enthaltungen angenommen (Cappato 2002, 4). Der finalen Abstimmung des Ausschusses über den Entwurf als Ganzes war allerdings eine Kampfabstimmung über einen Änderungsantrag der spanischen LIBE-Ausschussvorsitzenden Ana Palacio (EVP-ED, PP) vorangegangen. Palacio hatte im Rahmen eines informellen Trilogs am 16. April, also zwei Tage vor der LIBE-Abstimmung mit Vertretern der Kommission und des Rates verhandelt und dem Schattenberichterstatter der EVP-DE-Fraktion sowie dem britisch stämmigen LIBE-Ausschussmitglied Michael Cashman (SPE, Labour) einen Änderungsantrag vorgelegt, der den Standpunkt des Rates akzeptiert und damit dem Druck der spanischen Ratspräsidentschaft nachgab. Mit diesem Schritt brüskierte Palacio zudem die Ausschuss-Tradition gemäß der nicht noch einmal über Fragen abgestimmt wird, über die bereits zuvor einstimmig entschieden worden war. Palacios Änderungsantrag wurde schließlich mit 25 gegen 19 Stimmen abgelehnt. Die Mehrheit kam dadurch zustande, dass die sozialdemokratischen Ausschussmitglieder gemeinsam mit liberalen, grünen und

linken Ausschussmitgliedern gegen Palacios Vorschlag votierten. Befürwortet wurde dieser dagegen von den Ausschussmitgliedern der konservativen Fraktion, unterstützt von den nationalkonservativen/euroskeptischen sowie europakritischen Fraktionen (Statewatch 2002c).

Nachdem Palacios Vorstoß gescheitert war und die Position des LIBE-Ausschusses angenommen wurde, intensivierte die spanische Ratspräsidentschaft ihre Bemühungen dahingehend, einzelne Abgeordnete unmittelbar zu kontaktieren, um diese von der Annahme eines *Kompromissantrages* bei der für den 15. Mai 2002 angesetzten Abstimmung im Parlamentsplenum zu überzeugen. Ein Blick auf die Größe der Fraktionen zeigt, dass dies aus Ratsperspektive eine vielversprechende Strategie war. So bestand das Parlament zu diesem Zeitpunkt aus insgesamt 626 Abgeordneten. Für die Beschlussfassung wurden 314 Stimmen benötigt, von denen allein 233 durch die konservative EVP-DE-Fraktion beigesteuert werden konnten. Unterstützt wurde sie von den übrigen rechtsgerichteten Fraktionen, der UEN mit 22 Abgeordneten sowie der EDD bestehend aus 18 Abgeordneten, sodass insgesamt bereits 273 der erforderlichen Stimmen erreicht wurden. Dadurch musste die Ratspräsidentschaft *nur* 41 weitere Abgeordnete zur Unterstützung ihres Vorschlags motivieren, um die Verabschiedung ihres Vorschlags abzusichern. Daneben saßen im Parlament insgesamt 32 fraktionslose Abgeordnete, von denen wiederum 18 ehemalige Mitglieder der rechtskonservativ bis rechtsextremen Fraktion[167] der Technischen Fraktion der Unabhängigen Abgeordneten (TDI) waren, die Ende 2001 aufgelöst worden war. Die übrigen, gegenüber der Vorratsdatenspeicherung kritisch eingestellten Fraktionen kamen allerdings gemeinsam auf 321 Stimmen (PSE 179, ELDR 53, Grüne/EFA 45, GUE/NGL 44), sodass für die Ratspräsidentschaft von zentraler Bedeutung war, mögliche Abweichler aus deren Reihen zur Unterstützung der Ratsposition zu bewegen (Statewatch 2002d, 2002e). Um mehr Zeit für ihre Intervention zu haben, erreichte die Ratspräsidentschaft, dass der Abstimmungstermin im Parlament vom 15. Mai auf den 30. Mai verschoben wurde. Währenddessen arbeitete die zuständige Ratsarbeitsgruppe auf ihren Sitzungen am 3. und 13. Mai an der Formulierung eines Kompromissvorschlags, den man dem Parlament unterbreiten würde. Ohne Rücksprache mit dem Berichterstatter Cappato

167 Eine Ausnahme war die Mitgliedschaft der linksliberal-radikalen *Lista Emma Bonino*. Abgesehen davon war die Fraktion Heimat für rechtsextreme Parteien wie *Lega Nord*, *Front National* (der heutigen *Rassemblement National*) und *Vlaams Blok* (der heutigen Vlaams Belang) (European Parliament 1999).

zu halten, initiierte Ana Palacio schließlich am 15. Mai die Übersendung eines Kompromissvorschlags im Namen des Parlaments an den Ministerrat. Der sogenannte Kompromissvorschlag war praktisch derselbe Vorschlag, über den der Ausschuss etwa einen Monat zuvor bereits ablehnend abgestimmt hatte. Als Cappato von dem Vorgang erfuhr, konnte er die offizielle Übersendung verhindern. Allerdings griff die spanische Ratspräsidentschaft nur einen Tag später Palacios Vorschlag trotzdem auf und bewarb diesen beim AStV als grundsätzlich akzeptablen Kompromiss.[168] Während der Ministerrat einerseits auf Seiten des Parlaments auf Kompromissbereitschaft drängte, war er selbst nicht gewillt, Kompromisse einzugehen. Von den 23 Änderungsvorschlägen, die der Cappato-Bericht in Bezug auf die Ratsposition formulierte, war der Rat lediglich bereit, zwei kleinere anzunehmen, während alle anderen abgelehnt wurden (Statewatch 2002d).

Nachdem diese Bemühungen des Ministerrats und der Ausschutzvorsitzenden zum Kippen der Parlamentsabstimmung bekannt geworden waren, wandte sich die Global Internet Liberty Campaign (GILC), eine internationale Koalition bestehend aus 40 Bürgerrechtsorganisation aus 15 Staaten[169] an alle Europaabgeordneten, in der sie diese dazu aufforderten, für die vom LIBE-Ausschuss vorgelegte Empfehlung zu votieren. Interessanterweise wurde diese Forderung zudem nicht nur mit dem Verweis auf individuelle Privatheit, sondern auch mit Gemeinwohlargumenten begründet: „Neue Speicherungserfordernisse, wie sie in der gemeinsamen Position des Rates befürwortet wurden, würden neue Risiken für die persönliche Privatsphäre, die politische Freiheit, die Meinungsfreiheit und die öffentliche Sicherheit bedeuten." (GILC 2002) Daneben wurde eine internationale Unterschriftenkampagne der 2001 gegründeten, überwachungskritischen Bürgerinitiative *STOP1984* innerhalb kurzer Zeit von mehr als 17.000 Menschen in 48 Staaten unterzeichnet (Europäisches Parlament 2002c; Statewatch 2002a). Kritik kam auch von Seiten der Wirtschaft. Die von einer Vorratsdatenspeicherung betroffenen europäischen Internet Service Provider bzw. deren Verbände wandten sich in einer gemeinsamen Stellungnahme im April 2002 gegen die Einführung der Vorratsdatenspeicherung. Diese verwiesen einerseits auf die Grundrechtseingriffe infolge einer Vorratsdatenspeicherung und andererseits auf die im Zusammenhang mit

168 Für einen Überblick über die konkreten Änderungsvorschläge zu Art. 15 Abs. 1, siehe: (Statewatch 2002d).

169 Darunter ACLU, Bits of Freedom, CDT, DVD, EFF, EPIC, PI, Statewatch, quintessenz (GILC 2002).

der Einrichtung und dem Betrieb einer Vorratsdatenspeicherung zusammenhängenden Kosten (ETNO, EuroISPA, und ECTA 2002).

Währenddessen hatte auch der Ministerrat seinen Druck auf das Parlament weiter intensiviert. Nachdem die konservative LIBE-Ausschussvorsitzende Palacio bereits zuvor auf den Kurs des spanischen Ratsvorsitzes umgeschwenkt war, gelang es kurz vor der Abstimmung des Parlaments auch Elena Paciotti, das führende SPE-Mitglied im LIBE-Ausschuss davon zu überzeugen, der Ratsposition zuzustimmen. Der Meinungsumschwung der Konservativen und Sozialdemokraten wurde von diesen auf der folgenden Plenardiskussion des Parlaments am 29. Mai 2002, an der Ana Palacio[170] übrigens nicht teilnahm, damit begründet, dass die Mitgliedstaaten die entsprechenden Regelungen zur Vorratsdatenspeicherung selbst im Falle eines Parlamentsvetos, bei dem zudem das gesamte ePrivacy-Richtlinienvorhaben scheitern würde, ohnehin auf Basis mitgliedstaatlicher und/oder intergouvernementaler Maßnahmen durchsetzen würden.[171] Dies wiederum würde das Parlament jeglicher Mitgestaltung berauben, weshalb ein zugegebenermaßen unzureichender Kompromiss im Falle der ePrivacy-Richtlinie zu akzeptieren wäre (vgl. hierzu insb. die Ausführungen von Boettichers, Paciottis und Cederschiölds, in: Europäisches Parlament 2002c).[172] Dem

170 Die Verdienste Ana Palacios sollten schließlich nicht unbelohnt bleiben. Am 9. Juli schied die spanische Europaabgeordnete aus dem Parlament aus und trat ihre neue Stelle als erste spanische Außenministerin in der konservativen Regierung José María Aznars an und behielt diese Position bis zur Abwahl der Regierung am 16. April 2004 (Wikipedia 2019a).

171 Dies ist allerdings als eine leere Behauptung zu bewerten, da für einen intergouvernementalen Rahmenbeschluss die Einstimmigkeit im Rat erforderlich gewesen wäre, die es aber weder zu diesem Zeitpunkt noch später gegeben hat. Die Behauptung, dass der Erlass entsprechender Maßnahmen seitens einzelner Mitgliedstaaten schwerer wiege als eine Unionsmaßnahme kann jedoch nur von Relevanz sein, sofern die Unionsmaßnahme deutlich bürgerrechtsfreundlicher gestaltet wäre als die nationalen Maßnahmen. Wie sich im politischen Entscheidungsprozess der EG-Richtlinie zur Vorratsdatenspeicherung wenig später zeigen sollte, konnte das Parlament keinen nennenswerten Einfluss auf die Ausgestaltung der Unionsmaßnahme nehmen (vgl. 3.3.4.2 zur Richtlinie 2006/24/EG).

172 So etwa die konservative Cederschiöld, die für den *Kompromiss* stimmte: „Leider ist es schwer, Befriedigung angesichts des Ergebnisses zu empfinden, aber nationale Vorschriften würden noch größere Unterschiede und umfassendere Probleme schaffen." (Europäisches Parlament 2002c) Paciotti verteidigte ihr Vorgehen folgendermaßen: „Wie jede Lösung, die einen Ausgleich zwischen verschiedenen Interessen herstellen soll, muss auch diese hier im Ganzen beurteilt werden. Mir erscheint sie vernünftig und unterstützenswert, da es gewiss nicht in der Macht des Europäischen Parlaments steht, vom Rat zu erreichen, dass er den Mitgliedstaaten die

Ministerrat spielte zudem der Umstand in die Hände, dass die übrigen fünf Richtlinien des neuen Rahmens für die elektronische Kommunikation bereits zum 24. April 2002 in Kraft getreten waren und alle beteiligten Akteure daher möglichst bemüht darum waren, die bereits zu diesem Zeitpunkt verspätete Verabschiedung der ePrivacy-Richtlinie durch die Initiierung eines Vermittlungsverfahrens nicht noch weiter zu verzögern oder gar die Verabschiedung grundsätzlich zu gefährden.[173] Daneben war der Ministerrat Paciotti im Hinblick auf die von den Sozialdemokraten favorisierte und von Berichterstatter Cappato abgelehnte Opt-in-Regelung entgegenkommen und trat im Rahmen der Einigung gegen die im Cappato-Bericht vorgeschlagene europaweite Opt-out-Regelung ein und überlies die Entscheidung den Mitgliedstaaten, sodass Paciotti bei dieser ihr wichtigen Frage durchaus auch einen Teilerfolg verzeichnen konnte. Darüber hinaus war insbesondere Paciotti darum bemüht, die mit dem Ministerrat erzielte Einigung als Kompromiss darzustellen. Sowohl in ihrer Antwort an die Bürgerrechtskoalition als auch während der Plenardebatte vertrat sie die Ansicht, dass die mit dem Ministerrat erzielte Einigung deshalb als Kompromiss zu bezeichnen wäre, weil sie es geschafft hätte, in den zur Debatte stehenden Artikeln explizite Verweise auf die Vereinbarkeit der zu verabschiedenden Maßnahmen mit der EMRK, Art. 6 EUV und der Rechtsprechung des EGMR unterzubringen, die andernfalls keine Erwähnung gefunden hätten (Europäisches Parlament 2002c; Statewatch 2002b). Der Ministerrat dagegen hatte keine Probleme mit den entsprechenden Verweisen, da sie ohnehin auf jede Gemeinschaftsmaßnahme Anwendung fanden und damit als keine zusätzliche Maßregelung der von den Strafverfolgungsbehörden geforderten Maßnahmen zu verstehen waren. Aufgrund dessen wurde Paciotti dann auch berechtigterweise Augenwischerei vorgeworfen (Statewatch 2002b) – fraglich ist allein, ob sie persönlich tatsächlich der Ansicht war, einen wirklichen Kompromiss erzielt zu haben oder dies aus anderen Gründen lediglich behauptete. Deutlich klarer artikulierte ihr britischer Parteikollege Michael Cashman seine Befürwortung der Ministerratsposition: „Vielleicht darf ich Sie daran erinnern, dass die bürgerlichen

Aufbewahrung von Verkehrsdaten aus Gründen der nationalen Sicherheit untersagt. Wir können das nicht verbieten; wir können einen Rahmen der Garantien, der Sicherheiten und des Schutzes der Grundrechte abstecken, damit diese durch die künftige Gesetzgebung gewahrt werden müssen." (ebd.)

173 Wie den Äußerungen von Kommissar Liikanen zu entnehmen ist, war dies offenbar einer der ausschlaggebenden Gründe für den Positionswechsel der Kommission (Europäisches Parlament 2002c).

Freiheiten vor international operierenden Terroristen geschützt werden müssen, vor Drogenhändlern, internationalen Verbrechern, Frauen- und Kinderhändlern. Das sind die bürgerlichen Freiheiten, die wir mit den angemessenen und ausgewogenen Bestimmungen zur Datenspeicherung in den dem Parlament vorliegenden Vorschlägen schützen wollen." (Europäisches Parlament 2002c) Hervorzuheben ist zudem, dass in der Kritik der ELDR und der EVP-DE neben bürgerrechtlichen Erwägungen die für die Wirtschaft drohenden Kosten einer Vorratsdatenspeicherung thematisiert wurden.[174] Lediglich die Vertreterin der Linken, Ilka Schröder, verwies auf die potentiellen gesellschaftlichen Folgen einer durch die Vorratsdatenspeicherung ermöglichten Massenüberwachung (ebd.).

Bei der finalen Abstimmung im Parlament am 30. Mai 2002 votierte schließlich eine aus EVP-DE und SPE geformte Mehrheit der Europaparlamentarier gegen die Empfehlungen des Cappato-Berichts und für den *Kompromiss*, der die Ministerratsposition bestätigte. So wurde der umstrittene zweite Teil des Änderungsantrags 46 mit 351 Stimmen (bei 133 Gegenstimmen und 13 Enthaltungen) angenommen. Während es bei den Konservativen und Sozialdemokraten kaum Abweichler gab, erhielten sie von der Mehrheit der EDD- und der UEN-Fraktion, von einigen liberalen und fraktionslosen sowie seitens eines grünen Abgeordneten Unterstützung. Dagegen stimmten die vollständige GUE/NGL-Fraktion, die Mehrheit der ELDR, der Grünen/EFA und fraktionslosen Abgeordneten sowie einzelne Abgeordnete der übrigen Fraktionen (Europäisches Parlament 2003, 54 f.). Der Ministerrat bestätigte die in zweiter Lesung des Parlaments angenommenen Änderungsanträge am 25. Juni, sodass die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG am 12. Juli 2002 vom Präsidenten des Parlaments und der Ratspräsidentschaft unterzeichnet wurde und am darauffolgenden Tag in Kraft trat (Das Europäische Parlament und der Rat der Europäischen Union 2002).

Wie schon zuvor im Falle der DS-RL und der ISDN-RL erfolgte auch die Umsetzung der ePrivacy-Richtlinie teils mit erheblicher Verzögerung. Die ePrivacy-Richtlinie musste in den alten Mitgliedstaaten bis zum 30. Oktober 2003 und in den zehn neuen Mitgliedstaaten bis zum 1. Mai 2004 umgesetzt werden. Dieser Verpflichtung kam nur ein Teil der Mitgliedstaaten nach, sodass die Kommission Ende 2004 Vertragsverletzungsverfahren gegen die fünf Mitgliedstaaten Belgien, die tschechische Republik, Estland,

174 Vgl. hierzu die Ausführungen der Liberalen Plooij-van Gorsel und der Konservativen Charlotte Cederschiöld (Europäisches Parlament 2002c).

Griechenland und Luxemburg initiierte (EU Commission 2004, 6 f. EU-Kommission 2004, 9). Die Richtlinie wurde schließlich in Estland Ende 2004 (EU-Kommission 2005, 30), in Belgien, in Tschechien und in Luxemburg im Laufe des Jahres 2005 (EU-Kommission 2006, 19, 26, 78) sowie in Griechenland erst 2006 (Europäische Kommission 2008a, 57) in nationales Recht umgesetzt.

3.3.2.7 Zwischenfazit

Der politische Aushandlungsprozess der ePrivacy-Richtlinie war aus mehreren Gründen wichtig für die EU-Datenschutzpolitik. *Erstens* zeichneten sich hier erstmals in aller Deutlichkeit die Fronten zwischen den parteipolitischen Akteuren ab, die fortan relativ stabil bleiben sollten. Während das Europäische Parlament in den 1970er- und 1980er-Jahren noch als Datenschutzbefürworter aufgetreten und für den Erlass von Datenschutzregelungen eingetreten war, hatte es während der Aushandlung der DS-RL eine eher ambivalente Rolle eingenommen. An den Konflikten bei der Aushandlung der ePrivacy-Richtlinie differenzierte sich diese Rolle nun aus: Es zeigte sich erstmals in offensichtlicher Weise auf EU-Ebene, dass es vier Fronten gab: Eine *liberale Perspektive* auf Datenschutz, die unter Verweis auf die Selbstbestimmungsfähigkeit des Einzelnen und unter Absehung der Verwirklichungsbedingungen dieser für weniger Einschränkungen gegenüber privatwirtschaftlichen Datenverarbeitern eintrat, aber zugleich eine stärkere Rolle des Staates strikt ablehnt. Privatwirtschaftliche Datenverarbeiter standen dieser Perspektive am nächsten. Daneben eine *konservative Perspektive*, die einen möglichst weitreichenden Verarbeitungsspielraum sowohl für privatwirtschaftliche als auch für staatliche Akteure einfordert. Eine *grundrechtsorientierte Perspektive* auf Datenschutz, die einen möglichst umfassenden Schutz personenbezogener Daten vor privatwirtschaftlichen sowie staatlichen Akteuren fordert. Dieser Perspektive standen sowohl Datenschutzaufsichtsbehörden als auch zivilgesellschaftliche Datenschützer nahe. Und schließlich eine *sozialdemokratische Perspektive* auf Datenschutz, die einer grundrechtsorientierten Perspektive zwar nahestand und für Einschränkungen gegenüber privatwirtschaftlichen Akteuren eintrat, aus Gründen der Staatsraison allerdings letztlich einer weitgehenden staatlichen Datenverarbeitung zustimmte. Die politische Einigung, die letztlich erzielt wurde, spiegelt einen Kompromiss zwischen konservativer und sozialdemokratischer Perspektive wider.

Zweitens bildete der Aushandlungsprozess der ePrivacy-Richtlinie den ersten politischen Konflikt auf EU-Ebene, bei dem sich eine transnationale Koalition aus Bürgerrechtsorganisationen[175] auf die Seite der parlamentarischen Vertreter der grundrechtsorientierten Perspektive schlug und damit den ersten Grundstein zur Bildung einer längerfristigen Advocacy-Koalition der Datenschutzbefürworter legte.[176]

Schließlich und *drittens* bildete der Erfolg der Überwachungsbefürworter den Anfangspunkt einer Reihe von politischen Niederlagen, denen sich Datenschutzbefürworter in den Folgejahren gegenübersahen. Diese politischen Niederlagen bzw. der dabei erreichte Ausbau der Überwachungsmöglichkeiten sollte später wesentlich dazu beitragen, dass die EU-Datenschutzreform als eine Reaktion auf diese Prozesse eingeleitet und letztlich auch erfolgreich zu Ende gebracht wurde.

3.3.3 Berichte der Kommission über die Durchführung der DS-RL

In Art. 33 der DS-RL 95/46/EG wurde geregelt, dass die Kommission dem Europäischen Parlament und dem Ministerrat regelmäßig einen Bericht über die Durchführung der Richtlinie vorlegen und gegebenenfalls geeignete Änderungsvorschläge machen sollte. Art. 33 sah die Veröffentlichung des ersten Berichts drei Jahre nach Ablauf der in Art. 32 Abs. 1 vorgesehenen dreijährigen Umsetzungsfrist (1998), also im Jahr 2001 vor. Aufgrund der verzögerten Umsetzung der DS-RL in den Mitgliedstaaten (vgl. 3.2.2.9) verschob sich die Veröffentlichung des Berichts allerdings um 18 Monate, sodass die Kommission diesen erst am 15. Mai 2003 vorlegte (KOM 2003, 3). Bei der Erarbeitung des Berichts stützte sich die Kommission auf ihre neue, insb. im Kommissionsweißbuch vom Juli 2001 für das Europäische Regieren niedergelegte, Governance-Strategie (EU-Kommission 2001b), mit der eine breite Beteiligung verschiedener gesellschaftlicher Gruppen

175 So insb. die GILC, zu deren Mitgliedern zu diesem Zeitpunk ACLU, Bits of Freedom, CDT, DVD, EFF, EPIC, Privacy International, Statewatch, quintessenz zählten (GILC 2002).

176 Die Ausweitung von Überwachungsmaßnahmen auf EU-Ebene war dann auch ein wesentlicher Grund, der zur Entstehung der European Digital Rights Initiative (EDRi) im Sommer 2002 führte (Ziegler 2002). EDRi sollte schließlich die GILC, die ihre Aktivitäten seit 2003 einstellte, ablösen und zum zentralen zivilgesellschaftlichen Akteur der Community der Datenschutzbefürworter aufsteigen (vgl. 3.4.2.3.1).

gewährleistet werden sollte (KOM 2003, 3). Zu diesem Zweck stellte die Kommission im Jahr 2002 „Fragen an die Regierungen der Mitgliedstaaten und getrennt an die Datenschutzbehörden […]; [gab] zwei wissenschaftliche Studien in Auftrag […]; [veröffentlichte] im Amtsblatt und auf der Kommissionswebsite eine Aufforderung zur Abgabe von Stellungnahmen […]; [stellte] zwei Fragebogen über zwei Monate lang auf ihre Website […], einen, der sich an für die Verarbeitung Verantwortliche richtete, und einen für von der Verarbeitung Betroffene; [und veranstaltete] eine internationale Konferenz […], auf der in sechs verschiedenen Workshops ein umfangreiches Themenspektrum erörtert wurde." (ebd., 7)[177] Während Wirtschaftsvertreter und Behörden der Aufforderung zur Abgabe von Stellungnahmen folgten, beteiligte sich aus den Reihen jener Organisationen, die Bürgerrechtsinteressen vertraten, lediglich BEUC[178] am schriftlichen Konsultationsprozess (ebd.).

3.3.3.1 Die Ergebnisse des Berichts: Kritikpunkte

Im Hinblick auf den *Hauptzweck* der Richtlinie in Gestalt der Gewährleistung des freien Datenverkehrs stellte die Kommission fest, dass trotz des Vorhandenseins subtilerer Behinderungen des freien Datenverkehrs[179] keine Aussetzung oder Ablehnung eines grenzüberschreitenden Datentransfers zwischen Mitgliedstaaten stattgefunden habe, der Hauptzweck der

177 An der internationalen Konferenz nahmen neben Kommissions-, Parlaments und Ministerratsangehörigen insb. Vertreter aus den nationalen Datenschutzaufsichtsbehörden, der Industrie und Verbraucher- bzw. Datenschutzorganisationen teil. Folgende Akteure, die später am Aushandlungsprozess der DSGVO beteiligt waren, partizipierten auch an dieser Konsultation: GDV, Yahoo, UNICE/Businesseurope und FEDMA auf Seiten der Industrie. Vonseiten der Zivilgesellschaft waren BEUC, EPIC und Privacy International beteiligt. Darüber hinaus beteiligten sich auch Vertreter der US Federal Trade Commission, der OECD und des EGMR an der Konferenz (European Commission 2002). An der schriftlichen Konsultation nahmen die folgenden Akteure teil: ACCIS, AmCham EU, BITKOM, EMOTA, ENPA, EPC, ETNO, Eurofinas, BEUC, FEDMA, GDD, IAB, ICC, Telefónica, UNIC/Businesseurope, ZAW (EU-Kommission 2003).

178 BEUC ist ein 1962 gegründeter europäischer Zusammenschluss nationaler Verbraucherschutzorganisationen. Ihm gehören mehrere Dutzend nationale Verbände an (BEUC 2013).

179 Etwa der Erlass unterschiedlich strenger Vorschriften in verschiedenen Mitgliedstaaten, die „zunächst die interne Verarbeitung personenbezogener Daten in diesem Mitgliedstaat und in der Folge auch den Export dieser Daten in andere Mitgliedstaaten einschränken." (ebd., 11)

Richtlinie daher als erfüllt zu bewerten sei. Auch das Ziel der Gewährleistung eines hohen Datenschutzniveaus sah die Kommission – trotz anderslautender Ergebnisse der Online-Befragung, in der die teilnehmenden EU-Bürgerinnen und -Bürger sowohl das Schutzniveau als auch den Informationsstand über den Datenschutz kritisierten – als weitgehend erfüllt an (ebd., 10 f.). Vertreter multinationaler Unternehmen bemängelten derweilen insbesondere die abweichende Umsetzung der Richtlinienvorgaben (beispielsweise Schwierigkeiten beim anwendbaren einzelstaatlichen Recht, die unterschiedliche Umsetzung der Meldepflicht sowie abweichende Bedingungen für grenzüberschreitende Datentransfers) in verschiedenen Mitgliedstaaten. Die von einigen dieser Unternehmen vorgeschlagene Harmonisierung der nationalen Divergenzen auf dem Wege einer Änderung der Richtlinie lehnte die Kommission unter Verweis darauf, dass mit der Richtlinie eine Annäherung und nicht vollständige Vereinheitlichung angestrebt werde, nationale Divergenzen also zu verkraften sein sollten, ab (ebd., 12). Zugleich sah die Kommission aber durchaus ein, dass selbst in Bereichen, für die eine weitgehende Harmonisierung vorgesehen war, inakzeptable Divergenzen entstanden seien: „z. B. bei den ‚Begriffsbestimmungen' oder den abschließenden Aufzählungen in der Richtlinie wie in Artikel 7 (Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung), 8 Abs. 1 (sensible Daten), 10 (Informationen der Betroffenen), 13 (Ausnahmen, 26 (Ausnahmen bezüglich der Übermittlung in Drittländer usw.)." (ebd.)

Eine der am häufigsten kritisierten Bestimmungen war jene des *Art. 4 zum anwendbaren einzelstaatlichen Recht*. In diesem Zusammenhang forderten einige der betroffenen Verantwortlichen die Einführung des Herkunftslandprinzips, da dieses den „internationalen Organisationen ermöglichen würde, innerhalb der EU mit einem einzigen Regelwerk arbeiten zu können." (ebd., 18) Zudem wurde die Regel kritisiert, dass EU-Recht lediglich auf außerhalb der EU niedergelassene für die Verarbeitung Verantwortliche anwendbar war, sofern diese zum Zwecke der Verarbeitung personenbezogener Daten auf Mittel (i. S. v. Gerätschaften zur Verarbeitung) zurückgriffen, die im Hoheitsgebiet eines Mitgliedstaates belegen waren.

Eine weitere sehr häufig kritisierte Bestimmung war die in den Art. 18 und 19 geregelte *Meldepflicht*. Unternehmensvertreter forderten die Vereinfachung der Regelungen und ihre gemeinschaftsweite Harmonisierung (ebd., 19).

Schließlich stellte die Kommission im Zusammenhang mit der *Übermittlung personenbezogener Daten in Drittländer* fest, dass einige Mitgliedstaaten die Beurteilung der Angemessenheit des vom Empfänger garantierten

Schutzniveaus auf unzulässige Weise dem für die Verarbeitung Verantwortlichen übertrugen, während andere Mitgliedstaaten alle Übermittlungen in Drittländer auch dann von einer Genehmigung abhängig zu machen versuchten, wenn für das entsprechende Drittland bereits ein Angemessenheitsbefund vorlag. Im Zusammenhang mit dem zu nachsichtigen Umgang mit grenzüberschreitenden Datenübermittlungen wies die Kommission auf die Gefahr hin, „dass der Schutz in der gesamten EU geschwächt wird, weil aufgrund des durch die Richtlinie garantierten freien Datenverkehrs die Datenströme wahrscheinlich über die ‚am wenigsten aufwändigen' Ausfuhrwege geleitet werden." (ebd., 20) Andererseits betonte die Kommission, dass ein zu strenger Ansatz „die legitimen Erfordernisse des internationalen Warenverkehrs und die Realität der globalen Telekommunikationsnetze ignorieren und die Gefahr bergen [würde], dass sich eine Kluft zwischen Gesetz und Praxis [auftue], die der Glaubwürdigkeit der Richtlinie und der Rechtsvorschriften der Gemeinschaft generell [schade] […]." (ebd.)

Neben diesen Punkten wurden Mängel auch bei der Umsetzung von Art. 6 (Abs. 1 lit. b hinsichtlich der Weiterverarbeitung zu historischen, statistischen oder wissenschaftlichen Zwecken) und von Art. 7 festgestellt. Die Liste der Gründe für eine rechtmäßige Verarbeitung sei auf unzulässige Weise von einigen Mitgliedstaaten erweitert und von anderen Mitgliedstaaten gekürzt worden. Zudem seien Divergenzen im Hinblick auf die Interpretation der Einwilligung ohne jeden Zweifel (Art. 7 lit. a) und der ausdrücklichen Einwilligung (Art. 8) festzustellen, die zu klären seien. Die Kommission stellte zudem fest, dass die Information der Betroffenen gemäß den Art. 10 und 11 eine Reihe von Abweichungen aufgewiesen habe, die auf divergierende Umsetzungen in den Mitgliedstaaten und auf abweichende Auslegungen und Praktiken der Datenschutzaufsichtsbehörden zurückzuführen seien, in deren Ergebnis die Verantwortlichen mit unterschiedlichen Anforderungen konfrontiert seien und ihre Informationspflichten nicht im Sinne des zu erreichenden Schutzniveaus wahrnehmen könnten (ebd., 19).

Neben diesen von den konsultierten Akteuren benannten Punkten machte die Kommission auch selbst auf drei miteinander verflochtene Phänomene aus den Bereichen der Rechtsdurchsetzung, Rechtsbefolgung und Sensibilisierung aufmerksam: So seien die auf Seiten der Datenschutzaufsichtsbehörden vorhandenen Ressourcen zur Erfüllung ihres breiten Aufgabenspektrums unzureichend, sodass zu selten auf Durchsetzungsmaßnahmen zurückgegriffen werde. Verantwortliche, die die Datenschutzvorschriften nicht befolgten, würden sich in der Folge nur einem sehr geringen

Risiko ausgesetzt sehen, weshalb sie wiederum ein geringes Interesse an der Änderung ihrer Verarbeitungspraktiken zeigten. Aufgrund des geringen Kenntnisstands der Betroffenen über ihre Betroffenenrechte würden zudem nur wenige Betroffene die ihnen zustehenden Rechte wahrnehmen, sodass die von den Datenschutzaufsichtsbehörden nicht aufgedeckte mangelnde Vorschriftenbefolgung der Verantwortlichen auch seitens der Betroffenen nicht wahrgenommen bzw. angegangen werde (ebd., 13 f.).

3.3.3.2 Die Ergebnisse des Berichts: Lösungsvorschläge und Arbeitsprogramm der Kommission

Nach Ende der Konsultation lagen mehrere Maßnahmenvorschläge zum Umgang mit den identifizierten Defiziten vor. Seitens einiger Wirtschaftsvertreter sowie Österreichs, Schwedens, Finnlands und des Vereinigten Königreichs wurden detaillierte Vorschläge zur Änderung der DS-RL vorgelegt, die zum Ziel hatten, den bürokratischen Aufwand der für die Verarbeitung Verantwortlichen bei der Befolgung der Richtlinie zu senken und die Richtlinie besser an die neuen Erfordernisse der Online-Umgebung anzupassen (ebd., 7 f.).[180] Lediglich BEUC machte im Gegensatz zu dieser Position geltend, dass „es die Online-Umgebung sei, die angepasst werden müsse, um sicherzustellen, dass die Grundsätze der Richtlinie uneingeschränkt beachtet werden." (ebd., 7)

Die Kommission selbst vertrat die Position, dass eine Änderung der Richtlinie *in nächster Zukunft* aufgrund mehrerer Faktoren nicht sinnvoll wäre. Zunächst sei aufgrund der verspäteten Umsetzung der Richtlinie in den Mitgliedstaaten keine ausreichende Erfahrungsgrundlage gegeben, eine Änderung zu dem Zeitpunkt also noch verfrüht. Daneben konstatierte die Kommission, dass viele der im Konsultationsprozess benannten Schwierigkeiten ohne eine Änderung der Richtlinie behoben werden könnten (vgl. das von der Kommission verabschiedete Arbeitsprogramm weiter unten): Nicht die Richtlinie, sondern die divergierende Umsetzung von deren Vorgaben im mitliedstaatlichen Recht seien das Problem, das adressiert werden müsse. Schließlich sprach sich die Kommission auch deshalb gegen die

180 Während Wirtschaftsvertreter in der Vergangenheit europäische Datenschutzregelungen mehrheitlich prinzipiell abgelehnt hatten (vgl. Unterabschnitt 3.2.2), vertrat nunmehr eine Mehrheit von 69,1% der Antwortenden die Ansicht, dass Datenschutzvorschriften notwendig seien. Lediglich 2,64% forderten die vollständige Abschaffung von Datenschutzregelungen (ebd., 10).

Änderung der Richtlinie aus, da viele der vorgeschlagenen Änderungen zugleich die Senkung des Datenschutzniveaus nach sich gezogen hätten. Stattdessen hob die Kommission hervor, dass alle potentiellen Änderungen „auf die Aufrechterhaltung des Datenschutzniveaus zielen und mit dem Gesamtrahmen in Einklang stehen [sollten], der durch die bestehenden internationalen Instrumente [gemeint sind die OECD-Richtlinien und die Datenschutz-Konvention des Europarats, M. K.] vorgegeben ist." (ebd., 8). Daher setzte die Kommission insbesondere auf freiwillige Harmonisierungsmaßnahmen der Mitgliedstaaten sowie auf die engere Zusammenarbeit zwischen den Kontrollstellen unter der Anleitung der Kommission bzw. der Art. 29-Datenschutzgruppe und in einzelnen Fällen auch unter Beteiligung der Verantwortlichen (ebd., 13 und 24).

Das für die Jahre 2003 und 2004 vorgesehene Arbeitsprogramm der Kommission für eine bessere Durchführung der DS-RL sah zehn Maßnahmen vor, mit denen die identifizierten Kritikpunkte angegangen werden sollten und die im Folgenden kurz vorgestellt werden. Maßnahme 1 sah die Erörterung erforderlicher Änderungen mit den Mitgliedstaaten und gegebenenfalls auch mit den zuständigen Datenschutzaufsichtsbehörden sowie im Rahmen der Art. 29-Datenschutzgruppe vor (ebd., 24). Maßnahme 2 sah die intensivierte Einbeziehung der EU-Beitrittsländer[181] in die Bemühungen um eine bessere und einheitliche Durchführung der DS-RL vor, um die bestmögliche Harmonisierung der Rechtsvorschriften der neuen Mitgliedstaaten an die Richtlinienvorschriften zu erreichen (ebd., 25). Maßnahme 3 beinhaltete organisatorische und kommunikative Maßnahmen, mit denen zum einen weitere Daten über die Durchführung der Richtlinie erhoben werden sollten, indem die nationalen Datenschutzaufsichtsbehörden und die Mitgliedstaaten zu mehr Kooperation und Kommunikation angehalten würden. Daneben sah die Maßnahme die Veröffentlichung zentraler Informationen auf der Webseite der Kommission vor (ebd.). Mit Maßnahme 4 wurde die Art. 29-Datenschutzgruppe damit beauftragt, ihre Anstrengungen auf dem Gebiet der Durchsetzung zu intensivieren, indem sie sektorale Untersuchungen auf EU-Ebene durchführt und auf Basis der gewonnenen Daten den betroffenen Sektoren gemeinsame Empfehlungen und praktische Hinweise an die Hand gibt, die eine harmonisierte Umsetzung der Richtlinienvorgaben gewährleisten (ebd., 26). Im Hinblick auf die

181 Estland, Lettland, Litauen, Polen, Tschechien, Slowenien, Slowakei, Ungarn, Malta sowie Zypern traten am 1. Mai 2004 der EU bei.

Kritik im Zusammenhang mit der uneinheitlichen Umsetzung der Meldepflicht sah Maßnahme 5 vor, dass die Art. 29-Datenschutzgruppe Vorschläge – inklusive Vorschläge zur Änderung einzelstaatlicher Rechtsvorschriften – für „eine wesentliche Vereinfachung der Meldeanforderungen in den Mitgliedstaaten und für Zusammenarbeitsmechanismen zur Vereinfachung der Meldungen internationaler Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten unterbreitet" (ebd.). Im Hinblick auf das Problem der divergierenden Bestimmungen zu Informationspflichten kündigte die Kommission im Rahmen der Maßnahme 6 einen Dialog mit den Mitgliedstaaten an, an dessen Ende korrigierende rechtliche Maßnahmen stehen sollten. Zudem rief die Kommission die Datenschutzgruppe dazu auf, bei der Suche nach einer Harmonisierung der Informationspflichten mitzuwirken (ebd., 26 f.). Mit Maßnahme 7 bezweckte die Kommission die Vereinfachung der Anforderungen für internationale Übermittlungen. In Zusammenarbeit mit der Art. 29-Datenschutzgruppe und dem Artikel-31-Ausschuss sah die Maßnahme Fortschritte in vier Bereichen vor: Von einer Ausweitung der Angemessenheitsentscheidungen über die Genehmigung von mehr Standardvertragsklauseln und mehr unternehmensinternen Vorschriften auf Basis von Selbstregulierung bis hin zur einheitlichen Auslegung der Ausnahmeregelungen (ebd., 27). Maßnahme 8 sah die Förderung von Technologien zur Verbesserung des Datenschutzes vor: „Die Idee, die hinter den PETs steht, ist die von Informations- und Kommunikationssystemen und -technologien, die so ausgelegt sind, dass die Erhebung und Nutzung personenbezogener Daten minimiert wird und unzulässige Verarbeitungsformen verhindert werden. *Die Kommission hält den Einsatz geeigneter technologischer Maßnahmen für eine unverzichtbare Ergänzung rechtlicher Maßnahme und ist der Auffassung, dass sie integraler Bestandteil jeglicher Bemühungen um einen [sic] ausreichendes Datenschutzniveau sein sollten.*" (ebd., 17, Hervorhebung M. K.) Dabei unterschied die Kommission zwischen solchen Produkten, die (1) voll und ganz den Anforderungen der Richtlinie entsprechen, die (2) einen Schritt weitergehen und bestimmte Aspekte des Datenschutzes für Benutzende besser zugänglich machen, bspw. durch Benutzerfreundlichkeit und die (3) einen maximalen Datenschutz unter Rückgriff auf Anonymisierungstechniken gewährleisten (ebd.). Die Kommission kündigte an, einen Fach-Workshop zum Thema PETs zu veranstalten, auf dem auch mögliche Implementierungsmaßnahmen

wie Gütesiegel, Zertifizierungssysteme[182] oder PIAs[183] diskutiert werden sollten. Die Datenschutzgruppe wurde dazu angehalten, die Frage der PETs weiter zu erörtern und über Möglichkeiten der Förderung von PETs auf nationaler Ebene nachzudenken. Zudem wies die Kommission darauf hin, „dass Regierungen und Einrichtungen des öffentlichen Sektors ermutigt werden müssen, mit gutem Beispiel voranzugehen und PETs bei ihren Verarbeitungen, z.B. [sic] in den E-Government-Anwendungen, zu benutzen." (ebd., 28) Mit der Maßnahme 9 drückte die Kommission zunächst ihre Enttäuschung darüber aus, dass die Möglichkeit der Vorlage sektoraler Verhaltenskodizes nur von sehr wenigen Einrichtungen wahrgenommen worden war, forderte aber Branchen und Interessengruppen dennoch ein weiteres Mal dazu auf, „eine viel aktivere Rolle zu übernehmen, da sie glaubt, dass die Selbstregulierung und insbesondere Verhaltenskodizes eine wichtige Rolle bei der zukünftigen Entwicklung des Datenschutzes innerhalb und außerhalb der EU spielen sollten, nicht zuletzt, um zu detaillierte Rechtsvorschriften zu vermeiden." (ebd., 28) Maßnahme 10 sah schließlich die verstärkte Thematisierung von Datenschutzfragen in der Öffentlichkeit vor. Dazu kündigte die Kommission zum einen die Durchführung einer Eurobarometer-Umfrage unter der europäischen Bevölkerung an und forderte zum anderen die Mitgliedstaaten dazu auf, mehr Ressourcen für die Sensibilisierung der Öffentlichkeit insbesondere in den Haushalten der nationalen Datenschutzaufsichtsbehörden bereitzustellen (ebd., 29).

182 Dass die Kommission bereits zu diesem Zeitpunkt ernsthaft über die Ausweitung von Zertifizierungssystemen und Gütesiegeln nachdachte, verdeutlichen die beiden folgenden Zitate: „Die Kernfrage ist daher nicht nur, wie Technologien entwickelt werden können, die tatsächlich den Datenschutz verbessern, sondern wie dafür gesorgt werden soll, dass diese Technologien ordnungsgemäß als solche gekennzeichnet und von den Nutzern erkannt werden. Zertifizierungssysteme spielen hier eine entscheidende Rolle […]." (ebd., 17) Und: „Die Kommission ist der Meinung, dass solche Systeme gefördert und weiterentwickelt werden sollten, […] ferner sollten diejenigen, die in die Gewährleistung und sogar die Verbesserung des Datenschutzes investieren Gelegenheit gegeben werden, ihre Leistung auf diesem Gebiet darzustellen und Wettbewerbsvorteile daraus zu ziehen." (ebd., 17 f.)

183 Als Beispiel für Privacy Impact Assessments nannte die Kommission Kanada, „dessen Bundesregierung die erste Zentralregierung war, die obligatorische Datenschutz-Folgenabschätzungen für alle Bundesministerien und -agenturen vorgeschrieben hat, bei allen Programmen und Diensten, bei denen der Datenschutz berührt werden könnte. Die Agenturen müssen in der Frühphase der Konzeption oder Überarbeitung eines Programms oder eines Dienstes eine solche Folgenabschätzung vornehmen, damit der Entwicklungsprozess entsprechend gesteuert und dafür gesorgt wird, dass der Datenschutz eines der Hauptkriterien ist." (ebd., 17)

Die Kommission bezeichnete ihren Bericht als einen ersten Schritt zur Auswertung der Durchführung der DS-RL und kündigte an, den weiteren Verlauf der Umsetzung zu verfolgen und weiterhin (gegen Ende 2004) Bericht über den Stand der Umsetzung zu erstatten (ebd., 30).

3.3.3.3 Stellungnahme des Europäischen Parlaments

Nach Erhalt des Kommissionsberichts über die Durchführung der DS-RL am 15. Mai 2003 wurde der LIBE-Ausschuss am 4. September 2003 mit der Ausarbeitung eines Initiativberichts beauftragt. Der JURI-Ausschuss und der ITRE-Ausschuss wurden als mitberatende Ausschüsse am Verfahren beteiligt. In seiner Sitzung vom 8. September 2003 benannte der LIBE-Ausschuss Marco Cappato als Berichterstatter. Dessen Berichtsentwurf wurde auf den LIBE-Ausschusssitzungen vom 22. Januar 2004 und vom 19. Februar 2004 geprüft und auf der letztgenannten Sitzung einstimmig angenommen (Cappato 2004, 4). Der Bericht wurde am 24. Februar an das Parlamentsplenum überwiesen und auf der Plenarsitzung vom 9. März 2004 mit 439 Stimmen (bei 39 Gegenstimmen und 28 Enthaltungen) angenommen. Gegen die Entschließung des Parlaments stimmten lediglich einige konservative Europaparlamentarier vor allem der EVP-ED sowie drei Abgeordnete der EDU (Europa der Demokratien und der Unterschiede, engl. Europe of Democracies and Diversities EDD). Die Enthaltungen setzten sich aus einigen Abgeordneten der EDU, der Mehrzahl der UEN-Angehörigen, fraktionslosen Abgeordneten sowie einem Abgeordneten der EVP-ED zusammen (Europäisches Parlament 2004, 62 f.).

Inhaltlich fokussierte der Cappato-Bericht vor allem den Schutz der europäischen Bürgerinnen und Bürger vor sicherheitspolitisch motivierten Datenzugriffen. Während der *formelle Schutz des Rechts auf Achtung des Privatlebens* zumindest im Bereich der ersten Säule als im Wesentlichen recht zufriedenstellend zu bewerten sei, müsse der Aushöhlungsprozess des *inhaltlichen Schutzes dieses Rechts* mit Sorge betrachtet werden, da zahlreiche Staaten *so genannte Vorschriften zur Terrorismusbekämpfung* verabschiedet hätten, die jene Grundrechte und Grundfreiheiten gefährdeten, auf denen die Demokratie und Rechtsstaatlichkeit aufbauen: „Das Recht auf Privatsphäre ist eines der ersten Opfer dieses legislativen Notstandsaktivismus, der die delikaten Grenzen zwischen Grundrechten und rechtmäßigen und notwendigen Eingriffen in eine demokratische Gesellschaft zu Zwecken der ‚öffentlichen Ordnung' neu festlegen soll." (Cappato 2004, 14)

Im Hinblick auf den eigentlichen Inhalt des Kommissionsberichts über die Durchführung der DS-RL teilte der Cappato-Bericht die Auffassung der Kommission, dass die Richtlinie wegen der Langsamkeit und des noch begrenzten Umfangs ihrer Umsetzung „vorläufig […] nicht geändert werden sollte und dass derzeitige Mängel in der Anwendung der Richtlinie durch [die von der Kommission vorgeschlagenen] Maßnahmen überwunden werden sollten" (ebd., 8). Für den Fall, dass nach Ende eines angemessenen Zeitraums von einem Jahr noch immer einige hartnäckige Mitgliedstaaten *gegen den Buchstaben und den Geist der Richtlinie* verstoßen, forderte das Parlament eine entschlossene Vorgehensweise inkl. der Wahrnehmung der Möglichkeit der Einleitung von Vertragsverletzungsverfahren (ebd., 8 f. und 15 f.).

