Walter Hallstein-Institut
für Europäisches Verfassungsrecht

Humboldt-Universität zu Berlin

WHI - Paper 15/04

Datenschutz im Europäischen Recht

Alessandra di Martino

2004

DATENSCHUTZ IM EUROPÄISCHEN RECHT

von Alessandra Di Martino*

* LL.M. (Berlin), Doktorandin am Institut für Staatstheorie und Vergleich politischer Institutionen an der Universität von Rom „La Sapienza“. Den Professoren Ingolf Pernice und Paolo Ridola danke ich für Ihre wissenschaftliche Betreuung. Ralf Tietz, LL.M. (Chicago) danke ich für seine Geduld.

Einleitung

Dem Datenschutz wird in den letzten Monaten wieder eine größere Aufmerksamkeit in der europäischen Öffentlichkeit geschenkt. Ausgelöst wurde die Debatte von dem zwischen der Europäischen Kommission und den US-Behörden ausgetragene „Streit" hinsichtlich des von den USA erbetenen Zugriffs auf Daten europäischer Flugpassagiere.[1]

Seit Beginn der Datenschutzregulierung wiesen der europäische und der amerikanische Ansatz politisch-kulturelle Unterschiede auf. Im *post*-11.09.2001 globalen Kontext hatte man sich damit nun erneut auseinanderzusetzen. Jede offene und demokratische Gesellschaft steht vor der unumgänglichen Herausforderung: S*ecuritas* zu gewährleisten, ohne *libertas* einzubüßen. Nicht von ungefähr gehört es zu den Aufgaben der EU, gerade *durch* das Recht einen Raum der Freiheit *und* der Sicherheit zu gewähren (Art. 2 EUV 4. Spiegelstrich i.V.m. Art. 29 EUV und Art. 61 EGV).

Dass der Datenschutz im Europarecht ein zentrales Anliegen geworden ist, bestätigt auch der jüngste Entwurf eines Verfassungsvertrages für Europa. Zusätzlich zum Grundrecht auf Datenschutz der Grundrechtscharta (Art. II-8 VE) wurde eine weitere Bestimmung zum Schutz personenbezogener Daten in dem Titel über „das demokratische Leben der Union" verankert (Art. I-50 VE).

Ziel dieser Arbeit ist es, einen Überblick über den Datenschutz im Europarecht darzulegen und dabei auf einige Aspekte hinzuweisen, welche für den europäischen Stand des Grundrechtsschutzes exemplarisch sind.

Um die der Datenschutzregulierung zugrunde liegenden Wertvorstellungen zu verdeutlichen, sollen zunächst die gesellschaftlichen Voraussetzungen des Datenschutzes erläutert und die sich darauf beziehenden soziologischen Überlegungen dargelegt werden (Teil I). Ist der europäischen Grundrechtscharta vor allem eine objektive Dimension, im Sinne des Begriffes *assiologica* (=Werteordnung), beizumessen,[2] verkörpert auch der Datenschutz einen Wert, hinsichtlich dessen europäische Bürger einen Grundkonsens als Basis einer gemeinsamen Verfassung entwickeln können.

Einen weiteren Exemplarischen Aspekt zum Grundrechtsschutz innerhalb des Europäischen Rechts betrifft die Kompetenzfrage. Am Beispiel des Datenschutzes lässt sich zeigen, inwiefern sich die Schaffung eines Binnenmarkts nicht von der Grundrechtsgewährleistung trennen lässt (Teil II). Das Ziel des zweiten Teils dieser Arbeit liegt daher darin, die Grundrechtsrelevanz einer zur Förderung des Binnenmarktes erlassenen europäischen Datenschutzregelung (vor allem die Datenschutzrichtlinie 95/46/EG) zu erörtern. Ein solcher Grundrechtsgehalt ergibt sich aus einer historischen sowie rechtsvergleichenden Auslegung[3] der Datenschutzrichtlinie. Um diesen Grundrechtsgehalt nachzuweisen, orientiert sich die Arbeit vor allem an der deutschen Rechtsliteratur zum Datenschutz, da diese nicht nur die Entwicklung des Datenschutzes in verschiedenen Perioden der „Datenschutz-gesetzgebung" unterteilt und damit nicht nur einen funktionalen Vergleich zwischen den nationalen und internationalen Datenschutzregelungen ermöglicht, sondern dadurch gleichfalls auch den Grundrechtsgehalt der verschiedenen Datenschutzregelungen hervorhebt (siehe Teil 2 B I 2 a).