Der Rest der Parlamentsentschließung widmete sich dagegen den verschiedenen zu diesem Zeitpunkt akuten Streitpunkten hinsichtlich sicherheitspolitisch motivierter Datenverarbeitungen: der Zugriff amerikanischer Behörden auf Fluggastdaten europäischer Bürgerinnen und Bürger; die Übermittlung von Daten, die bei Europol, Eurojust, SIS usw. gespeichert sind, an Drittstaaten; und die in Art. 15 der ePrivacy-Richtlinie eingeführte Möglichkeit einer Vorratsdatenspeicherung. Im Besonderen bemängelte das Parlament in diesem Zusammenhang das anhaltende Fehlen einer der DS-RL vergleichbaren Regelung für die dritte Säule, während zugleich im Rahmen der ersten Säule erhobene personenbezogene Daten für Aktivitäten, die in den Bereich der dritten Säule fallen, genutzt würden (Zugriff auf Fluggastdaten) bzw. werden sollten (Vorratsdatenspeicherung) (ebd., 9 f. und 16 f.).

Daher forderte das Parlament die Kommission dazu auf, im ersten Halbjahr 2004 ein Rechtsinstrument zum Schutz der Privatsphäre im Rahmen der dritten Säule vorzuschlagen, das verbindlich sein sollte und welches das für die erste Säule geltende Schutzniveau auf die Aktivitäten der dritten Säule ausweite und eine Harmonisierung herbeiführe (ebd., 7). Zugleich machte das Parlament klar, dass es auf lange Sicht – und insbesondere mit Blick auf die angekündigte Aufhebung der Säulen in der EU durch die Europäische Verfassung – die Anwendung der DS-RL inkl. der zu diesem Zeitpunkt nötigen Anpassungen auf alle dann ehemaligen Säulen fordere (ebd., 7 und 15). In diesem Zusammenhang verlangte das Parlament zudem, dass es „künftig zu jedem Vorschlag, der sich auf den Schutz der Privatsphäre in der EU bezieht oder auswirkt, beispielsweise internationale Vereinbarungen ihrer Institutionen, Angemessenheitsentscheidungen usw., mit Entscheidungsbefugnissen konsultiert wird" (ebd., 8).

3.3.3.4 Folgebericht

Über den Stand des Arbeitsprogramms für eine bessere Durchführung der DS-RL resümierte die Kommission doch deutlich später als angekündigt. Statt *gegen Ende 2004* wurde die entsprechende Mitteilung der Kommission mehr als zwei Jahre später erst Anfang März 2007 veröffentlicht (KOM 2007). Im Gegensatz zum ersten Bericht ging der 2007er-Bericht deutlich oberflächlicher auf viele der diskutierten Punkte ein, wie sich insbesondere am Umgang mit den drei im Vorläuferbericht als zentral bezeichneten Punkten zeigte.[184] Aufgrund dessen, dass die Potentiale bei der Umsetzung der Richtlinie noch immer nicht vollständig ausgeschöpft worden seien und weil die bestehenden Abweichungen keine Gefahr für das Funktionieren des Binnenmarktes oder für die Gewährleistung eines hohen Schutzniveaus darstellten, sah die Kommission trotz einzelner Kritikpunkte[185] keine Notwendigkeit für eine Änderung der Richtlinie (ebd., 10). Ebenso wurden die Grundsätze der Richtlinie für weiterhin gültig und nicht änderungsbedürftig erklärt (ebd., 11).

Trotz der auch erfolgten Erwähnung des durch die Richtlinie garantierten hohen Schutzniveaus hob die Kommission an mehreren Stellen interessanterweise vor allem die wirtschaftliche Bedeutung der Richtlinie hervor. In den Schilderungen der bestehenden Divergenzen bei der Umsetzung der Richtlinie im Kapitel zur aktuellen Situation hob der Text vor allem auf die Auswirkungen für den Binnenmarkt ab, während das Schutzniveau lediglich in einem Nebensatz Erwähnung fand. Noch augenfälliger äußerte sich der Fokus auf die wirtschaftliche Bedeutung der Richtlinie, als die Kommission die Bedeutung des Grundrechts auf den Schutz personenbezogener Daten mit der folgenden Argumentation herausstellte: „Der Einzelne soll so Vertrauen in die Art und Weise der Verwendung seiner Daten gewinnen, denn ohne dieses Vertrauen wäre eine Ausweitung des elektronischen Geschäftsverkehrs nicht denkbar." (ebd., 10) Wie zu erwarten war, nahm der EDSB in seiner Stellungnahme im Hinblick auf die Bewertung der Grundrechts- bzw. Binnenmarktdimension der Richtlinie eine der Kommissionsmitteilung entgegengesetzte Position ein (EDSB 2007b): So kritisierte der EDSB den Wortlaut der Kommission und hob hervor, dass die Richtlinie in erster Linie ein Grundrecht darstelle. Die Förderung des freien Datenver-

184 So aber auch am Seitenumfang: Während der 2003er-Bericht noch 30 Seiten umfasste, war der neue Bericht nur 12 Seiten lang.

185 Darunter insb. die lückenhafte bzw. divergierende Umsetzung in einigen Mitgliedstaaten (ebd.).

kehrs im Binnenmarkt sei zwar ebenfalls wichtig, aber letztlich zweitrangig (ebd., 3, Nr. IV. A. 15-19).

Über die Kommissionsmitteilung hinausgehend schlug der EDSB zudem folgende Instrumente vor, die „für eine künftige Änderung der Richtlinie in Erwägung gezogen oder in andere horizontale Rechtsvorschriften aufgenommen werden könnten" (ebd., 10, Nr. VI. F. 67): *Sammel- bzw. Verbandsklagen*,[186] *Meldung von Datenschutzverletzungen* sowie *grenzüberschreitende Bestimmungen zu Datenschutzgütesiegeln oder Datenschutz-Audits durch Dritte*.

Schließlich begrüßte der EDSB auch die möglicherweise bevorstehende Aufhebung der Säulenstruktur der EU und das Rechtswirksamwerden der EU-Grundrechtecharta infolge des potentiellen Inkrafttretens des EU-Reformvertrags (ebd., 8, Nr. V. E.). Aufgrund der sich zu diesem Zeitpunkt noch in der Schwebe befindenden Debatte über den weiteren Umgang mit dem EU-Reformvertrag (siehe 3.4.1.2) äußerte sich die Kommission nur auf sehr defensive Weise zu den möglichen neuen Kompetenzen im Bereich des Datenschutzes. So erwähnte die Kommission zwar die geplante Ausweitung ihrer Gesetzgebungskompetenz auf nahezu alle Politikbereiche infolge der vorgesehenen Auflösung der Säulenstruktur. Bis allerdings „geklärt ist, wie es mit dem Ratifizierungsprozess des Verfassungsvertrags weitergeht," (ebd., 9) kündigte die Kommission an, sich weiterhin an die im Rahmen der Umsetzung des Haager Programms vereinbarten Maßnahmen zu halten (ebd.).

3.3.3.5 Zwischenfazit

Die Berichterstattung der Kommission über die Durchführung der DS-RL war ein wichtiger Zwischenschritt auf dem Weg zur Datenschutzreform, da durch diesen klar wurde, in welchen inhaltlichen Bereichen noch immer Defizite anzutreffen waren.

186 Mit seiner Forderung nach kollektiven Rechtsbehelfen knüpfte der EDSB an eine seit dem Jahr 2005 auf EU-Ebene stattfindende Diskussion an, die ihren Anfang mit der Veröffentlichung eines Grünbuchs der Kommission im selben Jahr genommen hatte und schließlich in der Ankündigung der Schaffung von Mechanismen des kollektiven Rechtsschutzes im Rahmen der verbraucherpolitischen EU-Strategie 2007–2013 kulminierte (Dawidowicz 2014, 239–41).

3.3.4 Datenschutz-Bestimmungen im Sicherheitsbereich

Wie bereits in Unterabschnitt 3.3.1.2 erwähnt, wurde das Subsystem der Europäischen Datenschutzpolitik in den 2000er-Jahren in entscheidendem Maße von den Entwicklungen im Bereich der Sicherheitspolitik beeinflusst. Die dabei ausgefochtenen Konflikte und insbesondere die politischen Niederlagen, die Datenschutzbefürworter in dieser Zeit erlitten, sollten später ausschlaggebend für die Initiierung und den erfolgreichen Abschluss der Datenschutzreform sein.

Der vorliegende Unterabschnitt widmet sich der Untersuchung der politischen Auseinandersetzungen beim Zustandekommen der Datenschutz-Bestimmungen im Sicherheitsbereich. Angefangen mit den ersten Gemeinschaftsaktivitäten auf diesem Gebiet (3.3.4.1), wird außerdem das Zustandekommen der wichtigsten und umstrittensten politischen Ergebnisse dieser Phase untersucht: der Richtlinie zur Vorratsdatenspeicherung (3.3.4.2), des Zugriffs auf Fluggastdaten (3.3.4.3) sowie des JI-Rahmenbeschlusses (3.3.4.4).

3.3.4.1 Erste Aktivitäten auf dem Gebiet

Bereits im Rahmen ihres 1990er-Legislativbündels hatte die Kommission die Mitgliedstaaten dazu eingeladen, die für den Gemeinschaftsbereich vorgesehenen Datenschutz-Grundsätze (der späteren DS-RL) mittels einer Ministerratsentschließung auch auf jene Bereiche mitgliedstaatlicher Datenverarbeitung im öffentlichen Bereich anzuwenden, die nicht von Gemeinschaftsbereich abgedeckt sind (COM 1990, 73 f.). Zu diesem Zeitpunkt umfasste der vom Gemeinschaftsrecht abgedeckte Politikbereich vor allem wirtschaftliche und seit Mitte der 1980er-Jahre auch einige wenige soziale Fragen. Die Initiative der Kommission hatte zum Ziel, die Anwendung der Datenschutz-Grundsätze auch auf den Justiz- und Inneres-Bereich sicherzustellen, um ein EG-weit einheitliches und hohes Datenschutzniveau auf allen von der Verarbeitung personenbezogener Daten betroffenen Politikbereichen zu gewährleisten (ebd.).[187] Wie bereits in Unterabschnitt 3.2.2.4.3 dargelegt, konnte diese Initiative der Kommission trotz ihrer Befürwortung seitens der Datenschutzaufsichtsbehörden keine Unterstützung bei den

187 Die von der Kommission 1990 vorgeschlagene Ministerratsentschließung hätte eine freiwillige Bindung seitens der Mitgliedstaaten dargestellt, die keine eigenständige Grundlage in den Gemeinschaftsverträgen gehabt hätte.

Mitgliedstaaten generieren, sodass der Vorschlag bis auf Weiteres fallen gelassen wurde.

Erst eine Kette von Ereignissen sollte später wieder Bewegung in die Thematik bringen und zum Abschluss des Justiz und Inneres-Rahmenbeschlusses 2008/977/JHA führen. Den Anfang markierte das Inkrafttreten des Maastrichter Vertrags Ende 1993. Dieser weitete die intergouvernementale Zusammenarbeit der EG über die Wirtschaftskooperation (nunmehr als erste Säule bezeichnet) hinaus auf die teil-vergemeinschafteten Politikbereiche der gemeinsamen Außen- und Sicherheitspolitik (GASP) (zweite Säule) sowie die Justiz- und Innenpolitik (JI)[188] (dritte Säule) aus, sodass der Erlass von Gemeinschaftsmaßnahmen im Bereich der JI-Politik prinzipiell ermöglicht wurde (Europäische Gemeinschaften 1992). Im Maastrichter Vertrag wurde auch erstmals im Rahmen eines Gemeinschaftsvertrags die Idee einer gemeinschaftlichen Polizeibehörde erwähnt, die für grenzüberschreitende Verbrechen wie Terrorismus und Drogenschmuggel zuständig sein sollte. Das sog. Europol-Übereinkommen zur Gründung der Europol (European Police Office), wurde am 26. Juli 1995 unterzeichnet und trat zum 1. Oktober 1998 in Kraft. Schon die Präambel des Übereinkommens unterstrich *die besondere Aufmerksamkeit*, die dem Schutz der Rechte des Einzelnen und insbesondere dem Schutz personenbezogener Daten zuteilwerden sollte. Letztlich orientierte sich das Übereinkommen hinsichtlich des Datenschutzniveaus allerdings lediglich an der Datenschutz-Konvention des Europarats.[189] Das Problem beim Datenschutz im Bereich der dritten EU-Säule war, dass kein gemeinschaftlich festgelegter Datenschutzrahmen existierte, der die Standards für sektorspezifische Regelungen (Europol, Eurojust und SIS) vorgab. Stattdessen waren in Umkehrung der gewöhnlichen Regulierungslogik noch vor einer Rahmenrichtlinie die sektorspezifischen Regelungen mit eigeständigen Datenschutzvorgaben erlassen worden, die sich mehr oder weniger an der Datenschutz-Konvention des Europarats orientierten. Die für die dritte Säule bestehenden Re-

188 Nachdem die justizielle Zusammenarbeit in Zivilsachen und die flankierenden Maßnahmen zum freien Personenverkehr mit dem Vertrag von Amsterdam 1997 in die erste Säule verschoben worden waren, verblieb die polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS) in der dritten Säule, die fortan entsprechend bezeichnet wurde (Wessels 2008, 94).

189 Bzw. an der Empfehlung Nr. R (87) 15 des Ministerkomitees des Europarats über die Nutzung personenbezogener Daten im Polizeibereich, die zwischenzeitlich am 17. September 1987 verabschiedet worden war (vgl. auch Boehm 2012, 96 ff. Council of Europe 1987).

gelungen waren also einerseits zersplittert und uneinheitlich und wurden von Datenschutzexperten andererseits als unzureichend im Hinblick auf das Schutzniveau bewertet. Schließlich lag ein entscheidender Grund für die Erarbeitung der DS-RL darin, dass das Schutz-Niveau der Datenschutz-Konvention als unzureichend bewertet wurde (P. de Hert und Papakonstantinou 2009, 405 f.).

Den ersten konkreten politischen Schritt in Richtung der Festlegung eines gemeinschaftlichen Datenschutzrahmens in der dritten Säule unternahm im Jahr 1998 die italienische Ministerratsdelegation (JAI 15 8321/98), die von den Datenschutzbeauftragten der EU-Mitgliedstaaten Unterstützung in Form einer Resolution erhielt (JAI 16 8563/98). Die italienische Initiative regte vor dem Hintergrund der Befürchtung einer Zersplitterung der Datenschutzregelungen für verschiedene komplexe Informationssysteme wie SIS, Europol oder ZIS (Zollinformationssystem) sowie für den Abschluss bi- oder multilateraler Abkommen die Herausbildung einheitlicher Standards und Datenschutzkontrollen an – während die Resolution der Europäischen Datenschutzbeauftragten auf Harmonisierung sowie ein hohes Schutzniveau drängte (Vorsitz - Rat der Europäischen Union 1999). Zeitgleich erhielt das im Rahmen des Vertrags von Amsterdam beschlossene Ziel des *Aufbaus eines gemeinsamen Raumes der Sicherheit, der Freiheit und des Rechts* mit dem Inkrafttreten des Vertrags am 1. Mai 1999 Geltung (Europäische Union 1997). Ende 1998 nahm der Europäische Rat schließlich den sog. Wiener Aktionsplan an.[190] In diesem wurde beschlossen, innerhalb von zwei Jahren nach Inkrafttreten des Amsterdamer Vertrags die Harmonisierung der Datenschutzvorschriften in der PJZS zu prüfen (Rat der Europäischen Union 1998, 24; Vorsitz - Rat der Europäischen Union 1999, 2). Die Annahme einer zu diesem Zweck ausgearbeiteten Ministerratsentschließung scheiterte jedoch im April 2001 – offenbar am Widerstand jener während der Verhandlungen der DS-RL als nördlicher Block bezeichneten Mitgliedstaaten (P. de Hert und Papakonstantinou 2009, 405, Fn. 15; Ministerrat 2001).

Als das von den Vereinigten Staaten und dem Vereinigten Königreich unter Zuarbeit Australiens, Neuseelands und Kanadas betriebene weltweite

190 Der *Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags* (Rat der Europäischen Union 1998).

Spionagenetzwerk Echelon[191] zu einem öffentlichen Thema wurde, eröffnete sich kurzzeitig ein politisches Gelegenheitsfenster für Europäische Reaktionen (Dix 2000). Doch wirkten die Terroranschläge vom 11. September 2001 als externer Schock, der jegliche Reaktionen in Richtung der Verschärfung datenschutzrechtlicher Standards verhinderte und dafür sorgte, dass stattdessen die weitere Ausdehnung von Überwachungsmaßnahmen die politischen Agenden dominierte (H. Busch 2002).

Im Juni 2003 unternahm schließlich der griechische Ratsvorsitz einen erneuten Anlauf und unterbreitete auf der Ministerratssitzung der Justiz- und Innenminister einen Vorschlag zur Erarbeitung gemeinsamer Regeln für den Schutz personenbezogener Daten im Rahmen der dritten Säule, die sich am Schutzniveau der DS-RL und der EU-GRCh, die in der Zwischenzeit verabschiedet worden war (vgl. 3.4.1.1), orientieren sollten. Doch scheiterte auch dieser Vorstoß an der mangelnden Bereitschaft der Mehrheit der Mitgliedstaaten (Ministerrat 2003, 32).

Schließlich erhielt die Debatte um die Verbesserung des Informationsaustauschs zwischen den Mitliedstaaten vor allem nach den Anschlägen vom 11. März 2004 in Madrid weiteren Auftrieb. Im Rahmen ihres neuen mehrjährigen Programms, dem Haager Programm,[192] einigten sich die EU-Organe auf den sog. Verfügbarkeitsgrundsatz, der ab dem 1. Januar 2008 inkrafttreten sollte und mittels dessen mitgliedstaatliche Strafverfolgungsbehörden zur gegenseitigen Bereitstellung ihrer Datenbestände verpflichtet wurden. Zugleich legte das Haager Programm zur Verwirklichung des Verfügbarkeitsgrundsatzes die strenge Einhaltung mehrerer Hauptbedingungen fest, zu denen auch die Gewährleistung von Datenschutzrechten zählte (Europäischer Rat 2005a, 7 f.). Die Befürwortung der Erarbeitung von strengen Bedingungen[193] im Rahmen des Haager Programms stieß dann auch auf die ausdrückliche Unterstützung der europäischen Datenschutzbeauftragten. In der sog. Erklärung von Krakau forderten die Datenschutzbeauftragten der Mitgliedstaaten sowie der EDSB Ende April 2005 dann auch die Erarbeitung eines eigenständigen Instruments für den Datenschutz in der dritten Säule. Mehr noch, wurde gefordert, „dass, sobald der Euro-

191 Siehe insb. den Echelon-Bericht des Sonderausschusses des Europäischen Parlaments (Europäisches Parlament 2001a). Für eine kurze Chronologie der Ereignisse, siehe: (Campbell 2001).

192 Der bereits im Tampere-Programm vorhandene Fokus auf innere Sicherheit wurde im Rahmen des für den Zeitraum 2005 bis 2010 gültigen Haager Programms weiter verstärkt (Pütter 2006).

193 Als *streng* galt in diesem Zusammenhang das Schutzniveau der DS-RL.

päische Verfassungsvertrag in Kraft tritt, ein umfassendes Europäisches Datenschutzgesetz gelten sollte, das sämtliche Bereiche [also sowohl die dann ehemalige erste als auch dritte Säule, M. K.] der Verarbeitung personenbezogener Daten abdeckt." (Frühjahrskonferenz der Europäischen Datenschutzbeauftragten 2005) Am 7. Juni 2005 nahm auch das Europäische Parlament eine Empfehlung an, in der es den Europäischen Rat und den Ministerrat dazu aufforderte, die bestehenden Datenschutz-Regeln bei den Instrumenten der dritten Säule zu harmonisieren, indem diese in ein eigenständiges Datenschutz-Instrument überführt würden, und dabei zugleich das Datenschutzniveau, das im Rahmen der ersten Säule bestand, aufrecht zu erhalten (Europäisches Parlament 2005, 260 vgl. Nr. 1. h)).

Zwischenzeitlich unterzeichneten Belgien, Deutschland, Frankreich, Luxemburg, die Niederlande, Österreich und Spanien auf eine Initiative von Bundesinnenminister Schily (SPD, BRD) aus dem Jahr 2003 hin, am 27. Mai 2005 den Prümer Vertrag. Dieses zwischenstaatliche Abkommen sah unter Einhaltung datenschutzrechtlicher Garantien den automatischen und direkten Zugriff der Strafverfolgungsbehörden eines Vertragsstaates auf die von einem anderen Vertragsstaat gespeicherten personenbezogenen Daten (z. B. DNA-Daten oder Fingerabdrücke) vor (Prümer Vertrag 2005).[194] Doch noch bevor es zur Verabschiedung eines Datenschutz-Rahmeninstruments im Bereich der dritten Säule kam, wurde der Zugriff auf personenbezogene Daten zu Sicherheitszwecken zunächst auf mehreren Gebieten weiter ausgedehnt. Dies betraf vor allem die EG-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung, daneben aber auch die Übertragung von Fluggastdaten an Regierungsstellen in den Vereinigten Staaten. Diese Maßnahmen werden im Folgenden näher betrachtet und dabei einerseits im Hinblick auf ihre Bedeutung für die EG-Rahmenrichtlinie im Bereich der dritten Säule im Besonderen und andererseits auf ihre Bedeutung für die Datenschutzpolitik der Europäischen Union im Allgemeinen analysiert.

3.3.4.2 Richtlinie 2006/24/EG zur Vorratsdatenspeicherung

Die Idee einer EU-weiten, einheitlichen Vorratsdatenspeicherung wurde erstmals formell von der rechtskonservativen dänischen Regierung im Rahmen ihrer EU-Ratspräsidentschaft im August 2002 vorgebracht, konnte bei

194 Der Ministerratsbeschluss 2008/615/JI überführte die Vorgaben des Prümer Vertrags, das außerhalb des Gemeinschaftsrechts abgeschlossen worden war, im Juni 2008 in das Gemeinschaftsrecht (EU-Ministerrat 2008a).

den übrigen Mitgliedstaaten allerdings keine ausreichende Unterstützung finden. Im Sinne eines Minimalkompromisses konnten sich die Regierungen der Mitgliedstaaten jedoch im Rahmen der Verhandlungen zur ePrivacy-Richtlinie darauf einigen, dass denjenigen Mitgliedstaaten, die ein Interesse an der Vorratsdatenspeicherung hatten, der Erlass entsprechender Regelungen nicht erschwert werden sollte, sodass die im Kommissionsvorschlag und in den Parlamentspositionen zur ePrivacy-Richtlinie vorgesehenen Beschränkungen auf Druck des Ministerrats aus dem finalen Richtlinientext entfernt wurden (vgl. 3.3.2). In der Folge verfolgten mehrere EU-Mitgliedstaaten nationale Pläne zur Einführung einer Vorratsdatenspeicherung. Allerdings vertraten insb. die Strafverfolgungsbehörden die Ansicht, dass eine Vorratsdatenspeicherung nur dann wirksam sein könne, wenn diese in der gesamten EU entlang harmonisierter Gemeinschaftsvorgaben eingeführt werde. Da nicht alle Regierungen in gleichem Maße von dieser Ansicht überzeugt waren, konnte dieser Vorschlag zunächst allerdings noch keine Mehrheit finden (Hayes, Peers, und Bunyan 2004).

Erst mit den Anschlägen von Madrid im März 2004 und den Londoner Anschlägen vom 7. Juli 2005 wandelte sich die Debatte zugunsten der Vorratsdatenspeicherungsbefürworter. Im Nachgang der Madrider Anschläge veröffentlichte der Europäische Rat eine Erklärung zum Kampf gegen Terrorismus, in der der Ministerrat u. a. vorrangig mit der Beratung von *Vorschlägen für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter* und mit der Annahme der entsprechenden Vorschläge bis Juni 2005 beauftragt wurde (Europäischer Rat 2004, 4 f.). Daraufhin legten Frankreich, Großbritannien, Irland und Schweden bereits Ende April 2004 einen Entwurf für einen Rahmenbeschluss zur Vorratsdatenspeicherung im Ministerrat vor (EU-Ministerrat 2004a). Der Vorschlag sah eine Mindestspeicherfrist von 12 Monaten und eine Höchstspeicherdauer von 36 Monaten vor. Während der dänische Vorschlag aus dem Jahr 2002 die Vorratsdatenspeicherung noch lediglich zur Aufklärung bereits erfolgter Straftaten und eine Beschränkung auf besonders schwere Straftaten und Terrorismus vorgesehen hatte, sollte die Vorratsdatenspeicherung zudem nunmehr auch zur Straftatenprävention dienen dürfen und auch bei leichteren Delikte wie Urheberrechtsverletzungen greifen (EU-Ministerrat 2004b).

Doch auch dieser neue Vorschlag konnte sich zunächst nicht durchsetzen. Da der Vorschlag auf Grundlage der Art. 31 Abs. 1 lit. c sowie Art. 34

Abs. 2 lit. b gestützt wurde, d. h. als Rahmenbeschluss[195] zur Harmonisierung im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen vorgeschlagen wurde, musste über diesen im Ministerrat einstimmig entschieden werden. Allerdings konnte zu keinem Zeitpunkt ein Konsens unter allen Mitgliedstaaten gefunden werden, da die Vorratsdatenspeicherung vor allem von Deutschland, Österreich und den Niederlanden abgelehnt wurde (EDRi 2005a). Aufgrund des gewählten Konsultationsverfahrens musste der Ministerrat das Parlament zudem zwar anhören, aber formell keine Rücksicht auf dessen Position nehmen. Diese Vorgehensweise des Ministerrats führte wiederum zu massiver Kritik vonseiten des Europäischen Parlaments. Die von Berichterstatter Alexander Alvaro im LIBE-Ausschuss ausgearbeitete Parlamentsposition zum Rahmenbeschluss hob auf drei Kritikpunkte ab: *Erstens* wurde, aufgrund dessen, dass die im Vorschlag benannten, auf Vorrat zu speichernden Datenkategorien teilweise in den Bereich der ersten Säule fielen, die Rechtsgrundlage des Vorhabens angezweifelt. *Zweitens* wurde, aufgrund der im Vorschlag vorgesehenen weitreichenden Zugriffsmöglichkeiten, die Verhältnismäßigkeit bzw. Notwendigkeit der Maßnahme angezweifelt und schließlich, *drittens*, wurde auf die Möglichkeit einer Verletzung des Art. 8 der Europäischen Menschenrechtskonvention hingewiesen (A. N. Alvaro 2005, 6 ff.). Entsprechend sprach sich das Parlamentsplenum am 27. September 2005 gegen den Vorschlag aus und forderte Frankreich, Großbritannien, Irland und Schweden dazu auf, ihre Initiative zurückzuziehen. In der Zwischenzeit schlossen sich der Juristische Dienst des Ministerrats sowie die Kommission der Parlamentsposition hinsichtlich der Kritik an der Rechtsgrundlage an (A. N. Alvaro 2015, 33). Die Kommission legte Anfang 2005 einen diesbezüglichen Prüfungsvorbehalt ein und rief den Ministerrat unter Verweis auf ein noch von der Kommission auszuarbeitendes Rechtsinstrument im Bereich der ersten Säule ebenfalls zur Aufgabe der Initiative auf (EDRi 2005c).

195 Ein Rahmenbeschluss konnte bis zum Inkrafttreten des Lissabon-Vertrags (am 1. Dezember 2009) vom Ministerrat ohne Zustimmung des Parlaments für Angelegenheiten im Rahmen der dritten Säule der EU erlassen werden. Darin wurden lediglich die zu erreichenden Ziele und nicht die Art und Weise der Zielerreichung festgelegt. Damit sind Rahmenbeschlüsse das Gegenstück zu Richtlinien, die im Rahmen der ehemaligen ersten Säule erlassen wurden. Seit Inkrafttreten des Lissabon-Vertrags und der damit einhergehenden Aufhebung der Säulenstruktur müssen die ehemals im Rahmen der dritten Säule behandelten Angelegenheiten nunmehr im ordentlichen Gesetzgebungsverfahren und mit der Zustimmung des Parlaments verhandelt werden (Schönberger 2007).

Der Verlauf der Verhandlungen sollte sich allerdings schon bald darauf infolge der Anfang Juli 2005 in London verübten Terroranschläge drastisch ändern. Am 21. September 2005 veröffentlichte die Kommission schließlich, gestützt auf Art. 96 des EG-Vertrags und unter dem noch sehr frischen Eindruck der jüngsten Terroranschläge und aufgrund des politischen Drucks der britischen Ratspräsidentschaft,[196] die auf der Verabschiedung eines EG-Instruments zur Vorratsdatenspeicherung unbedingt beharrte, ihren Vorschlag für eine im Rahmen des Mitentscheidungsverfahrens auszuarbeitende Richtlinie des Parlaments und des Rates (Europäische Kommission 2005b). Dieser Vorschlag war zwar als Kompromiss gedacht, griff allerdings nur wenige der inhaltlichen Bedenken des Parlaments auf, während die Position des Ministerrats weitgehend übernommen wurde (A. N. Alvaro 2015, 33; Ripoll Servent 2015, 77). Die britische Ratspräsidentschaft übte daraufhin massiven Druck auf das Europäische Parlament aus, damit die Verhandlungen während ihrer Präsidentschaft und somit noch vor Ende des Jahres abgeschlossen werden konnten. Dahinter lag die Befürchtung der britischen Regierung, dass die auf sie nachfolgende österreichische Ratspräsidentschaft, die zu den erklärten Gegnern der Vorratsdatenspeicherung zählte, die Verhandlungen nicht oder nicht in ihrem Sinne abschließen würde (Maras 2011, 6).

Charles Clarke, sozialdemokratischer britischer Innenminister von Dezember 2004 bis Mai 2006 in der Regierung Blair, der sich im Rahmen der britischen Ratspräsidentschaft innerhalb der Ministerratskonfiguration Justiz und Inneres für die Verhandlungen zu den Instrumenten zur Vorratsdatenspeicherung verantwortlich zeichnete, setzte alle Hebel in Gang, um jegliche nennenswerte datenschutzrechtliche Ausbesserungen an der Vorratsdatenspeicherung zu verhindern. Dazu setzte Clarke die Mitglieder des LIBE-Ausschusses zunächst dahingehend unter Druck, dass, sollte das Parlament die von der britischen Ratspräsidentschaft gewünschte Vorratsdatenspeicherung nicht akzeptieren, die Vorratsdatenspeicherung als Rahmenbeschluss unter Ausschluss des Parlaments beschlossen würde. Außerdem hatte Clarke dem Parlament im Falle des Scheiterns der britischen Initiative damit gedroht, dass er dafür sorgen werde, dass das Europäische Parlament künftig an keiner einzigen Justiz und Inneres-Maßnahme mehr beteiligt würde (EDRi 2005a). Diese Drohung wurde im LIBE-Ausschuss, der mit den technischen Details des Verfahrens und den mitgliedstaatli-

196 Das Vereinigte Königreich hatte die EU-Ratspräsidentschaft Anfang Juli 2005 übernommen.

chen Positionen im Ministerrat gut vertraut war, als Bluff wahrgenommen. Schließlich hatte sich zuvor kein Konsens hinsichtlich der britischen Position im Ministerrat abgezeichnet, der zur Verabschiedung eines Rahmenbeschlusses jedoch nötig war. Außerdem schätzte der LIBE-Ausschuss das Zurückrudern des Ministerrats zu einem Rahmenbeschluss im Falle eines Parlamentsvetos im Rahmen des Mitentscheidungsverfahrens als eine politische Niederlage ein, welche die Ratspräsidentschaft einzugehen nicht bereit sein würde.

Dennoch kam der LIBE-Ausschuss bzw. Rapporteur Alvaro Clarkes Forderungen insofern entgegen, als der Parlamentsbericht innerhalb kürzester Zeit erarbeitet und im Rahmen informeller Trilog-Gespräche mit der Kommission und dem Ministerrat abgestimmt wurde. Allerdings beugte sich der LIBE-Ausschuss nicht den Maximalforderungen Clarkes und sah im Ausschussbericht Verbesserungsvorschläge hinsichtlich des Datenschutzniveaus vor. Dieser Bericht wurde am 24. November 2005 im LIBE-Ausschuss mit 33 Stimmen (bei 8 Gegenstimmen und 5 Enthaltungen) angenommen (Ripoll Servent 2015, 72). Auf Ablehnung stieß der Ministerratsvorstoß erneut insbesondere bei den Datenschutzaufsichtsbehörden, aber auch die europäische Wirtschaft erneuerte ihre Kritik – wenn auch in abgeschwächter Weise und vor allem mit Blick auf die entstehenden Kosten einer Vorratsdatenspeicherung.[197]

Nachdem der LIBE-Ausschuss sich gegen Clarkes Forderungen gestellt hatte, eskalierte letzterer den Konflikt und wandte sich an die Vorsitzenden der Parlamentsfraktionen. Insbesondere die Vorsitzenden der beiden größten Fraktionen (die *Europäische Volkspartei* EVP und die *Sozialdemokratische Partei Europas* SPE) reagierten im Gegensatz zu den LIBE-Ausschussmitgliedern deutlich hellhöriger auf Clarkes Drohungen und befürchteten auch eine Beeinträchtigung der anstehenden Verhandlungen des Lissabon-Vertrags, in deren Ergebnis sie sich eine allgemeine Stärkung der Mitwirkungsrechte des Parlaments erhofften. Im Sinne einer Zuckerbrot-und-Peitsche-Strategie eröffnete Clarke den Fraktionsvorsitzenden zugleich zwei Zugeständnisse: Zum einen versprach er, dass der Ministerrat im Falle der Unterstützung durch das Parlament das seit 1990 zur Debatte stehende aber nie erfolgreich zu Ende verhandelte Rahmeninstrument zum

197 So etwa seitens des BDI, bitkom, eco, UNICE (Businesseurope), ISPA und ETNO (EDRi 2005b; ETNO 2005; Hermida 2006; Scheffel 2016, 106)

Datenschutz in der dritten Säule endlich verabschieden würde.[198] Zum anderen versprach er die (bei den Mitgliedstaaten durchaus umstrittene) Ausweitung der Mitentscheidungsbefugnisse des Parlaments mittels der sog. Passerelle-Regelung auf weitere Maßnahmen im Bereich der dritten Säule (Ripoll Servent 2013, 978). Auf diese Weise schaffte es die britische Ratspräsidentschaft, die Haltung des Parlaments zur Vorratsdatenspeicherung als eine Entscheidung von besonderer Tragweite für die weitere Kooperation der EU-Organe darzustellen. Die Debatte wurde somit von den Details des Legislativvorschlags (Aufbewahrungsfristen, Verfassungsverträglichkeit, Regelungen zum Zugriff, Verwendungszwecke) erfolgreich losgelöst und als eine Meta-Debatte über verantwortungsbewusstes institutionelles Handeln (in dem Sinne, ob der Ministerrat bei einem ihm besonders wichtigen Thema auf die kompromisslose Unterstützung des Parlaments bauen konnte oder nicht) dargestellt. Bis auf die Forderung des Parlaments nach strafrechtlichen Sanktionen im Falle der Verletzung der datenschutzrechtlichen Pflichten konnte sich letztlich keine seiner übrigen Forderungen durchsetzen (vgl. dazu den Überblick über die verschiedenen Positionen und das Verhandlungsergebnis in: Ripoll Servent 2013, 975). Das Parlament verabschiedete den Kompromissvorschlag am 14. Dezember 2005 mit der Stimmenmehrheit (378 Stimmen dafür, 197 dagegen und 30 Enthaltungen) der *sozialistischen Fraktion im Europaparlament* (PES), der christdemokratisch-konservativen *Fraktion der Europäischen Volkspartei und europäischen Demokraten* (EVP-ED), etwa der Hälfte der *Fraktion der Allianz der Liberalen und Demokraten für Europa* (ALDE)[199] und der Mitglieder der nationalkonservativen und europaskeptischen *Union für das Europa der Nationen* (UEN) (European Union 2005; Ripoll Servent 2013, 977). Gegen den Kompromissvorschlag stimmten die vollständige *Konföderale Fraktion der Vereinten Europäischen Linken/Nordischen Grünen* (GUE/NGL) und bis auf eine Enthaltung auch die vollständige *Fraktion der Grünen/Europäischen Freien Allianz* (Grüne/EFA), etwa die Hälfte von ALDE, die fast vollständige europaskeptische *Fraktion Unabhängigkeit/Demokratie* (IND/DEM) sowie einige wenige Abweichler der EVP-ED, der PES und der UEN (Ripoll Servent 2015, 73).

198 Die Kommission hatte am 4. Oktober 2005 einen Vorschlag für einen Rahmenbeschluss zum Datenschutz in der dritten Säule vorgelegt (vgl. Unterabschnitt 3.3.4.4).

199 Darunter vor allem MEPs aus Italien, Belgien, Frankreich und Litauen (Ripoll Servent 2015, 72).

Nach Annahme des Kompromisstextes durch das Parlament in erster Lesung Ende 2005, nahm auch der Ministerrat den Text in erster Lesung Ende Februar 2006 an.[200] Die *Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG* wurde schließlich am 15. März 2006 von den Präsidenten des Parlaments und des Ministerrats unterzeichnet und trat am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der EU, also am 3. Mai 2006 in Kraft und sah die Umsetzung der Richtlinien-Vorgaben in nationales Recht bis zum 15. September 2007 vor (Europäische Union 2006).

3.3.4.3 Der Zugriff auf Fluggastdaten zu Sicherheitszwecken

Eine Folge der Anschläge vom 11. September war das Interesse der Vereinigten Staaten am Zugriff auf personenbezogene Daten von Menschen, die in die Vereinigten Staaten einreisen. Zu diesem Zweck verabschiedete der US-Kongress bereits am 19. November 2001 den *Aviation and Transportation Security Act* (US Congress 2001), um Zugriff auf möglichst umfassende personenbezogene Daten der in die Vereinigten Staaten einreisenden Fluggäste zu erhalten. Dazu verpflichtete das Gesetz alle Fluggesellschaften, die Flüge in, aus oder durch die USA anboten, dazu, Zugang zu ihren Fluggastdaten – dem sogenannten *Passenger Name Record* (PNR)[201] – zu gewähren. Jenen Fluggesellschaften, die das Gesetz nicht befolgten, wurde mit einem Landeverbot gedroht. Entsprechend befanden sich die betroffenen Fluggesellschaften in dem Dilemma, entweder durch die Nicht-Herausgabe der geforderten Informationen US-Recht oder durch die Herausgabe personenbezogener Daten EU-Recht zu verletzen. Zur Lösung des Konflikts nahm die Generaldirektion Binnenmarkt der Europäischen Kommission (die grundsätzlich am Erhalt des in der DS-RL festgelegten Schutzniveaus

200 Lediglich Irland und die Slowakei stimmten aufgrund der Verortung der Regelung in der ersten Säule gegen die Richtlinie zur Vorratsdatenspeicherung (Ripoll Servent 2013, 978).

201 Ein PNR wird bei jeder Buchung und Durchführung einer Flugreise erstellt und beinhaltet ein Datenset, bestehend aus über dreißig personenbezogenen Merkmalen. Darunter befinden sich neben dem Namen, Kreditkarteninformationen, der Anschrift und ggf. IP-Adresse auch Details über Speisewünsche (die Rückschlüsse auf die Religionszugehörigkeit erlauben können) und den gesundheitlichen Zustand des Reisenden (A. Busch 2012a, 420).

interessiert war) Verhandlungen mit dem zuständigen US-Heimatschutzministerium auf. Dieses drängte ohne Kompromissbereitschaft auf einen vollständigen Zugriff auf die geforderten Daten bei einem weitgehend unkontrollierten Zugang und konnte den anfänglichen Widerstand der EU insb. aufgrund der Androhung eines Landeverbots letztlich brechen. Daraufhin schloss der EU-Ministerrat 2004 ein erstes Fluggastdatenabkommen mit den Vereinigten Staaten, das von der EU-Kommission für angemessen im Hinblick auf die in der DS-RL verbrieften Drittstaatentransferregelungen befunden wurde. Diese Vereinbarung bzw. Entscheidung wurde vonseiten der europäischen Datenschutzbeauftragten sowie des Parlaments allerdings als mit Datenschutz-Vorgaben unverträglich scharf kritisiert. Das Europäische Parlament brachte den Fall schließlich vor den EuGH, der das Abkommen 2006 annullierte. Ausschlaggebend für die EuGH-Entscheidung waren allerdings weniger inhaltliche als vielmehr prozedurale Gründe: Demzufolge verfüge der Ministerrat nicht über die Befugnis zum Abschluss des Abkommens und die Kommission nicht über die Kompetenz der Formulierung eines Angemessenheitsbefundes im Rahmen der DS-RL, da der zur Debatte stehende Sachverhalt nicht der ersten, sondern dritten Säule der EU zuzuordnen sei. Aufgrund dieses *forum shift* war nicht mehr die Binnenmarkt-Generaldirektion, sondern die im Ministerrat versammelten nationalen Innen- und Justizminister sowie der EU-Justizkommissar für die weiteren Verhandlungen zuständig (A. Busch 2012a, 428 ff. Hummer 2011, 238 ff.). Der seinerzeitige EU-Justizkommissar Franco Frattini handelte in der Folge gemeinsam mit dem damaligen deutschen Bundesinnenminister Wolfgang Schäuble, die beide deutlich offener gegenüber weitreichenden Sicherheitsregelungen eingestellt waren, unter Umgehung des Europäischen Parlaments 2007 ein neues Abkommen mit den Vereinigten Staaten aus, das u. a. aufgrund der Verlängerung der Vorhaltungsdauer der PNR-Daten von 3,5 auf 15 Jahre als ein weiteres Zugeständnis gegenüber den Wünschen des transatlantischen Verhandlungspartners gewertet wurde (Rötzer 2007). Nachdem der *forum shift* durch die Verlagerung der Zuständigkeit an sicherheitspolitisch motivierte Akteure zunächst die Schwächung der Parlamentsposition zur Folge hatte, führte das Inkrafttreten des Lissabon-Vertrags Anfang Januar 2009 zu einer Aufwertung der Mitentscheidungsbefugnisse des Parlaments. Sachverhalte, die zuvor der dritten Säule zugeordnet waren, wurden durch die Abschaffung der Säulenstruktur dem in Art. 14 des EU-Vertrags geregelten ordentlichen Gesetzgebungsverfahren zugeordnet, wodurch das Parlament eine faktische Vetomacht erhielt. Auf Grundlage seiner erweiterten Kompetenzen und unter Verweis

auf die Einhaltung bestimmter, durch das Parlament definierter Mindeststandards, lehnte das Parlament im Mai 2010 die Kommissionsinitiative vom Dezember 2009 zur endgültigen Regelung des Sachverhalts nach den Regeln des Lissabon-Vertrags ab (A. Busch 2012a, 430). In Kooperation mit dem Parlament wurde in der Folgezeit ein neues transatlantisches Abkommen zum Transfer von Flugpassagierdaten ausgehandelt und 2012 vom Ministerrat und Parlament verabschiedet (VoteWatch Europe 2012). Für den vom rumänischen konservativen Traian Ungureanu ausgearbeiteten Bericht stimmten im Parlamentsplenum 409 Abgeordnete, darunter praktisch die gesamte EVP- und EKR-Fraktion, zwei Drittel der S&D-Abgeordneten, die halbe EFD-Fraktion, ein Viertel der ALDE-Fraktion sowie einige unabhängige Abgeordnete. Die 226 Gegenstimmen setzten sich aus der vollständigen GUE/NGL und Grünen/EFA, knapp drei Viertel der ALDE-Fraktion, einem Drittel der S&D-Fraktion sowie einigen EFD- und unabhängigen Abgeordneten zusammen. Die 33 Enthaltungen verteilten sich vor allem auf einige wenige ALDE-, EVP- und S&D-Abgeordnete (EU-Parlament 2012f, 19 f.).

3.3.4.3.1 Zwischenfazit

Auch am Beispiel der Fluggastdatentransfers wiederholte sich das Muster, das bereits mit dem Kompromiss bei der ePrivacy-Richtlinie seinen Anfang genommen hatte. Sobald die Staatsräson in den Vordergrund rückte, verließ die S&D ihren datenschutzbefürwortenden bzw. überwachungskritischen Standpunkt und unterstützte die EVP und die übrigen konservativen Akteure in ihren Bestrebungen zur Ausweitung der Überwachung. Im Vergleich zu den vorherigen datenschutzpolitischen Auseinandersetzungen war am Beispiel des Fluggastdatentransfers zusätzlich problematisch, dass die Inhalte des Abkommens im Laufe der Jahre zunehmend überwachungsfreundlicher geworden waren. Nicht nur erlaubte das Abkommen auch weiterhin die Speicherung der PNR-Daten für 15 Jahre, im Falle der Anonymisierung der Daten wurde eine unbegrenzte Aufbewahrungsfrist vorgesehen. Weder eine unabhängige Aufsicht, noch die elementaren Betroffenenrechte in Form der Rechte auf Auskunft, Berichtung und Löschung oder Rechtsschutz wurde den europäischen Bürgerinnen und Bürgern zuerkannt (A. Busch 2012a).

Sowohl der EDSB als auch die in der Art. 29-Datenschutzgruppe versammelten EU-Datenschutzbeauftragten kritisierten das Verhandlungsergebnis

im Hinblick darauf, dass es den europäischen Grundrechten nicht gerecht werde (Krempl 2012c). Während zu Beginn der 2000er-Jahre der Zugriff auf Fluggastdaten zu sicherheitspolitischen Zwecken noch als weitgehender Eingriff in Freiheits- und Datenschutzrechte gewertet wurde, hatte sich die Debatte im Laufe der Jahre dermaßen verschoben, dass nicht nur weitere PNR-Abkommen mit Kanada und Australien abgeschlossen wurden, sondern die EU-Kommission 2007 sogar eine Initiative für die Sammlung von Fluggastdaten in der EU selbst startete (EU-Kommission 2011).

3.3.4.4 Die Erarbeitung des JI-Rahmenbeschlusses 2008/977/JHA

Nachdem mehrere seit den 1990er-Jahren betriebene Initiativen zur Festlegung gemeinsamer Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (PJZS) aufgrund des Widerstands einiger Mitgliedstaaten[202] gescheitert waren, hatte sich im Laufe des Jahres 2005 ein Gelegenheitsfenster geöffnet, in dessen Ergebnis die Verabschiedung des JI-Rahmenbeschlusses erfolgen sollte. So hatten sich die EU-Organe im Rahmen des Haager Programms auch zur Festlegung von Datenschutzstandards auf dem Schutzniveau der DS-RL für den Bereich der Politiken der dritten Säule entschlossen. Zudem erneuerten die europäischen Datenschutzbeauftragten sowie das Europäische Parlament ihren Wunsch nach Datenschutzregelungen für die dritte Säule Mitte 2005 und ermutigten die Kommission und den Ministerrat zur Verabschiedung entsprechender Regeln (vgl. die vorangegangenen Unterabschnitte).

Schließlich wurde im Rahmen des Maßnahmenpakets, das nach den Londoner Anschlägen von den EU-Justiz- und Innenminister auf einer Sondersitzung des Ministerrats verabschiedet wurde, die Kommission zur Vorlage eines entsprechenden Legislativvorschlags bis Oktober 2005 aufgefordert (EU-Ministerrat 2005a, 7). Dieser Aufforderung kam die Kommission nach und veröffentlichte am 4. Oktober 2005 ihren *Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden* (Europäische Kommission 2005c).