---

[1] *Schröder*, C., Der Zugriff der USA auf Daten europäischer Flugpassagiere- Neue Gefahren durch Passagier-Profilbildung? (CAPPS II), RDV 2003, S. 285ff.

[2] *Pernice-Kanitz*, Fundamental Rights and multilevel constitutionalism in Europe, WHI-Paper 7/04, S. 5, unter www.whi-berlin.de; *Ridola, P.,* La carta dei diritti fondamentali dell'Unione europea e le "tradizioni costituzionali comuni" degli stati membri, in: Panunzio/Sciso (Hrsg.), Le riforme istituzionali e la partecipazione dell'Italia all'Unione Europea, Milano 2002, S. 91.

[3] Zur Rechtsvergleichung als fünfte Auslegungsmethode s. *Häberle, P.,* Grundrechtsgeltung und Grundrechtsinterpretation im Verfassungsstaat, JZ 1989, 923ff.

Im Rahmen der genannten Periodisierung lässt sich die Gewährleistung europäischen Datenschutzes (die Datenschutzrichtlinie 95/46/EG) als eine eigene, sogn. dritte Etappe verstehen. Dabei wird die Besonderheit des europäischen Datenschutzrechts gerade darin gesehen, dass es *seiner Natur nach* besonders auf Rechtsvergleichung angelegt ist. Historisch lässt sich beweisen, dass das deutsche Recht auf informationelle Selbstbestimmung eine maßgebliche Rolle für die Entwicklung des europäischen Datenschutzkonzeptes gespielt hat (siehe Teil 2 B II 2).
Die Verflechtung zwischen nationaler und europäischer Datenschutzregelungen, und dessen Integration durch bisherigen (insbesondere durch EMRK gewährleisteten) internationalen Datenschutzstandard, lässt sich dabei begrifflich mit dem Modell eines Verfassungsverbundes bzw. eines *multilevel constitutionalism* erfassen[4].

Durch die europäische Datenschutzrichtlinie wird der Tatbestand der Übermittlung personenbezogener Daten in Drittländer zum ersten Mal umfassend reguliert. Fraglich ist, inwiefern die oben angesprochene Übermittlung von Flugpassagierdaten an die USA von der Richtlinien erfasst wird (Teil III).

Die Spannung zwischen Sicherheit und Freiheit wird im Bereich der dritten Säule der Union besonders deutlich. Sowohl das Schengen-Recht, als auch Europol und die jüngst mit den USA abgeschlossenen Abkommen weisen Bedenken im Hinblick auf das Rechtsstaats- und Demokratieprinzip auf (Teil IV A).

Ähnlich wie die zur dritten Säule der Union gehörenden Maßnahmen zur Datenverarbeitung waren auch die durch europäische Organen und Einrichtungen durchgeführten Datenverarbeitungen von der Datenschutzrichtlinie nicht erfasst. Aus diesem Grund wurde Art. 286 in den EGV eingeführt, sowie durch die VO 45/2001/EG das Amt des europäischen Datenschutzbeauftragten errichtet (Teil IV B), welche die jüngste der sich auf europäisches Primärrecht stützenden Institutionen ist.

Teil 1 : Datenschutzrecht in der Informationsgesellschaft

A. Informationsgesellschaft als Risikogesellschaft im Spiegel der technologischen Entwicklung

Aus einer historischen Perspektive heraus betrachtet ist das „Datenschutzrecht“ noch ein recht junges Rechtsgebiet.[5] Seine Entstehung ist mit der technologischen Umwandlung im Bereich der Datenverarbeitung eng verknüpft und seine Entwicklung erstreckt sich über die Informationsgesellschaft, „einer Gesellschaft, die stark von der Informationstechnik in den Bereichen Arbeit, Freizeit und Produktion bestimmt wird und in der ein zunehmender Teil der Beschäftigten im Informationssektor tätig ist“[6], hinaus. In der Literatur wurde sogar behauptet, dass „kein anderes Recht den Übergang zur Informationsgesellschaft treffender bezeichnet, als der Datenschutz“[7].
Es mag anachronistisch sein, im Jahr 2004 von einer „technologischen Revolution“ infolge der Anwendung des Computers in allen Lebensbereichen zu reden. Nicht verfehlt ist aber der Terminus in Bezug auf die 60er und 70er Jahre, in denen jene radikale Umänderung stattgefunden hatte. Die

4 *Pernice, I.*, Europäisches und nationales Verfassungsrecht, VVDStRL (2003), 60, 149ff.; *ders.* Multilevel constitutionalism in the European Union, ELR 2000, 511ff.
5 *Abel, R.B.*, Geschichte des Datenschutzes, in: Roßnagel (Hrsg.), Handbuch des Datenschutzrechts, München 2003, Rn. 1
6 *Ellger, R.*, Datenschutz im grenzüberschreitenten Datenverkehr, Baden-Baden 1990, S. 59.
7 *Donos, P.K.*, Datenschutz, Prinzipien und Zielen, Baden-Baden 1998, S. 19.