Der Veröffentlichung war ein Prozess der Konsultation unter den EU-Organen und -Institutionen vorangegangen. Dabei wurden Vertreter

202 Der Widerstand einzelner Mitgliedstaaten im Bereich der Politiken der dritten Säule war insofern von herausgehobener Bedeutung, als Beschlüsse im Rahmen der dritten EU-Säule grundsätzlich einstimmig gefasst wurden (Wessels 2008, 201 ff.).

der Mitgliedstaaten (am 22. November 2004 und am 21. Juni 2005), der nationalen Datenschutzaufsichtsbehörden, des EDSB, von Europol und Eurojust (am 11. Januar 2005) und die erwähnte Resolution der Europäischen Datenschutzbeauftragen bzw. des Europäischen Parlaments berücksichtigt. Außerdem partizipierten Kommissionsvertreter an Treffen der von der Frühjahreskonferenz der Europäischen Datenschutzaufsichtsbehörden mandatierten *Arbeitsgruppe Polizei* (am 12. April und 21. Juni 2005) sowie an einer einschlägigen Veranstaltung des LIBE-Ausschusses (EU Commission 2005, 6). Die Kommission stellte fest, dass die Datenschutzaufsichtsbehörden und das EP dabei ihre vollständige Unterstützung für das Gesetzesvorhaben der Kommission zum Ausdruck gebracht hätten, während die Vertreter der Mitgliedstaaten und von Europol und Eurojust keine einheitliche Position vertreten hätten. Klar sei geworden, dass die Mitgliedstaaten Interesse an einem Datenschutzinstrument nur dann hätten, sofern es unter Wahrung von Datenschutz-Grundsätzen dem von den Polizei- und Justizbehörden anvisierten Ziel der europaweiten Verfügbarkeit dienlich wäre (ebd., 6 f.).

Obwohl die Erarbeitung des Kommissionsvorschlags nicht mehr unter der Verantwortung des in der Binnenmarkt-GD angesiedelten Datenschutz-Referats, sondern unter dem in der Direktion D „Innere Sicherheit und Strafjustiz" der Generaldirektion „Justiz, Freiheit und Sicherheit" angesiedelten Referat „Bekämpfung von Terrorismus, Sicherheit und Strafjustiz" erfolgte (Zerdick 2008, 3),[203] sah der Vorschlag der Kommission entgegen zivilgesellschaftlichen Befürchtungen (Statewatch 2005) ein hohes, entlang der Vorgaben der DS-RL erarbeitetes Datenschutzniveau vor. Begründet wurde dieser Schritt damit, dass die „Grundprinzipien des Datenschutzes […] für den Datenschutz sowohl im Rahmen des ersten als auch im Rahmen des dritten Pfeilers [gelten]." (Europäische Kommission 2005c, 5) Entsprechend waren vergleichbare Betroffenenrechte wie in der DS-RL vorgesehen (Informationsrechte in Art. 19 und 20 sowie die Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten in Art. 21 JI-Rahmenbeschluss-E). Auch die Datenschutz-Grundsätze (Art. 4 JI-Rahmenbeschluss-E) waren den Grundsätzen der DS-RL ähnlich. Darüber hinaus sah der Vorschlag besondere Regeln für Drittstaatentransfers (Art. 15),

203 Im Zuge des Kommissionsaktionsplans zur Umsetzung des Haager Programms war das bis dahin in der GD-Binnenmarkt angesiedelte Datenschutz-Referat im Laufe der ersten Hälfte des Jahres 2005 *im Interesse eines kohärenten Konzepts* in die Direktion C „Ziviljustiz, Grundrechte und Unionsbürgerschaft" der GD Justiz, Freiheit und Sicherheit übertragen worden (Europäische Kommission 2005a, 10),

die Einrichtung unabhängiger Aufsichtsbehörden bzw. die Übertragung dieser Aufgabe an die bestehenden Datenschutzaufsichtsbehörden (Art. 30) sowie die Einrichtung einer EU-weiten Arbeitsgruppe – ähnlich der Art. 29-Datenschutzgruppe – vor (Art. 31). Der Anwendungsbereich des Vorschlags umfasste sowohl den Datenaustausch zwischen den EU-Mitgliedstaaten als auch Verarbeitungen in den Mitgliedstaaten selbst. Ausgenommen vom Anwendungsbereich waren jedoch Europol, Eurojust und ZIS (Art. 3).

3.3.4.4.1 Stellungnahmen der Datenschutzaufsichtsbehörden

Nach der Veröffentlichung des Kommissionsentwurfs setzten sich das Parlament und der Ministerrat sowie die europäischen Datenschutzbehörden mit diesem auseinander. Zunächst veröffentlichte der EDSB im Dezember 2005 eine erste Stellungnahme. Ausgehend von der ausdrücklichen Unterstützung des Kommissionsentwurfs machte die EDSB-Stellungnahme zahlreiche Vorschläge hinsichtlich der Verbesserung des Schutzniveaus, etwa im Hinblick darauf, dass die Verarbeitung von Daten über unterschiedliche Personengruppen (Verdächtige, Verurteilte, Opfer, Zeugen, Kontaktpersonen, Nicht-Verdächtige) nach unterschiedlichen, angemessenen Bedingungen und Schutzbestimmungen erfolgen, dass in Bezug auf automatisierte Einzelentscheidungen besondere Schutzbestimmungen eingeführt werden und schließlich, dass der Austausch personenbezogener Daten mit Drittländern auf Basis angemessener Datenschutzgarantien erfolgen sollte (EDSB 2005, 45–47). Der EDSB kam den Forderungen der Strafverfolgungsbehörden aber auch in mehreren Punkten entgegen, so wurde der Ausschluss geheim- und nachrichtendienstlicher Datenverarbeitung aus dem Anwendungsbereich des Rahmenbeschlusses nicht infrage gestellt, sondern lediglich darauf verwiesen, dass die einzelstaatlichen Rechtsvorschriften für diesen Bereich einen angemessenen Schutz für die Betroffenen vorsehen müssten (EDSB 2005, 31, Nr. 33). Zudem verwies der EDSB zwar auf die Bedeutung der Zweckbindung im europäischen Datenschutzrecht, vertrat jedoch zugleich die Ansicht, „dass hinsichtlich der Weiterverwendung eine gewisse Flexibilität möglich sein" (EDSB 2005, 34, Nr. 62), d. h. eine Ausnahmeregelung vorhanden sein müsse, auf deren Grundlage die Weiterverarbeitung für Zwecke, die mit dem ursprünglichen Zweck unvereinbar seien, möglich werde, während zugleich Datenschutzgarantien berücksichtigt würden (EDSB 2005, 34, Nr. 60-65). Auf die Stellungnahme des Europäischen Datenschutzbeauftragten folgte Ende Januar 2006

eine erste Stellungnahme der Konferenz der europäischen Datenschutzbeauftragten. In dieser wurden das dem Entwurf zugrundeliegende hohe, an der DS-RL 95/46/EG orientierte, Schutzniveau sowie die Anwendbarkeit der Regeln sowohl auf den Datenaustausch zwischen EU-Mitgliedstaaten als auch auf Datenverarbeitungen in den Mitgliedstaaten selbst, gelobt (Conference of European Data Protection Authorities 2006, 6). Zudem wiesen auch die mitgliedstaatlichen Datenschutzbeauftragten auf zahlreiche Mängel in Bezug etwa auf die Betroffenenrechte, die Weiterverwendung von Daten zu anderen Zwecken und die vorgesehenen Regelungen zu automatisierten Einzelentscheidungen hin. Auf ihrer jährlichen Frühjahreskonferenz verabschiedeten die mitgliedstaatlichen Datenschutzbeauftragten zudem die sog. Erklärung von Budapest (*Budapest declaration*), in der zum einen ihre vorgenannten Forderungen bekräftigt wurden, aber insbesondere das Europäische Parlament und die Parlamente der Mitgliedstaaten dazu aufgerufen wurden, auf die Regierungen der Mitgliedstaaten dahingehend einzuwirken, dass für den Rahmenbeschluss ein hohes Datenschutzniveau realisiert werden könne. An die Regierungen der Mitgliedstaaten wurde lediglich appelliert, die bürgerlichen Freiheiten der in der EU lebenden Bürger zu achten und zu stärken, wenn sie die Möglichkeiten für den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten erweiterten (European Data Protection Authorities 2006a).

3.3.4.4.2 Positionierung des Parlaments

Gemäß dem Konsultationsverfahren bat der Ministerrat das Europäische Parlament am 13. Dezember 2005, zu dem Kommissionsentwurf Stellung zu nehmen. Das Parlamentspräsidium übergab den Richtlinienentwurf im Januar 2006 an den LIBE-Ausschuss, der sich mit diesem auf drei Sitzungen auseinandersetzte und schließlich am 15. Mai 2006 den Berichtsentwurf der Berichterstatterin Martine Roure (SPE, PS, Frankreich) einstimmig annahm (Roure 2006, 47). Der Roure-Bericht, der viele der Änderungsanträge und Vorschläge des Europäischen Datenschutzbeauftragten aufgriff, wurde schließlich am 13. Juni 2006 im Parlamentsplenum debattiert. Während der Sitzung wurde die Intention des Parlaments bekräftigt, die innerstaatliche polizeiliche und justizielle Verarbeitung von Daten im Anwendungsbereich des Rahmenbeschlusses zu belassen und für die dritte Säule insgesamt ein Schutzniveau zu etablieren, das dem der ersten Säule

entsprach. Begründet wurde die Haltung des Parlaments nicht nur mit dem Schutz personenbezogener Daten, sondern auch mit der Verbesserung der Interoperabilität der nationalen Datenbanken, also der Effizienzsteigerung strafverfolgungsbehördlicher Tätigkeiten. Interessanterweise vermied es das Parlament, den gesellschaftlichen Sicherheitsinteressen der Strafverfolgungsbehörden nur individuelle Datenschutzinteressen entgegenzustellen, wie es der folgende Kommentar des Abgeordneten Alexander Alvaro gut auf den Punkt bringt: „Das Problem ist aber, dass Leute, die Daten schützen wollen, oft in eine Ecke gestellt werden, als wären sie irgendwelche Knallschoten, die nicht in der Lage sind, Grundrechte und Sicherheitsrechte in irgendeiner Weise vernünftig gegeneinander abzuwägen. Gott sei Dank hat sich dieses Parlament in diesem Fall nicht in diese Ecke treiben lassen, dass wir Grundrechte gegen Sicherheitsrechte ausspielen würden, *denn das Weniger an Grundrechten gefährdet definitiv die Sicherheit der Bevölkerung*." (Alexander Alvaro, in: Europäisches Parlament 2006c, Hervorhebung M.K.) Zudem erinnerte Martine Roure an die *moralische Verpflichtung* hinsichtlich der raschen Verabschiedung von Datenschutzregelungen im Bereich der dritten Säule *unter Einhaltung einer fairen Zusammenarbeit zwischen den europäischen Organen*, die der Ministerrat im Rahmen der Verabschiedung der Richtlinie über die Vorratsdatenspeicherung gegenüber dem Parlament eingegangen war (vgl. die entsprechenden Ausführungen des britischen Ratsvorsitzes in 3.3.4.2). Da sich die Einigung im Rat erheblich verzögert hatte und die für Ende 2006 vorgesehene Verabschiedung des Rahmenbeschlusses zunehmend schwieriger zu realisieren schien, forderte Roure die an der Plenardebatte teilnehmenden Vertreter des Ministerrats dazu auf, noch am selben Tag *eindeutige Zusagen zu den für das Europäische Parlament wesentlichen Punkten* zu machen und dem Parlament einen *Zeitplan für die Verabschiedung des Rahmenbeschlusses* vorzulegen. Roure gab zu verstehen, dass sie bereits stark enttäuscht vom Rat sei und, sollte der Rat den geäußerten Wünschen nicht nachkommen, das Parlament sich hintergangen fühlen und dies das Vertrauen des Parlaments künftig ernsthaft beeinträchtigen würde (Martine Roure, in: Europäisches Parlament 2006c). Tatsächlich hatte das Parlament durchaus ein Druckmittel in der Hand, da es im Rahmen des Mitentscheidungsverfahrens an der Aktualisierung des Schengener Informationssystems (SIS)[204] beteiligt war und somit

204 Am sog. Schengener Informationssystem der zweiten Generation (SIS II) (EU 2007).

über ein Veto-Recht verfügte. Zwar zeigten sich die Fraktionen der Linken und Grünen bereit, dieses Druckmittel auch zu nutzen, doch die konservative Fraktion weigerte sich und Berichterstatterin Roure übte lediglich dahingehenden Druck auf den Ministerrat aus, den Rahmenbeschluss gemeinsam mit SIS II zu verabschieden (Europäisches Parlament 2006c; Roure 2006, 44 f.). Auf die Forderungen, die Roure gegenüber dem Ministerrat geäußert hatte, erhielt sie allerdings keine Antwort, da keine Ratsvertreter während des Plenums anwesend waren. Nachdem der Roure-Bericht am 14. Juni 2006 vom Parlamentsplenum mit überwältigender Mehrheit angenommen wurde, wurde auf den Antrag von Berichterstatterin Roure hin die Vertagung der Abstimmung über die Legislativentschließung des Parlaments bis zur Stellungnahme des Ministerrats beschlossen (Europäisches Parlament 2006e). Schließlich nahm die finnische Ratspräsidentschaft am 27. September im Rahmen der Parlamentsdebatte über die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts Stellung zu den Forderungen des Parlaments. Der sozialdemokratische Ratspräsident Kari Rajamäki (finnischer Innenminister von 2003–2007) erklärte, dass die Präsidentschaft beabsichtige, den Rahmenbeschluss schnellstmöglich anzunehmen und „die erste Lesung des Vorschlags noch während der laufenden Sechsmonatsperiode abzuschließen." (Europäisches Parlament 2006f)[205] Nachdem die moralische Verpflichtung des vorangegangenen britischen Ratsvorsitzes von der finnischen Ratspräsidentschaft bekräftigt

205 Zudem hatte sich das Parlament zwischenzeitlich endgültig gegen die Blockade von SIS II und der vom Ministerrat im Alleingang verhandelten VIS entschieden und damit ein weiteres Mal sein äußerstes Entgegenkommen gegenüber den Wünschen des Ministerrats demonstriert, was die Ratspräsidentschaft durchaus zur Kenntnis nahm: „Der Vorsitz ist sich des Charakters des Vorschlags für einen Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen der dritten Säule – ich beziehe mich jetzt auf den Vorschlag von Frau Roure – und seiner Bedeutung für die Bürger Europas sehr wohl bewusst, ebenso auch der Tatsache, das sich das Europäische Parlament für die Vorschläge über Rahmenbeschlüsse zu den Informationssystemen VIS und SIS II ausgesprochen hat. In diesem Zusammenhang und im Namen des Ratsvorsitzes möchte ich dem Europäischen Parlament für seine Arbeit danken und sagen, dass wir alles in unseren Möglichkeiten Stehende tun werden, um noch vor Ablauf unserer Präsidentschaft eine Einigung über den Vorschlag für den Rahmenbeschluss zu erzielen. Soweit möglich, werden wir bei unserer weiteren Arbeit die Stellungnahme und die Auffassungen des Europäischen Parlaments im Kontext der Bestimmungen des EG-Vertrags berücksichtigen, um letztlich mit einem brauchbaren legislativen Instrument ein hohes Maß an Schutz der persönlichen Daten durch die Schaffung gemeinsamer Regeln für den Datenschutz im Rahmen der dritten Säule zu gewährleisten." (Kari Rajamäki, in: Europäisches Parlament 2006f)

und konkretisiert worden war, stimmte das Parlament noch am selben Tag für die Legislativentschließung, in der es den Ministerrat dazu aufforderte, das Parlament zu unterrichten, sofern die Parlamentsänderungen nicht angenommen würden und im Falle einer weitergehenden Änderung des Kommissionsentwurfs das Parlament erneut zu konsultieren (Europäisches Parlament 2006b).

3.3.4.4.3 Verhandlungen im Ministerrat

Auf Seiten des Ministerrats übernahm keine mit Datenschutz befasste Ratsarbeitsgruppe die Verantwortung für die Beratungen und Verhandlungen zum JI-Rahmenbeschluss, sondern die sog. MDG, multidisziplinäre Gruppe „Organisierte Kriminalität" (Working Group for Organized Crime and other Horizontal Issues) (Vorsitz - EU-Ministerrat 2006).[206] Die seit ihrer Einsetzung am 21. Februar 1991 für die Verhandlungen zur DS-RL, ISDN-RL sowie DS-VO zuständige Ratsarbeitsgruppe Datenschutz[207] war zwischenzeitlich unter Verweis auf ihre Inaktivität seit April 2001 am 24. Januar 2002 aufgelöst (General Secretariat of the Council of the European Union 2002) und erst unter der österreichischen Ratspräsidentschaft Anfang 2006 wieder reaktiviert worden. Die wiedereingerichtete Gruppe *Datenschutz* wurde zwar mit zahlreichen Aufgaben betraut, doch die Verantwortung der Beratungen zum Rahmenbeschluss verblieb – trotz der Einbindung der Gruppe Datenschutz in den Prozess – weiterhin bei der MDG (Statewatch 2006).

Die MDG, die sich aus Beamten der mitgliedstaatlichen Strafverfolgungsbehörden zusammensetzte (P. de Hert und Papakonstantinou 2009, 407), hatte allerdings zu keinem Zeitpunkt Interesse an einem ernsthaf-

206 Für die Datenschutzfragen im JI-Bereich im Kontext der dritten Säule war die Ratsarbeitsgruppe „Informationssysteme und Datenschutz" („Working Party on Information Systems and Data Protection") zuständig, die von ihrer ersten Sitzung am 11 Februar 1999 bis zum Juni desselben Jahres zunächst unter dem Namen „Informatik" als horizontale Gruppe tagte (Rat der Europäischen Union 1999). Die Funktionen der Ratsarbeitsgruppe „Informationssysteme und Datenschutz" wurden Anfang 2002 schließlich parallel zur Auflösung der Datenschutz-Ratsarbeitsgruppe in den Verantwortungsbereich der MDG übertragen (Swedish Delegation 2002, 5),

207 Bis zu ihrer Umbenennung im Sinne einer klareren Zuordnung im Jahr 1999 firmierte die Arbeitsgruppe unter dem Namen „Wirtschaftsfragen (Datenschutz)" bzw. „Economic Questions – Data Protection" (Presidency of the Council of the European Union 2006, 1).

ten inhaltlichen Austausch mit dem Europäischen Parlament oder den europäischen Datenschutzbeauftragten.[208] Stattdessen war die MDG von dem Ziel angetrieben, einen möglichst reibungslosen und weitgehenden Datenaustausch zwischen den Mitgliedstaaten zu gewährleisten. Mehrere Faktoren strukturierten das Handeln der Arbeitsgruppe und sollten die Verabschiedung eines hohen Datenschutzniveaus deutlich erschweren: *Erstens* war die für eine wirksame Ausgestaltung der Datenschutzregelungen erforderliche und EU-weit einheitliche Differenzierung zwischen Polizei- und Justizbehörden schwierig zu leisten, wie z. B. mit polizeilichen Daten umgegangen werden sollte, die auf Hörensagen beruhen, während die Unabhängigkeit des Justizbereichs deren Kontrolle erschwerte. *Zweitens* waren die existierenden Unterschiede zwischen den Polizei- und Justizsystemen enorm: Während z. B. die Polizei in einigen Mitgliedstaaten Strafmaßnahmen anordnen durfte, war dies in anderen Staaten einem Staatsanwalt vorbehalten. *Drittens* erschwerten nationale politische Sensibilitäten den Einigungsprozess in der Ratsarbeitsgruppe bzw. im Ministerrat generell: Einige Delegationen hatten ein außerordentlich einseitiges Interesse an der weitest möglichen Verfügbarkeit aller Daten und betrachteten Datenschutzvorkehrungen als Beeinträchtigung und nicht als elementaren Bestandteil ihrer täglichen Arbeit. *Viertens* hatten alle Mitgliedstaaten im Laufe der Jahre Pfadabhängigkeiten geschaffen, die nur schwer umzukehren waren. Viele Mitgliedstaaten hatten bilaterale Abkommen mit anderen, auch Nicht-EU-Staaten zum Datenaustausch abgeschlossen, deren Fortbestand von dem im Rahmenbeschluss festzulegenden Datenschutzniveau abhing. Schließlich und *fünftens* musste der Ministerrat über den Rahmenbeschluss einstimmig entscheiden, sodass jeder Mitgliedstaat das Vorhaben verhindern konnte. Da zudem die Gegner von Datenschutzregelungen im Bereich der dritten Säule mit dem Status Quo zufrieden waren, im Falle eines Scheiterns des Legislativvorhabens also nichts zu verlieren, aber viel zu gewinnen hatten, mussten sie keinerlei Kompromisse mit den Datenschutzbefürwortern eingehen. Dadurch gerieten die Verhandlungen im Ministerrat zu einem Wettlauf nach unten (P. D. Hert, Papakonstantinou, und Riehle 2008, 165 f.).

Die erste, von der MDG im November 2005 begonnene Lesung des Kommissionsentwurfs konnte aufgrund dieser Schwierigkeiten erst verspätet im September 2006 abgeschlossen werden. Kurz vor dem Ende ihrer

208 Ein Beobachter machte die Feststellung, dass ihr *"primary interest is to make life difficult for criminals, not to have regard to the interests of data subjects"* (Lord Avebury 2006).

Amtszeit legte die finnische Ratspräsidentschaft schließlich noch im November 2006 einen ersten Entwurf für eine gemeinsame Position des Rats vor. Dieser erste Ratsentwurf änderte den Kommissionsentwurf allerdings dermaßen stark, dass kaum ein Datenschutzelement übrig blieb, das nicht durch sehr weit und zugleich unklar gefasste Ausnahmeregelungen außer Kraft gesetzt werden konnte. So sah der November-Ratsentwurf, obwohl der Juristische Dienst des Rates, die Kommission, das Parlament, die Europäischen Datenschutzbeauftragten sowie auch die Mehrheit der EU-Mitgliedstaaten für den Einbezug innerstaatlicher Datenverarbeitung votierten, aufgrund des Widerstands einiger Mitgliedstaaten, angeführt vom Vereinigten Königreich, eine Abschwächung des Anwendungsbereichs vor.[209] Die Anforderung, dass Drittländer, in die personenbezogene Daten aus der EU übertragen werden sollten, ein angemessenes Datenschutzniveau garantieren müssten, wurde zwar von der Tschechischen Republik, der Schweiz, Finnland, Griechenland und Portugal befürwortet, doch von Deutschland, Dänemark, Spanien, Irland, Norwegen, Schweden und dem Vereinigten Königreich abgelehnt, sodass die Regelung dahingehend aufgeweicht wurde, dass bestehende bi- bzw. multilaterale Abkommen unberührt von der Regel, eine Angemessenheitsprüfung durchzuführen, sein sollten (Bunyan 2006, 10 f.).[210] Aufgeweicht wurden auch die Bestimmungen zur Weiterverarbeitung von personenbezogenen Daten zu anderen Zwecken als dem ursprünglichen Verarbeitungszweck und auch die Bestimmungen zur Verarbeitung besonderer Kategorien personenbezogener Daten (ebd.,

209 In diesem Zusammenhang wurde darauf hingewiesen, dass die Polizei- und Justizbehörden der Mitgliedstaaten dann zwei Datenbanken (eine für die nationale Datenverarbeitung und eine weitere für den unionsweiten Datenaustausch) führen müssten, woraufhin sich eine Reihe von praktischen und theoretischen Fragen stellen lässt: Wie kann die Polizei zuvor wissen, welche Daten in der Zukunft von den anderen Mitgliedstaaten angefragt werden? Und welche Arten von möglicherweise problematischen Verarbeitungen führen die Mitgliedstaaten durch, dass sie nicht gewillt sind, elementare Datenschutzgrundsätze auf diese Verarbeitungen anzuwenden? (P. D. Hert, Papakonstantinou, und Riehle 2008, 166) Letztere Frage wurde einige Jahre später, zumindest in Bezug auf das Vereinigte Königreich mit dem Bekanntwerden des Überwachungsprogramms Tempora teilweise recht eindeutig beantwortet.

210 In Bezug auf den Datentransfer in Drittstaaten berichtete beispielsweise die grüne niederländische Europaabgeordnete Kathalijne Maria Buitenweg später von einer *lustigen Begebenheit* während des deutschen Ratsvorsitzes, „als ein Vertreter des Rates ausführte, es sei manchmal tatsächlich notwendig, sehr schnell Daten in den Iran zu übermitteln. Das ganze Haus war sprachlos; das konnte nicht sein Ernst sein – Datentransfers in den Iran!“ (EP 2008c)

12–14). Gegen die in den Art. 19 und 20 des Kommissionsentwurfs vorgesehenen Informationsrechte der Betroffenen bzw. Informationspflichten der Verarbeiter votierten Belgien, die Tschechische Republik, Deutschland, Spanien, Griechenland, Italien, die Niederlande, Norwegen, Portugal, Schweden und das Vereinigte Königreich (ebd., 14). Zudem erfolgten auf den Wunsch Dänemarks, der Niederlande und des Vereinigten Königreichs hin auch Streichungen beim Betroffenenrecht auf Auskunft (ebd., 15) und auf den Wunsch Dänemarks, Frankreichs, Griechenlands, der Niederlande und Schwedens hin auch die Einschränkung der Vorgabe, rechtmäßige Berichtigungs- und Löschungswünsche an Dritte, denen die Daten zuvor übermittelt worden waren, weiterzureichen (ebd., 16).

3.3.4.4.4 Stillstand der Verhandlungen

Nachdem der erste Entwurf der gemeinsamen Ratsposition, die eine Einschränkung des Datenschutzniveaus vorsah, bekannt geworden war, veröffentlichten die Europäischen Datenschutzbehörden die Londoner Erklärung (*London declaration*), in der sie ihre Forderung nach einem hohen und harmonisierten Datenschutzniveau für den Bereich der dritten Säule ein weiteres Mal bekräftigten (European Data Protection Authorities 2006b). Am 29. November 2006 veröffentlichte der Europäische Datenschutzbeauftragte seine zweite Stellungnahme zum Rahmenbeschluss. Darin stellte der EDSB zunächst fest, dass die zirkulierenden Ratspositionen weder die vom Europäischen Parlament vorgeschlagenen Abänderungen noch jene des EDSB oder die der Konferenz der europäischen Datenschutzbehörden berücksichtigten und stattdessen sogar das Schutzniveau des Kommissionsentwurfs reduzierten: „Infolgedessen besteht die Gefahr, dass das Schutzniveau niedriger als dem [sic] Schutzniveau der Richtlinie 95/46/EG oder gar des allgemeiner gefassten Übereinkommens Nr. 108 des Europarates, das für die Mitgliedstaaten bindend ist [sic] sein wird." (EDSB 2006, 9, Nr. 4) Neben einer Reihe von Änderungsvorschlägen empfahl der EDSB dem Rat schließlich, aufgrund des Ziels einer zügigen Entscheidungsfindung nicht die Absenkung des Schutzniveaus in Kauf zu nehmen und sich lieber mehr Zeit für die Verhandlungen zu nehmen, damit im Ergebnis ein ausreichender Schutz geboten werde (ebd., 10, Nr. 8).

Am 13. Dezember fand die erste Aussprache zum Thema nach Bekanntwerden der Ratspositionen im Europäischen Parlament statt. Die liberale finnische Vertreterin des noch amtierenden Ratsvorsitzes, Paula Lehtomäki

(Zentrumspartei, finnische Ministerin für Außenhandel, Entwicklung und Europaangelegenheiten zwischen 2003 und 2007) gab während der Plenardebatte bekannt, dass es trotz der Bemühungen der finnischen Ratspräsidentschaft wohl nicht mehr in ihrer Amtszeit zu einer Einigung im Ministerrat kommen werde. Als Hauptgrund nannte Lehtomäki den Konflikt um den Anwendungsbereich des Rahmenbeschlusses, dessen Beschränkung auf grenzüberschreitende Datentransfers weiterhin von einigen Mitgliedstaaten gefordert werde (Europäisches Parlament 2006d). Parlamentsberichterstatterin Roure dankte dem finnischen Ratsvorsitz für seine Bemühungen, machte allerdings angesichts der beunruhigenden Entwicklungen der Ratsverhandlungen in Richtung einer Einigung auf dem kleinsten gemeinsamen Nenner, die hinter dem Schutzniveau der DS-RL und der Europaratskonvention deutlich zurückbleibe, auch deutlich, dass das Parlament das Visainformationssystem (VIS) nicht einführen werde, „ohne über Garantien zu verfügen, dass ein Rahmenbeschluss über den Datenschutz angenommen werden soll." (Europäisches Parlament 2006d) Am Tag darauf, dem 14. Dezember 2006, verabschiedete das Parlament schließlich eine an den Rat gerichtete Empfehlung, in der es diese Sorgen zum Ausdruck brachte (Europäisches Parlament 2006a).

3.3.4.4.5 Überwindung der politischen Pattsituation

Mit dem Jahresbeginn 2007 übernahm Deutschland die Ratspräsidentschaft und damit auch die Verantwortung über die Weiterführung der Verhandlungen zum Rahmenbeschluss, musste aber bereits im Januar feststellen, dass die Verhandlungen in eine Sackgasse geraten waren und aufgrund der Frage nach dem Anwendungsbereich zu scheitern drohten. Daraufhin bat der deutsche Ratsvorsitz die Kommission zunächst um die Erstellung eines überarbeiteten Kommissionsentwurfs, veröffentlichte im März 2007 dann aber einen eigenen überarbeiteten Entwurf. Zudem beschloss der Ratsvorsitz, das Parlament aufgrund der weitgehenden Änderungen ein weiteres Mal zu konsultieren (P. de Hert und Papakonstantinou 2009, 408; Roure 2007, 45). Der Vorschlag des deutschen Vorsitzes sah für den Kernkonflikt um den Anwendungsbereich des Rahmenbeschlusses die Einigung auf dem kleinsten gemeinsamen Nenner vor, mit dem Hinweis darauf, dass eine Erhöhung des Schutzniveaus für einzelne Bereiche seitens der Mitgliedstaaten explizit möglich sein sollte. Und auch im Hinblick auf die anderen Streitthemen (Datentransfers in Drittländer, Weiterverarbeitung,

Betroffenenrechte) stellte der Vorschlag eine Verschlechterung dar. Mehr noch, wurde die im Kommissionsentwurf (Art. 31) vorgesehene Einrichtung einer EU-weiten und sich aus Vertretern der nationalen Datenschutzbehörden zusammensetzenden Arbeitsgruppe weitgehend verworfen (Peers 2007, 2–5).

In der Folge bekräftigten der EDSB im Rahmen seiner dritten Stellungnahme (EDSB 2007a), die Konferenz der europäischen Datenbehörden im Rahmen ihrer Erklärung von Zypern (European Data Protection Authorities 2007) sowie das Parlament (Roure 2007) ein weiteres Mal ihren Wunsch nach einem hohen Datenschutzniveau, wiesen darauf hin, dass der vom deutschen Ratsvorsitz vorgelegte Text eine weitere Verschlechterung des Schutzniveaus darstelle, und zeigten sich erneut enttäuscht über die anhaltende Ignoranz des Ministerrats gegenüber ihren Änderungswünschen.

Nach weiteren mühevollen Verhandlungen konnte unter portugiesischer Ratspräsidentschaft auf der Tagung des gemischten Ausschusses auf Ebene der Justiz- und Innenminister am 8. November eine erste politische Einigung und am 30. November 2007 schließlich die endgültige Einigung auf Arbeitsgruppenebene erzielt werden (EU-Ministerrat 2007). Auf Grundlage dieser Einigung konsultierte der Ministerrat das Parlament schließlich Anfang 2008 zum dritten Mal und das Parlament verabschiedete am 23. September 2008 seine Position auf Grundlage des von Martine Roure ausgearbeiteten LIBE-Ausschuss-Berichts (Roure 2008). Am 27. November 2008 verabschiedete der Ministerrat schließlich den *Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*, dessen Vorgaben bis zum 27. November 2010 in nationales Recht umzusetzen waren (EU-Ministerrat 2008c).

Bemerkenswerterweise gaben die im Ministerrat versammelten Regierungsvertreter die Verabschiedung des Rahmenbeschlusses weder in der Pressekonferenz nach ihrer Tagung, auf der das Dokument verabschiedet wurde, noch in einer eigenen Pressemeldung bekannt (Krempl 2008a). Von allen sonstigen beteiligten Akteuren und Beobachtern wurde der Text, auf den sich der Ministerrat geeinigt hatte, hingegen rege kommentiert und als eine weitere Aushöhlung des ursprünglichen Kommissionsentwurfs wahrgenommen. So kommentierte etwa Berichterstatterin Roure: „Das Datenschutzniveau dieses Textes ist minimal und weist auch sehr erhebliche Defizite auf. In einigen Fällen könnte man sich sogar fragen, ob es die im Übereinkommen 108 festgesetzten Standards, insbesondere im Hinblick auf das Prinzip der Verhältnismäßigkeit einhält, das ein grundlegendes Daten-

schutzprinzip ist." (Roure 2008, 26) Etwas diplomatischer bezeichnete der Europäische Datenschutzbeauftragte Peter Hustinx den Rahmenbeschluss als ersten wichtigen Schritt auf dem Weg zu einem angemessenen Schutz personenbezogener Daten im Bereich der Polizei und Strafverfolgung, auf den allerdings noch weitere folgen müssten (EDPS 2008). Sowohl Parlament als auch EDSB bemängelten weiterhin insbesondere die Begrenzung des Anwendungsbereichs des Beschlusses auf die zwischen Mitgliedstaaten und EU-Behörden bzw. anderen Mitgliedstaaten ausgetauschten Daten. Daneben wurde aber auch die weiterhin fehlende Differenzierung zwischen Daten von unterschiedlichen Personengruppen (Verdächtige, Verurteilte, Opfer, Zeugen, Kontaktpersonen, Nicht-Verdächtige), das Fehlen gemeinsamer Standards beim Datentransfer in Drittstaaten, die Aushöhlung der Zweckbindung, die Untergrabung von Betroffenenrechten sowie die vollständige Streichung der sich aus den nationalen Kontrollstellen zusammensetzenden Arbeitsgruppe kritisiert (EDPS 2008; Roure 2008). Die wissenschaftlichen Analysen zum Rahmenbeschluss kritisierten die genannten Punkte ebenfalls, hoben aber zugleich hervor, dass der Text immerhin einen ersten, wichtigen Schritt auf dem Weg zu einem angemessenen Datenschutzrahmen im Bereich der dritten Säule darstelle (Belfiore 2013; Bigo u. a. 2011; Boehm 2012, 114 f. González Fuster 2014, 220–22; P. de Hert und Papakonstantinou 2009; Hijmans und Scirocco 2009).

3.3.4.4.6 Zwischenfazit

Zunächst lässt sich festhalten, dass der JI-Rahmenbeschluss einen Minimalkonsens zu den vielen offenen Datenschutzfragen im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen darstellt (P. de Hert und Papakonstantinou 2009). Vielmehr aber noch führte der schwierige Aushandlungsprozess den Datenschutzbefürwortern verschiedene kritische Punkte vor Augen.

So hatte die britische Ratspräsidentschaft das bei der Verabschiedung der Richtlinie zur Vorratsdatenspeicherung gegebene Versprechen bezüglich der Zusammenarbeit im Hinblick auf die Verabschiedung eines Rahmeninstruments zum Datenschutz in der dritten Säule unter Beachtung der Parlamentsposition schlicht gebrochen. Der bereits aus den Verhandlungen zur DS-RL bekannte nördliche Block opponierte auch bei diesem Vorhaben gegen fast jeden Vorschlag, der die Gewährleistung eines der

DS-RL entsprechenden Schutzniveaus vorsah. Der nördliche Block setzte sich – je nach Frage auch variierend – zusammen aus Schweden, Norwegen, den Niederlanden, Dänemark und Irland und wurde vom Vereinigten Königreich angeführt. Das Parlament hatte auf diesen bevorstehenden Vertrauensbruch des Ministerrats während der Verhandlungsjahre mehrfach in der Hoffnung, dass die Datenschutzgegner zur Räson kommen und ihre Opposition beenden würden, hingewiesen, war jedoch letzten Endes durch den getroffenen Minimalkonsens im Rat massiv enttäuscht worden (EP 2008c; vgl. z. B. Roure 2006, 2007, 2008). In anderen Worten hatte der Aushandlungsprozess zum JI-Rahmenbeschluss endgültig vor Augen geführt, dass auf Grundlage der Einstimmigkeitsregel keine angemessenen Datenschutzgesetze in der EU zu machen waren.

Der Hauptkritikpunkt der Datenschutzbefürworter am Rahmenbeschluss in Form des Ausschlusses der innerstaatlichen Datenverarbeitung aus dessen Anwendungsbereich sollte allerdings mittelfristig zu einer deutlichen Stärkung der datenschutzrechtlichen Regelungen in diesem Bereich führen. So hatten bereits jene Mitgliedstaaten, die etwas offener gegenüber einem höheren Datenschutzniveau eingestellt waren (z. B. Frankreich, Finnland und stellenweise auch die Tschechische Republik, die Schweiz, Griechenland, Portugal und Deutschland), in Reaktion auf die vonseiten der Datenschutzbefürworter geäußerte Kritik am unzureichenden Anwendungsbereich hin, den Rahmenbeschluss dahingehend ergänzt, dass im Erwägungsgrund 8 die Absicht der Mitgliedstaaten, den Datenschutzstandard des Rahmenbeschlusses auch bei innerstaatlichen Datenverarbeitungen zu gewährleisten, festgehalten wurde. Art. 27 sah zudem die Prüfung der Auswirkungen der Bestimmungen auf den Anwendungsbereich nach einem Zeitraum von fünf Jahren vor und eröffnete der Kommission die Möglichkeit, diesbezügliche Änderungsvorschläge vorzulegen. Deutlich bedeutsamer war allerdings das geplante Inkrafttreten des Lissabon-Vertrags zum 1. Januar 2009. Je wahrscheinlicher die Verabschiedung von Datenschutzbestimmungen auf lediglich dem kleinsten gemeinsamen Nenner während der Verhandlungen wurde, umso mehr begannen die Europaparlamentarier in der Konsequenz ihre Hoffnungen auf das Inkrafttreten des Lissabon-Vertrags zu legen und umso selbstbewusster forderten sie die Einbeziehung des Parlaments in Entscheidungen über Gesetzesvorlagen im Bereich

der dritten Säule auf Augenhöhe.[211] So stellte Berichterstatterin Roure in ihrem dritten Bericht klar, dass es notwendig sei, „eine Überarbeitung des Rahmenbeschlusses innerhalb von sechs Monaten nach Inkrafttreten des Vertrags von Lissabon insbesondere im Hinblick auf die Ausdehnung des Anwendungsbereichs vorzunehmen." (Roure 2008, 26) Während der Parlamentsaussprache verwies zudem selbst der Vertreter des Ministerrats, Jean-Pierre Jouyet (parteiloser französischer Staatssekretär für europäische Angelegenheiten im Bereich des französischen Außenministeriums, der während der Plenardebatte die Justizministerin Rachida Dati vertrat), dass der JI-Rahmenbeschluss lediglich einen ersten wichtigen Schritt darstelle, auf den weitere Folgen müssten (EP 2008c).

Schließlich sprach sich insbesondere der neue konservativ-republikanische Kommissar für Justiz, Freiheit und Sicherheit, Jacques Barrot[212] (UMP, Frankreich), klar für die Stärkung des europäischen Datenschutzrahmens aus: „Wie ich bereits sagte, und ich möchte dies nicht überstrapazieren, wäre natürlich auch die Kommission beim Datenschutz wie auch das Parlament gerne weitergegangen. Der Minister, Herr Jouyet, hat erwähnt, dass sich der französische Ratsvorsitz danach richten musste, ob ein Kompromiss erzielt werden konnte, obwohl er dasselbe wollte. Ich kann nur sagen, dass die Kommission versuchen wird, die Evaluierungsklausel und die Erwägung 6a gut umzusetzen. Daher hören wir auf den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres und versuchen, ihrem Wunsch nach einer gründlichen Revision des Rahmenbeschlusses nachzukommen, um eine Erweiterung seines Geltungsbereichs zu beurteilen. Das ist es, was die Kommission tun kann und was ich persönlich zu tun versuchen werde. Ich weiß, dass das Europäische Parlament eine baldige Revision anstrebt. Ich hoffe nur, der Rat wird einer Revision innerhalb eines Zeitrahmens zustimmen, der es ermöglicht, schon bald eine europäische Maßnahme zu entwickeln." (EP 2008c)

211 Siehe die Ausführungen von Ludford (Europäisches Parlament 2007). Siehe auch die Wortbeiträge von Alvaro, Dührkop, Ludford. Leichtfried und Lefrançois (EP 2008c).

212 Der amtierende Kommissar für Justiz, Freiheit und Sicherheit, Franco Frattini hatte im April 2008 bei den italienischen Parlamentswahlen kandidiert und trat Anfang Mai schließlich den Posten des Außenministers im Kabinett Berlusconi IV an, sodass der Kommissarsposten im selben Monat an Jacques Barrot überging, nachdem dieser den Posten zwei Monate lang bereits vertretungsweise ausgefüllt hatte (Barrot 2008, 2).

Diese Revision sollte schon weniger als ein Jahr später im Rahmen der Reform der EU-Vorschriften für den Schutz personenbezogener Daten erfolgen, an deren Ende wiederum die Verabschiedung der DSGVO und der JI-Richtlinie stehen sollte.

3.3.5 Novellierung der ePrivacy-RL zur Cookie-Richtlinie 2009/136/EG

Den Anfangspunkt der Debatten, die zur Novellierung der ePrivacy-RL führen sollten, bildete die Überprüfung der Lissabonner Strategie seitens des Europäischen Rates im März 2005. In diesem Rahmen wurde schließlich die Neubelebung der Strategie mit dem unabdingbaren Ziel der Priorisierung der Themen Wachstum und Beschäftigung entschieden. Angesichts der „Kluft zwischen dem Wachstumspotenzial Europas und dem seiner Wirtschaftspartner" (Europäischer Rat 2005b, 2) müsse Europa die „Grundlagen seiner Wettbewerbsfähigkeit erneuern, sein Wachstumspotenzial sowie seine Produktivität erhöhen und den sozialen Zusammenhalt stärken, indem es vor allem auf Wissen, Innovation und Erschließung des Humankapitals setzt." (ebd.) Als Kernpunkte der erneuerten Strategie wurden die Verbesserung der Politikgestaltung, die Reduzierung des Verwaltungsaufwands für die Wirtschaft und die Vollendung des Binnenmarktes identifiziert und die Europäische Kommission, der Ministerrat und die Mitgliedstaaten darum gebeten, die Neubelebung der Strategie in Gang zu setzen (ebd., 2 f.).

Der konkrete politische Prozess, der auch zur Überarbeitung der ePrivacy-Richtlinie führte, startete am 25. November 2005 (EC 2006b, 5). Die politische Verantwortung für den Gesamtprozess der Novellierung der EU-Telekommunikationspolitik hatte die EU-Kommissarin für Informationsgesellschaft und Medien, Viviane Reding (Luxemburg, CSV/EVP) und damit die Generaldirektion Informationsgesellschaft inne.[213] Im Rahmen einer ersten Konsultationsphase forderte die Kommission Stakeholder zur Einrei-

213 Bereits Anfang 2006 hatte die konservative Kommissarin Reding mit ihrem Vorstoß gegen die hohen internationalen Roaming-Gebühren der Telekommunikationsdienstleister und ihrer dabei vertretenen Überzeugung, einen bürgerfreundlichen Telekommunikationsmarkt zu schaffen, erfolgreich Aufmerksamkeit auf sich gezogen und sich als bürgernahe EU-Politikerin profiliert (Europäisches Parlament 2017; Reding 2006b).

chung von Stellungnahmen auf.[214] Im Ergebnis der knapp 160 schriftlichen Stellungnahmen, die eingingen, offenbarte sich, dass eine Überarbeitung des geltenden Rechtsrahmens von einer breiten Mehrheit der Stakeholder als erforderlich angesehen wurde. Die beiden auf Grundlage des Stakeholder-Inputs entwickelten Hauptvorschläge der Kommission waren die *Verwirklichung des strategischen Frequenzverwaltungskonzepts der Kommission* und die *Verringerung des Verwaltungsaufwands im Zuge der Vereinfachung der Verfahren im Zusammenhang mit der Überprüfung der Märkte, die für eine Vorabregulierung in Betracht kommen* (EC 2006c, 7). Daneben wurden die *Konsolidierung des Binnenmarktes*, die *bessere Wahrung der Verbraucher- und Nutzerinteressen*, die *Erhöhung der Sicherheit* und die *Aufhebung veralteter Vorschriften* vorgeschlagen (ebd.).

Die Kommission erachtete insbesondere eine größere Produkt- und Anbieterauswahl, innovative Dienste und ein besseres Preis-Leistungsverhältnis als zentrale Ziele im Rahmen der Verwirklichung echter Vorteile für die Verbraucher. Daneben wurden aber auch rechtliche Verpflichtungen für Bereiche wie Datenschutz als weitere Ziele definiert. Anders als in der früheren Telekommunikationsstrategie wurde zudem das Thema IT-Sicherheit als zentral erachtet. So begrüßte die Kommission die im Rahmen der Deregulierungspolitiken vollzogene Öffnung der Telekommunikationsmärkte als eine begrüßenswerte Entwicklung, die zu einer Steigerung des anbieterseitigen Wettbewerbs und dem Umstieg vieler Nutzerinnen und Nutzer auf IP-basierte Technologien geführt habe. In diesem Zusammenhang rechnete die Kommission den Themen Vertrauenswürdigkeit, Sicherheit und Zuverlässigkeit von Informations- und Kommunikationstechnologien eine zentrale Rolle im Hinblick auf ihre gesellschaftliche Akzeptanz und weitere Verbreitung zu. Des Weiteren stellte die Kommission fest, dass der Markt darin versagt habe, die Sicherheitsprobleme zur Zufriedenheit der Nutzerinnen und Nutzer zu lösen und die Zunahme von Spam, Viren,

214 Diese erste Konsultationsphase fand zwischen dem 25. November 2005 und dem 31. Januar 2006 statt. Auf diese folgte eine öffentliche Anhörung mit mehr als 440 Teilnehmern. Die Federführung hatte die GD Informationsgesellschaft bzw. das Referat B 1 „Politikentwicklung" inne (EC 2005, 2007c, 4). Wie schon bei den Konsultationen zur ePrivacy-Richtlinie partizipierten auch an dieser Konsultation zahlreiche Akteure, die später auch im Rahmen des Aushandlungsprozesses zur DSGVO eine wichtige Rolle spielen sollten: Aea Europe/TechAmerica, AmCham, BEUC, Bitkom, BSA, BT, ECTA, ETNO, EuroISPA, EPC, Google, Intel, Liberty Global Europe, GSM Europe, Microsoft, Nokia, Telefónica, UK Information Commissioner's Office (ICO), UNICE/Businesseurope (European Commission DG InfSo 2006).

Spyware und anderen Formen von Malware das Vertrauen der Nutzerinnen und Nutzer in elektronische Kommunikationsdienste verringere.