Durchsetzung der Informatik[8] erfolgte genauso irreversibel, wie der Ersatz der Handschrift durch den Buckdruck im 15. Jahrhundert.[9]
Im Gegensatz zu einer klassischen Maschine, welche durch ihre teilweise einzige Beschaffenheit beurteilt wird, ist ein Computer auf Grund seiner zugrunde liegenden Algorhytmen universell einsetzbar. Daten, welche ein Computer speichert und verarbeitet, vereinfachen die Realität zweiseitig. Zum einem wird die äußere Wirklichkeit zur Information. Ihre Komplexität wird dazu auf wenige zweckmäßige Strukturen reduziert. Des weiteren verzichtet EDV auf Sinn und Zweck der Informationen und verarbeitet sie so, als seien sie kontextfrei.[10] Informationen erlangen somit Datenform. Gespeicherte Daten werden in großen elektronischen Dateien (sog. Datenbanken) gesammelt, verknüpft und organisiert.
In einen Pionierbeitrag[11] zu diesem Thema wies *Simitis* darauf hin, dass was technisch betrachtet elektronische Datenverarbeitung ausmacht, für die Individuen und die Gesellschaft sowohl Chancen als auch Gefahren bewirkt.
Einerseits ermöglichen die bis dahin unerreichbare Geschwindigkeit und räumliche Verringerung potentiell unbegrenzte Informationssammlungen. Andererseits sind solche technologischen Umwandlungen in der Lage, das Wissen und das Tun der Menschen zu verändern. Beides hängt zusammen. Fehlt einem das eigene Wissen, wird der Einzelne orientierungslos oder vom heteronomen Wissen abhängig. Er verliert seine Selbständigkeit, da ihm seine Orientierungen nicht gehören.[12]
Diesen Gedanke hat das BVerfG 1983 in einer durchaus bekannten Formel ausgedrückt: Damit der Mensch frei und bewusst handeln kann, muss er überschauen können, „wer, was, wann, und bei welcher Gelegenheit über ihn (oder sie) weiß.“[13]
Die Entwicklung der EDV kann in vier Perioden aufgeteilt werden.

I. 70er Jahre: der Staat als Leviathan?

Figuren wie Hobbes Leviathan sowie Orwells *Big Brother* symbolisieren Tendenzen der Totalisierung des Staates und der Uniformisierung sowie Degradierung der menschlichen Person.[14] Ein ähnliche Furcht vor einer bevorstehenden totalen Überwachung schürten Anfang der 70er Jahre staatliche Großrechnungsanlagen.[15]
In Frankreich, Schweden und in den USA wurden Projekten geplant, welche alle staatlichen Register und Dateien automatisch steuern und verknüpfen konnten. Die amerikanische öffentliche Verwaltung erwarb sogar eine der am meist detaillierten Marketinglisten mit Angaben von über 2 Millionen Haushalten, um ihre Informationsgrundlage zu verbessern.[16]
Die wirtschaftlich angespannte Lage forderte eine Senkung der Sozialausgaben und Anhebung der Steuereinnahmen. Der Staat wollte sich vergewissern, dass Leistungen nur von wirklich Berechtigten bezogen und Steuerhinterziehungen wirkungsvoll aufgedeckt werden. Um diese Aufgaben zu erfüllen,

---

[8] Das Wort kommt aus der Zusammensetzung von Information und Automatik und deutet darauf, daß Informationen automatisch verarbeitet werden, vgl. *Frosini, V.,* Diritto alla riservatezza e calcolatori elettronici, in: Alpa/Bessone (Hrsg.), Banche dati Telematica e diritti della persona, Padova 1984, S. 31
[9] *Simitis, S.*, Virtuelle Presenz und Spurenlosigkeit - Ein neues Datenschutzkonzept, in: Hassemer (Hrsg.), 25 Jahre Datenschutz, Baden-Baden 1996, S. 38.
[10] *Hoffmann, B.,* Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes, Baden-Baden 1990, S. 148-9.
[11] *Simitis, S.,* Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, 673ff.
[12] *Tinnefeld/Ehmann,* Einführung in das Datenschutzrecht, München Wien 1998, S. 2
[13] BVerfG, „Volkszählungsentscheidung“, in NJW 1984, S. 422.
[14] Vgl. u.a. *Alpa, G.,* Privacy e Statuto dell'informazione, in: Alpa/Bessone (Hrsg.), Banche dati Telematica e diritti della persona, Padova 1984, S. 32.
[15] *Rodotà, S.*, Tecnlogie e diritti, Bologna 1995, S. 44.; *Walz,S.*, Multimedia- Ende des Datenschutzrechts? in: Hassemer (Hrsg.), 25 Jahre Datenschutz, Baden- Baden 1996., S.50; *Simitis, S.,* Virtuelle Presenz und Spurenlosigkeit,, a.o.O. (Fn. 9), S. 28-30.
[16] *Simitis, S.,* Reicht unser Datenschutz angesichts der technischen Revolution?, Strategien zur Wahrung der Freiheitsrechte, S . 21ff., in: Schöler (Hrsg.), Informationsgesellschaft oder Überwachungsstaat?, Opladen 1986, S. 26-29.

bediente sich der Staat vor allem der Rasterung von Informationen und deren Abgleich zwischen Finanz-, Arbeits-, Ordnungsämter.[17]
Allerdings, wenn auch in einem Sozialstaat Datenspeicherung und Verarbeitung eine unentbehrliche Voraussetzung sind, um den Bürgern Leistungen bereitstellen zu können, fragt sich inwiefern es jedem Einzelnen zugemutet werden kann, seine Daten zur Verfügung zu stellen. Die Inanspruchnahme der Datensammlungen wurde als autoritäres Mittel der Krisenbewältigung gesehen.[18]

II. 80er Jahre: die EDV in der Privatwirtschaft

Das folgende Jahrzehnt hat jedoch den oben dargelegten Befürchtungen widersprochen. Zumindest Drei der bis dahin geltenden Behauptungen erwiesen sich als unrichtig.[19] Zum einem wurde es für möglich gehalten, dass die Verarbeitung personenbezogener Daten in immer größeren Datenbanken zentralisiert werden könnte. Zweitens war man der Auffassung, dass die Automatisierung der Datenverarbeitung, nicht zuletzt aufgrund ihrer Kosten, nur bestimmte Personengruppen betreffen würde. Drittens, dachte man, dass feste Verarbeitungsprozesse weitgehend nur in staatlichen Datensammlungen erforderlich waren.
Stattdessen hat sich durch die breite und alltägliche Anwendung von PCs, Laptops und Notebooks die Datenverarbeitung dezentralisiert. Diese Tendenz hat sich später auf Grund der Vernetzung irreversibel verstärkt. Was die Subjekte der Datenverarbeitung anbelangt hat sich der Schwerpunkt der Datenverarbeitung immer mehr in die Privatwirtschaft verlagert.[20] Vergleichbar mit der Verwendung der AGB's zur Senkung der Transaktionskosten,[21] beschränkt sich die Wahrnehmung der Verbraucher auf eine Reihe von Personalangaben, welche das Unternehmen durch ein abgedrücktes Formular beansprucht.
Ähnliches findet innerhalb eines Arbeitsverhältnisses statt. Während in der Vergangenheit nur einzelne betriebliche Funktionen, wie die Lohnabrechnung und die Zugangskontrolle, per Computer gesteuert wurden, sind heutzutage der systematische Einsatz der Personalinformationssysteme sowie die sog. Betriebsdatenerfassung keine Besonderheit mehr. Sie gehören zum alltäglichen Betriebsleben.[22] Im Personalwesen wird der Arbeitgeber wegen der zahlreichen gesetzlichen Auskunfts-, Bescheinigungs- und Meldepflichten als eine Art „Inkassostelle" für den Staat gesehen.
Dass dadurch Anforderungsprofile für den jeweiligen Arbeitsplatz angefertigt und mit Arbeitsfähigkeitsprofilen der einzelnen abgeglichen werden können, welche z.B. aus Informationen über Krankheiten, Fehlzeiten, Alter, Leistung usw. bestehen, ist zweckdienlich für den Arbeitgeber, aber jedoch nicht gerade unproblematisch für den (potentiellen) Arbeitnehmer.[23]

III. 90er Jahre: Kreditkarten und Telekommunikation

Der Schwerpunkt der Datenverarbeitung in den 90er Jahre liegt deutlich im Telekommunikationsbereich. Hier sei zunächst[24] vor allem an das Netz ISDN[25] erinnert, dessen