Ausgehend von Art. 4 der ePrivacy-Richtlinie, der Vorgaben zu den seitens des Verantwortlichen vorzunehmenden *geeigneten technischen und organisatorischen Maßnahmen* formulierte, wurde daher die Ausweitung und Stärkung der Sicherheitsvorgaben vorgeschlagen. Insbesondere ging es dabei darum, den konkreten Gehalt der seitens eines Verantwortlichen zu treffenden *geeigneten technischen und organisatorischen Maßnahmen* zu spezifizieren. Daneben unterbreitete die Kommission auch erstmals Vorschläge zum Umgang mit Verstößen gegen die (Netz-)Sicherheit: Sofern im Zuge eines Verstoßes gegen die Netzsicherheit der Verlust personenbezogener Daten die Folgen wäre, sollte der Verantwortliche dazu verpflichtet werden, die zuständige nationale Aufsichtsbehörde wie auch die Nutzerinnen und Nutzer über den Vorfall zu informieren. Sofern die Aufsichtsbehörde der Ansicht sei, dass der Vorfall das öffentliche Interesse berühre, solle sie zudem die Öffentlichkeit über die Sicherheitsverletzung informieren dürfen (EC 2006a, 28–30). Daneben identifizierten die Berichte der Kommission ein massives Problem im Bereich der Rechtsdurchsetzung: So führe der rechtliche Status Quo dazu, dass eine Sanktionierung selbst größerer Sicherheitsversäumnisse durch die zuständigen Aufsichtsbehörden regelmäßig aufgrund verschiedener Faktoren nicht möglich gewesen sei, da die Betreiber nach der Genehmigungsrichtlinie die Möglichkeit hätten, Verstöße zu beheben, bevor Sanktionen verhängt würden. Selbst wenn eine Aufsichtsbehörde bereits im Vorfeld einer konkreten Sicherheitsverletzung Versäumnisse festgestellt und den Betreiber darauf hingewiesen habe, der Betreiber die Hinweise jedoch ignorierte, sei es der Aufsichtsbehörde – aufgrund von Bestimmungen zu unlauteren kommerziellen oder wettbewerbswidrigen Praktiken – nicht möglich gewesen, den entsprechenden Betreiber für die Nicht-Einhaltung zu sanktionieren (ebd., 22). Infolge der Nicht-Sanktionierung und des sehr niedrigen Strafmaßes im seltenen Falle einer Sanktionierung hätten die Betreiber wiederum keinen ausreichenden Anreiz für die Einhaltung von Sicherheitsvorgaben gehabt, was in manchen Fällen zu einem ineffektiven oder unzureichenden Schutz personenbezogener Daten und der Privatsphäre geführt habe. Daher befürwortete die Kommission die Erweiterung der Befugnisse der Aufsichtsbehörden, Betreiber zur Umsetzung spezifischer, grundlegender Sicherheitsmaßnahmen

verpflichten und sie ggf. auch sanktionieren zu können (ebd.).[215] Erstmals wurde seitens der Kommission im Kontext der Regelungen zum Datenschutz in der EU auch der Vorschlag eingebracht, die Strafhöhe ins Verhältnis zum Umsatz des jeweiligen Betreibers zu setzen und zu erwartende Strafen bei Verstößen im entsprechenden Gesetz bereits zu definieren. Daneben wurde auch erstmals ein Vorschlag eingebracht, der in Richtung eines Sammel- bzw. Verbandsklagerechts ging (ebd., 23).[216]

Mit der Veröffentlichung der Dokumente, in denen die oben skizzierte Strategie der Kommission bekanntgegeben wurde, leitete die Kommission zugleich die zweite Konsultationsphase ein, während der die Stakeholder dazu eingeladen wurden, die vorgenannten Vorschläge der Kommission zu kommentieren (EC 2007a, 4).[217] Die Art. 29-Datenschutzgruppe etwa begrüßte die Initiative der Kommission grundsätzlich, sah allerdings Verbesserungspotenzial in Bezug auf verschiedene Aspekte: Unter Verweis auf die Bedeutungszunahme privater Netzwerke im täglichen Leben und die Vermischung von privaten und öffentlichen Diensten plädierte die Datenschutzgruppe für die Überprüfung und ggf. Ausweitung des Geltungsbereichs der Richtlinie (Artikel 29-Datenschutzgruppe 2006, 3). In Bezug auf die angekündigte Verbesserung der Durchsetzungsmöglichkeiten

215 Die in diesem Zusammenhang für einzelne Unternehmen drohenden Kosten relativierte die Kommission unter Verweis auf den Gesamtnutzen für die Branche (EC 2006a, 34) Zudem machte die zuständige Kommissarin Viviane Reding auch deutlich, dass die Regulierung auch und gerade der Telekommunikationsmonopolisten fortgesetzt werde und steigende Kosten auf Unternehmensseite nicht als Grund für eine Deregulierung akzeptiert würden: „I firmly believe that the response to these challenges must be new and more successful business models, and certainly not protection, by regulators, from competition. I simply do not buy the argument that investment will only happen if we stop regulating monopolies." (Reding 2006a, 8)

216 „As regards the implementation of the e-Privacy Directive, new rules could be established providing for specific remedies (e.g. an explicit right of action against spammers, *possibly on behalf of consumers*)" (EC 2006a, 23, Hervorhebung in kursiv, M. K.).

217 Die zweite Konsultationsphase fand zwischen dem 29. Juni und dem 27. Oktober 2006 statt. Im Oktober 2006 wurde zudem ein öffentlicher Workshop unter Einbezug von Stakeholdern und Interessierten durchgeführt. Insgesamt 224 Antworten aus EU-Mitgliedstaaten und Drittländern gingen bei der Kommission ein (EC 2007c, 4). Auch diese Konsultation wurde von den Stellungnahmen privatwirtschaftlicher Akteure dominiert. Aus den Reihen der im Aushandlungsprozess zur DSGVO relevanten Akteure beteiligten sich: Aea Europe/TechAmerica, ACT, AmCham, BEUC, Bitkom, BSA, BT, ECTA, ETNO, EuroISPA, EPC, Google, GSM/GSMA Europe, Intel, Microsoft, Nokia, Telefónica, UK Information Commissioner's Office (ICO), UNICE/Businesseurope (EC 2007b).

seitens der Datenschutzaufsichtsbehörden verwies die Datenschutzgruppe vor allem auf die uneinheitliche Umsetzung der Richtlinie. Im Ergebnis verfügten einige der mitgliedstaatlichen Aufsichtsbehörden über unzureichende Ermittlungsbefugnisse, die „ihnen zum Beispiel keinen Zugriff auf die Kommunikationsdaten ermöglichen, die zum Nachweis eines Verstoßes gegen die Richtlinie erforderlich sind." (ebd., 4) Im Hinblick auf die mögliche Befugniserweiterung der Aufsichtsbehörden um die Verpflichtung von Diensteanbietern zur Ergreifung spezifischer Sicherheitsmaßnahmen äußerte sich die Datenschutzgruppe skeptisch. So seien die Anbieter bereits unter den geltenden Bestimmungen zur Umsetzung von Sicherheitsmaßnahmen verpflichtet bzw. stelle die Missachtung der Leitlinien der Aufsichtsbehörden längst einen Verstoß gegen die Richtlinie dar. Schließlich sei der Sektor „so beschaffen, dass den Datenschutzbehörden nicht möglich ist, Sicherheitsbestimmungen in Form verbindlicher Anweisungen festzulegen" (ebd., 6), da die Behörden nicht die Kapazitäten innehätten, den gesamten Sektor zu überwachen und Leitlinien zu sektorspezifischen Sicherheitsmaßnahmen zu veröffentlichen. Daher begrüße die Datenschutzgruppe stattdessen die Einführung der Meldepflicht von Sicherheitsverstößen, da dieses ein geeignetes Instrument dafür sei, die Anbieter zur Verabschiedung angemessener Schutzmaßnahmen zu motivieren. Jene Anbieter, die regelmäßig mit Sicherheitsvorfällen Negativschlagzeilen produzierten, würden von den Kundinnen und Kunden eher gemieden und an deren Stelle sichere Dienste eher genutzt. Insofern stelle die Meldepflicht ein *echtes marktgesteuertes Abschreckungsmittel* für diejenigen dar, die Sicherheitsvorschriften umgehen wollen (ebd.). Allerdings bemängelte die Datenschutzgruppe drei Aspekte der Kommissionsüberlegungen: *Erstens* müsse es den Aufsichtsbehörden ermöglicht werden, die Nichtanwendung der Meldepflicht zu sanktionieren. *Zweitens* stellten die vor allem aus den USA gemeldeten Sicherheitsverstöße (hier werden Choicepoint, LexisNexis, Bank of America und Time Warner genannt) kein Problem öffentlicher Internetdiensteanbieter, sondern privater Akteure wie Datenmakler, Banken und anderer Anbieter von Onlinediensten dar. Für eine wirksame Regelung sei es daher erforderlich, dass die Regelung nicht nur für die Betreiber öffentlicher Telekommunikationsdienste, sondern auch für private Diensteanbieter greife. Schließlich, *drittens*, müsse die Kommission in ihrem Legislativvorschlag Regeln für die Einteilung der Verstöße in Schweregrade und abgestufte Informationsverpflichtungen festlegen (ebd.).

3.3.5.1 Kommissionsentwurf

Die Kommission gab an, dass ihre datenschutzpolitischen Vorschläge vor allem seitens der Verbraucherorganisationen unterstützt wurden. Während die Datenschutzbehörden weitergehende Maßnahmen gefordert hätten, seien *einige Netzbetreiber und Dienstleister* vor allem aufgrund möglicher Folgekosten besorgt gewesen. Die Mitgliedstaaten hätten dagegen eine vorsichtige Unterstützung zum Ausdruck gebracht (ebd., 13). Im Ergebnis der Konsultation reduzierte die Kommission ihre datenschutzpolitischen Maßnahmenvorschläge etwas in ihrer Intensität, blieb aber grundsätzlich bei ihrer vorherigen Position, dass das Datenschutz- und Datensicherheitsniveau nicht in erster Linie durch Maßnahmen seitens des Individuums, sondern durch legislative und betreiberseitige Maßnahmen angehoben werden sollte. So sah der aktualisierte Maßnahmenkatalog auch weiterhin „mehr Verantwortung der Betreiber und NRB [nationalen Regulierungsbehörden, M. K.] für die Sicherheit und Integrität aller elektronischen Kommunikationsnetze und -dienste" (EC 2007a, 14) vor. Zwar wurde die angekündigte Erweiterung der Sanktionsbefugnisse der zuständigen Aufsichtsbehörden (und damit auch die Idee der Setzung der Strafhöhe ins Verhältnis zum Umsatz des Betreibers) gestrichen, doch wurden immer noch „größere Umsetzungs- und Durchsetzungsbefugnisse der zuständigen Behörden, insbesondere im Kampf gegen ‚Spam'" (ebd.) angekündigt. Schließlich bildete den Kern der datenschutzpolitischen Kommissionsvorschläge die Einführung einer Meldepflicht, wonach die Betreiber im Falle einer Schutzverletzung personenbezogener Daten infolge eines Verstoßes gegen die Netzsicherheit die Nutzer(-innen) über den Vorfall informieren sollten (ebd.). Gestrichen wurde jedoch die Pflicht zur Benachrichtigung der zuständigen Aufsichtsbehörde bzw. der Öffentlichkeit durch die Aufsichtsbehörde. Ihre Maßnahmenvorschläge begründete die Kommission damit, Verbraucherinteressen in der EU zu wahren: „Dazu ist unter anderem ein umfassender Schutz der personenbezogenen Daten und der Privatsphäre sicherzustellen und die Integrität und Sicherheit der öffentlichen Kommunikationsnetze zu gewährleisten. Angesichts der wachsenden Zahl elektronischer Bedrohungen in den letzten Jahren, etwa durch Viren, unerbetene Werbung (‚*Spam*'), Spähsoftware (‚*Spyware*') und das Ausspionieren persönlicher Zugangsdaten (‚*Phishing*'), sind diese Ziele heute wichtiger denn je." (ebd., 13, Hervorhebungen im Original)

Zeitgleich mit der Bekanntgabe der Konsultationsergebnisse veröffentlichte die Kommission am 13. November 2007 auch ihren Richtlinienvorschlag,[218] der unter anderem die Änderung der ePrivacy-Richtlinie 2002/58/EG vorsah (EC 2007c). Darin wurden die folgenden fünf zentralen Änderungen an der ePrivacy-Richtlinie vorgeschlagen (ebd., 6):

(1) Im Rahmen der Änderung von Art. 3 Abs. 1 wurde intendiert, dass öffentliche Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte (z. B. kontaktlos arbeitende RFID-Geräte) unterstützen, ebenfalls in den Anwendungsbereich der Richtlinie fallen.

(2) *Die Einführung einer Meldepflicht für Sicherheitsverletzungen, die zum Verlust oder zur Preisgabe personenbezogener Daten der Nutzer führen.* In Art. 4 Abs. 3 wurde vorgeschlagen, dass der *Teilnehmer* und die nationale Regulierungsbehörde unverzüglich benachrichtigt werden und dass die Benachrichtigung des Teilnehmers *zumindest eine Darlegung der Art der Verletzung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten* müssten. In der Meldung an die zuständige Aufsichtsinstanz sollte der Betreiber *zusätzlich die Folgen der Verletzung und die vom Betreiber nach der Verletzung ergriffenen Maßnahmen* darlegen. die Festlegung der Details *in Bezug auf die Umstände, Form und Verfahren der in diesem Artikel vorgeschriebenen Informationen und Benachrichtigungen* sollte dagegen nicht in der Richtlinie selbst, sondern auf Basis eines Ausschussverfahrens nach Konsultation der sog. Europäischen Behörde für die Märkte der elektronischen Kommunikation und des EDSB mittels technischer Durchführungsmaßnahmen erfolgen.

(3) Mit der Änderung von Art. 5 Abs. 3 wurden die Bedingungen festgelegt, die gölten, wenn ein Zugriff auf Informationen oder die Speicherung von Informationen im Endgerät des Nutzers (u. a. mittels Cookies) erfolgt. Demnach sollten die Nutzer gemäß der DS-RL klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhalten und die Möglichkeit haben, einer derartigen Verarbeitung umstandslos widersprechen zu können.

218 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

(4) Mit der Ergänzung von Art. 13 um den Abs. 6 wurde insbesondere Internet-Diensteanbietern die Möglichkeit eingeräumt, gegen Spam-Versender wegen Missbrauchs ihrer Netze oder gegen Stellen, die Sender-Adressen fälschten oder Server hackten, um sie als Spam-Relays zu missbrauchen, rechtlich vorzugehen.
(5) Während die ePrivacy-Richtlinie 2002/58/EG selbst keine ausdrücklichen Bestimmungen zur Durchsetzung enthielt, sondern stattdessen lediglich auf den Abschnitt zur Durchsetzung in der DS-RL verwies, wurde mit der Hinzufügung von Art. 15a die ausdrückliche Regelung der Materie im Rahmen der ePrivacy-Richtlinie vorgeschlagen.

3.3.5.2 Stellungnahmen des EDSB und der Art. 29-Datenschutzgruppe

Der Europäische Datenschutzbeauftragte veröffentlichte seine Stellungnahme am 10. April 2008 (EDSB 2008) und die Art. 29-Datenschutzgruppe ihre Stellungnahme am 15. Mai 2008 (Artikel 29-Datenschutzgruppe 2008). Beide Institutionen begrüßten den Kommissionvorschlag zur Änderung der ePrivacy-Richtlinie grundsätzlich: Besonders die mit der Änderung von Art. 3 vorgeschlagene Ausweitung des Anwendungsbereichs auf RFID, die Cookie-/Spyware-Regelungen mit der Änderung von Art. 5 Abs. 3 sowie die im Rahmen von Art. 15a vorgeschlagenen Änderungen im Hinblick auf die Verbesserung der Durchsetzung (Artikel 29-Datenschutzgruppe 2008; EDSB 2008, 13). Zudem begrüßten beide Institutionen die von der Kommission vorgeschlagene Klärung der Details bzgl. der Umstände, der Form und Verfahren der Meldung von Verletzungen des Schutzes personenbezogener Daten im Rahmen des Ausschussverfahrens (Artikel 29-Datenschutzgruppe 2008, 4; EDSB 2008, 13). Die Art. 29-Datenschutzgruppe kritisierte lediglich, dass sie nicht unter den zu konsultierenden Akteuren aufgelistet worden war und hob die Notwendigkeit ihres Einbezugs hervor (Artikel 29-Datenschutzgruppe 2008, 4). Trotz der Begrüßung der Einführung der Meldepflicht bei Datenschutzverletzungen bemängelten beide Institutionen, dass die vorgesehenen Regelungen ausschließlich für die Anbieter öffentlicher elektronischer Kommunikationsdienste gelten würden, nicht aber für die Anbieter von Diensten der Informationsgesellschaft (wie Online-Banken, Daten-Broker, Online-Unternehmen, Online-Anbieter von Gesundheitsdiensten usw.). Entsprechend vertraten beide Institutionen die Position, dass Art. 4 Abs. 3 dahingehend abzuändern sei, dass die Meldepflicht auch bei Diensten der Informationsgesellschaft greife

(Artikel 29-Datenschutzgruppe 2008, 3; EDSB 2008, 12).[219] In ähnlicher Weise begrüßte der EDSB zwar die Ergänzung der ePrivacy-Richtlinie um das in Art. 13 Abs. 6 vorgeschlagene Recht, das juristische Personen, und damit vor allem die Anbieter elektronischer Kommunikationsdienste, aber auch Verbraucherverbände und Gewerkschaften, die die Interessen Spam-geschädigter Verbraucher verträten, in die Lage versetzen würde, gerichtlich gegen Spam-Versender vorzugehen. Doch wurde das Fehlen der Möglichkeit von Sammelklagen kritisiert, mittels derer eine Gruppe von von Spam betroffener Nutzerinnen und Nutzer gemeinsam gegen den Spam-Versender hätten vorgehen können. Schließlich begrüßten beide Institutionen die Ausweitung des Anwendungsbereichs auf RFID-fähige Geräte, doch bedauerten sie zugleich, dass der Kommissionsvorschlag die Problematik der sich in zunehmendem Maße verwischenden Unterscheidung zwischen privaten und öffentlichen Netzen unberücksichtigt ließ. Aufgrund der wachsenden Bedeutung gemischter (privater/öffentlicher) und privater Netze im täglichen Leben und aufgrund des dabei entstehenden Risikos für personenbezogene Daten forderten die Institutionen die Ausweitung des Anwendungsbereichs der ePrivacy-Richtlinie auch auf jene Anbieter. Bemängelt wurde seitens sowohl des EDSB als auch der Datenschutzgruppe zudem, dass sich das in Art. 13 vorgesehene Verbandsklagerecht lediglich auf Situationen beschränkte, in denen die in Art. 13 festgelegten Bestimmungen hinsichtlich unerbetener E-Mails verletzt würden, Verstöße gegen andere Bestimmungen der ePrivacy-Richtlinie jedoch unberücksichtigt blieben (Artikel 29-Datenschutzgruppe 2008, 6; EDSB 2008, 10 f.). Darüber hinaus betonte die Datenschutzgruppe im Hinblick auf ihre Befürwortung eines standardmäßig hohen Datenschutzniveaus die Bedeutung des Prinzips der Datensparsamkeit und des Einsatzes datenschutzfreundlicher Technologien und forderte die Festlegung dieser Prinzipien in Art. 1 der Richtlinie (Artikel 29-Datenschutzgruppe 2008, 6). Schließlich vertrat die Datenschutzgruppe unter Bezugnahme auf eine ihrer Stellungnahmen (Artikel 29-Datenschutzgruppe 2007) die Position, dass IP-Adressen im Zweifel als personenbezogene Daten zu behandeln seien (ebd., 6 f.).

219 Unterstützt wurde der Vorschlag auch seitens Privacy International (PI 2011, 6).

3.3.5.3 Position des Europäischen Parlaments

Das Europäische Parlament entschied über das Verfahren zur Erarbeitung der Parlamentsposition Ende 2007. Zum federführenden Ausschuss wurde der Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO-Ausschuss) unter Berichterstatter Malcolm Harbour (Vereinigtes Königreich, Conservative Party/EVP bzw. EKR)[220] benannt.[221] Für die Datenschutzaspekte des Richtlinienvorschlags war der LIBE-Ausschuss (seit dem 13. März 2008 auch als assoziierter Ausschuss) zuständig. Die Aufgabe des Berichterstatters übernahm erneut Alvaro. Überdies waren am Verfahren die Ausschüsse ECON, ITRE, CULT und JURI mitberatend tätig (Harbour und Alvaro 2008, 251). Der LIBE-Ausschuss nahm seine Stellungnahme am 26. Juni 2008 an und der Entwurf der Parlamentsstellungnahme wurde schließlich am 18. Juli 2008 angenommen (ebd.). Der Harbour-Bericht fand im Europäischen Parlament eine breite Mehrheit. Nachdem einige der Änderungswünsche der Sozialdemokraten (vgl. hierzu die Plenardebatte in: EP 2008b, 67 ff.) berücksichtigt worden waren und diese dem Bericht zugestimmt hatten, wurde der geänderte Berichtsvorschlag am 24. September 2008 mit den Stimmen der Fraktionen ALDE, EVP-DE, SPE und UEN, die praktisch geschlossen für den Bericht stimmten, mit 561 Für-Stimmen angenommen. Die 99 Gegenstimmen setzten sich vor allem aus den Stimmen der GUE/NGL, der Grünen/EFA und IND/DEM sowie einiger fraktionsloser Europaabgeordneter zusammen, während sich die 13 Enthaltungen auf verschiedene Fraktionen verteilten (EP 2008a, 123 f.). Die Grüne Fraktion bemängelte insbesondere einige der die Richtlinie 2002/22/EG betreffenden Vorschläge (etwa hinsichtlich urheberrechtspolitischer Änderungen, die mit einer Filterung des Internets einhergehen sollten) des Berichterstatters Harbour (vgl. z. B. die Äußerungen Staes' in: EP 2008d). Im Hinblick auf den Alvaro-Bericht kritisierten die Grünen (z. B. Rebecca Harms) den Nicht-Einbezug von IP-Adressen. Die GUE/NGL teilte die Kritik an den urheberrechtspolitischen Maßnahmen, kritisierte aber darüber hinaus auch

220 Harbour war bereits beim ursprünglichen Universaldienste-Richtlinienvorschlag 2001 Berichterstatter (Harbour und Alvaro 2008, 114). Bis zur Europawahl 2009 gehörte Harbour der EVP an, schloss sich nach der Wahl jedoch der neu gegründeten nationalkonservativen bzw. EU-skeptischen Fraktion EKR an (EP 2020d).

221 Der größere Teil der Änderungen betraf die Richtlinie über den Universaldienst und die Nutzerrechte. Die ePrivacy-Richtlinie war dagegen von einer vergleichsweise kleinen Zahl von Änderungen betroffen. Daher wurde der für Verbraucherschutzfragen zuständige IMCO-Ausschuss mit der Hauptverantwortung der Berichterstellung betreut (Harbour und Alvaro 2008, 114 f.).

die aus ihrer Perspektive generelle Fokussierung der Parlamentsposition auf die Wünsche der Wirtschaft (vgl. die Äußerungen Svenssons und de Brúns in: EP 2008a, 84 und 98; vgl. auch die Äußerungen Droutsas' in: 2008d).

3.3.5.3.1 Inhalt der Parlamentsposition

Folgende Änderungsvorschläge finden sich in der verabschiedeten Parlamentsposition: So sollten beispielsweise jüngste Entwicklungen im Verfassungsrecht der Mitgliedstaaten – durch einen Verweis auf das *Recht auf Vertraulichkeit und Sicherheit der Systeme der Informationstechnologie* gemäß der Änderungsanträge 1 und 16 – berücksichtigt werden. Das Parlament befürwortete zudem die Ergänzung des EG 34 um eine Passage hinsichtlich der Ermutigung der Endnutzer zu Selbstdatenschutzmaßnahmen (ebd., 229 f., Änderungsantrag 37).

Unter Bezugnahme auf die Stellungnahmen der Art. 29-Datenschutzgruppe und des EDSB trat das Parlament zudem für die Ausweitung des Anwendungsbereichs der ePrivacy-Richtlinie auf private Kommunikationsnetze sowie auf öffentlich zugängliche private Netze ein (vgl. Änderungsantrag 18). In diesem Zusammenhang forderte das Parlament auch die Ausweitung der Klagemöglichkeiten juristischer Personen, nicht nur bei Verstößen gegen Art. 13, also im Falle unerbetener Nachrichten, sondern bei jeglichen Verstößen gegen die Bestimmungen der ePrivacy-Richtlinie gerichtlich vorgehen zu können. Nicht übernommen wurde jedoch die Forderung der Datenschutzgruppe nach Einführung eines Sammelklagerechts (vgl. Änderungsantrag 31). Im Hinblick auf die Meldepflicht bei Datenschutzverletzungen folgte das Parlament ebenfalls der Position der Datenschützer und forderte die Ausweitung des Umfangs der Verpflichtung auf Dienste der Informationsgesellschaft (vgl. Änderungsantrag 20). Dagegen rückte das Parlament von der Spezifizierung der Details bzgl. der Umstände, der Form und Verfahren der Meldung im Rahmen des Ausschussverfahrens, die von der Kommission vorgeschlagen worden war, ab und trat für eine unmittelbare Spezifizierung der entsprechenden Punkte in der Richtlinie ein. Im Gegensatz zur Kommission plädierte das Parlament dabei für eine Zwei-Stufen-Meldepflicht: Damit es nicht zu einer Überforderung der Nutzerinnen und Nutzer aufgrund zu häufiger Meldungen komme, sollte die Meldung nicht mehr zeitgleich an die zuständige Aufsichtsbehörde und die Betroffenen erfolgen. Stattdessen sollte eine Verletzung zunächst unverzüglich an die zuständige Aufsichtsbehörde gemeldet

werden, die daraufhin auf Grundlage der Ernsthaftigkeit der entstandenen Verletzung die Notwendigkeit der Benachrichtigung der Betroffenen prüfen und den Verantwortlichen zu einer Meldung auffordern können sollte (vgl. Änderungsantrag 21). Gemäß des Änderungsantrags 22 sollte der Ernst einer Verletzung, die eine Benachrichtigung erforderlich mache, nach „den Umständen der Verletzung bestimmt [werden], z. B. dem Risiko für die von der Verletzung betroffenen personenbezogenen Daten, der Art der von der Verletzung betroffenen Daten, der Zahl der betroffenen Teilnehmer und der unmittelbaren oder potenziellen Auswirkungen der Verletzung auf die Bereitstellung der Dienste." (ebd., 238) Schließlich sah der Änderungsantrag 23 die Befreiung von der Benachrichtigungspflicht der Betroffenen vor, sofern der Verantwortliche nachweisen könne, „dass aufgrund der Anwendung geeigneter technologischer Schutzmaßnahmen nach vernünftigem Ermessen kein Risiko für die von der Verletzung betroffenen personenbezogenen Daten besteht." (ebd.) Nachdem das Parlament im Rahmen der Verhandlungen der ePrivacy-Richtlinie noch keine Einigung bezüglich der Einwilligung im Kontext von Cookies hatte erzielen können und am Ende lediglich ein Kompromiss, der die Entscheidung den Mitgliedstaaten überließ, verabschiedet worden war (vgl. 3.3.2), einigten sich die Fraktionen im Rahmen der Richtliniennovelle darauf, dass die vorherige Einwilligung der Betroffenen verpflichtend sein sollte, doch wurde zugleich vorgesehen, dass bereits eine entsprechende Browser-Einstellung eine solche vorherige Einwilligung darstellen können sollte (vgl. Änderungsantrag 25).

3.3.5.3.2 Geänderter Vorschlag der Kommission

Nachdem das Parlament seine Position verabschiedet hatte, veröffentlichte die Kommission am 6. November 2008 einen geänderten Richtlinienvorschlag (EC 2008), in dessen Rahmen einige der Änderungen des Parlaments akzeptiert, dessen zentralen Forderungen jedoch abgelehnt wurden. So folgte die Kommission weder dem Wunsch des Parlaments und der Datenschutzbehörden, nach der Ausweitung des Anwendungsbereichs der Richtlinie auf private Kommunikationsnetze sowie auf öffentlich zugängliche private Netze noch dem Wunsch nach der Ausweitung der Meldepflicht bei Datenschutzverstößen auf Dienste der Informationsgesellschaft. In ähnlicher Weise wurde auch die vom Parlament geforderte Ausweitung der Klagemöglichkeiten juristischer Personen, wonach das Verbandsklagerecht nicht nur bei Verstößen gegen Art. 13, sondern bei jeglichen Verstößen

gegen die Bestimmungen der ePrivacy-Richtlinie greifen können sollte, abgelehnt (ebd., 29).

Die vom Parlament vorgeschlagene Spezifizierung der Umstände, der Form und Verfahren der Meldung sowie das vorgeschlagene Zwei-Stufen-Modell wurden dagegen in modifizierter Form übernommen. So sollte die unverzügliche Meldung an die Behörde in jedem Fall (siehe Abänderung 187rev und 184) sowie die unverzügliche Meldung an die Betroffenen grundsätzlich immer erfolgen, sofern die zuständige Aufsichtsbehörde keine Ausnahme genehmige. Eine Verletzung des Schutzes personenbezogener Daten sollte gemäß der Kommissionsposition immer dann vorliegen, sobald es zu einer „unbeabsichtigten oder unrechtmäßigen Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von oder zum Zugang zu personenbezogenen Daten" (vgl. neuen Art. 2 lit. i) komme. Die vom Parlament vorgeschlagene (Änderungsvorschlag 125) Spezifizierung der Ernsthaftigkeit einer Verletzung, die eine Benachrichtigung erforderlich mache, wurde dagegen nicht übernommen. Nach der Kommission sollte diese Spezifizierung im Ermessen der Aufsichtsbehörden liegen (ebd., 25 f., 3a. und 3b.).

Ein weiterer Vorschlag der abgelehnt wurde, war Änderungsvorschlag 128, wonach eine Browsereinstellung als Einwilligung gelten können sollte. Die vom Parlament eingebrachten Verweise auf das *Recht auf Vertraulichkeit und Sicherheit der Systeme der Informationstechnologie* wurden ebenfalls ersatzlos gestrichen (ebd., 9 und 29).

Mit kleineren Änderung angenommen wurde der Änderungsantrag 37, wonach die Endnutzer mittels öffentlicher Aufklärungskampagnen zu Selbstdatenschutzmaßnahmen ermutigt werden sollten (ebd., 9 f.).

3.3.5.4 Gemeinsamer Standpunkt des Ministerrats

Der Ministerrat setzte sich erstmals im Rahmen des Ratstreffens „Verkehr, Telekommunikation und Energie" Ende November bzw. Anfang Dezember 2007 mit dem Richtlinienvorschlag der Kommission auseinander, behandelte jedoch zunächst lediglich die nicht den Datenschutz betreffenden Elemente des Telekom-Reformpakets (Council of Ministers 2007, 9 f.). Auf der Arbeitsebene lag die Zuständigkeit für die Erarbeitung des Gemeinsamen Standpunkts des Ministerrats bei der Ratsarbeitsgruppe „Telekommunikation und Informationsgesellschaft" (Gruppe „Telekommunikation und Informationsgesellschaft" 2008). Mitte 2008 kristallisierte sich schließlich allmählich die finale Position des Rats heraus. So wurden die von der

Kommission mit der Reform verfolgten politischen Ziele hinsichtlich der Stärkung der Rechte der Verbraucher und des Schutzes personenbezogener Daten zwar begrüßt, im Hinblick auf die von der Kommission vorgebrachten konkreten Änderungsvorschläge verwies der Ministerrat jedoch auf die Notwendigkeit „to maintain an appropriate balance of proportionality and subsidiarity, as well as to avoid unnecessary burdens for both national regulatory authorities and the undertakings concerned while ensuring competition and benefits for end-users." (Council 2008, 8) Der Rat gab an, dass in Bezug auf die ePrivacy-Richtlinie zu diesem Stadium Fragen betreffend die Sicherheit der Verarbeitung und Fragen bezüglich der Umsetzung und Durchsetzung ungeklärt seien (ebd.). Die zuständigen Minister konnten schließlich zunächst Ende November 2008 eine politische Einigung im Rat erzielen (EU-Ministerrat 2008b, 9) und verabschiedeten den Gemeinsamen Standpunkt des Ministerrats schließlich am 16. Februar 2009 (EU-Ministerrat 2009b).

Die von Kommission, Parlament sowie den Datenschutz-Institutionen befürwortete Klarstellung, dass der Anwendungsbereich neue Technologien wie RFID umfasse, wurde auch vom Ministerrat übernommen (ebd., 19, EG 44). Nicht übernommen wurde dagegen die von den Datenschutz-Institutionen und dem Parlament geforderte Ausweitung des Anwendungsbereichs der Richtlinie auf private Kommunikationsnetze und auf öffentlich zugängliche private Netze. Ebenso wurde auch die Ausweitung des Umfangs der Verpflichtung zur Meldung von Datenschutzverletzungen auf Dienste der Informationsgesellschaft vom Ministerrat nicht übernommen. Zudem machte der Ministerrat Änderungsvorschläge, die zu einer deutlichen Schwächung der Verpflichtung geführt hätten. So sollte eine Meldung an die *Teilnehmer*[222] nur im Falle einer ernsthaften Bedrohung der Privatsphäre erfolgen müssen. Zu einer solchen ernsthaften Bedrohung zählte der

222 Dem ursprünglichen Kommissionsvorschlag gemäß, sollten lediglich die *Teilnehmer* eines Dienstes im Falle einer Datenschutzverletzung benachrichtigt werden. Nachdem die Art. 29-Datenschutzgruppe darauf hingewiesen hatte, dass der Begriff des Teilnehmers in einigen Fällen, in denen es sich bei dem Betroffenen formal nicht um einen Teilnehmer handele, zu einer Nicht-Benachrichtigung führen könnte (Artikel 29-Datenschutzgruppe 2008, 3), änderten das Parlament und die Kommission die entsprechenden Textstellen (vgl. Änderungsantrag 123, in: Harbour und Alvaro 2008, 92; vgl. Abänderung 187rev und 184, in: EC 2008, 25). Lediglich der Ministerrat blieb beim Begriff des Teilnehmers, äußerte sich gleichzeitig im Rahmen seiner Begründung aber ansonsten nicht zu dieser Entscheidung (EU-Ministerrat 2009a) und nahm somit die daraus resultierende Schutzlücke in Kauf (EU-Ministerrat 2009b, 55).

Ministerrat u. a. Identitätsdiebstahl oder -betrug, physische Schädigung, erhebliche Demütigung oder Rufschaden (ebd., 21, EG 47). Zudem sollte entgegen der von allen anderen beteiligten Akteuren vertretenen Position nicht die für einen Dienstleister zuständige Aufsichtsbehörde darüber entscheiden, ob eine Mitteilung an die Teilnehmer erfolgen solle oder nicht, sondern der Dienstleister selbst. Dadurch, dass dem Dienstleister auch die Entscheidung über die Benachrichtigung der zuständigen Aufsichtsbehörde überlassen bleiben sollte, wäre die Meldepflicht schließlich jeglicher Kontrollmöglichkeit beraubt worden, sodass ein Verantwortlicher selbst ernsthafte Sicherheitsverletzungen hätte verschweigen können (ebd.).[223] Auch die von den Datenschutz-Institutionen und dem Parlament befürwortete Ausweitung der von der Kommission in Art. 13 Abs. 6 vorgeschlagenen Verbandsklage auf alle Verstöße gegen die ePrivacy-Richtlinie – sowie die besonders vom EDSB geforderte Einführung eines Sammelklagerechts – wurde vom Ministerrat überhaupt nicht aufgegriffen (ebd., 61). Im Hinblick auf den Umgang mit Cookies folgte der Rat der Kommission und sah neben der verpflichtenden Information der Nutzerinnen und Nutzer seitens des Verantwortlichen u. a. über die Zwecke der Verarbeitung auch die Einholung der Einwilligung des Nutzers für die Platzierung bspw. eines Cookies vor (ebd., 57).

Wesentlich weitreichender als die datenschutzrechtlichen Meinungsunterschiede waren jedoch die Unterschiede in den Positionen der Organe im Hinblick auf die übrigen, den Verordnungsvorschlag zur Einrichtung eines Regulierungsgremiums und den Richtlinienvorschlag zur besseren Rechtsetzung betreffenden, Elemente des Telekom-Reformpakets, auf die an dieser Stelle aber nicht weiter eingegangen werden soll (Bundesnetzagentur 2009, 56 ff. EC 2009b, 3 f.).[224]

223 Der Erwägungsgrund 47 sah zudem vor, dass der Dienstleister nicht verpflichtet sein sollte, den Teilnehmer zu benachrichtigen, sofern er der zuständigen Aufsichtsbehörde glaubhaft machen konnte, „dass er geeignete technische Schutzmaßnahmen für die betroffenen Daten ergriffen hat und diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewandt wurden. Diese technischen Schutzmaßnahmen sollten die Daten für alle unbefugten Personen verschlüsseln." (EU-Ministerrat 2009b, 21)

224 Erwähnt sei lediglich die Diskussion zu urheberrechtspolitischen Fragen im Kontext der sehr kontrovers geführten europäischen Debatte zum Thema der Internetsperren. Die Debatte wurde vor allem von der konservativen französischen Regierung unter Nicolas Sarkozy vorangetrieben, die im Inland über das HADOPI-Gesetz beriet, mittels dessen eine sog. *three-strikes*-Regelung eingeführt werden sollte. So sollte nach zwei Verwarnungen infolge von Urheberrechtsverstößen ohne weitere

3.3.5.5 Einigung im Trilog und Verabschiedung des Kompromisstextes

Wie in derartigen Fällen üblich, vereinbarten Kommission, Parlament und Rat den Beginn informeller Trilog-Verhandlungen, um noch vor der zweiten Lesung des Parlaments und des Rates einen Kompromiss zu erzielen. Der Trilog wurde unverzüglich nach der am 16. Februar erfolgten Annahme des Gemeinsamen Standpunkts des Ministerrats einberufen und tagte bis Ende April (Council Presidency 2009). Den schwierigsten Teil der Verhandlungen bildete die Frage nach der Meldepflicht bei Datenschutzverstößen. Das Parlament blieb hartnäckig bei seiner Forderung nach dem Einbezug von Diensten der Informationsgesellschaft, der Rat und die Kommission vertraten dagegen die Position, dass der Anwendungsbereich der sektorspezifischen ePrivacy-RL klar auf den Bereich der elektronischen Kommunikation begrenzt bleiben sollte. Kommission und Ministerrat verwiesen das Parlament im Zusammenhang mit der Ausweitung des Anwendungsbereichs auf die mögliche Revision der DS-RL 95/46/EG (Council 2009, 4). Somit wurden letztlich alle vom Parlament und den Datenschutz-Institutionen befürworteten Elemente im Hinblick auf die Ausweitung des Anwendungsbereichs der Richtlinie verworfen: Dies betraf zunächst die Definition des Anwendungsbereichs in Art. 3, darüber hinaus die Meldepflicht bei Datenschutzverstößen in Art. 4 sowie die vorgeschlagene Ausweitung des Verbandsklagerechts aus Art. 13 auf alle Artikel der Richtlinie.

Bei den übrigen umstrittenen Elementen der Meldepflicht konnte allerdings ein Kompromiss erzielt werden: Die vom Rat gewünschte Ermächtigung der Verantwortlichen, selbst über eine Benachrichtigung zu entscheiden, wurde gestrichen. Stattdessen wurde den Positionen der Kommission und des Parlaments entsprechend gemäß Art. 4 Abs. 3 festgelegt, dass im Falle einer Verletzung die zuständige Aufsichtsbehörde unverzüglich zu benachrichtigen sei. Die Kommission und das Parlament konnten sich zudem auch in Bezug auf die Anforderung, wer zu benachrichtigen sei, durchsetzen. So sollten nicht nur – wie vom Rat gefordert – Teilnehmer, sondern *Teilnehmer* und *Personen* unverzüglich benachrichtigt werden, sofern anzunehmen sei, dass durch eine Schutzverletzung deren personenbezogenen Daten oder Privatsphäre beeinträchtigt würden. Dem Vorschlag des Rates entsprechend wurde zudem festgelegt, dass die Pflicht zur Benachrichtigung entfallen sollte, sofern der Verantwortliche „zur Zufriedenheit

richterliche Überprüfung der Internetzugang von Beschuldigten gesperrt werden können (Filippi und Bourcier 2016).

der zuständigen Behörde nachgewiesen hat, dass er geeignete technische Schutzmaßnahmen getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden." (ebd.)[225]

Im Hinblick auf den in Art. 5 geregelten Umgang mit Cookies wurde lediglich die Opt-in-Pflicht vereinbart und der vom Parlament befürwortete Verweis auf Browser-Einstellungen gestrichen. In der Öffentlichkeit führte diese Verpflichtung zum Opt-in noch kurz vor der Verabschiedung der Richtlinie zu einigen Pressemeldungen, in denen aufgrund der Cookie-Regelung eine unnötige Verkomplizierung der Internetnutzung befürchtet wurde. Auf Spiegel Online war beispielsweise zu lesen, dass die Einwilligungspflicht zu *endlosen Pop-up-Kaskaden* führen werde (Patalong 2009). Insbesondere Akteure aus der Wirtschaft, darunter ein Zusammenschluss verschiedener auf EU-Ebene tätiger Lobbyverbände[226], warnten vor den wirtschaftlichen Folgen aufgrund der zu befürchtenden negativen Auswirkungen auf das Benutzererlebnis (EPC 2009). In der Folge wichen mehrere Mitgliedstaaten von der Verpflichtung zum Opt-in ab und setzen die Vorgabe praktisch als eine Opt-out-Lösung um (A. Schneider 2014).

Schließlich wurden die im politischen Aushandlungsprozess weitgehend unumstrittenen Elemente hinsichtlich der Klarstellung, dass neue Technologien wie RFID in den Anwendungsbereich der Richtlinie fallen sollten, (EG 56) und die Aktualisierung der Vorgaben zur Umsetzung und Durchsetzung (Art. 15) ebenfalls verabschiedet.

In der Folge nahm das Parlament den Kompromisstext am 6. Mai 2009 in zweiter Lesung bei 493 zu 130 Stimmen und 6 Enthaltungen an. Die Fraktionsfronten blieben dieselben, wie sie es bereits bei der ersten Lesung waren: Auf der Seite der Befürworter fanden sich ALDE, EVP-DE, SPE sowie UEN. Auf der Gegenseite fanden sich GUE/NGL, Grüne/EFA und IND/DEM sowie mehrere fraktionslose Abgeordnete und einige Abweichler aus den Reihen der EVP-DE und der SPE (EP 2009c, 9, Nr. 14; epic.org 2009, 65 f.). Nachdem auch der Rat den Kompromisstext am 26. Oktober 2009 angenommen hatte, wurde die *Richtlinie 2009/136/EG zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und*

225 Wobei diese Regelung freilich etwas paradox ist. Wenn der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsnetzes eine Schutzverletzung sowohl der zuständigen Aufsichtsbehörde als auch den Betroffenen unverzüglich mitzuteilen hat, bleibt dem Betreiber eigentlich keine Zeit, die Aufsichtsbehörde hinsichtlich der Nicht-Benachrichtigung zu konsultieren. So müsste der Betreiber in Kauf nehmen, seine Meldepflicht gegenüber dem Betroffenen ggf. nicht zu erfüllen.

226 Beteiligt waren u. a. ENPA, EPC, FEDMA, WFA, IAB und EuroISPA (EPC 2009).

Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, die aufgrund der enthaltenen Cookie-Regelung auch den Beinamen *Cookie-Richtlinie* erhalten sollte, am 25. November 2009 von den Präsidenten des Europäischen Parlaments und des Ministerrats unterzeichnet und damit erfolgreich verabschiedet (EU 2009).

3.3.5.6 Zwischenfazit

Die Verhandlungen zur Cookie-Richtlinie stellten die letzte politische Auseinandersetzung vor Beginn der Datenschutzreform dar. Während bei der Aushandlung der DS-RL noch die Frage im Raum gestanden hatte, ob gemeinschaftsweite Datenschutzregelungen überhaupt erforderlich sind, war diese Frage im Rahmen der Aushandlung der ePrivacy-RL zugunsten von inhaltlichen Punkten etwas in den Hintergrund gerückt. Im Kontext der ePrivacy-RL-Novelle erreichte die datenschutzpolitische Debatte nunmehr eine neue Qualität: Die verantwortliche Kommissarin Viviane Reding agierte auf Basis ihrer Policy-Kernüberzeugung, dass Datenschutz zu mehr Vertrauen in digitale Dienste und dadurch zu gesteigertem wirtschaftlichen Erfolg führe, als Policy-Entrepreneurin und forcierte die Anhebung des Datenschutzniveaus im Bereich der elektronischen Kommunikation vor allem durch die Stärkung der Verarbeiterpflichten und die Entlastung der Betroffenen. Kernelemente dieser Politik waren die Einführung der Meldepflicht bei Datenschutzverstößen sowie die Einführung des Verbandsklagerechts. Mit der Einführung der Opt-in-Pflicht wurde zudem angestrebt, die informationelle Selbstbestimmung der Betroffenen im Zusammenhang mit Cookies besser zu gewährleisten.

Weitergehende Forderungen, vor allem des Europäischen Parlaments, hinsichtlich der Ausweitung des Anwendungsbereichs der Cookie-Richtlinie (und damit der Meldepflicht bei Datenschutzverstößen sowie des Verbandsklagerechts) auf alle Dienste der Informationsgesellschaft konnten sich zwar nicht durchsetzen. Die Vertröstung des Parlaments unter Verweis auf die mögliche anstehende Revision der DS-RL verdeutlichte jedoch, dass eine Reform des Datenschutzrahmens in greifbare Nähe gerückt war.

3.3.6 Fazit

Der vorangegangene Abschnitt 3.3 zur EU-Datenschutzpolitik seit der Jahrtausendwende hat die relevantesten datenschutzpolitischen Auseinandersetzungen in Gestalt der ePrivacy-RL, des ersten Berichts zur Überprüfung der DS-RL, der Bestimmungen im Sicherheitsbereich (darunter die EU-Richtlinie zur Vorratsdatenspeicherung, der Zugriff auf Fluggastdaten sowie die Erarbeitung des JI-Rahmenbeschlusses) sowie der Cookie-RL untersucht. Die der Untersuchung zugrundeliegende Zielsetzung war die Identifikation der langfristig relevanten Kontextbedingungen der EU-Datenschutzpolitik.

So hat die Untersuchung der Verabschiedung der ersten internationalen Datenschutz-Instrumente in Abschnitt 3.1 und insb. die Entstehung der DS-RL in Abschnitt 3.2 zuvor gezeigt, dass die Entstehung der ersten Datenschutz-Bestimmungen zunächst vor allem im Spannungsfeld zwischen Grundrechtsschutz und der wirtschaftlichen Bedeutung der Datenverarbeitung im Zusammenhang mit der Ermöglichung gemeinschaftsweiter grenzüberschreitender Datentransfers eingebettet war. Die aus dieser Spannung resultierende Kontroverse hatte jedoch schließlich zu einem Stillstand während der Verhandlungen zur DS-RL geführt. Die Überwindung der Pattsituation war letztlich vor allem dadurch möglich, dass die Gegner der Einführung von Datenschutzregelungen mittels des Arguments, dass Datenschutz als vertrauensbildende Maßnahme fungieren und zu mehr wirtschaftlichem Erfolg beitragen würde, überzeugt werden konnten. Diese Überzeugung sollte seit Mitte der 1990er-Jahre als Bindeglied zwischen Datenschutzbefürwortern und Datenschutzgegnern fungieren und zu einer relativen De-Radikalisierung der jeweiligen Standpunkte beitragen.