---

17 *Simitis, S.*, Reicht unser Datenschutz angesichts der technischen Revolution?, a.o.O (Fn. 16), S. 29.
18 *Rodotà, S*, Tecnologie e diritti, Bologna 1995, S. 58
19 *Simitis, S.*, Virtuelle Presenz und Spurenlosigkeit, a.o.O. (Fn.9), S. 30
20 *Simitis, S.*, Virtuelle Präsenz und Spurenlosigkeit, a.o.O. (Fn.9), S. 30-33.
21 Um nachteilige Transaktionskosten zu ersparen, bedienen sich Unternehmen der Allgemeinen Geschäftsbedingungen. Wenn einerseits dadurch ein Gewinn an Effizienz erreicht wird, werden andererseits die vertraglichen Konditionen gegenüber allen Kunden egalisiert.
22 *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, Köln 1994, S. 23ff; *Tinnefeld/Ehmann*, a.o.O. (Fn.12), S. 22.
23 *Tinnefeld/Ehmann*, a.o.O. (Fn.12), S. 23.
24 Hinsichtlich des Internets sei auf den nächsten Abschnitt verwiesen.
25 *Integrated Service Digital Network*, vgl. Empfehlung des Rates vom 22 Dezember 1986, Abl. 1986 L 382, 36ff; Entschließundg des Rates vom 18. Juli 1989, Abl. 1989 C 196, 4ff.Entschließung des Rates vom 5. Juni 1992 zur Entwicklung des ISDN in der Gemeinschaft als europaweite Telekommunikationsinfrastruktur, Abl. 1992 C 158, 1ff.; Entschließung des Rates vom 9. November 1995, Abl. 1995 L 282, 16ff. Innerhalb der EG unterliegt das ISDN außerdem den Regeln über die Liberalisierung der Telekommunikation. Hierzu zählen insbesondere die (Rahmen)richtlinie des Rates

Einführung europaweit durch die EG erfolgte. Leistungsmerkmale wie eine Anrufumleitung oder „Rückruf bei belegt“ können Dritten von einem vertraulichen Kontakt in Kenntnis setzen. Darüber hinaus, anders als bei analogen Netzen, werden bei einem digitalen Netz wie dem ISDN alle Verbindungsdaten, welche potentiell für alle verfügbar sind, in einem Vermittlungsrechner gespeichert. Gleiches gilt für Mobilfunknetze, welche zusätzlich ermöglichen, den Ort zu identifizieren und zu speichern, wo sich ein Gerät befindet.[26]
Bemerkenswert ist, dass sich solche Speicherungen automatisch abspielen, also ohne dass irgendeine externe Handlung eines Dritten vonnöten ist. Sie sind bereits in der Struktur der Systeme angelegt. Daraus folgt, dass Verletzungen in den Rechtspositionen der Einzelnen so leicht sein können, dass versucht wird, sie zu banalisieren.[27]
Die Selbstverständlichkeit der Datenverarbeitungsprozesse wird durch die Verbreitung der Bezahlungen mittels Kreditkarten und die damit verbundene *co-branding* Strategien zwischen Unternehmen bestätigt.[28] Die „Gläsernen Kunden“[29] werden zudem selbst zum Schaufenster, wenn Systeme der sog. „Data Warehouses“ (welche Daten aus den operativen Datenbanken aller eingebundenen Unternehmensbereiche integrieren und aggregieren) und „Data Mining“ (welche es erlauben, selbständig große Datenbestände durch datenverarbeitungsgestütze Algorithmen auf Zusammenhänge hin zu analysieren)[30] unbegrenzte Anwendung finden.

IV. Herausforderungen am Anfang des 21. Jahrhunderts

Wird die gegenwärtige Gesellschaft als Informations- und Risikogesellschaft verstanden, sind sowohl das Internet als auch das Genom andererseits ihrer Symbole.

1) Internet

Internet wird oft als das „Netz der Netze“[31] oder die „Datenautobahn“ bezeichnet.[32] Im Internet befindet sich eine unbegrenzte Menge an Daten im Umlauf. Die zugängliche Datenpalette umfasst neben Aktienkursen, Kreditkarteninformationen und Personalien auch Daten über den Gesundheitszustand Einzelner. Die Methode der Datengewinnung und Übertragung vollzieht sich oftmals ohne Kenntnisnahme der Betroffenen. Als Beispiele gelten die sog. „*cookies*“ (welche die Festplatte eines *surfers* ausspähen können) sowie „*mail-grabbing*“ Programme (welche die in sogn. *Newsgroups* stattfindenden Diskussionen rastern und nach bestimmen Schlagworten filtern – eine Methode, die in den USA vor allem zum Zwecke der Personalauswahl nicht unüblich ist[33]). Betreiber der Netze bzw. Access-Provider speichern automatisch grundsätzlich jede Kommunikation eines Teilnehmers. Dadurch wird eine vollständige Dokumentation des Kommunikationsverhaltens einer Person erreicht, was wiederum auf ihre/seine Gewohnheiten und Vorlieben schließen lässt.

---

zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provision- ONP), vom 28 Juni 1990 , Abl. 1990 L 192, 1ff. und die Richtlinie über den Wettbewerb auf dem Markt für Telekommunikationsdienste vom 28 Juli 1990, Abl. 1990 L 192, 10ff.

26 *Gridl, R.,* Datenschutz in globalen Telekommunikationssystemen, Baden-Baden 1999, S. 33-34 und 75.

27 *Gridl, R.*, a.o.O (Fn. 26), S. 74.

28 *Simitis, S.*, Virtuelle Präsenz und Spurenlosigkeut, a.o.O. (Fn.9), S. 32.

29 *Gola/Klug,* Grundzüge des Datenschutzrechts, München 2003, S. 127.

30 *Scholz, R.,* Datenschutz bei Data Warehousing und Data Mining, in Roßnagel (Hrsg.), Handbuch des Datenschutzrechts, München 2003, Rn. 17 und 28.

31 *Simitis, S.,* Internet oder der entzauberte Mythos, in: Assmann (Hrsg.), Festschrift für Kübler, Heidelberg 1997, S. 292.

32 *Arndt, H.W.*, Datenschutz im Internet, in: Festschrift für Arndt, Heidelberg 2001, S. 393

33 *Grippo, V.,* Analisi dei dati personali presenti su Internet, La legge 675/96 e le reti telematiche, Rivista critica di diritto privato 1997, S. 654.

2) Das Genom

Das menschliche Genom ist die größte Sammlung personenbezogener Daten, die jeder einzelne ständig mit sich trägt. Es besteht aus genetischen Daten, welche Träger von Angaben über die körperliche und psychische Struktur einer Person sind und deren Identifizierung ermöglichen.[34] Diese Daten[35] enthalten eine ganz besondere Art von Information,[36] denn im Gegensatz zu den üblichen personenbezogenen Daten können sie erstens nicht wirklich anonymisiert werden und zweitens, verschwimmen die Besonderheiten des Betroffenes, sog. *data subject*, indem die Analyse jeder DNA zugleich Informationen über die Eltern, Geschwister und Kinder der betroffenen Person preisgibt. Des weiteren ist der Informationsgehalt genetischer Daten häufig unübersichtlich, da die Reaktion der sozialen Umgebung eine entscheidende Rolle spielt. Viertens haben einige genetische Informationen existentielle Auswirkungen auf das weitere Leben der getesteten Person (z.B. Veranlagung zu unheilbaren Krankheiten). In diesen Fällen kann das Nichtwissen über seine eigene Daten zu befürworten sein.
Erhebliche Bedenken ruft auch der Gebrauch genetischer Daten im Arbeitsbereich und Versicherungswesen hervor, da ein genetisches Ausleseverfahren zum Schaden „nicht resistenter" Arbeit- bzw. Versicherungsnehmer befürchtet wird[37].

B. Der soziologische Gegenstand des Datenschutzes

Um eine teleologische Auslegung der Datenschutznormen zu fördern sowie deren Wertgehalt hervorzuheben, erscheint es hilfreich, den Lebenssachverhalt des Datenschutzrechtes mit sozialwissenschaftlichen Methoden zu definieren. *Domos*[38] folgend lohnt es sich dazu vor allem auf die Systemtheorie Luhmanns und die Kommunikative Handlungstheorie Habermas einzugehen. Obwohl der funktionell strukturelle Ausgangspunkt *Luhmanns* zu der eher individualistischen Perspektive *Habermas* wenig im Einklang zu stehen scheint,[39] können beide Ansätze in relativierter Form als Ergänzung des jeweils anderen betrachtet werden.

I. Habermas

Nach Habermas ist freies kommunikatives Handeln die erforderliche und ausreichende Voraussetzung unabhängiger Reproduktion der Lebenswelt.[40] Kommunikatives Handeln funktioniert als kulturelle Reproduktion, sowie soziale Integration und Sozialisation. Damit sich eine Gesellschaft reproduziert, ist die Erhaltung symbolischer Strukturen der Lebenswelt durch die Sprache erforderlich. Die Entwicklung der Informationssysteme und deren Dezentralisierung und Vernetzung könnte eine „kommunikative Metaebene" erzeugen. Letztere könnte die intuitiven und unabhängigen

---

34 *Schladebach, M.*, Genetische Daten im Datenschutzrecht, CR 2003, S. 226, subsumiert so genetische Daten unter § 3 Abs. I BDSG.