So gaben die Gegner von Datenschutzregelungen ihre prinzipielle Ablehnung größtenteils auf und arrangierten sich mit der Einführung von Datenschutz-Gesetzen.[227] Die Datenschutzbefürworter hingegen rückten teilweise von ihrer stark grundrechtsorientierten Haltung ab und arrangierten sich damit, dass zur Verabschiedung von Datenschutzgesetzen das Eingehen von Kompromissen zugunsten der wirtschaftspolitischen Bedeutung der Datenverarbeitung notwendig war. Kurz nach der Jahrtausendwende kippte diese fragile Balance jedoch aus zwei Gründen: Zum einen führte das un-

227 Freilich forderten sie, dass die Einführung staatlicher Datenschutzmaßnahmen möglichst wirtschaftsfreundlich ausfällt und auf Elementen der Selbstregulierung aufbaut.

gebremste Bedeutungswachstum, das die Verarbeitung personenbezogener Daten erfuhr, in Kombination mit dem Zeitgeist einer regulierungsskeptischen politischen Haltung zu einer Verschiebung der Balance zugunsten der Befürworter einer möglichst ungezügelten Datenverarbeitung. Datenschutz galt zunehmend als individueller Luxus, dem das potentielle Wirtschaftswachstum infolge der gesteigerten Verarbeitung personenbezogener Daten als Allgemeinwohlinteresse gegenübergestellt wurde. Zum anderen führten die Terroranschläge vom 11. September 2001 und von Madrid und London zu einer deutlichen Verschärfung sicherheitspolitischer Maßnahmen. In der Folge wurden EU-weit zahlreiche Maßnahmen verabschiedet, in denen der Beachtung datenschutzrechtlicher Garantien kaum Wert beigemessen wurde. Die Befürworter von Datenschutzregelungen standen somit einer Legitimationskrise gegenüber und gerieten an allen Fronten in die Defensive.

Eine Veränderung, die schon bald zur Initiierung der Datenschutzreform führen sollte, zeigte sich erst während der Verhandlungen zur Cookie-RL. Die Gründe für diese Veränderung und der Wandel in den relevanten Kontextbedingungen sind Gegenstand des folgenden Abschnitts.

3.4 Wandel weiterer relevanter Kontextbedingungen, die für die Initiierung der Datenschutzreform entscheidend waren

Mehrere Faktoren waren für die Initiierung der Datenschutzreform ausschlaggebend. An Subsystem-*internen* Faktoren sind hier die Verabschiedung der EU-GRCh und insbesondere das Inkrafttreten des Lissabon-Vertrags, aber auch das zunehmend selbstbewusste, aber auch überzeugungsgetriebene politische Handeln der Kommission und des Parlaments zu nennen. An Subsystem-*externen* Faktoren sind hingegen insbesondere die Zunahme von Datenschutzskandalen sowie eine relative Steigerung der öffentlichen Sensibilität für den Datenschutz seit Mitte der 2000er-Jahre zu nennen. Dieser Abschnitt widmet sich der Untersuchung der Frage, welche Faktoren in welchem Maße wesentlichen Einfluss auf die Initiierung der Datenschutzreform hatten.

3.4.1 Veränderungen in der grundlegenden verfassungsmäßigen Struktur, im Grad der erforderlichen Zustimmung für wesentlichen Wandel sowie der relativen Offenheit des politischen Systems

3.4.1.1 Die Erarbeitung der EU-Grundrechtecharta

Über viele Jahrzehnte hinweg wurden in den EU-Organen verschiedene Bestrebungen unternommen, um die Verpflichtung der Europäischen Gemeinschaften bzw. Union im Hinblick auf den Grundrechtsschutz ihrer Bürgerinnen und Bürger auszubauen. Zu diesem Zweck wurde einerseits die Strategie des Beitritts der EG – so etwa von der Kommission im Jahr 1979 vorgeschlagen – zur EMRK verfolgt und andererseits die Strategie der Erarbeitung eines eigenen Katalogs an europäischen Grundrechten (González Fuster 2014, 185). Letztere wurde seit Ende der 1970er-Jahre vor allem vom Europäischen Parlament (1979) vorangetrieben[228] und sollte schließlich in den 1990ern auch Anklang bei der Kommission finden. Wie bereits im Abschnitt zur DS-RL (3.2.2) erwähnt, hatte Ende der 1980er bzw. Anfang der 1990er ein Wandel im Selbstverständnis der EG hin zu einer politischen Union stattgefunden. Nachdem im Jahr 1989 die Gemeinschaftscharta der sozialen Grundrechte der Arbeitnehmer von den EG-Mitgliedstaaten[229] verabschiedet worden, aber die genaue Beziehung zwischen der Charta und EU-Recht noch unklar geblieben war, hatte die Europäische Kommission die Gründung des sog. *Komitees der Weisen* initiiert, um das Verhältnis zwischen der Charta und den geplanten Reformen im Kontext des Amsterdamer Vertrags zu untersuchen (González Fuster 2014, 189). Das Komitee der Weisen, das sein Aufgabenspektrum weiter fasste und das grundsätzliche Verhältnis zwischen EU-Recht und Bürgerrechten diskutierte, empfahl in seinem Abschlussbericht von 1996 die „Aufnahme eines Kernbestands von politischen und sozialen Grundrechten (‚Bill of Rights') in die Verträge" (Komitee der Weisen 1996, 9, Nr. VII.). Zudem vertrat das Komitee die Ansicht, dass der Katalog an Grundrechten nicht unveränderlich, sondern die Entwicklung auch neuer Grundrechte geboten sei, „weil das Konzept des Individuums weiter vertieft wird und die Rechte und

228 So etwa von Altiero Spinelli, der zwischenzeitlich aus der Kommission in das Europäische Parlament gewechselt war und auch von Karel De Gucht (González Fuster 2014, 186–89).

229 Lediglich das Vereinigte Königreich verabschiedete diese erst 1998 unter Tony Blair, da Margaret Thatcher die Verabschiedung stets blockiert hatte (González Fuster 2014, 189).

Pflichten, die ihm die gleichberechtigte Teilhabe an einer lebendigen Gesellschaft ermöglichen, immer umfassender und genauer bestimmt werden; und zum anderen, weil der technische Fortschritt und die Entwicklung allgemein Gefahren für den einzelnen, aber auch neue Aktionsmöglichkeiten mit sich bringen, die hinsichtlich ihrer möglichen Auswirkungen auf den einzelnen reglementiert werden müssen." (ebd., 44) Unter anderem verwies das Komitee darauf, dass die Informationsgesellschaft die *individuelle Privatheit* gefährde (ebd.).

Als der Vertrag von Amsterdam am 2. Oktober 1997 unterzeichnet worden, die vorgeschlagene Aufnahme von EU-Grundrechten allerdings – trotz der im Vertrag von Amsterdam formulierten Bekenntnis der Europäischen Union zu Grundrechten – ausgeblieben war, rief die Europäische Kommission eine weitere Expertengruppe ins Leben. Den Vorsitz der Expertengruppe „Grundrechte" übernahm Spiros Simitis (Expertengruppe „Grundrechte" 1999), der zwischen 1982 und 1986 bereits den Vorsitz des Datenschutzkomitees des Europarates innehatte und seit dem Jahr 1988 als Berater der Europäische Kommission in Datenschutzfragen fungierte (Simitis 2001, 99). Die Aufgabe der Expertengruppe „bestand darin, zu analysieren, welchen Status die sozialen Grundrechte in den Verträgen haben - insbesondere im neuen Vertrag von Amsterdam -, mögliche Lücken aufzuzeigen und die rechtlichen und konstitutionellen Implikationen zu untersuchen. Dabei sollte insbesondere die Möglichkeit geprüft werden, bei der nächsten Revision der Verträge die Grundrechte in Form einer ‚Bill of Rights' zu verbürgen." (Expertengruppe „Grundrechte" 1999, 3)

In seinem Abschlussbericht vom Februar 1999 kritisierte die Expertengruppe den Zustand des Grundrechtsschutzes in der Union schließlich als unzureichend und forderte die Anerkennung der Grundrechte insbesondere auf Grundlage der EMRK auf. Diese habe sich durch die Rechtsprechungsorgane ohnehin bereits zu einer gemeinsamen europäischen „Bill of Rights" entwickelt und müsse daher vollständig in das Gemeinschaftsrecht überführt und durch zusätzliche Bestimmungen spezifiziert und ergänzt werden (ebd., 7). Insbesondere im Bereich der dritten Säule der EU identifizierte die Expertengruppe Mängel und Unstimmigkeiten, die auf die *restriktive Politik* der Mitgliedstaaten zurückzuführen seien, die unter Verweis auf den intergouvernementalen Kooperationscharakter stets danach strebten, die Auswirkungen der Grundrechtsbindung zu begrenzen, wie es insbesondere am Widerstand gegen Datenschutzbestimmungen für die dritte Säule deutlich werde (ebd., 13). Daher vertrat die Expertengruppe die Ansicht, dass der Grundrechtskatalog der EMRK durch weitere Rechte,

insb. um „das Recht, über die Verwendung personenbezogener Daten zu bestimmen“ (ebd., 26) erweitert werden sollte.

3.4.1.1.1 Entwurfsprozess

Auf dem Treffen des Europäischen Rats in Köln im Juni 1999 wurde schließlich der Beschluss gefasst, dass „die auf der Ebene der Union geltenden Grundrechte in einer Charta zusammengefaßt und dadurch sichtbarer gemacht werden sollten.“ (Europäischer Rat 1999a, 18, Nr. 44) Da sich die Regierungschefs im Hinblick auf die Frage, ob die Charta einen rechtlich verbindlichen Charakter annehmen sollte, indem sie in die Verträge aufgenommen würde, nicht einigen konnten, wurde zunächst ausschließlich deren feierliche Proklamation beschlossen (ebd., Anhang IV). Der Beschluss sah zum Zwecke der Erarbeitung der Charta die Gründung eines Gremiums vor, „das aus Beauftragten der Staats- und Regierungschefs und des Präsidenten der Europäischen Kommission sowie Mitgliedern des Europäischen Parlaments und der nationalen Parlamente besteht. Vertreter des Europäischen Gerichtshofs sollten als Beobachter teilnehmen. Vertreter des Wirtschafts- und Sozialausschusses, des Auschusses [sic] der Regionen und gesellschaftlicher Gruppen sowie Sachverständige sollten angehört werden. Das Sekretariat soll vom Generalsekretariat des Rates wahrgenommen werden.“ (ebd., 43) Das Gremium wählte als Selbstbezeichnung den Titel „Europäischer Konvent“. Die Vorgaben zur genauen Zusammensetzung und Arbeitsweise des Europäischen Konvents wurden auf dem Folgetreffen des Europäischen Rates in Tampere am 15. und 16. Oktober 1999 verabschiedet (Europäischer Rat 1999b). Die Europäische Union umfasste zu diesem Zeitpunkt 15 Mitgliedstaaten. Die wahlberechtigten Mitglieder des Konvents setzten sich aus insgesamt 15 Repräsentanten der Staats- und Regierungschefs der Mitgliedstaaten, 30 Vertretern der nationalen Parlamente (2 pro Parlament), 16 Mitgliedern des Europäischen Parlaments sowie einem Beauftragten des Präsidenten der Europäischen Kommission zusammen (Europäischer Rat 1999b).

Mehrere Mitglieder des Europäischen Konvents hatten einschlägige Erfahrungen im Bereich des Privatheitsschutzes bzw. des Schutzes personenbezogener Daten gesammelt, und sollten entscheidenden Einfluss auf den Einbezug entsprechender Schutzregelungen in den Text der Grundrechtecharta nehmen. Den Vorsitz des Europäischen Konvents übernahm der frühere Bundespräsident Deutschlands, Roman Herzog, der CDU-Mitglied

und zudem von 1983 bis zu seiner Wahl zum Bundespräsidenten 1994 Richter und ab 1987 zudem Präsident am Bundesverfassungsgericht war. Herzog war daher in besonderem Maße mit der Rechtsprechung des BVerfG vertraut, das der informationellen Selbstbestimmung im Rahmen des Volkszählungsurteils 1983 den Charakter eines Grundrechts zugesprochen hatte. Daneben nahm Guy Braibant als Vertreter Frankreichs sowie als stellvertretender Vorsitzender am Konvent teil. Erste datenschutzrechtliche Erfahrungen hatte Braibant während der Ausarbeitung des französischen Datenschutzgesetzes (Loi Informatique et Liberté) Ende der 1970er gesammelt und zuletzt einen Bericht für die französische Regierung zur DS-RL 95/46/EG verfasst. Einer der Parlamentsrepräsentanten Spaniens, Jordi Solé Tura, hatte aktiv am Entwurf der spanischen Verfassung von 1978 mitgewirkt und einen entscheidenden Beitrag zum Wortlaut der Bestimmung geleistet, die später als die Einführung eines spanischen Grundrechts auf den Schutz personenbezogener Daten bekannt werden sollte. Zudem war Stefano Rodotà als Vertreter der italienischen Regierung am Konvent beteiligt. Rodotà war zu diesem Zeitpunkt zugleich seit dem Jahr der Gründung der italienischen Datenschutzaufsichtsbehörde 1997 deren Vorsitzender, stellvertretender Vorsitzender der Art. 29-Datenschutzgruppe zwischen 1998 und 2000 (ab 2000 hatte Rodotà den Vorsitz der Art. 29 Datenschutzgruppe inne) sowie eines von zwölf Mitgliedern der *Europäischen Beratungsgruppe für Ethik im Bereich der Wissenschaft und der neuen Technologien*, die die Europäische Kommission seit 1991 beriet (González Fuster 2014, 194). Der Konvent tagte vom 17. Dezember 1999 an und verabschiedete nach etwa 30 Sitzungstagen am 2. Oktober 2000 den Entwurf der Grundrechtecharta (ebd.).

3.4.1.1.2 Konflikte während des Entwurfsprozesses

Einer der Hauptkonflikte während des Entwurfsprozesses entstand infolge des Mandats des Europäischen Konvents. So hatte der Beschluss des Europäischen Rates die *Zusammenfassung und Sichtbarmachung der auf der Ebene der Union geltenden Grundrechte*, allerdings nicht die *Ergänzung* der geltenden Grundrechte um neue vorgesehen.[230] Insbesondere das Vereinigte Königreich zählte zu den Staaten, die die Einführung neuer

230 Bestehende Grundrechte seien in diesem Zusammenhang verstanden als jene Rechte, die damals bereits in der Mehrzahl der EU-Mitgliedstaaten verbrieft waren. Abgesehen davon hatten zu diesem Zeitpunkt bereits einige Mitgliedstaaten moderne

Grundrechte vehement ablehnten. Die übrigen Staaten, insbesondere die EG-Gründungsmitglieder, waren dagegen der Ansicht, dass der Entwurfsprozess möglichst offen gehalten werden sollte, um auch moderne Gefährdungen des Menschen etwa aus den Bereichen der Bioethik, des Umweltschutzes, des Verbraucherschutzrechts und der Digitalisierung adressieren zu können (González Fuster 2014, 192). Unterstützt wurde die Perspektive der Modernisierungsbefürworter sowohl von der Art. 29-Datenschutzgruppe als auch vom Europäischen Parlament. Beide Institutionen sprachen bereits nach dem ersten Beschluss des Europäischen Ratstreffens von Köln ihre ausdrückliche Unterstützung für die Ausarbeitung einer europäischen Grundrechtecharta aus. Unter Verweis darauf, dass bereits „einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben [… und in] einigen anderen Ländern ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt" (Art. 29 DS-Gruppe 1999, 2) wurde, empfahl die Datenschutzgruppe die Aufnahme des Grundrechts auf Datenschutz in die Grundrechtecharta. Verwiesen wurde auch darauf, dass der Europäische Gerichtshof für Menschenrechte in seiner Spruchpraxis bereits ein Grundrecht aus dem datenschutzrechtlichen Gehalt verschiedener Menschenrechte herausgearbeitet und konkretisiert habe (ebd.). Das europäische Parlament betonte, dass die Charta grundsätzlich eines „offenen und innovativen Ansatzes bedürfe, sowohl hinsichtlich ihrer Merkmale und *der Art der darin aufzuführenden Rechte* als auch hinsichtlich ihrer Funktionen und ihrer Stellung bei der konstitutionellen Weiterentwicklung der Union" (EP 1999, Nr. 3, Hervorhebung durch M.K.).

Zu Beginn der Gespräche im Europäischen Konvent war zwar unklar, ob die zu erarbeitende Grundrechtecharta angesichts des Widerstands seitens einiger Mitgliedstaaten jemals einen unionsweit verbindlichen Charakter annehmen könnte, doch auf Herzogs Vorschlag hin entschieden sich die Mitglieder dazu, so zu arbeiten, *als ob* die Charta später einmal ein rechtlich bindendes Dokument darstellen würde, was laut den Beteiligten positive Auswirkungen auf die Qualität des Textes hatte (J. Meyer und Engels 2001, 89).

Grundrechte wie den Schutz personenbezogener Daten in ihren Verfassungen implementiert, sodass die Einführung derartiger Grundrechte auf EU-Ebene streng genommen kein völliges Novum dargestellt hätte. Abgelehnt wurde also insbesondere die Übertragung moderner Grundrechte über die EU-Ebene auf die Mitgliedstaaten, in denen diese nicht verbrieft waren (González Fuster 2014, 192).

Datenschutz wurde erstmals seitens des sozialdemokratischen Bundestagsabgeordneten Prof. Dr. Jürgen Meyer, eines der deutschen Parlamentsvertreter (J. Meyer und Engels 2001, 7), in einem Entwurf der am 6. Januar 2000 an die Konventsmitglieder verteilt wurde, erwähnt. Aufbauend auf der Entschließung des Parlaments aus dem Jahr 1989 schlug Meyer einen Artikel 6 zum Datenschutz sowie einen Artikel 7 zu Privatheit vor (European Convention Presidency 2000a, 4). Der Datenschutz-Artikel baute klar auf Kontrolltheorien, indem die Verantwortung zum Umgang mit personenbezogenen Daten in reduktionistischer Manier dem Individuum übertragen wurde und deren Begrenzung nur im Falle eines überwiegenden öffentlichen Interesses erlaubt sein sollte. Im Falle des Privatheitsartikels wurde diese Dichotomisierung dagegen unterlassen. Hier wurden als mögliche Gründe zur Begrenzung der häuslichen Privatheit beispielhaft spezifische Elemente wie die ernsthafte Gefährdung der öffentlichen Ordnung und besonders schwerwiegende Verbrechen im Kontext häuslicher Privatheit genannt. Eingriffe in die kommunikative Privatheit sollten dagegen nur unter den Bedingungen zulässig sein, die das Strafrecht vorsehe (ebd.). Auch die vom Präsidium[231] ausgearbeitete vorläufige Liste möglicherweise infrage kommender Rechte baute auf der Parlamentsentschließung von 1989 auf und sah – allerdings ohne die weitere Spezifizierung des Gehalts und möglicher Begrenzungsgründe – sowohl ein eigenständiges Recht auf Datenschutz (European Convention Presidency 2000c, 5) als auch ein weiteres Recht auf „Private and family life" (ebd., 4) vor. Bereits zu diesem frühen Stadium der Verhandlungen konnte sich somit die Idee durchsetzen, dass der Schutz personenbezogener Daten zumindest Erwähnung in der Charta finden sollte (González Fuster 2014, 196).

In einem weiteren Entwurf des Präsidiums vom 24. Februar tauchte Datenschutz schließlich erneut als ein eigenständiges Grundrecht auf. Die gewählte Formulierung (European Convention Presidency 2000b, 5) stützte sich auf die Europaratskonvention, sah allerdings abweichend von dieser auch eine spezifischere Alternativfassung (ebd.) vor, wonach die Verarbeitung personenbezogener Daten entweder auf Basis der Einwilligung des Betroffenen oder einer gesetzlich festgelegten legitimen Grundlage entsprechend erfolgen dürfen sollte (European Convention Presidency 2000b, 5). Andere Alternativen, wonach jede Person selbst über die Freigabe sie

231 „Das Präsidium hatte eine ausgesprochen wichtige Rolle, da es nicht nur die Tagesordnung festlegte und die Konventssitzungen leitete, sondern auch die Vorschläge für die Artikelformulierungen vorlegte." (J. Meyer und Engels 2001, 13)

betreffender personenbezogener Daten entscheiden können sollte, konnten sich nicht durchsetzen. Nach weiteren Debatten über das Ausmaß der zu verbriefenden informationellen Selbstbestimmung, über das Verhältnis zwischen Privatsphäre und Datenschutz sowie Versuchen, den Schutz der Privatheit mit dem Schutz der Ehre, des Rufes, des Hauses sowie der Freiheit und Vertraulichkeit der Kommunikation in Verbindung zu bringen (González Fuster 2014, 196 f.), konnte schließlich Ende Juli eine Einigung erzielt werden (Präsidium des Europäischen Konvents 2000, 4)

Zunächst stimmten die Konventsmitglieder dem Textentwurf für eine Charta der Grundrechte der Europäischen Union bereits Ende September zu und schlossen ihre Arbeit schließlich mit der Annahme der Charta am 2. Oktober 2000 ab (J. Meyer und Engels 2001, 67). Im Anschluss wurde der Entwurf Anfang Oktober an die Staats- und Regierungschefs der EU-Mitgliedstaaten übermittelt. Auf der informellen Sitzung des Europäischen Rates vom 13. und 14. Oktober 2000 in Biarritz wurde der Entwurf schließlich angenommen und das Parlament darum ersucht, gemeinsam mit dem Rat und der Kommission die Charta auf der formellen Sitzung des Europäischen Rates in Nizza feierlich zu proklamieren (J. Meyer und Engels 2001, 69). Nachdem das Europäische Parlament den Entwurf am 14. November gebilligt hatte (EP 2000), unterzeichneten die Präsidentin des Europäischen Parlaments, der Präsident des Rates und der Präsident der Kommission die Charta der Grundrechte auf dem Treffen des Europäischen Rates am 7. Dezember 2000 und verkündeten diese feierlich (Europäischer Rat 2000a).

3.4.1.1.3 Inhalt der Grundrechtecharta

Im Folgenden gehe ich auf die Bedeutung der Grundrechtecharta ein und lege einerseits dar, wie das Verhältnis zwischen Art. 7 und 8 GRCh zu bewerten ist und andererseits, in welchem Verhältnis beide GRCh-Artikel zu Art. 8 EMRK stehen.

Die Grundrechtecharta beinhaltet zwei Artikel, die relevant im Hinblick auf den Datenschutz sind. Art.7 GRCh[232] widmet sich der Achtung des

232 Art. 7 GRCh – *Achtung des Privat- und Familienlebens*: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation." (EU 2010)

Privat- und Familienlebens und Art. 8 GRCh[233] dem Schutz personenbezogener Daten. Der Inhalt von Art. 7 GRCh entspricht weitgehend Art. 8 der EMRK,[234] während Art. 8 GRCh ein eigenständiges Recht auf den Schutz personenbezogener Daten formuliert und damit ein Novum darstellt. Denn bis zu diesem Zeitpunkt hatte beispielsweise der EGMR den Schutz personenbezogener Daten als Ausfluss des in Art. 8 EMRK verbrieften Rechts auf Achtung des Privat- und Familienlebens interpretiert. In ähnlicher Weise wurde der Schutz personenbezogener Daten in der Datenschutz-Konvention des Europarats und auch in der DS-RL stets als bedeutsam im Hinblick auf den Schutz von Rechten und Freiheiten im Allgemeinen bezeichnet. Zwar hatten einige europäische Staaten bereits ein Recht auf Datenschutz anerkannt, allerdings wurde der Schutz personenbezogener Daten mit der Grundrechtecharta erstmals auf internationaler Ebene als eigenständiges Grundrecht verbrieft. Nach González Fuster (2014, 199) könne die Existenz von zwei voneinander getrennten privatheitsrelevanten Artikeln als Kompromiss zwischen jenen Staaten, die Datenschutz als Teil des Privatheitsschutzes betrachteten und jenen, die Datenschutz als eigenständiges Grundrecht verbrieft hatten, bewertet werden. Andererseits könne es auch als das Ergebnis des Konflikts der europäischen Staaten zwischen Konservierung bestehender Grundrechte und grundrechtlicher Innovation bewertet werden. Insofern spiegele die Aufrechterhaltung eines eigenen Artikels zur Achtung des Privat- und Familienlebens und dessen Ergänzung um ein eigenständiges Recht auf Datenschutz den Versuch dar, Konservierung und Innovation in ein Gleichgewicht zu bringen.

233 Art. 8 GRCh – *Schutz personenbezogener Daten*: „(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht." (EU 2010)

234 Art. 8 EMRK – *Recht auf Achtung des Privat- und Familienlebens*: „1. Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. 2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer." (Europarat 2010)

Der erste Unterschied zwischen den Regelungen der Europäischen Grundrechtecharta und der Europäischen Menschenrechtskonvention liegt in der Ersetzung des Begriffs der Korrespondenz durch den Begriff der Kommunikation. Dies ist auf die in der Zeit zwischen der Verabschiedung der beiden internationalen Dokumente erfolgte Rechtsprechung des EGMR zurückzuführen, in der angesichts technologischer Entwicklungen der allgemeinere Begriff der Kommunikation gegenüber dem Begriff der Korrespondenz, der lediglich den Schriftverkehr umfasst, bevorzugt wurde. Hinsichtlich möglicher Einschränkungen der Achtung des Privat- und Familienlebens sind beide Instrumente weitgehend deckungsgleich, doch sieht die Grundrechtecharta – und dies ist der zweite Unterschied – im Gegensatz zur EMRK „von der Union anerkannte[…] dem Gemeinwohl dienende Zielsetzungen" als einen weiteren möglichen Einschränkungsgrund vor. Während dies als eine Abschwächung der EMRK-Regelungen bewertet werden kann, bietet der erste Satz desselben Artikels aber zugleich eine Stärkung, da darin vorgegeben wird, dass jede Einschränkung den Wesensgehalt der entsprechenden Rechte und Freiheiten zu achten hat (González Fuster 2014, 200–202).[235]

Zunächst sei erwähnt, dass die oben ausgeführten Gedanken zur Einschränkung des Art. 7 GRCh auf Basis des horizontalen Artikels 52 Abs. 1 GRCh sich auch auf Art. 8 GRCh übertragen lassen (González Fuster 2014, 203). Gestützt wurde Art. 8 GRCh dagegen auf Art. 286 des EWG-Vertrags,[236] auf die DS-RL 95/46/EG, auf Art. 8 EMRK sowie auf die Datenschutz-Konvention des Europarates. Während die Präambel der Charta die gemeinsamen Verfassungstraditionen und die gemeinsamen internationalen Verpflichtungen der Mitgliedstaaten, die EMRK, sowie die Rechtsprechung des EuGH und des EGMR als Grundlage anführt (EU 2010, 391), fehlen die gemeinsamen Verfassungstraditionen der Mitgliedstaaten sowie

235 Da der Europäische Konvent den Text der Grundrechtecharta im Hinblick auf eine bessere Lesbarkeit möglichst kurzhalten wollte, wurden mögliche Einschränkungsgründe nicht in den entsprechenden Artikeln selbst, sondern an späterer Stelle niedergelegt. Mit Art. 8 Abs. 2 EMRK korrespondiert daher Art. 52 Abs. 1 GRCh: *Tragweite und Auslegung der Rechte und Grundsätze*: (1) Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen." (EU 2010)

236 Nunmehr Art. 16 AEUV und Art. 39 EUV.

die Rechtsprechung des EuGH und des EGMR in der Begründung von Art. 8 GRCh (González Fuster 2014, 203).

Darüber hinaus ist eine Besonderheit des Art. 8 GRCh, dass er sich nicht nur auf den abstrakten Schutz personenbezogener Daten, wie er im ersten Absatz geregelt ist, beschränkt, sondern in den folgenden beiden Absätzen insgesamt sechs spezifische Elemente benennt, die bei der Verarbeitung der Daten zu beachten seien: 1. Die Verarbeitung nach Treu und Glauben, 2. das Zweckbindungsprinzip, 3. die Anforderung einer rechtmäßigen Verarbeitungsgrundlage, entweder mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten Grundlage, 4. das Auskunftsrecht, 5. das Recht auf Berichtigung, und 6. die Überwachung der Datenschutz-Vorschriften durch eine unabhängige Aufsichtsstelle. Zudem macht der Artikel keine Unterscheidung zwischen der automatisierten und der manuellen Verarbeitung personenbezogener Daten, ist daher also auf beide Verarbeitungsarten anwendbar. Nicht genannt wurden dagegen einige der zu diesem Zeitpunkt in den geltenden internationalen Datenschutzinstrumenten festgeschriebenen datenschutzrechtlichen Elemente (González Fuster 2014, 204 f.). So waren bereits in den OECD-Richtlinien auch Verarbeiterpflichten in Form von Sicherheitsmaßnahmen, Transparenzvorgaben (wobei fairerweise erwähnt sei, dass das in der GRCh benannte Recht auf Auskunft zumindest als ein wichtiges Element im Rahmen der Transparenzpflichten der Verarbeiter aufgefasst werden kann) sowie die Rechenschaftspflicht der Verarbeiter benannt (vgl. 3.1.1.3). In der Datenschutz-Konvention des Europarats waren zusätzlich die Datenschutzprinzipien der Datenminimierung, der Richtigkeit und der Speicherbegrenzung enthalten. Zudem sah die Europaratskonvention 108 im Gegensatz zu Art. 8 der Grundrechtecharta ein erhöhtes Schutzniveau für besondere Arten personenbezogener Daten sowie das Betroffenenrecht auf Löschung vor. Schließlich hatte die Datenschutz-Konvention zwar keine Vorgaben zur Einrichtung einer Aufsichtsstelle gemacht, sah allerdings im Gegensatz zur GRCh die Schaffung von Sanktionsstrukturen und die Bereitstellung von Rechtsmitteln vor (vgl. 3.1.2.3). Ebenso fehlten die aus der DS-RL bekannten Rechte auf Widerruf bzw. auf Schutz vor automatisierten Einzelentscheidungen (vgl. 3.2.2.7).

3.4.1.1.4 Zwischenfazit

Die Grundrechtecharta war das erste internationale Rechtsinstrument, das den Schutz personenbezogener Daten als eigenständiges Grundrecht verbriefte und stellte insofern eine enorme Innovation dar.

Die in der Charta genannten sechs datenschutzrechtlichen Elemente bezogen sich zwar nur auf einen kleinen Teil des bereits damals verbrieften Schutzes personenbezogener Daten, was jedoch nicht verwundern sollte: Die Verabschiedung der DS-RL lag nur wenige Jahre zurück und nur wenige Mitgliedstaaten hatten diese im vorgegebenen Zeitrahmen in nationales Recht umgesetzt. Zudem war die wirtschaftspolitische Bedeutung personenbezogener Daten zwar bereits während der Aushandlung der DS-RL von Bedeutung, doch Forderungen nach einer Aufweichung der Datenschutzprinzipien zugunsten wirtschaftspolitischer Ziele konnten erst um die Jahrtausendwende stärkere politische Unterstützung auf sich ziehen. Im Ergebnis waren die Befürworter von Datenschutzregelungen in dieser Periode eher darum bemüht, einige als zentral betrachtete, aber politisch umstrittene Datenschutz-Grundsätze zunächst klar zu verankern, anstatt zu versuchen, diese umstrittenen Grundsätze um weitere möglicherweise noch umstrittenere Regelungen zu erweitern.

Auf der inhaltlichen Ebene bedeutete die Vorgabe zur Aufrechterhaltung des Wesensgehalts des Datenschutzes gemäß Art. 52 GRCh (allerdings nur unter der Bedingung, dass die Charta auch tatsächlich Rechtsverbindlichkeit erhalte), dass eine Außerkraftsetzung der Datenschutzprinzipien weder auf Basis von wirtschaftspolitischen Erwägungen noch auf Grundlage sicherheitspolitischer Interessen *so wichtig diese auch sein mögen* erfolgen durfte, wie etwa die Datenschutzgruppe 2002 anmerkte (Artikel 29-Datenschutzgruppe 2002, 5).

Die Verabschiedung der Grundrechtecharta und die Inkorporation insb. eines eigenständigen Datenschutz-Artikels sind als klarer Erfolg der Datenschutzbefürworter zu bewerten. Die Kommission, das Europäische Parlament, institutionelle Datenschützer sowie einzelne bedeutsame Figuren wie Roman Herzog trugen gemeinsam entscheidend zur Aufnahme des Schutzes personenbezogener Daten bei. Zudem stellt die Verabschiedung der GRCh ein Beispiel für *Venue Shopping* dar, bei der Akteure zur Erreichung ihrer politischen Ziele alle sich bietenden politischen Gestaltungsräume auf allen sich bietenden Entscheidungsebenen nutzen (Beyers und Kerremans 2012).

Da die Charta zunächst nur feierlich proklamiert wurde, sie also weder eine unmittelbare Rechtsverbindlichkeit entfaltete noch absehbar war, ob sie dies jemals können würde, hatte sie allerdings zunächst keine direkten Auswirkungen auf die Datenschutzpolitik.[237] Diese sollte sie später mit dem Inkrafttreten des Lissabon-Vertrags in Form des Wandels nicht nur der verfassungsmäßigen Struktur, sondern auch des Grades der erforderlichen Zustimmung für wesentlichen Wandel und der relativen Offenheit des politischen Systems erhalten. Der Entstehung des Lissabon-Vertrags widmet sich das folgende Unterkapitel.

3.4.1.2 Der Vertrag von Lissabon

Wie bereits erwähnt, waren die Mitgliedstaaten der Europäischen Union gespalten im Hinblick auf die Frage des anzustrebenden Rechtscharakters der Grundrechtecharta. Während die Mehrheit der Mitgliedstaaten für eine in die Verträge eingefügte, rechtsverbindliche Charta eintrat, befürworteten Großbritannien, Irland, die Niederlande und die skandinavischen Länder eine lediglich feierlich proklamierte Charta ohne Rechtsverbindlichkeit (P. Becker und Leisse 2005, 48; González Fuster 2014, 229).

Aufgrund dieses Dissenses hatten sich die Staats- und Regierungschefs auf dem Kölner Treffen des Europäischen Rats im Jahr 1999 zunächst lediglich auf die feierliche Proklamation der Charta geeinigt, die Frage nach der endgültigen Rechtsnatur der Charta dagegen bewusst offengelassen und auf die Zeit nach der Proklamation verschoben (Europäischer Rat 1999a, 43). Nachdem auch der Europäische Rat von Nizza, auf dem die feierliche Proklamation der Charta am 7. Dezember 2000 erfolgt war, die Klärung der Frage erneut auf einen späteren Zeitpunkt verlegte (Europäischer Rat 2000a, 1),[238] intensivierte sich die politische Debatte (P. Becker und Leisse 2005, 57–66) und führte auf dem Treffen des Europäischen Rates in Laeken

237 Eine der direkten Folgen der Proklamation der CRCh war die Gründung von FRA, der *Agentur der Europäischen Union für Grundrechte* (Fundamental Rights Agency) im Jahr 2007, die mit der Aufgabe betraut wurde, die bereits in EU-Recht umgesetzten Elemente der Grundrechtecharta zu überwachen und die relevanten Organe, Einrichtungen, Ämter und Agenturen der EU sowie die Mitgliedstaaten bei diesbezüglichen Fragen zu beraten (FRA 2012, 33 f.).

238 Bei der Regierungskonferenz von Nizza war es insbesondere um die Reform der EU gegangen, um ihre Handlungsfähigkeit (im Hinblick auf Größe und Zusammensetzung der Kommission, auf die Reform der Stimmgewichtung im Ministerrat und auf die Ausweitung der qualifizierten Mehrheit) auch angesichts der bevorstehenden Erweiterung der Union um zunächst zehn (bis 15) neue Mitgliedstaaten sicherzu-

Ende 2001 zur Einberufung eines neuen Konvents zur Zukunft Europas (Europäischer Rat 2001, 21 ff.).

3.4.1.2.1 Entwurfsphase

Dieser zweite Konvent, auch als „Verfassungskonvent" bezeichnet, sollte alle wesentlichen die zukünftige Entwicklung der Europäischen Union betreffenden Fragen prüfen. Die Debatte über die Zukunft der Europäischen Union war deshalb notwendig geworden, weil viele der geltenden Gemeinschaftsmechanismen (darunter insb. die hervorgehobene Stellung des Ministerrats und die Schwäche des Europäischen Parlaments, kurzum: das Demokratiedefizit) noch immer auf den Strukturen der 1950er-Jahre basierten und die Mitgliedstaaten sich im Rahmen der Regierungskonferenzen unfähig gezeigt hatten, langfristige Lösungen für diese und weitere strukturelle Probleme zu finden (P. Becker und Leisse 2005, 50–55). In der Hoffnung, dass an den Erfolg des ersten Konvents angeknüpft und nicht die auf den Regierungskonferenzen begangenen Fehler wiederholt würden, übertrug der Europäische Rat von Laeken die Aufgabe zur Schaffung einer demokratischeren, transparenteren und effizienteren Europäischen Union an den besagten zweiten Konvent. Der Konvent sollte sich aus 16 Mitgliedern des Europäischen Parlaments, 30 Mitgliedern der nationalen Parlamente (2 für jeden Mitgliedstaat), 2 Vertretern der Europäischen Kommission und 15 Regierungsvertretern zusammensetzen. Die EU-Beitrittskandidaten wurden ebenfalls mit je zwei parlamentarischen Vertretern und einem Regierungsvertreter in die Verhandlungen eingebunden. Den Vorsitz des zweiten Konvents übernahm der frühere französische Präsident Valéry Giscard d'Estaing (Europäischer Rat 2001, 24 f.). Der Verfassungskonvent tagte zwischen dem 28. Februar 2002 und dem 20. Juli 2003. Der dabei entstandene Entwurf für eine EU-Verfassung wurde daraufhin im Rahmen des Europäischen Rates hitzig debattiert (P. Becker und Leisse 2005, 220–38). Nach weiteren Verhandlungen konnte dann zunächst im

stellen. Die Ergebnisse der Konferenz wurden von der Mehrheit der wissenschaftlichen und politischen Beobachter als Ausdruck des Stillstands des europäischen Integrationsprozesses abgelehnt: „Die enttäuschenden Ergebnisse und die komplizierten Verhandlungen über die Machtfragen über die Machtfragen, insbesondere bei der Frage der Stimmengewichtung im Rat, hatten nochmals deutlich bestätigt, dass nationales Prestigedenken und kurzfristige Interessenpolitik sowie das Denken in Blockadekategorien an Stelle von Handlungs- und Gestaltungsmöglichkeiten die Debatte bestimmten." (P. Becker und Leisse 2005, 53)

Juni 2004 eine politische Einigung erreicht werden, die schließlich auf dem Treffen des Europäischen Rates in Rom am 29. Oktober 2004 mit den Unterschriften der Staats- und Regierungschefs auch förmlich besiegelt wurde. Geplant war, dass der Verfassungsvertrag nach einer zweijährigen Phase der Ratifikation durch alle Mitgliedstaaten zum 1. November 2006 in Kraft treten sollte (P. Becker und Leisse 2005, 239–58). Je nach Mitgliedstaat musste die Ratifikation entweder per Parlamentsbeschluss oder Volksabstimmung erfolgen. In der Mehrzahl der Mitgliedstaaten – beginnend mit Litauen am 11. November 2004 – erfolgte die Ratifikation auf Grundlage eines Parlamentsbeschlusses. Nachdem der Verfassungsvertrag bei den Referenden in Frankreich am 29. Mai 2005 bzw. in den Niederlanden am 1. Juni 2005 abgelehnt worden war, scheiterte die Annahme des Verfassungsvertrags, sodass der Ratifikationsprozess in der Mehrzahl der übrigen Mitgliedstaaten abgebrochen wurde, der Verfassungsvertrag damit also scheiterte (Hellmann 2009, 6).

In der Folge trat die Europäische Union in eine mehr als zwei Jahre andauernde Reflexionsphase ein, in der über den Umgang mit der gescheiterten Annahme des Verfassungsvertrags diskutiert wurde. Zentrale Diskussionspunkte bildeten „institutionelle Fragen wie die Sitzverteilung im Europäischen Parlament […] und die Zusammensetzung der Kommission […]. Zu den nichtinstitutionellen Fragen gehörten die Einbindung der Charta der Grundrechte […], die Gemeinsame Außen- und Sicherheitspolitik […], die Unionsbürgerschaft […] sowie die Symbole der Union […]. Eine bis zuletzt umstrittene Frage bildete die Definition der qualifizierten Mehrheit im Europäischen Rat und im Ministerrat […]." (Hellmann 2009, 11) In der Nacht zum 19. Oktober 2007 konnten sich die Staats- und Regierungschefs der Mitgliedstaaten schließlich auf einen Kompromiss einigen (ebd., 11), dessen endgültige Fassung von diesen am 13. Dezember 2007 als „Vertrag von Lissabon" unterzeichnet wurde. Der ursprüngliche Zeitplan, wonach der Lissabonner Vertrag am 1. Januar 2009 in Kraft treten sollte, konnte aufgrund des gescheiterten irischen Referendums im Juni 2008 allerdings nicht eingehalten werden. Nachdem Irland vertragliche Zugeständnisse[239] gemacht wurden und die irische Bevölkerung den abgeänderten Vertrag in einem Folgereferendum mit ca. 67 % der Stimmen befürwortet

239 So etwa die Hervorhebung der nationalen Souveränität in Steuerfragen und die Beibehaltung des bisherigen Prinzips, dass jedes Land ein eigenes Kommissionsmitglied stellt, das ursprünglich zum Zwecke der effektiveren Regierbarkeit aufgrund der Größe der Union eingeschränkt werden sollte (Hellmann 2009, 44).

hatte, trat der Vertrag von Lissabon schließlich zum 1. Dezember 2009 in Kraft (Leisse 2010, 389).

Mit dem Vertrag von Lissabon verzichteten die Mitgliedstaaten auf ihr ursprüngliches Ziel der Ersetzung der geltenden Verträge durch einen einzelnen, neuen Verfassungsvertrag. Stattdessen kehrten sie zur alten Formel der Reform der geltenden Verträge zurück, weswegen der Vertrag von Lissabon auch als *Reformvertrag* bezeichnet wird.[240] Abgesehen davon wurden allerdings die wesentlichen Bestimmungen des Verfassungsvertrags übernommen. Diese betrafen einerseits institutionelle Fragen, etwa die Zusammensetzung der EU-Organe, die Spezifika für Mehrheitsentscheidungen im Ministerrat oder die Auflösung der Säulenstruktur der EU, und andererseits nicht-institutionelle Fragen wie die Kompetenzabgrenzung, die Grundrechtecharta, den Beitritt der Union zur Europäischen Menschenrechtskonvention, die gemeinsame Sicherheits- und Verteidigungspolitik oder auch die Regelungen zum Beitritt zur bzw. zum Austritt aus der Union (Hellmann 2009, 12 ff.).

Im Folgenden möchte ich auf die für die vorliegende Arbeit zentralen Aspekte in Gestalt der Grundrechtecharta, die institutionellen Neuerungen in Bezug auf das Europäische Parlament, die Spezifika für Mehrheitsentscheidungen im Ministerrat sowie die Auflösung der Säulenstruktur der EU näher eingehen.

3.4.1.2.2 Inkrafttreten der Grundrechtecharta

Infolge des Vertrags von Lissabon bilden seither der Vertrag über die Europäische Union (EUV) und der Vertrag zur Gründung der Europäischen Gemeinschaft (EGV), der mit dem Lissaboner Vertrag in „Vertrag über die Arbeitsweise der Europäischen Union" (AEUV) umbenannt wurde, die primärrechtlichen Grundlagen der Europäischen Union. Nachdem die im Verfassungsvertrag vorgesehene direkte Einbindung der Grundrechtecharta als Teil II des Vertrages gescheitert war, sah der Vertrag von Lissabon zwar keine direkte Einbettung der Charta in die Verträge vor, setzte diese allerdings dem EU-Primärrecht durch einen Verweis in Art. 6 EUV gleich. Abs. 2 des Artikels 6 EUV sah den Beitritt der Europäischen Union zur

240 Zudem wurde im Rahmen des Vertrags von Lissabon u. a. auf die formelle Einführung staatstypischer Symbole (z. B. eine Europaflagge, Europahymne, Europatag), die Verkleinerung der Kommission und die wörtliche Übernahme der GRCh verzichtet (Hellmann 2009, 12 ff.).

Europäischen Menschenrechtskonvention vor und der dritte Absatz nahm wiederum Bezug auf die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten: „Artikel 6 normiert somit eine dreifache Säule des Grundrechtsschutzes in der Union. Die in der Charta aufgeführten Grundrechte, die Menschenrechte der Europäischen Menschenrechtskonvention und die – künftig weiterhin geltenden – richterrechtlich entwickelten europäischen Grundrechte bilden ein dichtes, wohl lückenloses Netz, das hinreichenden Rechtsschutz gegen die Hoheitsakte der Europäischen Union ermöglicht." (Borowsky 2010, 154) Dies sollte weitreichende Konsequenzen für die Datenschutzpolitik der EU haben, da die Grundrechtecharta dadurch rechtswirksamen, bindenden Charakter erhielt. Zusammen betrachtet mit dem Beitritt der Union zur EMRK wurden die allgemeinen Prinzipien des Unionsrechts fortan mittels der Grundrechtecharta und der EMRK konstituiert. In der politischen Praxis bedeutete diese Verschiebung, dass die Achtung des Privatlebens gemäß Art. 8 EMRK und Art. 7 GRCh sowie der Schutz personenbezogener Daten nach Art. 8 GRCh in legislativen Abwägungsprozessen nunmehr ausdrücklich berücksichtigt werden mussten (Tinnefeld 2009, 504).

3.4.1.2.3 Institutionelle Neuerungen in Folge des Vertrags von Lissabon

Eine weitere Neuerung des Reformvertrags war die Neuregelung der Strukturen der EU sowie der Kompetenzen und Funktionsweisen ihrer Organe. So sah Art. 14 EUV eine deutliche Aufwertung der Stellung des Europäischen Parlaments und dessen weitgehende Gleichstellung gegenüber dem Ministerrat vor. Durch die Überführung des Mitentscheidungsverfahrens zum neuen ordentlichen Gesetzgebungsverfahren wurde zudem vorgesehen, dass die EU-Gesetze fortan von Parlament und Rat gemeinsam und gleichberechtigt entschieden werden sollten. Die Bedeutung dieser Regelung wurde zudem insbesondere durch die Auflösung der Säulenstruktur der EU verstärkt, sodass fortan 95 % der EU-Gesetze von Parlament und Rat gemeinsam entschieden werden sollten.[241] Bedeutsam ist dies vor dem Hintergrund der Schilderungen in Unterabschnitt 3.3.4.2 zur Richtlinie

241 Bis zum Inkrafttreten des Vertrags von Lissabon basierte das politische System der EU auf den drei Säulen: 1. den Europäische Gemeinschaften (Euratom und Europäische Gemeinschaft), 2. der Gemeinsamen Außen- und Sicherheitspolitik (GASP) und 3. der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (PJZS). Mit dem Vertrag von Lissabon wurde die Unterscheidung zwischen supranationa-

zur Vorratsdatenspeicherung, während deren Aushandlung der Ministerrat dem Parlament stets mit dem Entzug seiner Mitwirkungsrechte durch das Umschwenken zum Instrument des Rahmenbeschlusses gedroht hatte. Nach dem Vertrag von Lissabon mussten nunmehr auch jene Gesetze von Parlament und Rat gemeinsam entschieden werden, die die ehemalige dritte Säule betreffen, sodass eine Übergehung des Parlaments nicht mehr möglich war.

3.4.1.3 Das Stockholmer Programm

Das Inkrafttreten des Lissabon-Vertrags ebnete zwar den grundsätzlichen Weg zu einer Reform des Datenschutzrechts auf Grundlage insb. der Vorgaben der EU-Grundrechtecharta. Der typische Weg des EU-Agenda-Settings sah allerdings vor, dass die Kommission nicht einfach einen entsprechenden Legislativvorschlag vorlegt, sondern, dass die entsprechende Legislativmaßnahme zunächst in einen politischen Maßnahmenkontext eingebettet wird, in dem Zielvorgaben gemacht werden. Aufgrund der Bedeutung des Datenschutzes für die PJZS wurden die Materie daher im Rahmen des nächsten Mehrjahresprogramms der Union diskutiert. Der folgende Unterabschnitt widmet sich der Entstehung dieses neuen Mehrjahresprogramms, das den Namen Stockholmer Programm erhalten sollte und das im Rahmen der unionspolitischen Zielvorgaben für die Jahre 2010 bis 2014 auch die Reform des EU-Datenschutzrahmens vorsah. Die Grundlage für das Stockholmer Programm bildeten die Abschlussberichte zweier informeller Arbeitsgruppen, deren Ergebnisse im Folgenden zunächst vorgestellt werden.

3.4.1.3.1 Empfehlungen der Zukunftsgruppe Inneres

Bereits im Jahr 2007 hatte der Ministerrat für Justiz und Inneres zunächst auf einer informellen Sitzung zwischen dem 14. und 16. Januar in Dresden und später am 14. Februar 2007 auf seiner formellen Sitzung den Vorschlag des damaligen deutschen Innenministers und Ratsvorsitzenden Wolfgang Schäuble sowie des Kommissionsvizepräsidenten und Justiz- und Innen-

lem Gemeinschaftsrecht (Binnenmarkt) und intergouvernementalem Unionsrechts (PJZS) aufgehoben (Tinnefeld 2009, 504).

kommissars Franco Frattini aufgegriffen, eine hochrangige Beratungsgruppe zur Zukunft der europäischen Innenpolitik einzuberufen. Der Gruppe sollten ein Mitglied der Kommission, Franco Frattini, sowie die für Innenpolitik zuständigen nationalen Minister des amtierenden (Deutschland, Portugal, Slowenien) und folgenden Dreiervorsitzes (Frankreich, die Tschechische Republik, Schweden) sowie im Rotationsverfahren ein Mitglied des darauffolgenden Ratsvorsitzes (Spanien, Belgien und Ungarn) angehören. Ein Vertreter des LIBE-Ausschusses, der für Justiz und Inneres zuständige Generalsekretär des Ministerrats sowie ein Vertreter der mit *common law* regierten Mitgliedstaaten sollten als Beobachter partizipieren. Der Vorsitz der Gruppe sollte schließlich zwischen dem Kommissionsvertreter und dem amtierenden Ratsvorsitzenden rotieren (The Future Group 2008, 13, Nr. 8). Die Gruppe erhielt den Beinamen Zukunftsgruppe und wurde vor dem Hintergrund des möglichen Scheiterns auch des Lissabon-Vertrags mit der Erarbeitung eines Konsenses im Bereich der EU-Innenpolitik beauftragt (Monroy 2009b). Von zivilgesellschaftlicher Seite erntete der im Juni 2008 veröffentlichte Abschlussbericht der Zukunftsgruppe massive Kritik. Statewatch äußerte insbesondere große Besorgnis im Hinblick auf die weitere Ausweitung der EU-weiten Überwachungs- und Datensammlungspraktiken sowie die geplante Ausweitung der Zusammenarbeit mit den Vereinigten Staaten auf dem Gebiet der Überwachung. Angesichts der Dominanz von Mitte-Rechts- und Rechtsaußen-Positionen im Ministerrat und im Europäischen Rat wurden die in den Dokumenten der Zukunftsgruppe geäußerten Beteuerungen im Hinblick auf die Herstellung einer Balance zwischen Sicherheit und Freiheit angezweifelt (Bunyan 2008, 59). Konkret lautete der Vorwurf, dass zwar einer Balance das Wort gesprochen werde, jeder praktische Vorschlag der Zukunftsgruppe jedoch vielmehr die Intensivierung der Sammlung und des Austauschs von Bewegungs- und Telekommunikationsdaten und von Fingerabdrücken vorsehe, während ausgleichende Datenschutzmaßnahmen nicht angesprochen oder nur vage skizziert würden.[242] Bemerkenswert ist insbesondere ein Kommentar Franco Frattinis. Auf der ersten Sitzung der Zukunftsgruppe hatte dieser die folgende Aussage getätigt: „Finding a new balance between the right to

242 So wurde im Kapitel zu „Public security, privacy and technology" zwar erwähnt: „In order to achieve a sufficient level of protection, „privacy-enhancing technologies" are absolutely essential to guarantee civil and political rights in the age of cyberspace." (The Future Group 2008, 43, Nr. 132) Zur konkreten Umsetzung äußert sich das Papier hingegen mit keinem Wort.

security and the protection of fundamental rights is another main challenge for policy-makers. There is a need to overcome the traditional dogma of seeing *collective security* and *individual freedom* as two opposed concepts which exclude each other. Individual rights can only flourish in an atmosphere of collective security." (The Future Group 2007, 3, Hervorhebungen in kursiv: M. K.) Die Aussage, dass die in Sicherheitsdebatten häufig geäußerte Trade-off-Mentalität überwunden werden müsse, wurde allerdings auf die Weise ausgelegt, dass ein mehr an kollektiver Sicherheit erst die Grundlage für die Auslebung individueller Rechte schaffen würde – was freilich weder zu einer Überwindung der Diskrepanz führen würde, noch für eine Balance sprach, sondern die Bedeutung der Sicherheit klar über die Bedeutung von Freiheit stellte.[243] Zudem rahmte Frattini Sicherheit als kollektive Angelegenheit (*collective security*), Freiheit hingegen als Sache des Individuums (*individual freedom*).

3.4.1.3.2 Empfehlungen der Zukunftsgruppe Justiz

Ebenfalls im Jahr 2007 wurde auch die *Hochrangige Beratende Gruppe zur Zukunft der Europäischen Justizpolitik* ins Leben gerufen. Das Ziel der Gruppe war es, Vorschläge für das künftige EU-Programm im Bereich der EU-Justizpolitik zu unterbreiten. Die Mitgliedschaft der Gruppe war vergleichbar jener der Zukunftsgruppe Innenpolitik: Ihr gehörten die nationalen Justizminister des amtierenden (Deutschland, Portugal, Slowenien) und folgenden Dreiervorsitzes (Frankreich, die Tschechische Republik, Schweden) sowie im Rotationsverfahren ein Mitglied des darauffolgenden Ratsvorsitzes (Spanien, Belgien und Ungarn) an. Daneben partizipierten Vertreter des Europäischen Parlaments, insb. Mitglieder des LIBE-Ausschusses und des Rechtsausschusses sowie Irland als Vertreter der mit *common law* regierten Mitgliedstaaten an den Sitzungen der Zukunftsgruppe Justiz. Geleitet wurde die Gruppe vom amtierenden Vorsitz des Ministerrats gemeinsam mit dem Vizepräsidenten der Europäischen Kommission (Hochrangige Beratende Gruppe zur Zukunft der Europäischen Justizpolitik 2008, 5).

243 Es sei daran erinnert, dass Datenschutzbefürworter im Kontext der Balance-Debatten stets darauf hinweisen, dass es einen Kernbereich von Grundrechten gäbe, der solchen Abwägungsprozessen nicht unterworfen werden dürfe und die Gewährleistung von Sicherheit auch ohne die Einschränkung von Grundrechten möglich sei (Bendrath 2009).

Die Gruppe nahm ihre Arbeit im September 2007 auf und legte ihren Abschlussbericht im Juni 2008 vor (ebd., 6).

Wie von den mit Justiz befassten Ministern bzw. ihren Mitarbeitern zu erwarten war, legte die Zukunftsgruppe Justiz deutlich mehr Wert auf ein hohes Schutzniveau: Der Schutz personenbezogener Daten und das Recht auf Privatleben wurden in dem Dokument als eine Grundsatzfrage demokratischer Gesellschaften bezeichnet und auch das voraussichtliche baldige Inkrafttreten des Lissaboner Vertrags und die damit einhergehende Anwendbarkeit der Grundrechtecharta erwähnt. Der Schutz personenbezogener Daten sei angesichts informationstechnologischer Entwicklungen bedroht, da zunehmend mehr personenbezogene Daten verarbeitet würden, die *die Merkmale, Gewohnheiten oder ein einmaliges Verhalten von Personen offenbarten* und sich zeitlich fast unbegrenzt speichern und mit anderen Datenbanken abgleichen ließen (ebd., 28). Insbesondere wurden die Verarbeitung personenbezogener Daten für andere Zwecke als denjenigen, für den sie erfasst worden waren, sowie der unbegrenzte Abgleich mit anderen Datenbanken bemängelt. In diesem Kontext stellte die Gruppe zudem klar, dass die daraus resultierenden Gefahren nicht nur für den Einzelnen, sondern für die Gesellschaft insgesamt bedrohlich seien. Zudem vertrat die Zukunftsgruppe Justiz die Ansicht, dass eine Unterschreitung des hohen Datenschutzniveaus, insbesondere im Falle terroristischer Bedrohungen und von Großkriminalität, angemessen sei. Demgegenüber forderten Innenpolitiker regelmäßig die Ausweitung umfangreicher Datenverarbeitungen auch auf kleinere Delikte. Zugleich stellten die Justizminister aber klar, dass „das Recht auf Privatsphäre, einschließlich des speziellen Bereichs des Datenschutzes, […] nicht den Notwendigkeiten der Strafverfolgung geopfert werden [sollte]." (ebd., 30) Die sich aus der Europaratskonvention 108, der DS-RL sowie aus dem JI-Rahmenbeschluss ableitenden Grundprinzipien des Datenschutzes dürften auch angesichts der „Notwendigkeit, der globalen Bedrohung durch den Terrorismus und das organisierte Verbrechen zu begegnen, nicht aus der Rechtsordnung ausgeschlossen werden." (ebd.) Denn: „Ein angemessener Ausgleich zwischen den Rechten bedeutet nicht, dass der Rechtsschutz unter bestimmten gesetzlich definierten Umständen völlig fallen gelassen werden kann." (ebd.) Daher formulierte die Zukunftsgruppe Justiz fünf zentrale Anforderungen, die an einen wirksamen Datenschutz im Sicherheitsbereich gestellt werden müssten:

- „Datenschutzregeln sind für jeden speziellen Bereich erforderlich.
- Datenschutzregeln müssen angemessen und möglichst genau formuliert sein. Insbesondere müssen diese Vorschriften die spezielle Eingriffsintensität in die Grundrechte bei der Datenerhebung und Datenverwendung für Strafverfolgungszwecke angemessen berücksichtigen.
- Darüber hinaus ist stets sicherzustellen, dass die Betroffenen ein wirksames Recht auf Auskunft, Berichtigung, Löschung, Sperrung und Entschädigung haben.
- Es muss eine unabhängige Datenschutzaufsichtsbehörde mit angemessener Personal- und Sachmittelausstattung sowie wirksamen Befugnissen geben.
- Schließlich müssen die personenbezogenen Daten wirksam geschützt werden, um unbefugten Zugang und Nutzung durch Dritte zu verhindern.“ (ebd., 29)

3.4.1.3.3 Kommissionsentwurf

Am 10. Juni 2009 veröffentlichte die Europäische Kommission schließlich ihren Entwurf für das nächste Mehrjahresprogramm. Als zentrale Herausforderungen benannte die Kommission das Vorantreiben der Unionsbürgerschaft, Cyberkriminalität, Terrorismus, die Sicherung der EU-Außengrenzen, die Bekämpfung der „illegalen“ Einwanderung und die Vereinheitlichung der nationalen Asylsysteme (EC 2009a, 4 f.). Gerade im Bereich der innenpolitisch relevanten Themen basierten die Kommissionsvorschläge weitestgehend auf dem Abschlussbericht der Zukunftsgruppe Inneres und sahen eine Verschärfung sicherheitspolitischer Maßnahmen, insb. die weitere Verbesserung des Informationsaustauschs zwischen nationalen Sicherheitsbehörden, vor (ebd., 16 f.).

Zu Fragen des Datenschutzes äußerte sich die Kommission allerdings in deutlich stärkerer Anlehnung an den Abschlussbericht der Zukunftsgruppe Justiz. Unter Bezugnahme auf die Grundrechtecharta und vor dem Hintergrund der rasanten Entwicklungen auf dem Gebiet datenverarbeitender Technologien problematisierte die Kommission den wachsenden Austausch personenbezogener Daten. Die Kommission hob die Bedeutung der Verarbeitungsgrundsätze der Zweckbindung, Verhältnismäßigkeit und Rechtmäßigkeit der Verarbeitung, der zeitlich begrenzten Speicherung, Vertraulichkeit und Sicherheit der Daten, die Wahrung der Rechte des Einzelnen sowie die Beaufsichtigung durch eine unabhängige Stelle hervor und stellte die

Ausarbeitung zusätzlicher Maßnahmen zum Zwecke der Aufrechterhaltung der Grundsätze in Aussicht. Während im Haupttext offengelassen wurde, ob diese Maßnahmen legislativer oder sonstiger Art sein würden (ebd., 9), formulierte der Anhang eine konkretere Vorstellung in Richtung eines gemeinsamen legislativen Instruments, das für alle Politikbereiche der Union (also die dann ehemalige erste und dritte Säule) gelten sollte: „Die Union muss eine umfassende Regelung zum Schutz personenbezogener Daten schaffen, die für sämtliche Zuständigkeitsbereiche der Union gleichermaßen gilt." (ebd., 33) Mit diesem Vorschlag ging die Kommission zudem deutlich über die Vorschläge der Zukunftsgruppe Justiz hinaus. Darüber hinaus hob die Kommission die Bedeutung *datenschutzfreundlicher Technologien*, *internationaler Datenschutzstandards* und von *Informations- und Aufklärungskampagnen für die Bevölkerung*, insb. die am stärksten gefährdeten Personengruppen, hervor (ebd., 9). Im Hinblick auf die verbesserte Verbreitung datenschutzfreundlicher Technologien wurde vorgeschlagen, Produkte und Dienstleistungen eventuell mit einem europäischen Datenschutzprüfsiegel zu versehen, um deren Marktchancen zu erhöhen (ebd.).

3.4.1.3.4 Stellungnahme des Europäischen Datenschutzbeauftragten zum Kommissionsentwurf

Nachdem der EDSB bereits im Vorfeld der Veröffentlichung des Kommissionsentwurfs informell konsultiert worden war (EDSB 2009, 8, Nr. 2), nahm er am 10. Juli 2009 auch formell Stellung. In seiner Stellungnahme zeigte sich der EDSB erfreut darüber, dass die Kommission den Schutz der Grundrechte und insbesondere den Schutz personenbezogener Daten „als eine der zentralen Fragen für die Zukunft des Raums der Freiheit, der Sicherheit und des Rechts" (ebd., 10, Nr. 21) anerkannt und den Beitritt zur der EU zur EMRK zu einem Handlungsschwerpunkt erklärt habe. Insgesamt bescheinigte der EDSB dem Kommissionsentwurf, dass der „Notwendigkeit eines ausgewogenen Verhältnisses [zwischen Sicherheit und Freiheit], einschließlich der Notwendigkeit des Schutzes personenbezogener Daten, auf gute Weise Rechnung getragen [wird]" (ebd., 10, Nr. 23), weil der Entwurf praktisch auf die Erhöhung des bisherigen Schutzniveaus abziele. Entsprechend formulierte der EDSB dem Ministerrat gegenüber die Hoffnung, dass dieser dem Vorschlag der Kommission folge (ebd.).

Inhaltlich stellte der EDSB die mit dem Kommissionsentwurf verfolgte Verbesserung des Schutzniveaus als eine notwendige Folge der jahrelang praktizierten Ausweitung von sicherheitsorientierten Initiativen im Bereich des Raums der Freiheit, der Sicherheit und des Rechts dar (ebd., 10, Nr. 19). Im selben Zusammenhang wies der EDSB auch auf die gewachsene öffentliche Aufmerksamkeit im Hinblick auf Datenschutzfragen hin (ebd., 11, Nr. 26). Zwar fokussierte sich der EDSB stärker auf die mit dem voraussichtlichen Inkrafttreten des Vertrags von Lissabon geänderte rechtliche Situation als es die Kommission in ihrer Mitteilung tat (ebd., 10, Nr. 18), doch stellte der EDSB dem Kommissionsentwurf folgend klar, dass die von der Kommission vorgeschlagene *Schaffung einer umfassenden Regelung zum Datenschutz, die für sämtliche Zuständigkeitsbereiche der EU gleichermaßen* gelte, auch dann zu begrüßen sei, falls der Vertrag nicht in Kraft träte (ebd., 11, Nr. 27). Unabhängig davon, ob auf Grundlage des Vertrags von Lissabon ein einziger Rechtsrahmen oder mehrere Instrumente in Kraft träten, sei das dabei anzustrebende Ziel die Gewährleistung von Kohärenz, „nötigenfalls durch Harmonisierung und Konsolidierung der verschiedenen Rechtsakte, die für den Raum der Freiheit, der Sicherheit und des Rechts gelten." (ebd., 11, Nr. 28) Allerdings sei ein einzelnes Instrument insbesondere deshalb zu bevorzugen, weil „hierdurch in Zukunft die Schwierigkeiten vermieden [würden], die auftreten, wenn es darum geht, eine Trennungslinie zwischen den Säulen zu ziehen, wenn Daten, die im privaten Sektor zu Geschäftszwecken erhoben wurden, zu einem späteren Zeitpunkt für Strafverfolgungszwecke genutzt werden." (ebd., 12, Nr. 35) Insofern bekräftigte der EDSB die im Kommissionsentwurf genannte Schaffung einer umfassenden Regelung noch einmal und befürwortete insbesondere die Aufnahme der Überarbeitung des JI-Rahmenbeschlusses als einen Handlungsschwerpunkt in das Stockholmer Programm (ebd., 12, Nr. 36). Im Hinblick auf die Frage der Zweckbindung befürwortete der EDSB deren sorgfältige Abwägung und klare politische Regelung im Rahmen des Stockholmer Programms, sodass eine Abweichung in konkreten Einzelfällen und auf Basis eines politischen Konsenses möglich würde, es aber nicht regelmäßig den datenverarbeitenden staatlichen Stellen freigestellt wäre, darüber selbst zu entscheiden.[244] Den Vorschlag der Kommission hinsichtlich der Unterstützung datenschutzfreundlicher Technologien

244 Als Grundsatz formulierte der EDSB dazu: „Wenn immer derartige Maßnahmen vorgeschlagen werden, muss sehr eindeutig nachgewiesen werden können, dass eine derart in die Privatsphäre eingreifende Maßnahme erforderlich ist. Kann dieser

mittels der Schaffung eines Zertifizierungssystems für Hersteller und Nutzer von Informationssystemen griff der EDSB befürwortend auf, ergänzte diesen allerdings um die Forderung der Einführung „einer rechtlichen Verpflichtung für Hersteller und Nutzer von Informationssystemen, nur solche Systeme zu verwenden, die mit dem Grundsatz des ‚eingebauten Datenschutzes' vereinbar sind." (ebd., 19, Nr. 87) Schließlich unterstützte der EDSB auch die im Kommissionsentwurf genannten Elemente in Bezug auf den Datenaustausch mit Drittstaaten (ebd., 19 f., Nr. 88).

3.4.1.3.5 Ratsentwurf

Nach Bekanntgabe des Kommissionsentwurfs kommentierten die Mitgliedstaaten diesen und die amtierende schwedische Ratspräsidentschaft erarbeitete auf Basis der mitgliedstaatlichen Rückmeldungen einen neuen Entwurfstext, der am 16. Oktober 2009 veröffentlicht wurde (Ratsvorsitz 2009b). Entgegen dem Kommissionsentwurf, der den wachsenden Austausch personenbezogener Daten klar problematisierte, hob der Ratsentwurf auf „ein ausgewogenes Verhältnis zwischen dem Bedarf an einem zunehmenden Austausch personenbezogener Daten und einer größtmöglichen Achtung des Schutzes der Privatsphäre" (ebd., 10) ab. Zudem war die infolge des Inkrafttretens des Lissabonner Vertrags bzw. der Grundrechtecharta erforderlich gewordene Überarbeitung der Datenschutzregelungen der EU (der ersten und dritten Säule) etwas defensiver formuliert. Während die Kommission die Schaffung einer umfassenden Regelung für alle Datenschutzbereiche vorgesehen hatte, schlug der Rat lediglich vor, die Funktionsweise der geltenden Instrumente zunächst zu bewerten, um dann gegebenenfalls weitere legislative und nicht-legislative Initiativen vorzulegen (ebd.). Abgesehen davon wurden die übrigen Punkte des Kommissionsentwurfs übernommen: Auch der Ratsentwurf sprach sich für die Erhaltung und Bekräftigung der Grundprinzipien *wie Zweckgebundenheit, Verhältnismäßigkeit und Rechtmäßigkeit der Verarbeitung, zeitlich begrenzte Speicherung, Sicherheit und Vertraulichkeit*, für die *Aushandlung eines Abkommens mit den Vereinigten Staaten*, die *Ausarbeitung eines Rechtsinstruments mit Datenschutz-Grundsätzen für die Weitergabe von Daten, die sich in privatem Besitz befinden, an Drittstaaten zu Strafverfolgungszwecken*, die *Prü-*

Nachweis geführt werden, so muss sichergestellt werden, dass die Rechte des Einzelnen uneingeschränkt gewahrt werden." (ebd., 16, Nr. 64)

fung der Einführung eines europäischen Prüfsiegels für „datenschutzfreundliche" Technologien, Produkte und Dienstleistung und für *Informationskampagnen insbesondere zur Sensibilisierung der Öffentlichkeit* aus (ebd., 10 f.). Zudem übernahm der Ratsentwurf auch weitestgehend den Kommissionsvorschlag, wonach die Europäische Union bei der Entwicklung und Förderung internationaler Standards im Bereich des Datenschutzes und beim Abschluss geeigneter bilateraler oder multilateraler Instrumente als treibende Kraft fungieren solle (ebd., 11).

3.4.1.3.6 Parlamentsposition

Auf Seiten des Parlaments waren der Rechtsausschuss (Berichterstatter: Luigi Berlinguer (Italien, sozialdemokratisch/linksliberal/christlich-soziale Partito Democratico/S&D)), der LIBE-Ausschuss (Berichterstatter: Juan Fernando López Aguilar[245] (Spanien, sozialdemokratische PSOE/S&D)) sowie der Ausschuss für konstitutionelle Fragen (Berichterstatter: Carlo Casini (Italien, christdemokratische UDC/EVP)) mit den Entwürfen der Kommission und des Ministerrats befasst (Berlinguer, López Aguilar, und Casini 2009). Der Entschließungsantrag des Parlaments wurde am 25. November 2009 mit der Stimmenmehrheit von ALDE, EVP, SDE sowie mit Hilfe einiger grüner Stimmen mit 487 Für-Stimmen – bei 122 Gegenstimmen von EKR, EFD, GUE/NGL, NI und einigen wenigen Abgeordneten der Grünen und 49 Enthaltungen durch vor allem grüne Europaabgeordnete – angenommen (EP 2009e, 104 f., 2009d, 15). Die Grünen gaben als Grund für ihre Wahlentscheidung weniger inhaltliche als prozedurale Bedenken an: Das Ausschussverfahren, das zur Erarbeitung der Entschließung geführt habe, sei *in hohem Maße intransparent und teils chaotisch* gewesen. Zudem seien die kleinen Fraktionen gezielt von der Erarbeitung der Entschließung weitestgehend ausgeschlossen worden (Jan Philipp Albrecht, in: EP 2009f). Die GUE/NGL begründete ihre Wahlentscheidung mit der generellen Ablehnung des „volksfeindlichen" Stockholmer Programms: „Der Raum der Freiheit, der Sicherheit und des Rechts der EU und die Programme zu dessen Umsetzung dienen nicht den Interessen der Menschen; sie bilden im Gegenteil einen Maßnahmenkatalog, der individuelle und

245 López Aguilar, der zwischen 2004 und 2007 in der Regierung Zapatero das Amt des Justizministers innehatte, war im Juli 2009 zum Vorsitzenden des LIBE-Ausschusses gewählt worden. Das Amt hatte er bis Ende Juni 2014 und damit noch während der DSGVO-Verhandlungen inne (EP 2020c).

soziale Rechte und demokratische Freiheiten erstickt und Autoritarismus und Repression zu Lasten von Arbeitern, Einwanderern und Flüchtlingen intensiviert, das politische System und die Herrschaft von Monopolen aufrecht erhält und darauf abzielt, Arbeiter- und Volksbewegungen zu zerschlagen, was die Voraussetzungen für den brutalen Angriff des Kapitals auf Arbeitnehmerrechte und soziale Rechte der Arbeiterklassen und des Volkes schafft." (Charalampos Angourakis, in: EP 2009g) Von der EKR wurden Elemente des Stockholmer Programms, wie „die Zusammenarbeit und Solidarität in den Bereichen Polizei, Bekämpfung von grenzüberschreitender Kriminalität und Korruption, Schutz der Grundrechte und das Erzielen von Lösungen in Einwanderungsfragen durch die Unterstützung der Länder in Südeuropa, die sich großen Einwanderungsproblemen gegenübersehen," (Timothy Kirkhope, in: EP 2009g) zwar begrüßt, das Stockholmer Programm als Ganzes jedoch trotzdem abgelehnt, da mit ihm zu viel Entscheidungsmacht in strafrechtlichen und asylpolitischen Belangen an die EU-Ebene übertragen werde (ebd.). In ähnlicher Weise kritisierten auch die beiden rechtsgerichteten fraktionslosen Abgeordneten Philip Claeys (Vlaams Belang, Belgien) und Bruno Gollnisch (Front National, Frankreich) die Machtverlagerung auf die Unionsebene (ebd.).

Im Entschließungsantrag bekräftigte das Parlament vor allem die von der Kommission angeführten Erwägungsgründe und datenschutzpolitischen Vorschläge, ging in einzelnen Bereichen allerdings noch weiter als die Kommission. So teilte das Parlament die Besorgnis der Kommission hinsichtlich der Zunahme der Verarbeitung personenbezogener Daten, konkretisierte die schriftlichen Äußerungen der Kommission allerdings um mehrere spezifische Probleme: Zum einen wurde als konkreter Grund für die Zunahme von Datenschutzproblemen auf die wachsende Bedeutung des Internets und grenzüberschreitender Datenverarbeitungen verwiesen. Darauf aufbauend wurde argumentiert, dass diese Entwicklungen die Verabschiedung weltumspannender Datenschutzstandards erforderlich machten (EP 2009f, Nr. 82). Zudem machte das Parlament klar, dass die Datenschutzvorschriften in einem etwaigen Drittstaat, in den personenbezogene Daten von EU-Bürgerinnen und -Bürgern übertragen werden sollten, den europäischen Vorschriften entsprechen müssten (ebd., Nr. 89). Daneben wurde auf die bei der weiteren Umsetzung des Grundsatzes der Verfügbarkeit anhaltende Gefahr verwiesen, auch solche personenbezogenen Daten intensiviert auszutauschen, die nicht rechtmäßig erhoben worden seien (ebd., Nr. 86). Auch die zunehmende Verbreitung der Praxis der Erstellung von Persönlichkeitsprofilen im Kontext von *data-mining*-Technologien und der

Vorratsdatenspeicherung für präventive und polizeiliche Zwecke wurden problematisiert (ebd., Nr. 88).

In Bezug auf die von Kommission und Rat hervorgehobene Bedeutung datenschutzfreundlicher Technologien drückte das Parlament lediglich aus, dass dieser Schritt begrüßt werde, schlug allerdings keine praktischen Umsetzungsschritte (etwa in Bezug auf Datenschutz-Gütesiegel bzw. Zertifizierungen) vor (ebd., Nr. 91). Deutlich umfangreicher widmete sich das Parlament hingegen dem von Kommission und Rat nicht erwähnten Prinzip des eingebauten Datenschutzes („privacy by design"), das „wesentlicher Bestandteil jeder Entwicklung sein muss, bei der die Sicherheit personenbezogener Daten sowie das Vertrauen in diejenigen und die Glaubwürdigkeit derjenigen, die über solche Daten verfügen, gefährdet werden könnten" (ebd., Nr. 85).

Schließlich forderte auch das Parlament „eine gründliche Evaluierung aller einschlägigen Rechtsvorschriften (betreffend u. a. Terrorismusbekämpfung, polizeiliche und justizielle Zusammenarbeit, Einwanderung, transatlantische Abkommen) im Bereich des Schutzes der Privatsphäre und des Datenschutzes" (ebd., Nr. 90) und forderte mehrfach die Einführung einer allumfassenden einheitlichen Regelung zum Schutz personenbezogener Daten in der Europäischen Union (ebd., Nr. 83, 146). Im Hinblick auf das bevorstehende Inkrafttreten des Vertrags von Lissabon kritisierte das Parlament die Kommission und den Rat dahingehend, dass dieser in Kraft treten werde, „ohne dass Rat und Kommission die notwendigen Maßnahmen für einen ‚Neubeginn' im Raum der Freiheit, der Sicherheit und des Rechts angemessen vorbereitet haben" (ebd., Nr. 148). Daher forderte das Parlament die Kommission dazu auf, einen Legislativvorschlag „zur Umsetzung von Artikel 16 AEUV und Artikel 39 EUV, insbesondere im Hinblick auf den Datenschutz bei Fragen der Sicherheit und gleichzeitig zur Ausweitung des Anwendungsbereichs der Verordnung (EG) Nr. 45/2001 im Hinblick auf den Datenschutz durch die Organe der Europäischen Union" (ebd.) zu unterbreiten.

3.4.1.3.7 Das finale Stockholmer Programm

Während der Monate Oktober und November setzte sich der Ministerrat auf weiteren Sitzungen mit dem Stockholmer Programm auseinander, nahm weitere Änderungen vor (Ratsvorsitz 2009a, 1) und entschied schließlich auf der JI-Ratssitzung vom 30. November über den finalen Ent-

wurf. Dieser wurde an den Europäischen Rat weitergeleitet, der das Stockholmer Programm schließlich auf seiner Sitzung vom 10. und 11. Dezember 2009 verabschiedete (Europäischer Rat 2009, 1).

Vor dem Eindruck des gescheiterten Verfassungsvertrags und des wachsenden Misstrauens (Piquer 2014) in die Europäische Union und ihre Institutionen war das Stockholmer Programm in besonderem Maße darum bemüht, die Bedeutung des Dokuments für die Bürgerinnen und Bürger der EU herauszustellen. Die Herausforderungen, denen sich die Union aus der Perspektive des Europäischen Rats gegenübersah, fanden sich nunmehr im Abschnitt „politische Prioritäten". Als solche wurden benannt: *Förderung der Unionsbürgerschaft und der Grundrechte*; *Europa als Raum des Rechts und der Justiz*; *ein Europa, das schützt*; *Zugang zu Europa in einer globalisierten Welt*; e*in Europa der Verantwortung, der Solidarität und der Partnerschaft in Migrations- und Asylfragen*; sowie *die Rolle Europas in der globalisierten Welt*. Somit knüpfte das Stockholmer Programm zwar an den bereits in den Vorläufer-Programmen vorhandenen Fokus auf die Einrichtung einer einheitlichen europäischen Sicherheitsarchitektur an und intensivierte diese Pläne weiter, doch zugleich räumte es erstmals grundrechtlichen Fragen einen zentralen Platz ein. Bereits unter dem Punkt „Förderung der Unionsbürgerschaft und der Grundrechte" wurde die herausgehobene Stellung deutlich, die dem Datenschutz im Rahmen des Stockholmer Programms zuerkannt wurde: „Die Achtung der menschlichen Person und ihrer Würde sowie der übrigen in der Grundrechtecharta der Europäischen Union und der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten verankerten Rechte zählen zu den zentralen Werten. Dazu gehören die Wahrung der persönlichen Rechte und Freiheiten, insbesondere der Privatsphäre, über Staatsgrenzen hinweg, vor allem durch den Schutz personenbezogener Daten." (Europäischer Rat 2010, 4, Nr. 1.1)

Detailliert wurde auf das Thema Datenschutz schließlich im Kapitel 2.5 „Schutz der Rechte der Bürger in der Informationsgesellschaft" eingegangen. Unter Bezugnahme auf die Grundrechtecharta wurde dargelegt, dass die Union „dem zunehmenden Austausch personenbezogener Daten und dem Erfordernis der Sicherstellung des Schutzes der Privatsphäre Rechnung tragen [müsse]." (ebd., 10, Nr. 2.5) Auf das kurz zuvor am 1. Dezember 2009 erfolgte Inkrafttreten des Vertrags von Lissabon wurde bereits in der Einleitung positiv Bezug genommen (ebd., 4, Nr. 1). Die Forderung des Parlaments und des EDSB nach einer umfassenden Strategie zum Datenschutz innerhalb der EU wurde übernommen, ebenso wie die Forderung

nach dem Beitritt der Union zur Datenschutzkonvention des Europarats. Übernommen wurde auch die zur Reduktion (sicherheits-)behördlicher Willkür gestellte Forderung, dass die Union klare Bedingungen festlegen solle, „unter welchen Umständen ein Eingriff öffentlicher Stellen in die Ausübung" der Datenschutzrechte gerechtfertigt sei (ebd.). Entgegen den üblichen Formulierungen aus ähnlichen Dokumenten aus der nahen Vergangenheit wurde zudem die Aussage, dass die *Union der Notwendigkeit zu einem verstärkten Austausch personenbezogener Daten Rechnung tragen müsse*, um die Aussage ergänzt, dass *dabei gleichzeitig eine größtmögliche Achtung des Schutzes der Privatsphäre* sicherzustellen sei. Übernommen wurde auch die Forderung der Einhaltungen der Datenschutz-Grundprinzipien der *Zweckbindung*, *Verhältnismäßigkeit* und *Rechtmäßigkeit der Verarbeitung*, der *Speicherbegrenzung*, der *Sicherheit und Vertraulichkeit*, der *Achtung der Betroffenenrechte*, der *Kontrolle durch unabhängige nationale Aufsichtsbehörden* sowie des *Zugangs zu einem wirksamen Rechtsschutz* (ebd.). Als konkrete Maßnahmen, um deren Umsetzung der Europäische Rat die Kommission ersuchte, wurden genannt (ebd., 11):

- die Bewertung der Funktionsweise der verschiedenen Datenschutz-Rechtsinstrumente und ggf. die Vorlage legislativer und nicht-legislativer Initiativen;
- die Verbesserung der Einhaltung der Datenschutzgrundsätze durch die Entwicklung geeigneter datenschutzfreundlicher Technologien, indem die Zusammenarbeit zwischen privatem und öffentlichem Sektor, speziell im Bereich der Forschung, verbessert werde.
- die Prüfung der Einführung eines europäischen Prüfsiegels für datenschutzfreundliche Technologien, Produkte und Dienstleistungen;
- die Durchführung von Informationskampagnen, insbesondere zur Sensibilisierung der Öffentlichkeit;
- die Vorlage einer Empfehlung zur Aushandlung von Abkommen mit den Vereinigten Staaten über Datenschutz und Datenaustausch zu Zwecken der Strafverfolgung;
- die Prüfung der notwendigen Hauptelemente für Datenschutzabkommen mit Drittstaaten für Strafverfolgungszwecke, bei denen möglicherweise im Bereich des privaten Datenschutzrechts gesammelte personenbezogene Daten an Sicherheitsbehörden weitergereicht werden könnten.

In abgeschwächter Weise gegenüber der EDSB- und Parlamentsposition wurde die Forderung nach einer Entwicklung und Förderung internationaler Datenschutzstandards übernommen. Dieser Aussage wurde die ab-

schwächende Formulierung, wonach die Union „in einem allgemeineren Rahmen" als treibende Kraft fungieren müsse, hinzugefügt.

Nicht übernommen wurde hingegen die zentrale Forderung von Kommission, EDSB und Parlament nach der Einführung einer allumfassenden, einheitlichen Regelung zum Schutz personenbezogener Daten in der EU, welche die ehemalige erste und dritte Säule einschließen würde. In diesem Zusammenhang verwies der Europäische Rat lediglich auf die Überprüfung der bestehenden Rechtsinstrumente, legte sich aber weder im Hinblick auf deren Überarbeitung eindeutig fest noch äußerte es sich dahingehend, ob ein allgemeiner Rahmen für alle ehemaligen Säulen wünschenswert sei (Europäischer Rat 2010, 11, Nr. 2.5). Die Streichung dieses Passus' ist daher als Kompromiss gegenüber jenen Staaten zu interpretieren, die kein Interesse an einer umfassenden Regelung hatten.

3.4.1.3.8 Reaktionen auf das Stockholm-Programm

Sowohl vor als auch nach seiner Verabschiedung erntete das Stockholmer Programm massive Kritik seitens bürgerrechtspolitischer Akteure. So wurde bereits vor seiner Verabschiedung der Erarbeitungsprozess des Programms vonseiten des European Civil Liberties Network (ECLN)[246] im Hinblick auf die mangelnde Umsetzung demokratischer Diskursstandards kritisiert.[247] Weder habe man die europäische Öffentlichkeit in ausreichendem Maße[248] miteinbezogen, noch sei es vertretbar, dass die Letztentscheidung beim Rat allein liege, die nationalen Parlamente und das Europäische Parlament dagegen nur unverbindlich konsultiert würden (ECLN 2009, 1). Der Datenschutzrat – die österreichische Datenschutzaufsichtsbehörde – bemängelte Mitte Juli 2009 die Beibehaltung des Verfügbarkeitsgrundsatzes

246 Das ECLN war im Jahr 2005 unter anderem von Statewatch, der Bürgerrechte & Polizei/CILIP sowie vom Komitee für Grundrechte und Demokratie gegründet worden. Im Jahre 2009 hatte das ECLN mehr als 40 Unterstützerorganisationen (Monroy 2009a).

247 Für einen Überblick über die Kritiken an der Erarbeitungsweise der Programme von Tampere und Haag, siehe: (Bunyan 2008, 3–4). Für eine ausführlichere Analyse des Entscheidungsprozesses, der zum Programm von Tampere führte, siehe: (Bunyan 2003).

248 Tatsächlich hatte die Kommission im Herbst 2008 eine öffentliche Online-Konsultation initiiert. Allerdings konnten die vorgegebenen Fragen nur mittels Multiple Choice beantwortet werden, es konnten also keine eigenen Antworten – in anderen Worten: Keine eigene Meinung – eingebracht werden (Monroy 2009a).

bzw. die Förderung der Interoperabilität unterschiedlicher Datenbanken und brachte sein generelles Misstrauen gegenüber den angekündigten datenschutzpolitischen Maßnahmen zum Ausdruck (Monroy 2009a). Nicht glaubwürdig erschienen die bürgerrechtlichen Beteuerungen des Ministerrats allerdings auch den Europaabgeordneten, die den Prozess beobachteten. So wies die linksliberale niederländische Europaabgeordnete Sophie in 't Veld (ALDE/D66) darauf hin, dass die Ankündigung des Ministerrats „einen Bruch mit der [bisherigen] Tradition bedeuten würde und dass man – ausgehend von den Erfahrungen mit den Urteilen zu SWIFT, ACTA und CIA und der Einschätzung von aktuellen Anti-Terrorismusmethoden – davon ausgehen müsse, dass sich nicht viel verändert habe." (McNamee 2009)

Nach der Verabschiedung des Stockholm-Programms fokussierte sich die Kritik besonders auf die im Rahmen der Interoperabilität geplante Zusammenführung von polizeilichen Großdatenbanken, die weitere Intensivierung des Verfügbarkeitsgrundsatzes, die Nutzung der Daten zu für präventive Zwecke sowie die Einführung eines europäischen Systems zur Fluggastdatensammlung (Krempl 2009b, 2009a)

3.4.1.3.9 Umsetzung des Stockholm-Programms: Die formelle Geburt der Datenschutzreform

Nachdem das Stockholm-Programm verabschiedet worden war, war es an der Kommission, die auf höchster EU-Ebene beschlossenen politischen Leitlinien im Rahmen eines Aktionsplans zu konkretisieren. Am 20. April 2010 veröffentlichte die Europäische Kommission daher ihren „Aktionsplan zur Umsetzung des Stockholmer Programms" (EC 2010). Bereits in der Einleitung des Aktionsplans machte die Kommission auf die infolge des Inkrafttretens des Vertrags von Lissabon veränderten europapolitischen Bedingungen aufmerksam: „Mit der Aufwertung der Rolle des Europäischen Parlaments, das ab jetzt in den meisten Bereichen Mitgesetzgeber ist, und der engeren Einbeziehung der nationalen Parlamente unterliegt die EU in Bezug auf ihr Handeln im Interesse der Bürger künftig einer größeren Rechenschaftspflicht, wodurch auch die demokratische Legitimität der Union gestärkt wird. Die Abstimmung mit qualifizierter Mehrheit, die künftig für die meisten Politikbereiche gilt, wird die Beschlussfassung im Rat erleichtern. Nicht zuletzt wird auch die gerichtliche Kontrolle verbessert, da dem Europäischen Gerichtshof jetzt die gerichtliche Nachprüfung aller Aspekte

des Bereichs Freiheit, Sicherheit und Recht obliegt und die Grundrechtecharta der EU rechtsverbindlich wird." (ebd., 3)

Gleich im ersten inhaltlichen Kapitel widmete sich die Kommission dem Schutz der Grundrechte und bekannte sich wortgewaltig und unzweifelhaft zum Schutz dieser: „Der Schutz der in der Grundrechte-Charta verankerten Rechte muss uneingeschränkt gelten, und die Rechte müssen effektiv und konkret wirken. Die Grundrechte-Charta muss zur Richtschnur unseres Handelns werden. Verstöße gegen die Charta wird die Kommission unter keinen Umständen dulden." (ebd.) Wie angesichts der bisherigen, im Rahmen der Erarbeitung des Stockholm-Programms gezeigten, Haltung der Kommission zu erwarten war, legte sie großen Wert auf das Thema Datenschutz: „In einer globalen Gesellschaft, die durch raschen technologischen Wandel mit grenzenlosem Informationsaustausch geprägt ist, kommt der Sicherung der Privatsphäre größte Bedeutung zu. Die Union muss deshalb für eine konsequente Anwendung des Grundrechts auf Datenschutz sorgen. Wir müssen die Position der EU bezüglich des Schutzes personenbezogener Daten bei allen EU-Maßnahmen, einschließlich jener in den Bereichen Strafverfolgung und Kriminalprävention, sowie in unseren internationalen Beziehungen stärken." (ebd.)

Im Maßnahmenkapitel machte die Kommission dann auch ihre datenschutzpolitisch bedeutsamste Ankündigung. Für das Jahr 2010 wurde die Vorlage eines „neuen umfassenden Rechtsrahmens für den Datenschutz" angekündigt. Daneben wurde für dasselbe Jahr eine „Mitteilung über einen neuen Rechtsrahmen für den Schutz personenbezogener Daten nach Inkrafttreten des Vertrags von Lissabon", eine weitere „Mitteilung über Datenschutz und Vertrauen im ‚Digitalen Europa': Stärkung des Vertrauens der Bürger in neue Dienste" sowie eine „Empfehlung zur Aufnahme von Verhandlungen mit den Vereinigten Staaten von Amerika über ein Datenschutzabkommen für Strafverfolgungszwecke" in Aussicht gestellt. Eine „Mitteilung über Hauptelemente für Datenschutzabkommen zwischen der Europäischen Union und Drittstaaten für Strafverfolgungszwecke" wurde für das Jahr 2012 angekündigt. Zudem teilte die Kommission mit, dass *Maßnahmen zur Aufklärung über die Datenschutzrechte* in Arbeit seien (ebd., 72). Im Hinblick auf sicherheitsbehördliche Datenverarbeitungssysteme wurde deren gründliche Prüfung im Hinblick auf ihre *Zweckmäßigkeit, Effizienz, Wirkung, Verhältnismäßigkeit* sowie die *Achtung des Rechts auf Privatsphäre* angekündigt. Schließlich sei prioritär eine Bilanz der in den letzten Jahren eingeführten Anti-Terror-Maßnahmen zu ziehen und diese auf Verbesserungsmöglichkeiten hin zu prüfen (ebd., 6).

3.4.1.3.10 Zwischenfazit

Die Erarbeitung des Stockholmer Programms stellt eindrucksvoll einerseits die Versuche der EU zur Schau, sich hin zu einer stärker am Bürger ausgerichteten Politik zu orientieren und veranschaulicht andererseits die inneren Widersprüche im Institutionengefüge der EU. Ursächlich für die weitere Fokussierung der EU-Politik auf die Bürgerinnen und Bürger der Union war das sinkende Vertrauen der Bevölkerung in die Unionspolitiken insbesondere im Zuge der Finanzkrise 2007 und des letztlich gescheiterten Verfassungsvertrags. Beunruhigend für EU-Politikerinnen und -Politiker war aber auch das verzögerte Inkrafttreten des Vertrags von Lissabon. Obwohl die Mehrheit der EU-Bevölkerung weiterhin hinter den verabschiedeten Anti-Terror-Politiken stand, wuchs in der Bevölkerung angesichts der zunehmenden Verarbeitung ihrer personenbezogenen Daten seitens privater und staatlicher Stellen das Misstrauen an. Nachdem die Ausweitung von Anti-Terror-Maßnahmen über Jahre hinweg konstant vorangetrieben worden war und die während dieser Zeit vom Europäischen Parlament und anderen eher bürgerrechtlich orientierten Akteuren vertretenen Positionen ignoriert worden waren, hatte sich mit dem Stockholmer Programm und dem Inkrafttreten des Vertrags von Lissabon die Gelegenheit ergeben, die Prioritäten der Union in Richtung des Schutzes der Grundrechte zu verschieben. Während der Erarbeitungsphase des Stockholm-Programms traten noch einmal die unterschiedlichen Positionen der Unionsorgane im Hinblick auf den Umgang mit Fragen des Grundrechtsschutzes offen zu Tage: Der Ministerrat auf dem einen Ende des Spektrums mit Vorschlägen, die eher der Fortsetzung vorheriger sicherheitsorientierter Politiken entsprachen, aber erstmals auch mehr Raum für Datenschutzpolitiken ließen als noch zur Hochphase der Anti-Terror-Politik. Das Parlament auf dem anderen Ende der Skala als Vertreter bürgerrechtlicher Positionen, der unnachgiebig auf eine Politikwende drängt. Und schließlich die Kommission als Vermittlerin zwischen den Polen mit Neigungen zum Datenschutz.