35 Allgemein wird zwischen nicht-codierten und codierten Sequenzen der DNA differenziert, wobei lediglich die letzten erbliche Informationsträger sind. Nicht-codierte Sequenzen werden im Rahmen der Verbrechensbekämpfung z.B. mittels des sog. Fingerabdrucks sowie des Vaterschaftsnachweises analysiert. Codierte Sequenzen werden auf Grund derer Aussagekraft über zukünftigen Gesundheitszustand bei der pränatalen Diagnostik sowie bei der Behandlung der Erbkrankheiten eingesetzt.

36 *Menzel, H.J.*, Brennpunkt: Datenschutz-DNA-Analysen, Die rechtliche Sicht, in: Sokol (Hrsg.), Der gläserne Mensch - DNA Analysen, eine Herausforderung an den Datenschutz, Düsseldorf 2003, S. 6.

37 *Tinnefeld/Ehmann*, a.o.O. (Fn. 12), S. 24-27; *Beckmann*, Selbstbestimmungsrecht - was bleibt? (Gen-)informationelles Selbstbestimmungsrecht. Ethische Fragen, in: Sokol (Hrsg.), Der gläserne Mensch - DNA Analysen, eine Herausforderung an den Datenschutz, Düsseldorf 2003, S. 122-127; *Menzel, H.J.*, a.o.O. (Fn. 16), S. 5-6.

38 *Donos, P.K.*, a.o.O. (Fn.7), S. 19.

39 *Cesareo*, V., Sociologia- Teorie e problemi, 6. Aufl., Milano 2004, S. 5-9, 80ff., 129ff. und 168ff.

40 *Habermas, J.*, Agire comunicativo e logica delle scienze sociali, Bologna 1980, S. 87ff und 319ff., *ders* in: *Habermas/Luhmann*, Theorie der Gesellschaft oder Sozialtechnologie, Frankfurt 1971, S. 142ff.

kommunikativen Handlungen der Individuen beeinträchtigen. Informationssysteme können ihre Imperative durch Entsprachlichung der Kommunikation auf die Lebenswelt übertragen.
In Anlehnung an das Habermas'sche Verständnis von Geld und Macht, sieht *Donos* Informationssysteme als ein Ersatz der Sprachfunktion und insofern als ein manipulatorisches Steuerungsinstrument. Die darin liegende Missbrauchsgefahr steigt vor allem dann, wenn der Einsatz von Informationssystemen gesellschaftlich weder thematisiert noch kritisiert wird.[41] Die Aufgabe des Datenschutzes liegt daher vor allem darin, kommunikative Räume zu schaffen, in denen sich individuelle Lebenswerte reproduzieren und Personen kommunikativ entfalten können.[42]

II. Luhmann

Während die Perspektive Habermas auf die Bedeutung der Integrität einer Kommunikation als Schutzgegenstand des Datenschutzes deutet, kann Luhmanns' Systemtheorie weitere relevante Aspekte hervorheben. Darunter zählen sowohl die Informationsasymmetrie, eine der Ursachen von Machtgefällen der heutigen Gesellschaft, als auch das Verständnis des heutigen Menschen als eine Summe verschiedener Rollen.[43]
Luhmann geht davon aus, dass das System „Gesellschaft" aus weiteren autopoietischen Subsystemen besteht, welche einem eigenem Reproduktionsprozess folgen. Indem sie die Komplexität der Umwelt überwinden, reproduzieren sich diese Teilsysteme und steigern ihre Funktionalität.[44] Neben anderen spielen Informationssysteme eine Schlüsselrolle. Durch schnelle Ausdifferenzierung der aus der Unwelt stammenden Daten favorisieren Informationssysteme die Selektions- und Entscheidungskapazität und damit die Systemfunktionalität anderer Subsysteme in entscheidendem Maße.[45] Nicht ohne Grund war ein ursprüngliches Anliegen des Datenschutzrechts, Informationsvorsprung einiger Subsysteme (z.B. der Regierung gegenüber dem Parlament sowie der Verwaltung gegenüber den Bürger innerhalb des politischen Systems) durch Informationsgleichgewicht zu ersetzen.[46]
Das Modell einer in Subsystemen geteilten Gesellschaft wirkt ebenso auf das Verhältnis einzelner Individuen mit deren Umwelt. Jeder Mensch kann nur dann mit einem System kommunizieren, wenn er die jeweilige Rolle übernimmt und das entsprechende Datenprofil als eigene Handlung anerkennt.[47] Es muss zwischen Person und Rolle getrennt werden, wobei die Zuverlässigkeit der Verhaltenserwartungen mehr durch Rollen, als durch Personen gewährleistet wird. Einerseits erscheinen solche Rollentypen als Fremdbeschreibungen, welche Rechtfertigungs- und Anpassungszwänge hervorbringen können. Andererseits spiegeln sie die unterschiedlichen sozialen Situationen in der gegenwärtigen hoch differenzierten Gesellschaft vereinfachend wieder.