Viel bemerkenswerter als die grundsätzlichen institutionellen Positionierungen sind am Erarbeitungsprozess des Stockholmer Programms allerdings die veränderten Nuancen: So hatte die für Justizfragen zuständige Zukunftsgruppe des Ministerrats vergleichsweise bürgerrechtsnahe Positionen vertreten und damit eine kleine Wende in der Ministerratspolitik bewirkt. Zeitgleich hatten sich die innerhalb der Kommission mit Grundrechts- bzw. Datenschutzfragen befassten Stellen dahingehend durchsetzen können, dass im Kommissionsentwurf eher die aus der Justizgruppe statt die

aus der Innenpolitik-Zukunftsgruppe stammenden datenschutzpolitischen Vorschläge aufgegriffen wurden. Nachdem die Bürgerrechtsorientierung der Kommission (insb. die Befürwortung der Vorlage eines neuen legislativen Rahmens für den Datenschutz) im finalen Stockholmer Programm noch einmal relativiert worden war, zeigte sich die Kommission im Gegensatz zu ihren früheren Rückziehern im Bereich der Datenschutzpolitik überraschenderweise unnachgiebig und nahm den Punkt in ihrem Aktionsplan wieder auf.

Diese Vorgehensweise der Kommission deckte sich auch mit der bereits begonnenen Konsultation zum EU-Datenschutzrahmen, die im Mai 2009 ihren Anfang genommen hatte. Auf die konkreten Reformschritte soll an späterer Stelle (vgl. 4) detailliert eingegangen werden.

3.4.1.4 Fazit und Auswirkungen auf die Datenschutzpolitik der EU

Mit dem Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 hatte ein *Wandel der grundlegenden verfassungsmäßigen Struktur* der EU stattgefunden. Der in der EU-Grundrechtecharta formulierte Schutz personenbezogener Daten war nicht mehr nur Teil des EU-Sekundärrechts, sondern nunmehr Teil des EU-Primärrechts, der zwingendermaßen gemäß den primärrechtlichen Vorgaben im Bereich des Sekundärrechts gewährleistet werden musste. Indem außerdem die Säulenstruktur der Union abgeschafft und das Parlament dem Ministerrat weitgehend gleichgestellt wurde, fand eine bedeutsame Änderung im *Grad der erforderlichen Zustimmung für wesentlichen politischen Wandel* und hinsichtlich der *relativen Offenheit des politischen Systems* der EU statt. Parlament und Ministerrat mussten künftig gem. Art. 16 Abs. 2 AEUV über die ehemalige erste und dritte Säule betreffende Datenschutzangelegenheiten auf Augenhöhe gemeinsam entscheiden. Problematischen Entscheidungen wie dem JI-Rahmenbeschluss, der nur deshalb eine Einigung auf dem kleinsten gemeinsamen Nenner darstellte, weil der Ministerrat einstimmig und ohne die formelle Beteiligung des Parlaments entscheiden musste, wurde mit den jüngsten Vertragsänderungen die Grundlage entzogen. Die zuvor seitens des Ministerrats praktizierte Strategie der Einforderung von Zugeständnissen vom Europäischen Parlament im Bereich von Politiken der ersten Säule konnte somit nicht mehr fortgeführt werden.

Die *Policy-Entscheidung aus einem anderen Subsystem* in Form des Stockholmer Programms beeinflusste die Reform des Datenschutzes ebenfalls, da sich die EU-Organe im Rahmen des Stockholmer Programms erst-

mals auf eine Datenschutzpolitik einigten, deren Eckpunkte auf einem bis dahin nicht da gewesenen Maß an interinstitutionellem Konsens aufbauten.

3.4.2 Weitere Faktoren: Veränderung sozioökonomischer Bedingungen und der öffentlichen Meinung

In etwa zur selben Zeit, in der der *Wandel der grundlegenden verfassungsmäßigen Struktur*, des *Grades der erforderlichen Zustimmung für wesentlichen politischen Wandel* als auch der *relativen Offenheit des politischen Systems* stattgefunden hatte, fand auch ein *Wandel in den sozioökonomischen Bedingungen* und *in der öffentlichen Meinung* statt, dessen Auswirkungen wichtig im Hinblick sowohl auf die Initiierung der Datenschutzreform als auch auf den politischen Aushandlungsprozess der DSGVO waren. Während die wirtschaftspolitisch motivierten Datenschutz-Gegner einerseits und die sicherheitspolitisch motivierten Datenschutz-Gegner andererseits an der Aushöhlung der datenschutzrechtlichen Grundlagen wirkten, formierte sich allmählich der Widerstand gegen die zunehmende Verarbeitung personenbezogener Daten zu Wirtschafts- und Sicherheitszwecken sowohl auf Ebene der politischen Entscheider als auch im Bereich der Zivilgesellschaft. Die folgenden Unterabschnitte widmen sich der Analyse der wichtigsten Eckpunkte dieser Entwicklung in Form der Zunahme von Datenschutzskandalen, des Wandels der öffentlichen Meinung, der Erstarkung des außerparlamentarischen Widerstands sowie in Gestalt des wachsenden Policy-Entrepreneurships für eine Stärkung des Datenschutzes insb. im Europäischen Parlament, aber auch in der Europäischen Kommission.

3.4.2.1 Zunahme von Datenschutzskandalen

Eine der wichtigsten Ursachen für die gesteigerte gesellschaftliche Sensibilität im Hinblick auf die Verarbeitung personenbezogener Daten stellte die Zunahme von Datenschutzskandalen dar. Die ersten großen Datenschutz-Skandale ereigneten sich bereits im Laufe der 1990er-Jahre (Culnan 1997; Siering 1999). In der breiten deutschen und europäischen Öffentlichkeit bekannt wurde das Thema Datenmissbrauch allerdings erst durch eine Reihe von öffentlichkeitswirksamen Skandalen seit der Mitte der 2000er-Jahre. Im Folgenden möchte ich auf einige der größten dieser Skandale eingehen.

Nachdem die Schwartz-Unternehmensgruppe bereits 2004 mit missbräuchlichem Verhalten gegenüber Mitarbeitern in Filialen des Tochter-Unternehmens Lidl aufgefallen war, kam 2008 heraus, dass Lidl-Mitarbeiterinnen und Mitarbeiter systematisch und sehr weitgehend per Videoüberwachung bespitzelt wurden (Ziegler 2008). Es folgten Skandale um illegalen Datenhandel, u. a. mit sensiblen personenbezogenen Daten aus den Datenbeständen der Deutschen Telekom und Bankkontendaten aus Datenbeständen der Südwestdeutschen Kassenlotterie (Krempl 2008b). Zudem wurde Mitte 2008 zunächst über die Deutsche Telekom (Balzli u. a. 2008) und Anfang 2009 über die Deutsche Bahn (Christ und Hildebrand 2009) bekannt, dass sie ihre Mitarbeiter ausspähten. Insbesondere die Telekom-Affäre zog große öffentliche Aufmerksamkeit auf sich, weil neben Mitarbeitern auch Aufsichtsräte, Gewerkschaftsfunktionäre, Betriebsratsangehörige und ein Vorstandsmitglied von der Überwachung betroffen waren (Schäfer 2010). Schließlich wurden im selben Zeitraum mehrere große Datenpannen bekannt: Darunter neben einer Datenpanne des deutschen Zolls (Regnery 2011) insbesondere der 2006 begangene Datendiebstahl an 17 Millionen Kundendaten von T-Mobile, der von der Deutschen Telekom fast zwei Jahre verheimlicht worden war (Murphy und dpa-AFX 2008).[249]

International aufsehenerregend war eine von Facebook Inc. im Jahr 2006 ins Leben gerufene Funktion, mit der die Freunde eines Facebook-Nutzenden sehr detailliert über dessen Aktivitäten auf Facebook informiert wurden (Westlake 2008). Trotz der Kritiken an dieser Praxis entschied sich der Konzern Ende 2009 dazu, die Standard-Einstellungen des Dienstes dahingehend zu ändern, dass Text-, Foto- und Videobeiträge der Nutzerinnen und Nutzer sowie Name, Profilfoto, die Liste der Freunde und Facebook-Seiten, denen man folgte, Geschlecht und regionale Zugehörigkeit nicht nur dem Freundeskreis, sondern standardmäßig sowohl allen anderen Facebook-Nutzerinnen und -Nutzern als auch Nicht-Nutzenden angezeigt wurden und sogar von Suchmaschinen indexiert werden konnten (Bahrke 2011, 45–47). Zudem ging Facebook im Jahr 2009 dazu über, die Daten der Nutzerinnen und Nutzer auch dann noch weiterzuverwenden, wenn diese von den Betroffenen selbst gelöscht oder das Konto deaktiviert worden war (Walters 2009). Eine weitere Änderung aus dem Jahr 2009

249 Die an dieser Stelle genannten Beispiele stellen freilich eine kleine, der deutschen Leserschaft bekannte, Auswahl an Datenpannen dar. International ereigneten sich seit der Jahrtausendwende dutzende vergleichbare Fälle. Für einen Überblick, siehe z. B.: (Wikipedia 2019b).

zeigte die Aktivitäten eines Facebook-Nutzers auf anderen Webseiten dessen Facebook-Freunden, sofern sich der Nutzer auf Facebook-Partnerseiten bewegte (McCarthy 2009).

Schließlich zogen mehrere im Vereinigten Königreich stattgefundene Datenverluste erhebliche Kritik auf sich und führten die mangelnde Sicherheit personenbezogener Daten im öffentlichen Bereich vor Augen: Im November 2007 kam zunächst heraus, dass die Daten von 25 Millionen Steuerzahlern abhandengekommen waren. Im Januar 2008 verschwand ein PC der britischen Streitkräfte, auf dem personenbezogene Daten von Rekruten gespeichert waren. Später verschwanden Daten über 80.000 Häftlinge und 33.000 Wiederholungstäter (Focus Online 2008). Schließlich kam im Oktober 2008 heraus, dass eine Festplatte des britischen Verteidigungsministeriums mit personenbezogenen Daten über 1,7 Millionen Rekruten verschwunden war. Unter den betroffenen Daten seien personenbezogene Daten über Angehörige, Pass- und Sozialversicherungsnummern, Führerschein- und Bankdaten sowie die Mitgliedsnummer beim National Health Service gewesen. Zudem gab das britische Verteidigungsministerium im Juli 2008 bekannt, dass im Laufe der vergangenen vier Jahre insgesamt 658 Laptops und 26 USB-Sticks verschwunden waren (BBC News 2008).

Anti-Terror-Maßnahmen

Neben den Datenschutzskandalen im Bereich wirtschaftlicher Datenverarbeitung wirkten sich auch einige der Skandale im Bereich der (internationalen) Sicherheitspolitik auf das Bürgerrechtsbewusstsein der europäischen Bevölkerung aus. So verabschiedeten die vom internationalen Terrorismus direkt und indirekt betroffenen Staaten zunächst eine Reihe von Anti-Terror-Maßnahmen, die von den jeweiligen Bevölkerungen mehrheitlich grundsätzlich begrüßt wurden (European Commission 2008, 47 ff. Priscilla M. Regan 2015, 59). Die Verabschiedung von staatlichen Anti-Terror-Maßnahmen stellt insofern eine *normale* Reaktion des Staates dar, als die Regierung eines Staates aufgrund der verübten oder befürchteten Anschläge zur Reaktion gezwungen wird: „Unternähme sie nichts, müsste sie befürchten, dass dies von der eigenen Bevölkerung, von anderen Staaten und nicht zuletzt von den Terroristen als Schwäche oder Nachgiebigkeit ausgelegt wurde. Deshalb muss sie zunächst versuchen, weitere Anschläge zu verhindern." (B. Meyer 2002, 3) Zugleich liegt dieser Handlungslogik eine inhärente Problematik zugrunde, denn „die Furcht, bei der Prävention Lücken zu lassen, verleitet wegen der Unbestimmbarkeit künftiger Risiken

dazu, die Freiheitsrechte der Bürger stärker einzuschränken als es mit Blick auf die wahrscheinlichen Gefahren erforderlich wäre." (ebd.)

3.4.2.2 Wandel in der öffentlichen Meinung gemäß Umfragewerten in den 2000er-Jahren

Im Laufe der 2000er-Jahre nahm insbesondere die Anfangs hohe Bereitschaft zur Unterstützung von Anti-Terror-Maßnahmen EU-weit signifikant ab, während die Datenschutz-Sorgen der Bevölkerung sowie die Unterstützung einer EU-weiten Datenschutzregelung eine leichte Zunahme verzeichneten.

So sprach sich zwar die Mehrheit der EU-Bürgerinnen und -Bürger für die Ausweitung von Sicherheitsgesetzen zum Zwecke der Terrorbekämpfung aus. Doch die Verarbeitung personenbezogener Daten für sonstige sicherheitsbehördliche und wirtschaftliche Zwecke wurde von der Mehrheit der EU-Bevölkerung mit Sorge betrachtet. Die EU-weit repräsentativen Eurobarometer-Studien aus den Jahren 2003 und 2008 demonstrierten etwa, dass eine Mehrheit der Bürgerinnen und Bürger der EU Einschränkungen ihrer Datenschutzrechte zum Zwecke der Bekämpfung des internationalen Terrorismus in Kauf zu nehmen bereit war. Im Jahre 2003 befürworteten 64 % der Befragten die Überwachung der Internetnutzung zum Zwecke der Terrorbekämpfung. Im Jahre 2008 stieg dieser Wert sogar auf 77 % an. Die Zahl der mit dieser Maßnahme nicht einverstandenen Menschen fiel im selben Zeitraum von 25 % auf 18 % (European Commission 2008, 51). Der Zuspruch für die Überwachung von Telefongesprächen zum Zwecke der Terror-Bekämpfung erhöhte sich im selben Zeitraum ebenfalls, von 61 % im Jahr 2003 auf 73 % im Jahr 2008 während die Ablehnung von 33 % auf 25 % sank (ebd., 52).

Im Hinblick auf das Thema der Datenschutz-Sorgen hatten in der ersten Eurobarometer-Studie aus dem Jahr 1991 66 % der Befragten ihre Besorgnis über den Schutz ihrer personenbezogenen Daten geäußert. Dieser Wert sank im Jahr 1996 auf 58 %, stieg 2003 leicht auf 60 % und schließlich im Jahr 2008 auf den Höchstwert von 68% an (European Commission 2008, 7). Den höchsten Anstieg verzeichnete der Wert zwischen 2003 und 2008 in Österreich, Deutschland und Dänemark: Die Zahl der über den Umgang mit ihren personenbezogenen Daten besorgten Menschen stieg in Österreich von 51 % im Jahr 2003 auf 86 % im Jahr 2008 an, in Dänemark von 42 % auf 73 % und in Deutschland von 58 % auf 86 % (European Commission 2008, 7 f.). Zudem korrelierte diese Entwicklung mit dem sinkenden

Bedrohungsgefühl der Bevölkerung vor Terroranschlägen: Während noch in der kurz nach dem 11. September 2001 durchgeführten Eurobarometer-Studie Anfang 2002 78 % der EU-Bevölkerung den Terrorismus als Hauptsorge einstuften (Europäische Kommission 2002, 5), sank dieser Wert im Laufe der Folgejahre kontinuierlich bis auf nur 7 % im Jahr 2007 (Europäische Kommission 2008b, 12). Daneben vertrat eine große Mehrheit von 82 % der im Jahr 2008 befragten EU-Bürgerinnen und -Bürger die Ansicht, dass die Übertragung personenbezogener Daten über das Internet unsicher sei (European Commission 2008, 41). Eine repräsentative Umfrage des Meinungsforschungsinstituts Forsa unter der deutschen Bevölkerung fand 2007 heraus, dass die sechsmonatige Vorratsdatenspeicherung von 54 % und die Online-Durchsuchung von 59 % der Befragten abgelehnt wurde. Schließlich gaben 54 % der Befragten an, dass sie die bestehenden Sicherheitsgesetze in der Bundesrepublik für ausreichend hielten, während 44 % für eine Ausweitung der Sicherheitsgesetzgebung eintraten (Datenspeicherung.de 2007).

Zeitgleich wurde auch der Ruf nach einer unionsweiten, statt nationalen, Lösung von Datenschutzproblemen lauter. Während im Jahr 2003 noch 41 % der befragten EU-Bürgerinnen und Bürger der Ansicht waren, dass die nationale Gesetzgebung für einen angemessenen Schutz personenbezogener Daten nicht ausreichend sei und 26 % der Befragten diese für ausreichend befanden, äußerten sich im Jahr 2008 56 % der Befragten dahingehend, dass nationale Gesetzgebung alleine nicht ausreichend sei (29 % hielten nationale Gesetzgebungsmaßnahmen für ausreichend) (European Commission 2008, 24).

3.4.2.3 Außerparlamentarischer Widerstand

Der Wandel in der öffentlichen Meinung zeigte sich auch und insbesondere am zunehmenden außerparlamentarischen Widerstand gegen die Ausweitung sicherheitspolitischer Maßnahmen. Nachdem zunächst ein allgemeiner Überblick über das Erstarken europaweiter zivilgesellschaftlicher Datenschützer geliefert wird, gehe ich näher auf das Beispiel des zivilgesellschaftlichen Widerstands gegen die Einführung der Vorratsdatenspeicherung in Deutschland ein.

3.4.2.3.1 Entstehung europaweiter digitaler Bürgerrechtsgruppen

Mit der zunehmenden gesellschaftlichen Bedeutung der Datenverarbeitung und der Zunahme sicherheitspolitischer Maßnahmen ging auch die Entstehung und Erstarkung netzpolitischer Aktivisten im Allgemeinen und zivilgesellschaftlicher Datenschutzbefürworter im Besonderen einher. In verschiedenen europäischen Staaten wurden entsprechende Organisationen ins Leben gerufen: *Bits of Freedom* (2000, Niederlande), *Associação Nacional para o Software Livre* (2001, Portugal), *IT-Political Association of Denmark* (2002, Dänemark), *Open Rights Group* (2005, Vereinigtes Königreich), *La Quadrature du Net* (2008, Frankreich), *Icelandic Digital Freedom Society* (2008, Island), *Panoptykon Foundation* (2009, Polen), *Digitale Gesellschaft* (2010, Deutschland).

Der für die Datenschutzpolitik bedeutendste Schritt der Zivilgesellschaft erfolgte allerdings im Jahr 2002 mit der Gründung von *European Digital Rights* (EDRi). Angetrieben von Bestrebungen zur Internet-Zensur auf EU-Ebene, planten Statewatch, CCC und GILC gemeinsam mit weiteren Organisationen Anfang 2002 die Gründung einer europäischen Dachvereinigung der nationalen netzpolitischen Bürgerrechtsorganisationen (Krempl 2002). Mitte 2002 wurde EDRi schließlich von insgesamt zehn Gruppierungen ins Leben gerufen, um gemeinsam gegen die auf EU-Ebene stattfindenden Entwicklungen in den Bereichen Vorratsdatenspeicherung, Telekommunikationsüberwachung, Cybercrime-Abkommen sowie Internet-Zensur vorzugehen (Ziegler 2002). Nachdem EDRi Anfangs zunächst eher auf Ebene des zivilgesellschaftlichen Aktivismus tätig war, trat sie auch zunehmend als Beobachter relevanter Entwicklungen auf und beteiligte sich in zunehmendem Maße an politischen Entscheidungsprozessen und an Multi-Stakeholder-Expertengruppen als Vertreter der europäischen Zivilgesellschaft (EDRi 2004, 2005a, 2007). Ihre enorme Mobilisierungsfähigkeit sollte EDRi schließlich während der erfolgreichen Proteste gegen das Anti-Counterfeiting Trade Agreement (ACTA), das aufgrund der massiven öffentlichen Kritik schließlich vom Europäischen Parlament abgelehnt wurde, zur Schau stellen (EDRi 2013b; James Losey 2014). Wie jüngere Forschungsergebnisse zeigen, ist der Einfluss internationaler zivilgesellschaftlicher Organisationen auf politische Prozesse auf EU-Ebene im Laufe der vergangenen Jahrzehnte insbesondere aufgrund ihrer Adaption an die Multi-Level-Governance-Struktur der EU und der damit einhergehenden Anpassung ihrer Mobilisierungs- und Lobbying-Strategien gewachsen (Caiani und Graziano 2018).

3.4.2.3.2 Zivilgesellschaftlicher Widerstand in Deutschland gegen die Einführung der Vorratsdatenspeicherung

Deutlich wird das Erstarken des netzpolitisch motivierten zivilgesellschaftlichen Widerstands besonders bei einem Blick auf die Entwicklungen in der Bundesrepublik. So kann der netzpolitische Aktivismus in Deutschland – neben dem in den Vereinigten Staaten (C. J. Bennett 2008) – auf eine vergleichsweise lange Tradition zurückblicken (Stöcker 2011). Als älteste Organisation auf dem Gebiet des bürgerrechtlichen Datenschutzes war insbesondere die Deutsche Vereinigung für Datenschutz (DVD) bereits seit dem Jahr 1977 an zahlreichen datenschutzpolitischen und öffentlichkeitswirksamen Aktivitäten beteiligt, darunter die Anti-Volkszählungskampagnen 1983 und 1987, die Begleitung der Novellierungsbemühungen des BDSG in den 1980ern sowie im Rahmen der Umsetzung der Vorgaben der DS-RL oder auch im Kontext der Kritik an der Videoüberwachung öffentlicher Räume. Die Aktivitäten der DVD stützten sich überwiegend auf die Arbeit des Vorstands, der sich in der Anfangszeit aus der Gesellschaft für Mathematik und Datenverarbeitung (GMD) bzw. dessen Umfeld rekrutierte (Weichert 2007).[250] Der Chaos Computer Club (CCC) etablierte sich 1981 und war entgegen der eher politisch, bürgerlich und zentralistisch agierenden DVD ein vergleichsweise offener und dezentral agierender Hort für Aktivisten aus Hacker-Kreisen und technologisch versierte bzw. interessierte Individuen. Dem Grundsatz *öffentliche Daten nützen, private Daten schützen* folgend, machte sich der CCC für die Stärkung des Datenschutzes (und insb. des Selbstdatenschutzes) stark und zog auch durch öffentlichkeitswirksame Aktivitäten wie etwa den BTX-Hack im Jahr 1984 schon früh Aufmerksamkeit auf sich (Golem 2018). Ein weiterer Verein, der durch öffentlichkeitswirksame Aktivitäten immer wieder gegen die zunehmende Verarbeitung personenbezogener Daten vorgegangen ist, ist Digitalcourage e. V. Insbesondere mit dem seit dem Jahr 2000 verliehenen Negativpreis, den BigBrotherAwards, konnte Digitalcourage regelmäßig öffentliche Aufmerksamkeit generieren (Tangens und padeluun 2011).

Einen vorläufigen Höhepunkt erreichten die zivilgesellschaftlichen Datenschutzbefürworter schließlich im Rahmen der Proteste gegen die Volkszählung von 1983: Zehntausende Menschen in vielen deutschen Städten

250 Andere Organisationen wie die *Gesellschaft für Datenschutz und Datensicherheit e. V. (*GDD) oder der *Berufsverband der betrieblichen Datenschutzbeauftragten* (BvD) sind nicht primär bürgerrechtlich orientiert und vertreten eher die Interessen betrieblicher bzw. behördlicher Datenschutzbeauftragter (Weichert 2007, 57).

gingen auf die Straße. Die Proteste wurden von 52 % der deutschen Bevölkerung befürwortet und mehr als tausend Verfassungsbeschwerden wurden eingereicht (Der Spiegel 1983b, 1983a). Nach dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahr 1983, dem Ausbleiben der Orwell'schen Dystopie im Jahr 1984, und der zunehmenden Verbreitung und Normalisierung der Computernutzung im weiteren Verlauf der 1980er-Jahre, wich die gesellschaftliche Angst vor den negativen Folgen der Computerisierung allerdings einer positiven, auf Chancen und Potentiale ausgerichteten Wahrnehmung (Berlinghoff 2013b, 106 ff.).

Eine vergleichbare öffentliche Mobilisierung gelang den zivilgesellschaftlichen Datenschützern erst mehr als 20 Jahre später: Der Auslöser war die Verabschiedung des Gesetzes zur Vorratsdatenspeicherung[251] in der Bundesrepublik im Jahr 2007, mit der die EG-Richtlinie zur Vorratsdatenspeicherung 2006/24/EG in nationales Recht umgesetzt wurde. Vor dem Hintergrund des generellen Trends hin zur Versicherheitlichung der Europäischen Politik hatten sich zahlreiche Bürgerrechtsorganisationen und zivilgesellschaftliche Datenschutzorganisationen wie der CCC, DVD und Digitalcourage seit Ende 2005 zunächst gegen die Verabschiedung der EG-Richtlinie und später gegen das deutsche Umsetzungsgesetz im Rahmen des *Arbeitskreis Vorratsdatenspeicherung* (AK Vorrat) zusammengeschlossen. Im Jahr 2006 organisierte der Zusammenschluss Demonstrationen in Berlin, Bielefeld und Frankfurt am Main, an denen zunächst nur wenige hunderte Personen teilnahmen (AK Vorrat 2006; Lüke 2006). Auf den Folgeveranstaltungen unter dem Titel „Freiheit statt Angst" konnte das Bündnis hingegen viele zehntausende Demonstranten anziehen. Den Höhepunkt markierte der *Freiheit statt Angst*-Aktionstag am 11. Oktober 2008, an dem in weltweit 15 Ländern Aktionen gegen zunehmende Überwachung stattfanden (AK Vorrat 2008b). Allein in Berlin beteiligten sich an der Demonstration nach Veranstalterangaben 100.000 und nach Polizeiangaben 15.000 bis 50.000 Menschen (DPA 2008). Das Besondere am Format des AK Vorrat war neben der breiten Unterstützung seitens der Bevölkerung auch die enorme Unterstützung seitens Organisationen, die sich in der Vergangenheit eher unkritisch oder passiv im Hinblick auf die Ausweitung von Sicherheits- und Überwachungsgesetzen gezeigt hatten. So wurde das Bündnis von insgesamt 117 Organisationen unterstützt, darunter nicht nur

251 „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, Bundesgesetzblatt 70/2007".

datenschutzpolitisch oder allgemein auf dem Gebiet der Bürgerrechte aktive Gruppen, sondern beispielsweise auch die Oppositionsparteien aus dem Bundestag sowie deren Jugendorganisationen, die Gewerkschaften ver.di, DGB und GEW, Friedensinitiativen und mehrere Berufsverbände (AK Vorrat 2008a). Zudem organisierte der AK Vorrat in den Jahren 2007 und 2008 die größte Verfassungsbeschwerde in der Geschichte der Bundesrepublik, an der sich 34.939 Personen beteiligten (AK Vorrat 2008c) und die bereits im März 2008 zur Einschränkung der Vorratsdatenspeicherung per einstweiliger Anordnung des BVerfG führte (BVerfG 2008). In der Folge konnten sich die Vertreter zivilgesellschaftlicher Organisationen als Netzpolitik-Experten einen festen Platz in zahlreichen Polit-Talkshows, in den großen Massenmedien, aber auch in parlamentarischen und parteipolitischen Diskussions- und Beratungsrunden sichern (Schütz und Karaboga 2015, 39; Wendelin und Löblich 2013). Ihr Erfolg zeigte sich nicht zuletzt auch am zeitweisen politischen Erfolg der Piratenpartei seit 2009 (Bieber 2012, 39 ff.).

Trotz des im Vergleich zu den zivilgesellschaftlichen Akteuren in den Vereinigten Staaten niedrigen Budgets europäischer zivilgesellschaftlicher Akteure (Schütz und Karaboga 2015, 38, Fn. 80), gelang es diesen somit während des Betrachtungszeitraums der Kontextanalyse, in zunehmendem Maße Einfluss auf die Politik-Gestaltung zu nehmen. Der im vorausgegangenen Unterabschnitt dargestellte Ausbau der Lobbying-Kapazitäten der Zivilgesellschaft auf EU-Ebene wurde somit durch den Ausbau der Mobilisierungsfähigkeit zivilgesellschaftlicher Akteure auf nationaler Ebene flankiert (Caiani und Graziano 2018).

3.4.2.4 Policy Entrepreneurship im Europäischen Parlament

Schließlich erzeugte die fortschreitende Versicherheitlichungspolitik in Verbindung mit den zunehmenden Datenschutz-Skandalen auch bei den politischen Entscheidern des Europäischen Parlaments deutlichen Widerstand. Dies war ein Novum, da gerade die Europaabgeordneten in den ersten Jahren nach den Terroranschlägen vom 11. September vonseiten des Ministerrats stets dazu aufgefordert worden waren, Verantwortung für die Gesellschaft und Europa auf die Weise zu übernehmen, dass sie die von einigen Mitgliedstaaten mit allen politischen Mitteln durchgesetzten Anti-Terror-Maßnahmen unterstützten (siehe insb. die Unterabschnitte zur ePrivacy-Richtlinie 3.3.2 und zur Vorratsdatenspeicherung 3.3.4.2). Das Europäische Parlament, das jahrzehntelang im Gegensatz zum Ministerrat

als ein offener Diskussionsort für bürgerrechts-, umweltschutz-, verbraucherschutz- oder auch geschlechterpolitische Anliegen gegolten hatte (Dür, Bernhagen, und Marshall 2013; Kluger Dionigi 2017), wandelte sich seit den 1990er-Jahren infolge seines allmählichen Aufstiegs zum Mitgesetzgeber deutlich zu Lasten der früheren Positionen (Greis 2015; Ripoll Servent 2013). Nachdem dutzende die Bürgerrechte einschränkende nationale und europäische Anti-Terror-Maßnahmen verabschiedet worden waren, diese nicht immer die erhofften Ergebnisse gezeitigt und teils zu massiven Datenpannen geführt hatten und die Mitgliedstaaten sich nicht einmal auf ein angemessenes Mindestmaß an Datenschutzbestimmungen für den Bereich der dritten Säule hatten einigen können (vgl. 3.3.4.4), wurde der europaparlamentarische Widerstand erstmals lauter. So äußerte der ALDE-Politiker Alexander Alvaro im Rahmen der Europaparlamentsdebatte zum JI-Rahmenbeschluss: „Mit einer unglaublichen Aktivität bemühen sich Kommission und Rat, im Bereich des wirtschaftlichen Schutzes personenbezogener Daten zu handeln. Wenn wir sehen, was in Großbritannien, in Deutschland und in anderen Mitgliedstaaten mit persönlichen Daten geschieht, die von öffentlichen Behörden verwaltet werden und zum Teil verloren gehen oder gestohlen werden, haben wir dort einen genauso dringenden Handlungsbedarf. Hier geht es schließlich mehr denn je um die Rechte des Bürgers, denn gegen das Verhalten seines Staates kann er sich nicht wehren. Bei einem Unternehmen kann er im Zweifelsfall noch ein anderes wählen." (EP 2008c) Unter direkter Bezugnahme auf die im Vereinigten Königreich stattgefundenen Datenpannen äußerte selbst der zu diesem Zeitpunkt der euroskeptischen UEN angehörende Europaabgeordnete Brian Crowley: „Wir müssen beim Thema Datenschutz und Erfassung personenbezogener Daten sehr vorsichtig sein, da viele von uns wissen, dass es in unseren eigenen Mitgliedstaaten zahllose Behörden auf nationaler und auf lokaler Ebene gibt, die zu jeder einzelnen Person Daten erfassen. Der größte Schrecken, der derzeit Großbritannien erschüttert, betrifft diese Angelegenheit des Identitätsdiebstahls und es gibt große Bedenken, weil Computer verloren gegangen sind, die Informationen von staatlichen Behörden enthalten – ob es nun Sozialämter oder Verteidigungs- oder Polizeibehörden sind – persönliche Daten, Informationen, die Sie selbst niemals weitergeben würden. Dennoch scheint es keinen Schutz für diese Daten zu geben." (EP 2008c) Die liberale Europaabgeordnete Sarah Ludford machte auf die Zweckentfremdung der im Rahmen der Vorratsdatenspeicherung gespeicherten sensiblen personenbezogenen Daten aufmerksam: „Ich kann dem Haus berichten, dass in Großbritannien die Richtlinie über die Vor-

ratsspeicherung von Daten – der Meilenstein des britischen Ratsvorsitzes vor drei Jahren – dazu genutzt wird, hunderten von Behörden, die nicht mit der Strafverfolgung befasst sind, Zugang zu persönlichen Daten zu gewähren. Gemeinden verwenden sie, um zu überprüfen, ob Eltern lügen, wenn sie angeben, im Einzugsbereich einer beliebten Schule zu leben – was nicht richtig wäre, aber kein schweres Verbrechen ist." (EP 2008c)

Schließlich wurde auch die Wirksamkeit der Anti-Terror-Maßnahmen infrage gestellt. Der italienische Sozialdemokrat Claudio Fava drückte sein Unbehagen im Namen der PSE-Fraktion folgendermaßen aus: „Nach sieben Jahren der Terrorismusbekämpfung glaube ich, dass wir jetzt in der Lage sind, die Risiken des Terrorismus, seine Auswirkungen und verheerenden Konsequenzen einzuordnen. Ich glaube auch, dass eine der dramatischsten Konsequenzen der Verlust der Ausgewogenheit ist – ein Verlust des Gespürs für Ausgewogenheit bei der Reaktion auf die Bedrohung durch den Terrorismus." (EP 2008c) Deutliche Kritik an dieser EU-Strategie wurde auch von der linken GUE/NGL geäußert. Der aus Italien stammende Giusto Catania befand etwa, „dass die Strategie zur Bekämpfung des Terrorismus der letzten Jahre nicht erfolgreich war, und dass sie sich mit der Formulierung der Terrorliste und den Einschränkungen des Rechtsstaatsprinzips zu stark den US-Interessen im Krieg im Irak und in Afghanistan untergeordnet hat. Es gab zu viele Fälle eines regelwidrigem [sic] Umgangs mit personenbezogenen Daten, und ich glaube, dass wir alle zusammenarbeiten müssen [...], um zu gewährleisten, dass wir die persönlichen Freiheiten nicht einschränken, um demokratische Bereiche zu erweitern und um sicherzustellen, dass wir nicht im Namen der Sicherheit und der Bekämpfung des Terrorismus dazu beitragen, dass die Terrororganisationen ihre eigentlichen Ziele erreichen." (EP 2008c) Die aus den Niederlanden stammende grüne Europaabgeordnete Kathalijne Maria Buitenweg verwies auch auf den Zusammenhang zwischen der Zunahme von Grundrechtseinschränkungen und dem wachsenden Misstrauen der Bevölkerung gegenüber ihren Regierungen: „Wenn wir die Beziehung zwischen Regierung und Bürger aus der historischen Perspektive betrachten, sehen wir, dass die Regierung das Gewaltmonopol innehat und die Bürger über Grundrechte verfügen, die von der Regierung nur verletzt werden dürfen, wenn dies notwendig, effektiv und angemessen ist. Wenn die Bürger aber allzu oft feststellen müssen, dass Maßnahmen der Regierung weder notwendig noch gerechtfertigt sind, wird ihr Vertrauen in diese Regierung und damit ihre Bereitschaft zur Zusammenarbeit mit ihr schwinden. Dann werden wir

langfristig massive Sicherheitsprobleme erleben. Vertrauen ist schwer zu gewinnen, aber leicht zu verlieren." (EP 2008c)

Die im linken und liberalen Spektrum des Parlaments angesiedelten Parteien und Fraktionen wandten sich somit, entgegen vorherigen Meinungsverschiedenheiten insb. auf Seiten der Sozialdemokraten und Liberalen, erstmals geschlossen und entschieden gegen die Fortsetzung der bis dahin praktizierten Anti-Terror-Strategie. Wie zu erwarten war, wurde die Ausweitung der Sicherheitsgesetzgebung hingegen von den konservativen und europaskeptischen bzw. feindlichen Parteien, insb. der EVP-ED sowie Polen-stämmigen Abgeordneten der UEN, befürwortet (EP 2008c).[252]

3.4.2.5 Policy Entrepreneurship auf Ebene der Kommission

Franco Frattini, EU-Kommissar für Justiz, Freiheit und Sicherheit, hatte noch Ende 2007 – den Ankündigungen im 2007er Bericht entsprechend – darauf gesetzt, einerseits die Implementierung der DS-RL weiter voranzubringen und andererseits die Erforderlichkeit von sektorspezifischen Regulierungsmaßnahmen zu überprüfen, um die Anwendbarkeit der Datenschutz-Grundsätze auch auf neue Technologien aber auch angesichts der Gefährdungen der Öffentlichkeit durch neue Formen der Kriminalität und terroristischer Gefahren zu gewährleisten. Trotz der Hervorhebung von nicht-unterlaufbaren Datenschutz-Prinzipien und der Betonung der Gleichwertigkeit von Datenschutz und Sicherheit hinterfragte Frattini allerdings keine der zu Sicherheitszwecken erlassenen EU-Maßnahmen, sondern identifizierte als Ziel lediglich die Erreichung einer angemessenen Balance zwischen beiden Polen (Frattini 2007).

Erst als Jacques Barrot 2008 zum neuen Kommissar für Justiz, Freiheit und Sicherheit wurde, änderte sich die Haltung der Kommission zur Reform des Datenschutzrechts. Bereits in seiner Vorstellungsrede vor dem Europäischen Parlament legte Kommissar Barrot, in einem deutlich gewandelten Zungenschlag im Vergleich zu seinem Amtsvorgänger, die Schwerpunkte seiner künftigen Arbeit auf die Stärkung der Unionsbürgerschaft und die Gewährleistung des Grundrechtsschutzes. Zudem kündigte er bereits zu jenem Zeitpunkt die Durchführung einer *umfassenden Konsultation, die auf eine Stärkung des Datenschutzes abziele*, an. Angesichts der

252 Ausnahmen bilden die weiter oben zitierten Äußerungen Brian Crowleys, aber auch des neofaschistischen italienischen Politikers Luca Romagnoli (NI) (EP 2008c),

jahrelangen Ignoranz des Ministerrats gegenüber den Vorschlägen des Parlaments und des EDSB kündigte Barrot zudem an, besondere Rücksicht auf deren Positionen zu nehmen (Barrot 2008, 4).[253] Die in dieser Phase von Kommissar Barrot eingenommene Rolle ist daher als die eines *Policy Entrepreneurs* zu bewerten, da er das Thema Datenschutz entgegen der bis dahin vom Kommissariat vertreten Position zunächst auf die Kommissionsagenda setzte und anschließend auf die Agenda des Stockholmer Programms. Zudem zeichnete er letzten Endes dafür verantwortlich, dass der Reformprozess des datenschutzrechtlichen Rahmens der EU eingeleitet wurde.

3.5 Zwischenfazit

Das Ziel des Abschnitts 3 bestand darin, die relevanten (polit-historischen) Kontextbedingungen der EU-Datenschutzpolitik zu identifizieren, die entscheidend im Hinblick auf das Zustandekommen der DSGVO waren, um so die zweite Forschungsfrage zu beantworten:

FF 2: Welche politischen und historischen Faktoren wirkten als kausale, treibende Faktoren auf dem Weg zur DSGVO?

Unter Rückgriff auf das ACF wurden relativ stabile Parameter, externe Systemereignisse im Vorfeld der DSGVO sowie langfristig wichtige politische Gelegenheitsstrukturen als die Eckpunkte dieses Analyseschrittes bestimmt, von denen mit dem ACF angenommen werden kann, dass sie entscheidend im Hinblick auf das Zustandekommen der DSGVO waren. Der folgende Unterabschnitt fasst die Ergebnisse des Abschnitts im Hinblick auf die Beantwortung der zweiten Forschungsfrage zusammen.

Im darauffolgenden Unterabschnitt wird schließlich auf Grundlage der Erkenntnisse aus der Kontextanalyse ein erster Überblick über die Advocacy-Koalitionen im Bereich der EU-Datenschutzpolitik geliefert, die als Grundlage für die Akerurs- und Prozessanalyse dienen werden.

253 Das Generaldirektorat Justiz, Freiheit und Sicherheit veröffentlichte zudem, noch während es von Barrot kommissarisch geleitet wurde, eine Ausschreibung für eine vergleichende Studie, die verschiedene Ansätze zur Bewältigung neuer Herausforderungen für den Schutz der Privatsphäre, insbesondere aufgrund technologischer Entwicklungen untersuchen sollte (European Commission: Directorate-General for Justice, Freedom and Security - Directorate C: Civil Justice, Fundamental Rights and Citizenship - The Director 2008). Douwe Korff und Ian Brown erhielten den Auftrag und veröffentlichten die Studienergebnisse im Jahr 2010 (Korff und Brown 2010).

3.5.1 Zusammenfassung

Die zweite Forschungsfrage lässt sich folgendermaßen beantworten: Die Initiierung der Datenschutz-Reform, die später in der Verabschiedung der DSGVO und der JI-Richtlinie mündete, war aufgrund einer Mischung aus verschiedenen Einflussfaktoren möglich. Veränderungen in der verfassungsmäßigen Struktur der EU in Gestalt des Inkrafttretens des Lissabon-Vertrags und des Verbindlichwerdens der EU-Grundrechtecharta machten den Erlass von umfassenden sekundärrechtlichen Datenschutzregelungen erforderlich. Die an stärkeren Datenschutzregelungen für den Sicherheitsbereich interessierten Akteure, insb. die EU-Parlamentsfraktionen links der Mitte sowie die liberale Fraktion, aber auch Teile der EU-Kommission (insb. das Kommissariat für Justiz, Freiheit und Sicherheit), deren Positionen trotz gegenüber dem Ministerrat erbrachter Zugeständisse und klarer Absprachen letztlich nicht erhört wurden, übten schließlich gemeinsam mit den Regierungen einiger Mitgliedstaaten Druck aus, damit die Datenschutzreform initiiert werden konnte. Eine abnehmende Anzahl an Terroranschlägen, eine wachsende Sorge vor dem Missbrauch personenbezogener Daten seitens privatwirtschaftlicher als auch staatlicher Akteure und zunehmende Proteste gegen Überwachungsmaßnahmen gaben den Forderungen der Datenschutzbefürworter zusätzlichen Auftrieb. Diese Punkte werden im Folgenden ausführlich diskutiert.

Grundlegende Merkmale des betrachteten Problems: Da es sich beim Thema Datenschutz um kein natürliches, sondern ein soziales Phänomen handelt, bildet das grundlegende Merkmal der Datenschutzpolitik die Bedeutung die der Verarbeitung personenbezogener Daten seitens verschiedener Akteure zugesprochen wird. Einig sind sich alle wesentlichen Akteure dahingehend, dass die Verarbeitung personenbezogener Daten grundsätzlich möglich sein sollte. Uneinigkeit herrscht jedoch im Hinblick darauf, inwieweit und auf Grundlage welcher Regeln diese Verarbeitung möglich sein sollte.

Verteilung natürlicher Ressourcen: Als die Kerncharakteristik aller datenschutzpolitischen Auseinandersetzungen in Europa im Betrachtungszeitraum (von den 1970er-Jahren bis ca. 2008/2009) lässt sich der Konflikt zwischen Akteuren, die an einer möglichst ungehinderten Verarbeitung personenbezogener Daten interessiert sind einerseits und Akteuren, die an der Eindämmung der Risiken jener Verarbeitung in Gestalt von Datenschutzgesetzen interessiert sind andererseits definieren. Wie die Ausführungen gezeigt haben, lassen sich die Befürworter einer ungehinderten

Verarbeitung wiederum in zwei Gruppen unterteilen: Solche, die aus einer wirtschaftspolitischen Perspektive und solche, die aus einer sicherheitspolitischen Perspektive heraus, jedoch in beiden Fällen stets unter Verweis auf den gesellschaftlichen Nutzen der Verarbeitung personenbezogener Daten, argumentieren. Den Befürwortern von Datenschutzregelungen gelang es im Laufe der Jahrzehnte trotz des Widerstands beider Gruppen Datenschutzregelungen zunächst auf nationaler und später auch auf internationaler Ebene zu erlassen.

Grundlegende soziokulturelle Wertvorstellungen und Sozialstruktur: Der wesentliche Disput im Hinblick auf soziokulturelle Wertvorstellungen besteht zwischen Akteuren, die grundsätzlich einer kontinentaleuropäischen Herangehensweise an Regulierung folgen und solchen, die einer anglo-amerikanischen Herangehensweise näherstehen. Erstere räumen der staatlichen Pflicht zur Verhinderung von individuellem und gesellschaftlichem Schaden durch Praktiken der Wirtschaftsteilnehmer größeren Raum ein, während letztere nicht den Staat, sondern die Wirtschaftsakteure selbst in der Pflicht sehen, mögliche Gefährdungen zu adressieren.

Auf nationaler Ebene war der Erlass von Datenschutzgesetzen in der Frühphase des Datenschutzes insbesondere auf die Beschränkung staatlicher Kontrollmacht fokussiert und von grundrechtlichen Erwägungen getrieben. Der entscheidende Anlass für die Verabschiedung internationaler Regelungen war hingegen nicht der grundrechtliche Schutzaspekt, wie seitens der Datenschutzbefürworter stets gefordert worden war, sondern die Assoziation wirtschaftlichen Wachstums mit der Gewährleistung eines möglichst ungehinderten Flusses personenbezogener Daten über nationale Grenzen hinweg, indem die nationalen Gesetze mittels internationaler Instrumente harmonisiert wurden. Alle allgemeinen Datenschutzgesetze, die bis zum Beginn der Datenschutzreform verhandelt wurden, waren von diesen Konfliktlinien in wesentlichem Maße geprägt.

Mit den Terroranschlägen auf das World Trade Center im Jahr 2001 und in Madrid und London 2004 bzw. 2005 wandelte sich der Datenschutzdiskurs fort vom Konflikt zwischen der grundrechtlichen und wirtschaftlichen Bedeutung schlagartig hin zur sicherheitspolitischen Bedeutung der Verarbeitung personenbezogener Daten. In der Folge konnten sich die staatlichen Befürworter einer möglichst ungehinderten Datenverarbeitung in praktisch allen datenschutzpolitisch relevanten Auseinandersetzungen gegenüber Datenschutzbefürwortern klar durchsetzen und die Ausweitung staatlicher Verarbeitungsspielräume vorantreiben.

Entgegen bisherigen Einschätzungen (Koops 2014; Sloot 2014) zeigt meine Analyse, dass der Schutz personenbezogener Daten insb. im Kontext sicherheitspolitisch motivierter Politiken seitens der Datenschutzbefürworter unter Rückgriff sowohl auf dessen individuelle als auch gesellschaftliche Bedeutung gefordert wurde. Weniger deutlich zeigte sich dies hingegen bei den allgemeinen Datenschutzpolitiken. Allerdings lag der Fokus der Kontextanalyse nicht auf der Untersuchung dieses Aspekts, sodass diese Einschätzung lediglich ergänzend erfolgt. Für eine sorgfältigere Bewertung dieses Aspekts wäre insb. eine tiefergehende Untersuchung der einzelnen Argumente und ggf. eine andere Methodik (Frage nach den Erwägungsgründen in persönlichen Interviews mit den Beteiligten) notwendig gewesen.

Grundlegende verfassungsmäßige Struktur: Die in der vorliegenden Arbeit untersuchten Datenschutzpolitiken[254] wurden im Rahmen der Zuständigkeit der Europäischen Union bzw. von deren Vorgänger in Form der Europäischen Gemeinschaften erlassen. Die verfassungsmäßige Struktur der EU baut auf den völkerrechtlichen Verträgen auf, die zwischen den EU-Mitgliedstaaten abgeschlossen wurden. Anders als im ACF (vor allem Hinblick auf Nationalstaaten) angenommen wird, unterlag die verfassungsmäßige Struktur der Union allerdings einem steten Wandel, der einen großen Einfluss auf das Subsystem der Datenschutzpolitik hatte. So war der Erlass von gemeinschaftlichen Datenschutzregelungen während der 1970er- und 1980er-Jahre deshalb nicht möglich, weil die Ziele der Gemeinschaft laut EWG-Vertrag bzw. den Römischen Verträgen in der Gewährleistung des freien Warenverkehrs, der Freizügigkeit von Arbeitnehmern, von Dienstleistungen sowie von Kapital lagen und der Datenschutz schlicht nicht Teil der Verträge war. Auch die 1977 verabschiedete gemeinsame Erklärung von Parlament, Rat und Kommission, in der diese sich der Wahrung der Grundrechte auf Grundlage der Verfassungen der Mitgliedstaaten und der EMRK verpflichteten, stellte lediglich eine freiwillige Maßnahme und keine bindende verfassungsrechtliche Verpflichtung dar. Erst die für 1992 vorgesehene Vollendung des Binnenmarktes ermöglichte schließlich vor allem aus wirtschaftspolitischen Erwägungsgründen heraus den Erlass der Datenschutzrichtlinie. Die formell verbindliche Achtung der Grundrechte auf Unionsebene fand schließlich erst viele Jahre später mit dem Inkrafttreten des Lissabon-Vertrags 2009 Eingang in das EU-Primärrecht, insb. indem die EU-Grundrechtecharta zum verbindlichen Teil

254 Mit Ausnahme der OECD-Richtlinien und der Europaratskonvention.

des EU-Primärrechts wurde. Der in der EU-Grundrechtecharta formulierte Schutz personenbezogener Daten ist seither Teil des EU-Primärrechts, das zwingendermaßen gemäß den primärrechtlichen Vorgaben im Bereich des Sekundärrechts gewährleistet werden muss.

Grad der erforderlichen Zustimmung für wesentlichen Wandel: Die EU-Datenschutzpolitik ist eingebettet in das komplexe politische Mehrebenensystem der Europäischen Union. Die in den Betrachtungszeitraum der Kontextanalyse fallenden datenschutzpolitischen Auseinandersetzungen spiegeln dieses Verhältnis stets wider, indem einzelne nationale Akteure den Transfer bestimmter Politiken auf die EU-Ebene vorangetrieben haben. Beispiele hierfür sind die nationalen Datenschutzaufsichtsbehörden, die mit ihrer Blockadeandrohung grenzüberschreitender Datentransfers in Mitgliedstaaten, die über keine Datenschutzgesetze verfügten, die Kommission zur Initiierung der Datenschutzrichtlinie antrieben oder die Mitgliedstaaten, die die Vorratsdatenspeicherung erfolgreich auf die EU-Agenda setzen konnten. Die konkreten Auseinandersetzungen zwischen den Unionsorganen spiegeln wiederum das über viele Jahre etablierte Kräfteverhältnis untereinander wider. Während das Europäische Parlament bei den allgemeinen Datenschutzgesetzen über ein formelles Mitspracherecht verfügte, die letztlichen Entscheidungen jedoch vor allem im Ministerrat getroffen wurden, hatte das EP im Bereich der sicherheitspolitischen Datenschutzmaßnahmen praktisch überhaupt keine Entscheidungsmacht. Allerdings ereignete sich am Ende des Betrachtungszeitraums ein signifikanter Wandel im Grad der erforderlichen Zustimmung für wesentlichen Wandel. Am 1. Dezember 2009 trat der Lissabonner Vertrag in Kraft, in dessen Folge das EP zum gleichberechtigten Mitgesetzgeber in nahezu allen Bereichen der Unionspolitik und durch die gleichzeitig erfolgte weitgehende Abschaffung der Säulenstruktur auch im Bereich der PJZS aufgestiegen ist.

Relative Offenheit des politischen Systems: Zentrale Charakteristika des politischen Systems der EU sind dessen Offenheit und die Involvierung einer großen Zahl an Akteuren. Sowohl Private als auch öffentliche Akteure aus allen Ebenen (lokal, national, europäisch) bilden auf EU-Ebene komplexe Akteursnetzwerke, die in Abhängigkeit von den behandelten Themen potentiell auf allen Ebenen im Hinblick auf die Beeinflussung von Politiken aktiv sind. Zudem gilt als ausreichend belegt, dass administrative Akteure, privatwirtschaftliche und zivilgesellschaftliche Interessengruppen sowie Wissenschaftler aus verschiedenen EU-Mitgliedstaaten z. B. ökologisch oder privatwirtschaftlich motivierte Koalitionen auf EU-Ebene bilden (Rozbicka 2013, 843 f.).

Traditionelle Konfliktlinien: Das Phänomen der traditionellen Konfliktlinien spielte in der Datenschutz-Politik keine größere Rolle. Der einzige Aspekt, der bei der Datenschutz-Politik an traditionelle Konfliktlinien erinnert, ist der, dass die Gegner staatlicher (Wirtschafts-)Regulierung häufig auf Seiten der Datenschutz-Gegner zu finden waren. Insbesondere die konservativen Parteien, aber auch die Liberalen stellten sich gegen die Einführung von aus ihrer Perspektive restriktiven Datenschutz-Gesetzen. Parteien, die eher grundsätzlich für eine Regulierung der Wirtschaft eintreten, forderten zugleich auch die Verabschiedung von Datenschutz-Gesetzen, so insb. Parteien links der Mitte.

Wandel sozioökonomischer Bedingungen: Einen signifikanten Wandel in den sozioökonomischen Bedingungen hat es im Betrachtungszeitraum im Hinblick auf das Bedeutungswachstum der Verarbeitung personenbezogener Daten gegeben. In dem Maße, in dem die Preisgabe personenbezogener Daten zu einer alltäglichen Praxis wurde, stieg auch die wirtschaftspolitische Bedeutung, die der Verarbeitung personenbezogener Daten zugesprochen wurde. In der Datenschutz-Politik äußerte sich diese Verschiebung in der Veränderung der Rahmung des Themas. Je stärker die wirtschaftspolitische Bedeutung in den Vordergrund rückte, umso weniger wurde über die grundrechtliche Bedeutung des Datenschutzes gesprochen. Stattdessen setzte sich allmählich die Vorstellung durch, dass Gesetze zum Schutz personenbezogener Daten letztlich Vertrauen schaffen und dadurch zu Wirtschaftswachstum auf Grundlage der Verarbeitung personenbezogener Daten führen sollten.

Wandel in der öffentlichen Meinung: Im Laufe der 2000er fand in mehrfacher Hinsicht ein Wandel in der öffentlichen Meinung statt. Obwohl die Unterstützung der europäischen Bevölkerung für Anti-Terror-Maßnahmen konstant hoch blieb und diese von einer Bevölkerungsmehrheit befürwortet wurden, nahmen zugleich auch die Datenschutz-Sorgen der Bevölkerung zu, sodass zwei Drittel aller europäischen Bürgerinnen und Bürger der Meinung waren, dass ihre personenbezogenen Daten nicht ausreichend geschützt seien. Gleichzeitig sank das Bedrohungsgefühl vor Terror-Anschlägen in signifikantem Maße und insbesondere in einigen Mitgliedstaaten wie Deutschland stieg die Ablehnung gegenüber Gesetzen, von denen ein zu weitreichender Eingriff in die Grund- und Persönlichkeitsrechte befürchtet wurde. Schließlich hielt erstmals eine Mehrheit aller Europäerinnen und Europäer im Jahr 2008 den Erlass nationaler Datenschutzgesetze für nicht ausreichend und trat stattdessen für die Verabschiedung von Datenschutzgesetzen auf EU-Ebene ein.

Wandel maßgeblicher (Regierungs-)Koalitionen: Im Bereich der EU-Datenschutzpolitik hat es keinen relevanten Wandel maßgeblicher Regierungskoalitionen gegeben. Eine Veränderung hat es dagegen durchaus auf Ebene der Koalitionen im EP gegeben. Während die Sozialdemokraten und teils auch die Liberalen immer wieder gegen die Stärkung des Datenschutzes stimmten, gelangten beide Fraktionen gegen Ende des Betrachtungszeitraums an einen Punkt, an dem sie sich mit der datenschutzrechtlichen Situation in der Union höchst unzufrieden zeigten und im Ergebnis an die Seite der Fraktionen der Linken und Grünen stellten.

Policy-Entscheidungen und Policy-Wirkungen aus anderen Subsystemen: Die im Feld der Datenschutz-Politik relevanteste Policy-Wirkung aus anderen Subsystemen erfolgte aus dem Bereich der Sicherheitspolitik infolge eines externen Schocks in Gestalt der Terroranschläge in New York, Madrid und London, die zur Versicherheitlichung der Politiken westlicher Staaten führten. Außerdem kann das für 1992 vorgesehen Inkrafttreten des Europäischen Binnenmarktes als ein externer Schock bezeichnet werden, den die Datenschutzaufsichtsbehörden als Policy Entrepeneure zu ihren Gunsten zu nutzen wussten.

3.5.2 Identifikation von Advocacy-Koalitionen

Entlang der während der Kontextanalyse diskutierten politischen Auseinandersetzungen lassen sich drei Koalitionen auf dem Feld der Europäischen Datenschutzpolitik unterscheiden.

Datenschutzbefürworter: Eine Koalition, die sich aus Datenschutzbefürwortern[255] zusammensetzt.

Sicherheitsbefürworter: Eine zweite, aus Befürwortern der Ausweitung von Sicherheitsgesetzen bestehende Koalition.

255 Die m. E. sprachlich präziseste Bezeichnung dieser Koalition ist „Datenschutz-Regulierungsbefürworter", da diese Formulierung deutlich macht, dass es bei deren Mitgliedern nicht nur um die Befürwortung von Datenschutz im Allgemeinen, sondern um die Befürwortung des Erlasses datenschutzspezifischer verbindlicher staatlicher Regelungen geht. Aus Gründen der Lesbarkeit bezeichne ich diese Koalition im Folgenden als „Datenschutzbefürworter". Diese sprachliche Vereinfachung hat jedoch den Nachteil, dass sie suggerieren könnte, dass die anderen Koalitionen homogene Datenschutz-Gegner seien. Tatsächlich sind unter deren Mitgliedern auch viele Akteure vorzufinden, die Sicherheitsaspekte bzw. Maßnahmen der Selbstregulierung priorisieren, ohne die Bedeutung des Schutzes personenbezogener Daten vollständig zu negieren.

Flexibilitätsbefürworter: Sowie eine dritte Koalition, die sich im Allgemeinen gegen staatliche Regulierung bzw. für die möglichst flexible Ausgestaltung erlassener staatlicher Regeln ausspricht.

Im Weiteren werde ich nun die Koalitionen der Datenschutzbefürworter und der Flexibilitätsbefürworter näher darstellen. Die Koalition der Sicherheitsbefürworter werde ich dagegen nicht näher betrachten, da ich den Betrachtungsrahmen der Arbeit auf das allgemeine Datenschutzrecht beschränke und sicherheitspolitisch relevante Aspekte lediglich dann diskutiere, wenn dies relevant im Hinblick auf die Beantwortung der Forschungsfragen ist. Während der Diskussion der Koalitionen der Datenschutzbefürworter bzw. der Flexibilitätsbefürworter nehme ich allerdings durchaus Bezug auf sicherheitspolitische Argumente und Akteure.

Zudem sei darauf hingewiesen, dass die an dieser Stelle erfolgende Identifikation der Advocacy-Koalitionen nicht auf einer ähnlich ausführlichen Methodik basiert, wie sie zur Identifikation der Advocacy-Koalitionen bei der Aushandlung der DSGVO verwendet wurde. Daher kann es etwa vorkommen, dass Akteure, die eigentlich auf Grundlage des ACFs einbezogen werden müssten, aus dem Blick geraten.

3.5.2.1 Datenschutzbefürworter-Koalition:

Die Koalition der Datenschutzbefürworter vereinigt alle Akteure, die für den Ausbau von gesetzlichen, verpflichtenden Regelungen zum Schutz personenbezogener Daten eintreten.

3.5.2.1.1 Zusammensetzung der Datenschutzbefürworter-Koalition

Die Koalition der Datenschutzbefürworter ist die am längsten bestehende Advocacy-Koalition im Bereich der Datenschutzpolitik. Den Kern dieser Koalition bilden die *Datenschutzaufsichtsbehörden*. Die Entstehung dieser Koalition lässt sich mindestens bis zur DS-RL 95/46/EG zurückverfolgen. Im Vorfeld und während der Verhandlungen der Richtlinie traten die nationalen Datenschutzaufsichtsbehörden in Gestalt eines *transgovernmental network of policy entrepeneurs* (A. L. Newman 2008a) gemeinsam und grenzübergreifend für die Stärkung der Datenschutzregelungen ein (vgl. 3.2.2). Nach der Verabschiedung der DS-RL bzw. der DS-VO kamen zur Gruppe der Datenschutzaufsichtsbehörden auch die *Art. 29-Datenschutz-*

gruppe im Jahr 1996 sowie die Institution des *Europäischen Datenschutzbeauftragten* im Jahr 2004 hinzu (vgl. 3.2.2.7 und 3.2.5). Das Parlament, das bereits in den 1970er-Jahren die Kommission mehrfach zum Erlass gemeinschaftlicher Datenschutzregelungen aufgefordert hatte, nahm zwar zwischenzeitlich – während der Aushandlung der DS-RL – eine ambivalente Rolle ein, setzte sich bei den folgenden Gesetzgebungsprozessen allerdings wieder für die Durchsetzung eines hohen Datenschutzniveaus ein (vgl. 3.2.4 ff.).[256] Noch etwas schwieriger ist diese Bewertung im Hinblick auf die Europäische Kommission. Während die Kommission zwar einerseits immer wieder als Verfechterin eines hohen Datenschutzniveaus aufgetreten ist,[257] war sie zugleich andererseits auch immer wieder jene Akteurin, die sich dem Druck des Ministerrates noch am ehesten beugte.[258] Da der Großteil der bedeutenden EU-Datenschutz-Instrumente dennoch auf die Kommission bzw. die in ihr mit dem Thema Datenschutz befassten Generaldirektionen bzw. Referate zurückgeht, werte ich die Kommission als Teil der Datenschutzbefürworter-Koalition.

Die Datenschutzbefürworter-Koalition setzte sich somit zunächst vor allem aus Akteuren aus dem politischen bzw. politik-nahen Umfeld zusammen. Weitere Akteure traten der Koalition erst im Laufe der Jahre bei.

Ende der 1990er-Jahre weitete der Europäische Verbraucherverband BEUC seine Aktivitäten auf das Feld der Datenschutzpolitik aus und vertrat eine verbraucher- und datenschutzfreundliche Linie. (vgl. die Fn. 153, 177 und 214).

Datenschutz-Organisationen aus dem Bereich der Zivilgesellschaft waren zwar auf nationaler Ebene seit längerer Zeit aktiv (vgl. 3.4.2.3.1), doch ein Engagement auf EU-Ebene erfolgte erst einige Jahre später. Die ersten zivilgesellschaftlichen Akteure aus diesem Bereich waren Privacy International und EPIC. Obwohl sich beide Akteure zwar in unregelmäßigen

256 Ich zähle das Europäische Parlament grundsätzlich zur Koalition der Datenschutzbefürworter hinzu. Bei näherer Betrachtung des Parlaments ergeben sich aber auch Widersprüche. Auf diese gehe ich im folgenden Unterabschnitt über die Überzeugungssysteme etwas näher ein.

257 Vgl. insbesondere die Kommissionsentwürfe zur DS-RL, zur ePrivacy-Richtlinie und zum JI-Rahmenbeschluss (vgl. 3.2.2, 3.3.2 und 3.3.4.4) bzw. die ursprüngliche Haltung der Kommission hinsichtlich der Vorratsdatenspeicherung oder auch des Zugriffs auf Fluggastdaten (vgl. 3.3.4.2 und 3.3.4.3).

258 Vgl. insbesondere die Änderung der Kommissionsposition im Zusammenhang mit der Vorratsdatenspeicherung und dem Zugriff auf Fluggastdaten (vgl. 3.3.4.2 und 3.3.4.3).

Abständen am Policy-Subsystem der EU-Datenschutzpolitik beteiligten, richtete sich ihr Fokus auf die Politik ihres jeweiligen Herkunftslandes. Erst mit EDRi formierte sich eine zivilgesellschaftliche Organisation, die ihren Fokus auf die EU-Politik setzte und die seit Mitte der 2000er-Jahre zunehmend sichtbarer wurde (vgl. 3.4.2.3.1).[259]

Akteur	Akteursgruppe
Nationale Datenschutzaufsichtsbehörden	Datenschutzbehörden
Art. 29-Datenschutzgruppe	Datenschutzbehörden
EDSB	Datenschutzbehörden
Europäische Datenschutz-Konferenz	Datenschutzbehörden
Europäisches Parlament (insb. GUE/NGL, Grüne/EFA, aber immer wieder auch S&D sowie ALDE)	EU-Politik
Europäische Kommission (genauer: die mit Datenschutz befassten Kommissionsstellen)	EU-Politik
BEUC	Verbraucherschutzverband
EPIC	Zivilgesellschaft
EDRi	Zivilgesellschaft
Privacy International	Zivilgesellschaft

3.5.2.1.2 Überzeugungssystem der Datenschutzbefürworter-Koalition

Da die Mitglieder der Koalition tendenziell eher dem linken und linksliberalen gesellschafts- bzw. parteipolitischen Spektrum entstammen, ist auf Ebene der Grundüberzeugungen eine Betonung individueller und gesellschaftlicher Freiheit vorherrschend, während im überwiegenden Teil der Koalition zugleich eine starke Abneigung insbesondere gegen sicherheitspolitisch motivierte Eingriffe in diese Freiheit vorhanden ist.

Die Policy-Kernüberzeugung, die die Mitglieder der Datenschutzbefürworter-Koalition in erster Linie eint, ist die Betrachtung des Schutzes personenbezogener Daten als Grundrecht. Zudem wird dieses Datenschutz-Grundrecht in der Tradition des Volkszählungsurteils als funktional wich-

259 Wissenschaftler(innen) und Fachjournalist(inn)en traten während der politischen Aushandlungsprozesse in eher geringem Maße in Erscheinung. Nennenswert sind hier insb. die deutsche Nachrichten-Webseite „Heise Online“ sowie das Blog Netzpolitik.org

tiges Element im Hinblick auf die Wahrung der Demokratie gesehen.[260] Neue Sicherheits- und Überwachungsmaßnahmen werden seitens der Datenschutzbefürworter-Koalition daher immer an ihren Auswirkungen auf die Demokratie gemessen. So wird im Zusammenhang mit JI-Politiken der Erhalt demokratischer Kontrollmechanismen gefordert. Aufgrund der Skepsis gegenüber zu großer staatlicher Macht werden insbesondere jene Sicherheits- und Anti-Terror-Maßnahmen abgelehnt, denen eine Untergrabung demokratischer Grundwerte zugerechnet wird.[261] Angesichts der in Folge des 11. Septembers zunehmend ausgeweiteten Sicherheits- und Anti-Terrorgesetze bestand das Kernanliegen dieser Koalition während der 2000er-Jahre darin, ein der DS-RL äquivalentes Schutzniveau für die im Rahmen der dritten EU-Säule stattfindenden Verarbeitungen zu etablieren. Allerdings vermochte es die Koalition weder dieses Anliegen in die Tat umzusetzen, noch konnte es andere, den Datenschutz direkt betreffende Überwachungsmaßnahmen wie den Zugriff auf Fluggastdaten verhindern. Insofern muss resümiert werden, dass sich die Koalition der Datenschutzbefürworter während der 2000er-Jahre in einer andauernden Defensiv-Rolle befunden hat.

Koalitionsinternes Konfliktpotential auf Überzeugungsebene besteht insbesondere zwischen den liberalen, sozialdemokratischen und linken Teilen der beteiligten Akteure, wie bei mehreren einschlägigen Auseinandersetzungen im Europäischen Parlament deutlich wurde. Am anschaulichsten zeigten sich die Fronten während der Verhandlungen der ePrivacy-Richtlinie. Als sich der politische Streit anfangs noch um die Frage des Opt-ins/Opt-outs drehte, forderte der liberale Parlamentsberichterstatter Cappato, dass die Lösung der Frage den Unternehmen überlassen bleiben und

260 Vgl. hierzu etwa das Selbstverständnis von EDRi: „To ensure a functioning democracy, basic rights and freedoms need to be guaranteed. In Europe, these rights are established by the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights and by national constitutions. In the digital environment, among the most relevant are the right to privacy and data protection, the right to a fair trial, freedom of thought, expression and information and the right to an effective remedy when our rights have been breached." (EDRi 2019)

261 In diesem Zusammenhang wird immer wieder auch auf das Missbrauchsanfälligkeitsargument verwiesen: „Was passiert denn etwa mit den Daten, die der Staat über Sie und Ihr Surfverhalten sammelt? Die Daten werden zusammen gespeichert. Sie werden an die nächste Regierung weiter gegeben. Ob dann Le Pen, Haider oder Rasmussen darauf Zugriff haben oder nur die normalen obrigkeitsstaatlichen Sozialdemokraten, weiß niemand." (vgl. Ilka Schröder, in: Europäisches Parlament 2002b)

nicht gesetzlich geregelt werden sollte. Am Ende der Auseinandersetzung brachten die sozialdemokratische, grüne und linke Fraktion den Berichtsvorschlag Cappatos schließlich zum Scheitern, da er nicht die von ihnen bevorzugte verbindliche Opt-in-Regel beinhaltete. Als Cappato später einen modifizierten Vorschlag vorlegte, der am Opt-out-Prinzip im Wesentlichen festhielt, kam der größte Widerstand seitens der linken und grünen Fraktionen, während die halbe sozialdemokratische Fraktion sich hinter Cappatos Vorschlag stellte. Schließlich verschoben sich die Fronten ein weiteres Mal, nachdem sich die Sozialdemokraten und die Christdemokraten wenig später dem Druck des Ministerrats im Zusammenhang mit der sicherheitspolitisch motivierten Speicherung von Verkehrsdaten elektronischer Kommunikation beugten. Während die Sozialdemokraten gemeinsam mit den konservativen Fraktionen den sog. Kompromissvorschlag annahmen, stimmten die Grünen, Linken und Liberalen gegen ihn (vgl. 3.3.2).

3.5.2.1.3 Ressourcen der Datenschutzbefürworter-Koalition

Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse

Die Koalition der Datenschutzbefürworter ist in hohem Maße in politische Entscheidungsprozesse eingebunden. Historisch kam diese Rolle insbesondere der EU-Kommission zu, da ihr gemäß Europäischer Verträge eine wesentliche Rolle bei der Vorbereitung, Verabschiedung, Durchführung und Kontrolle von EU-Politiken zukommt (Wessels 2008, 225). Allerdings hat die Macht der Kommission auch ihre Grenzen: Während sie zwar in der Regel (Lelieveldt und Princen 2015, 86) als einziges EU-Organ das Initiativrecht zur Einbringung von Legislativvorschlägen innehat, ist sie trotzdem an die durch die EU-Verträge bestimmten Grenzen gebunden. Diese Verträge wiederum werden seitens der Mitgliedstaaten geschlossen und können, müssen aber nicht zwangsläufig dem Kommissionsinteresse entsprechen (Princen und Rhinard 2006b).

Eine im Laufe der Jahrzehnte zunehmend wichtige Rolle hat das EP eingenommen. Noch zu Beginn der Aushandlung der DS-RL hatte das Parlament (im Rahmen des Kooperationsverfahrens) ein eingeschränktes Mitspracherecht. Mit der Einführung des Mitentscheidungsverfahrens im Rahmen des Maastrichter Vertrags entwickelte sich das Parlament allerdings in zunehmendem Maße zum Mitgesetzgeber. Alle das allgemeine Datenschutzrecht betreffenden Gesetzesvorschläge (Datenschutz-, ISDN-,

ePrivacy- und Cookie-Richtlinie) wurden im dem Mitentscheidungsverfahren verhandelt. Ausgeschlossen war das Parlament dagegen von allen die dritte EU-Säule betreffenden Angelegenheiten. Die Grenzen des Einflusses des Parlaments zeigten sich besonders offenkundig während der Verhandlung des JI-Rahmenbeschlusses. Trotz der Zusagen mehrerer Ratspräsidentschaften, dass die Parlamentsposition ernsthaft berücksichtigt werden würde, einigte sich der Ministerrat aufgrund des Widerstands einiger Mitgliedstaaten letztlich nur auf einen Minimalkonsens. Erst durch die Aufhebung der EU-Säulenstruktur und durch die Aufwertung des Mitentscheidungsverfahrens zum neuen ordentlichen Gesetzgebungsverfahren der EU stieg das Parlament endgültig zu einem formal gleichberechtigten Mitgesetzgeber auf.

Neben diesen beiden Akteuren sind die Art. 29-Datenschutzgruppe (gemäß Art. 30 DS-RL) sowie der Europäische Datenschutzbeauftragte (gemäß Art. 46 lit. d DS-VO) formell in politische Entscheidungsprozesse eingebunden. Allerdings beschränkt sich die Gestaltungsmacht beider Akteure formell auf eine rein beratende Funktion. Besonders seitdem die Kommission in ihrem Überprüfungsbericht aus dem Jahr 2003 feststellte, dass die DS-RL in den Mitgliedstaaten uneinheitlich angewendet wurde, kam der Datenschutzgruppe eine zentrale Rolle bei der Ausarbeitung von Harmonisierungsempfehlungen zu, die zu einer deutlichen Aufwertung ihrer Beratungsfunktion führte. Beide Institutionen stehen insbesondere in regem Austausch mit dem Datenschutz-Referat der Kommission, das für die Datenschutz-Aktivitäten der Kommission zuständig ist sowie dem LIBE-Ausschuss des Parlaments, der für die Ausarbeitung der Parlamentspositionen im Hinblick auf Datenschutzpolitiken zuständig ist. Insofern verfügen beide Akteure über eine besonders große informelle Handlungsmacht im Hinblick auf politische Entscheidungsprozesse. Schwieriger gestaltete sich dagegen das Verhältnis beider Institutionen gegenüber dem Ministerrat, da dieser ein eher geringes Interesse an den Positionen der Datenschützer zeigte.

Die Akteure aus dem Bereich des Verbraucherschutzes und der Zivilgesellschaft sind in legislative Entscheidungsprozesse allenfalls so stark eingebunden, wie die zentralen politischen Entscheider auf ihre Stellungnahmen Rücksicht nehmen.

Unterstützung durch die Öffentliche Meinung

Der Schutz personenbezogener Daten wird von einem Großteil der EU-Bevölkerung als wichtig angesehen. Eine konstante Mehrheit der im Rahmen

von EU-weit repräsentativen Eurobarometer-Studien befragten Personen gibt in allen seit 1991 durchgeführten Studien regelmäßig an, dass sie sich angesichts der praktizierten Datenverarbeitungen unwohl fühlt, während der gesetzliche Schutz personenbezogener Daten befürwortet wird. Allerdings kann nicht von einer uneingeschränkten Befürwortung des Datenschutzes die Rede sein. So befürwortete eine Mehrheit der europäischen Bürgerinnen und Bürger die Einschränkung von Datenschutzrechten zum Zwecke der Bekämpfung von Straftaten, insb. des internationalen Terrorismus. Diese Feststellung trifft jedoch nicht auf die Verarbeitung durch privatwirtschaftliche Akteure zu. Die Mehrheit der EU-Bürgerinnen und Bürger zeigte sich in den 1990ern und 2000ern über die Nutzung ihrer personenbezogenen Daten besorgt (vgl. 3.4.2.2).

Informationen/Informationshoheit

Als die für die Durchführung und Kontrolle aller Unionsmaßnahmen zum Datenschutz hauptverantwortliche Akteurin verfügt die Kommission über zentrales Wissen zu vielen datenschutzpolitischen Fragen. In ähnlicher Weise verfügen die nationalen Datenschutzbehörden bzw. die Art. 29-Datenschutzgruppe sowie der Europäische Datenschutzbeauftragte über erhebliches Praxiswissen hinsichtlich der Anwendung der Datenschutzbestimmungen und ihrer Wirksamkeit. Die zivilgesellschaftlichen Akteure, Verbraucherschutzverbände und Wissenschaftler erstellen Studien und erarbeiten auf diese Weise wertvolles Wissen zu verschiedensten Aspekten des Datenschutzes.

Fähigkeit zur politischen Mobilisierung,

Die Fähigkeit zur politischen Mobilisierung der Koalition ist zwar ausgeprägter als bei der Koalition der Flexibilitätsbefürworter, doch leiden die Datenschutzbefürworter unter dem grundsätzlichen Problem, die in der Bevölkerung vorherrschende generelle Zustimmung für Datenschutzmaßnahmen nicht in eine effektive politische Mobilisierung umsetzen zu können. Eine Ausnahme in diesem Zusammenhang bildeten die enormen Proteste gegen die Vorratsdatenspeicherung insb. in Deutschland, aber auch in einigen weiteren EU-Mitgliedstaaten (vgl. 3.4.2.3.2).

Finanzielle Ressourcen

Über nennenswerte finanzielle Ressourcen verfügen insbesondere die mit Datenschutz befassten Referate der Kommission sowie der LIBE-Ausschuss des Europäischen Parlaments. Beide Institutionen nutzen ihre finanziellen

Mittel für die Durchführung zahlreicher Aktivitäten im Bereich der Datenschutzpolitik. Die mit Datenschutz befassten Kommissionsstellen sind beispielsweise treibender Akteur im Hinblick auf die Diskussion verschiedener Themen wie PETs oder Datenschutzbedenken im Hinblick auf RFID gewesen. Diese und weitere formelle wie auch informelle Diskussionen wurden insbesondere durch die Durchführung von Konsultationen, Anhörungen, Konferenzen und Workshops vorangetrieben. Daneben geben die mit Datenschutz befassten Stellen der Kommission und des Parlaments bereits seit der Frühphase des Datenschutzes regelmäßig Studien zur Untersuchung datenschutzpolitischer Fragen in Auftrag (vgl. 3.2.2.1), (European Commission 2017; Karaboga 2018, 154).

Die zivilgesellschaftlichen Akteure der Koalition verfügen über weitaus geringere finanzielle Mittel. Die einzige im Betrachtungszeitraum auf EU-Ebene aktive zivilgesellschaftliche Organisation EDRi befand sich immer noch weitgehend in der Entstehungsphase. Die anderen Akteure (EPIC, Privacy International, usw.) sind als etablierter einzustufen, doch auch ihnen mangelte es während der 2000er-Jahre an finanziellen Mitteln (Dobusch 2014). Im Falle der niederländischen Bits of Freedom resultierte der Geldmangel – ausgerechnet zur Hochphase der Anti-Vorratsdatenspeicherungsproteste – in der Einstellung ihrer Aktivitäten (Sokolov 2006).

Das *Vorhandensein einer fähigen Führung*

Die Koalition der Datenschutzbefürworter verfügt über keine zentrale Führungsinstanz, die alle Mitglieder der Koalition umspannt. Auf Ebene der einzelnen Akteure kann hingegen durchaus von der Einnahme von Führungspositionen die Rede sein: Im Falle des Parlaments kam diese Rolle den jeweiligen Berichterstattern (z. B. Cappato) bzw. den Schattenberichterstattern (z. B. In't Veld) zu. Bei der Kommission kam eine vergleichbare Rolle zunächst Martin Bangemann zu, später dann auch Barrot und Reding. Auch einzelne Datenschutzbeauftragte bzw. Leiter von Datenschutzaufsichtsbehörden nehmen regelmäßig eine Führungsrolle ein, darunter insb. Peter Hustinx, der von 1996 bis 2000 zunächst Vorsitzender der Art. 29-WP war und von 2004 bis 2014 das Amt des EDSB inne hatte.

3.5.2.2 Flexibilitätsbefürworter-Koalition

Die Koalition der Flexibilitätsbefürworter vereinigt Akteure, die sich gegen eine staatliche Regulierung auf dem Felde der Datenschutzpolitik ausspre-

chen und die stattdessen für eine möglichst flexible Ausgestaltung erlassener staatlicher Regeln eintreten.

3.5.2.2.1 Zusammensetzung der Flexibilitätsbefürworter-Koalition und ihr Verhältnis zur Flexibilitätsbefürworter-Community

Die Flexibilitätsbefürworter-Koalition setzt sich aus Akteuren aus der Privatwirtschaft sowie aus den Regierungen einiger Mitgliedstaaten bzw. aus deren im Ministerrat versammelten Repräsentanten zusammen, unterstützt von den wirtschaftsnahen Kommissionsstellen sowie insb. dem konservativen Teil des EP. Die in dieser Koalition versammelten Akteure eint das gemeinsame Interesse an einem Datenschutzrahmen, der den Unternehmen das höchstmögliche Maß an Freiheit beim Umgang mit personenbezogenen Daten überlässt und keine Kosten durch verpflichtend zu ergreifende Datenschutzmaßnahmen verursacht. Den Nukleus dieser Koalition bilden folglich jene Unternehmen, deren Kerntätigkeit in der massenhaften Verarbeitung personenbezogener Daten liegt. Diese Unternehmen erhalten Unterstützung seitens der Regierungen verschiedener Mitgliedstaaten, die sich aus dieser Unterstützung wiederum vor allem eine Stärkung ihrer heimischen Volkswirtschaften versprechen (vgl. insb. 3.2.2).

Die Kooperation der Flexibilitätsbefürworter ist allerdings weniger stark ausgeprägt als bei den Datenschutzbefürwortern. In der Frühphase des Datenschutzes, während der 1970er- und 1980er-Jahre, verhinderten die Mitgliedstaaten gemeinschaftliche Datenschutzmaßnahmen zunächst noch eher *aus Gewohnheit*: Datenschutz war zu jenem Zeitpunkt noch kein gemeinschaftliches Aktionsfeld und die Bedeutung grenzüberschreitender Datentransfers im Kontext der Binnenmarktpolitik befand sich gerade erst im Entstehen. Folglich hatten die mitgliedstaatlichen Regierungen keine triftigen Gründe für die Abtretung ihrer nationalen – und sich selbst noch gerade erst im Entstehen befindenden – Kompetenzen auf dem Gebiet des Datenschutzes an die Gemeinschaftsebene. In ähnlicher Weise berührte das Thema Datenschutz Ende der 1980er bzw. Anfang der 1990er-Jahre zunächst nur wenige Wirtschaftsbereiche bzw. Unternehmen wie die Direktmarketing- und Kreditbranche, Banken und Versicherungen (Ellger 1990, 108–29; Priscilla M. Regan 1999, 200 f.). Erst mit dem Widerstand gegen den ursprünglichen Richtlinienvorschlag der Kommission, der die weitgehende Abtretung mitgliedstaatlicher Kompetenzen an die Kommission vorsah, wurde der gegenseitige Nutzen zwischen Privatwirtschaft und den

Regierungen der Mitgliedstaaten offenkundig: Die Mitgliedstaaten des sog. nördlichen Blocks traten für nationale statt Gemeinschaftsregelungen ein. Die Privatwirtschaft dagegen unterstützte diese Position, da sie in der Fragmentierung der mitgliedstaatlichen Gesetze kein Problem erkannte. Zum einen konnten durch die Verschiebung von Datenschutz-Kompetenzen in Richtung der Mitgliedstaaten hohe gemeinschaftliche Schutzstandards verhindert werden. Zum anderen eröffnete die Kompetenzverschiebung die Möglichkeit, niedrigere Schutzstandards im *eigenen* Mitgliedstaat als in anderen Mitgliedstaaten zu verabschieden (vgl. 3.2.2). Aus dieser losen *Koalition aus Gewohnheit* entwickelte sich in den Folgejahren schließlich eine zunehmend festere Struktur auf Basis geteilter Überzeugungen.

Dem in anderen Politikbereichen stattfindenden Lobbying im Mehrebenensystem der EU entsprechend (Dialer und Richter 2019), wird auch das Lobbying im Datenschutz-Subsystem in der Regel weniger von einzelnen Unternehmen als vielmehr von Unternehmensverbänden praktiziert. Die am längsten im Bereich der EU-Datenschutzpolitik aktiven Verbände sind FEDMA, der *Verband des europäischen Direkt- und interaktiven Marketings*, der die Interessen datengestützter Marketingspezialisten gegenüber den EU-Organen vertritt; die ICC (*International Chamber of Commerce* – Internationale Handelskammer) mit Sitz in Paris, die die Interessen von inzwischen mehr als 6 Millionen weltweiten Unternehmen und Verbänden aus nahezu allen Wirtschaftsbereichen vertritt; sowie Businesseurope (ehemals UNICE), der europäische Zusammenschluss 40 nationaler Arbeitgeberverbände. In dem Maße, in dem die Verarbeitung personenbezogener Daten zentraler für viele Geschäftsprozesse und für die Steigerung von Unternehmensgewinnen im Laufe der 1990er und 2000er-Jahre wurde, nahm auch die Zahl und die Verschiedenartigkeit der Branchen der Subsystem-Akteure zu. Die Interessen der Werbe- und Marketingbranche wurden in den Folgejahren auch vom *Interactive Advertising Bureau* (IAB) mit Sitz in den Vereinigten Staaten vertreten. Die Interessen der Versicherungsbranche wurden von der europäischen Dachorganisation *Insurance Europe* vertreten. Die *American Chamber of Commerce to the European Union (*AmCham EU) repräsentiert die Interessen der US-Wirtschaft in Europa.[262] Zu den langjährigen Akteuren auf dem Feld der EU-Datenschutzpolitik zählen zudem auch mehrere Verbände aus dem Bereich der Printmedien und des Fernsehens. Die *Association of Commercial Television in Europe*

262 https://lobbypedia.de/wiki/AmCham_EU

(ACT) vertritt die Interessen privater Fernsehsender. Die *European Newspaper Publishers' Association* (ENPA) vertritt die Interessen von über 5.000 Zeitungen aus 25 europäischen Staaten.[263] Das *European Publishers Council* (EPC) ist ebenfalls ein Zusammenschluss europäischer Zeitungs- und Magazinverleger.[264]

Akteur	Akteursgruppe
FEDMA	Privatwirtschaft
ICC	Privatwirtschaft
UNICE (Businesseurope)	Privatwirtschaft
IAB	Privatwirtschaft
AmCham EU	Privatwirtschaft
ACT	Privatwirtschaft
ENPA	Privatwirtschaft
EPC	Privatwirtschaft
EU-Ministerrat	EU-Politik

Tabelle 3-5: Zentrale Akteure der Flexibilitätsbefürworter-Koalition (eigene Zusammenstellung)

3.5.2.2.2 Überzeugungssystem der Flexibilitätsbefürworter-Koalition

Das Hauptinteresse der Flexibilitätsbefürworter besteht in der Reduzierung regulierungsbedingter Kosten bei der ökonomischen Nutzbarmachung personenbezogener Daten. Die in der Koalition versammelten Akteure vertreten tendenziell eher wirtschaftsliberale und konservative Grundüberzeugungen. so wird zwar ebenso wie vonseiten der Datenschutzbefürworter individuelle Freiheit betont, doch eher in einem stark marktwirtschaftlichen Sinne. Fokussiert wird also eher auf das Moment der Abwesenheit von Unterdrückung (negative Freiheit) statt auf die Erweiterung individueller Handlungsspielräume, um die Potentiale der negativen Freiheit auch real nutzen zu können. Das zentrale Argument der Datenschutzbefürworter-Koalition, wonach es sich beim Datenschutz um ein Grundrecht handele, das gegenüber konkurrierenden Interessen grundsätzlich bevorzugt werden sollte, wird abgelehnt. Stattdessen wurde mit verschiedenen Begründungen

263 https://www.enpa.eu/association/mission#board
264 http://epceurope.eu/about/

die Wichtigkeit des unternehmerischen Zugriffs auf personenbezogene Daten betont. Der größte gemeinsame Nenner der verschiedenen seitens der Flexibilitätsbefürworter vorgebrachten Argumente ist die Hervorhebung des gesellschaftlichen Nutzens der privatwirtschaftlichen Datenverarbeitung.[265]

Obwohl viele datenverarbeitende Unternehmen und mitgliedstaatliche Regierungen bzw. Ministerratsdelegierte schon in der Frühphase der EU-Datenschutzpolitik im Vorfeld der Erarbeitung der DS-RL ein gemeinsames Interesse an möglichst niedrigen Datenschutzregulierungsstandards hatten, könnte das damalige Akteursnetzwerk im Sinne des ACF allenfalls als *Advocacy-Community* (Stritch 2015, 442) oder als eine *coalition of convenience* (Koalition aus Bequemlichkeit) (Zafonte und Sabatier 2004, 100) bezeichnet werden. Zwar waren gemeinsame, grundsätzlich gegen eine gemeinschaftsweite Datenschutzregulierung gerichtete Überzeugungen vorhanden, doch hatte es bis zum DS-RL-Vorschlag der Kommission keine Notwendigkeit für eine Kooperation untereinander gegeben, da der Status Quo den Verarbeitungsbedürfnissen ausreichend Rechnung trug. Erst vor dem Hintergrund der als zu restriktiv wahrgenommenen Datenschutzregelungen der DS-RL-Entwürfe der Kommission entwickelten und verfestigten sich erste Kooperationsstrukturen (Priscilla M. Regan 1999). Zu jener Zeit und bis hinein in die Phase der Verhandlung der ePrivacy-Richtlinie lehnten Akteure aus dem Bereich der Wirtschaft jegliche verbindliche Regulierung des Schutzes personenbezogener Daten auf Gemeinschaftsebene ab und verwiesen stattdessen zur Lösung möglicherweise vorhandener Probleme auf Maßnahmen der Selbstregulierung (vgl. 3.2.2 und 3.3.2). Erst mit der Konsultation im Vorfeld des ersten Berichts der Kommission über die Durchführung der DS-RL setzte die datenverarbeitende Wirtschaft einen ernsthaften inhaltlichen Dialog in Gang und stellte Datenschutzregulierung nicht mehr grundsätzlich infrage (vgl. 3.3.3).[266] Stattdessen setzte die Koalition einerseits darauf, dass Datenschutzregeln möglichst flexibel ausgestal-

265 Ein relativ universalistisches Argument ist dabei, dass die gesamte Volkswirtschaft von der möglichst wenig regulierten Verarbeitung personenbezogener Daten profitiere (vgl. z. B. die Diskussion in: Culnan und Bies 2003). Aus der US-amerikanischen Tradition stammt das Argument, dass Datenschutz die für eine Demokratie notwendige, freie Zirkulation von Informationen verhindere (Walker 2001). Andere Argumente verweisen eher auf gesellschaftliche Teilbereiche, wie den Nutzen der Datenverarbeitung für Gesundheitszwecke (Lahmann 2015).

266 Dies ist auch der Grund, weshalb ich für die Koalition die Bezeichnung Flexibilitätsbefürworter statt Regulierungsgegner wähle.

tet werden und andererseits darauf, dass anstelle von *harten* Regulierungsinstrumenten (wie Verordnungen, Richtlinien, usw.) *weiche* Regulierungsalternativen (bspw. Kommissionsempfehlungen) verabschiedet werden.

Insofern besteht die zentrale Policy-Kernüberzeugung der Flexibilitätsbefürworter-Koalition in der Ablehnung staatlicher Regulierungsmaßnahmen. Im Falle einer staatlichen Regulierung setzt die Koalition schließlich vor allem auf Selbstregulierung.

3.5.2.2.3 Ressourcen der Flexibilitätsbefürworter-Koalition

Formelle, legale Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse

Eine ausgesprochen wirkmächtige Einbindung von Koalitionsmitgliedern in politische Entscheidungsprozesse besteht beim Ministerrat. Seit der Frühphase der Datenschutzpolitik hat der Ministerrat immer wieder erfolgreich auf die Reduzierung des von der Kommission und dem Parlament vorgeschlagenen bzw. geforderten Datenschutzniveaus gedrängt, indem entweder eine entsprechende Regelung unmittelbar abgeschwächt wurde oder die Details ihrer Umsetzung den Mitgliedstaaten überlassen wurde. Letzteres kam zwar nicht formal, aber doch praktisch der Durchsetzung eines niedrigeren Schutzniveaus gleich, da das von den Datenschutzbefürwortern angestrebte EU-weit einheitliche Schutzniveau somit untergraben werden konnte. Gerade in der Frühphase des Datenschutzes, aber auch noch bis in die 2000er-Jahre hinein, hatte der Ministerrat aufgrund der gemeinschaftsrechtlichen Situation eine dominante Position im Institutionengefüge der EU inne. Spätestens mit dem Inkrafttreten des Lissabon-Vertrags erfolgte allerdings eine deutliche Annäherung der Machtpotentiale des Parlaments und des Ministerrats (Pittella, Vidal-Quadras, und Papastamkos 2014, 5).

Die in der Koalition vertretenen privatwirtschaftlichen Akteure sind in die interinstitutionellen Entscheidungsprozesse der EU zwar nicht direkt eingebunden, doch kommt der Konsultation ihrer Positionen seitens des Ministerrats, der Kommission und des Parlaments, darunter insbesondere der in erster Linie mit wirtschaftlichen Themen betrauten Ausschüsse IMCO und ITRE, große Bedeutung zu. Daneben hatten und haben die nationalen Mitgliedsverbände eine wichtige Rolle bei der nationalen Implementierung von Richtlinien inne.

Unterstützung durch die Öffentliche Meinung

Obwohl viele Menschen datenverarbeitende Produkte und Dienstleistungen rege nutzen, wird der Verarbeitung personenbezogener Daten seitens privatwirtschaftlicher Akteure nur von einer gesellschaftlichen Minderheit ausdrücklich vertraut während sich die Mehrzahl besorgt über die Verwendung ihrer personenbezogenen Daten zeigt (vgl. 3.4.2.2). Insofern kann davon ausgegangen werden, dass die Flexibilitätsbefürworter nicht auf die Unterstützung durch die öffentliche Meinung bauen können. Den Umstand, dass viele Menschen ihre Produkte und Dienstleistungen nutzen, versuchten die Datenverarbeiter dennoch politisch nutzbar zu machen, indem darauf verwiesen wurde, dass bestimmte Regulierungen die Bedienung der entsprechenden Dienste und Produkte beeinträchtigen würden. Dies war etwa der Fall im Hinblick auf die von der Datenschutzbefürworter-Koalition geforderte Opt-in-Regelung beim Setzen von Cookies (vgl. 3.3.5).

Informationen/Informationshoheit

Die im Ministerrat versammelten Regierungsvertreter bringen große fachliche Expertise zu Datenschutzfragen mit und die Verbände akkumulieren das Wissen ihrer Mitglieder.

Fähigkeit zur politischen Mobilisierung

Die Koalition der Flexibilitätsbefürworter verfügt über keine nennenswerte Fähigkeit zur politischen Mobilisierung.

Finanzielle Ressourcen

Die Koalition verfügt über enorme finanzielle Ressourcen. Diese werden insbesondere seitens der privatwirtschaftlichen Koalitionsmitglieder erfolgreich dafür genutzt, sich systematisch in alle relevanten politischen Entscheidungsprozesse im Mehrebenensystem der EU einzubringen.

Das *Vorhandensein einer fähigen Führung*

Da die Koalition keinem hierarchischen Aufbau folgt, ist keine zentrale Führungsposition vorhanden. Differenziert werden kann dagegen durchaus zwischen den Koalitionsmitgliedern, die sich besonders aktiv in das datenschutzpolitische Geschehen einbringen und jenen, die sich dem seitens der zentralen Akteure vorgegebenen Kurs eher anschließen.