III. Kombination beider Ansätze im Bezug auf den Datenschutz

Obwohl *Luhmann* menschliches Verhaltens primär als eine Erfüllung der an normative Rollentypen gerichteten Erwartungen versteht, verneint er die Entwicklung menschlicher Individualität nicht gänzlich. Nach ihm ist Individualität als eine „freiwillige Leistung" zu verstehen, wodurch alle Teilaspekte einer Persönlichkeit in einer Biographie integriert werden.[48] Somit ergibt sich auch in einer hauptsächlich funktionalistisch Anschauung ein gewisser Spielraum für individuelle Handlungen. *Habermas* hingegen legt den Schwerpunkt seines normativen Ansatzes auf das Individuum: Durch Kommunikation werden Selbstreflexion und Handlungsfähigkeit angeregt, woraus eine progressive

---

41 *Donos*, a.o.O (Fn. 7), S. 45 und 59-61.
42 *Donos*, a.o.O (Fn. 7), S. 38-55.
43 *Cesareo, V.*, a.o.O. (Fn. 39), S. 129-134.
44 *Luhmann, N.*, Soziale Systeme, Frankfurt 1985, S. 30ff und 45ff.
45 *Luhmann, N.*, in: *Habermas/Luhmann*, a.o.O (Fn. 40), S. 16; vgl. *Donos, P.K.*, a.o.O. (Fn.7), S. 34.
46 Simitis u.a., BDSG-*Simitis*, Baden-Baden 2002, Einleitung, Rn. 21
47 *Luhmann, N.*, Grundrechte als Institution, Berlin 1974, S. 62ff.
48 vgl. sich auf Luhmann stützend *Trute, H.H.*, Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, Rn. 14-15.

Entstehung echter Individualität erfolgt Zugleich berücksichtigt er aber auch die heteronome Wirkung funktionalbedingter Systeme auf individuelle Kommunikationshandlungen. Beide Modelle enthalten eine Kombination individueller und funktionaler Verhaltenselemente, wobei jedoch deren Verhältnis zu einander unterschiedlich verstanden wird.
Hinsichtlich des Lebensbereiches des Datenschutzes erlangt somit vor allem die Kommunikationsintegrität im Habermas'schen Sinne Relevanz. Sie zu schaffen und zu bewahren kann als normatives Ziel einer Datenschutzregelung gesehen werden.
Nach Luhmann bewirken Informationssysteme die Reduktion der Umweltkomplexität. Die mit diesem verbesserten Datenzugriffsmöglichkeit verbundene Entstehung von Informations- bzw. Machtgefällen können, wie die ersten Datenschutzgesetze Hessens und Schwedens bewiesen, gerade durch Datenschutzregelungen bewältigt werden.
Des weiteren versteht Luhmann menschliche Vielfalt als durch Rollentypen schematisierbar an, was auch der Perspektive einer Datenbank entspricht, welche den Einzelnen z.B. lediglich als Kunde, Bürger, Arbeitnehmer oder Patient wahrnimmt. Durch den Datenschutz wird die Erstellung von Rollentypen nicht vermieden, sondern durch das Zweckbestimmungsprinzip sogar zum Postulat rechtmäßiger Datenverarbeitung gemacht. Nach ihm ist es gerade nicht erlaubt verschiedene Datenprofile, welche jeweils andere Rollentypen betreffen, beliebig zu verknüpfen.

Teil 2: Die europäische Datenschutzrichtlinie

A. Ziele und Kompetenz

1995, zwanzig Jahre nachdem eine Resolution des Europäischen Parlaments sich für eine einheitliche Regelung der Verarbeitung personenbezogener Daten ausgesprochen hatte, wurde die Richtlinie des Europäischen Parlaments und des Rates „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" verabschiedet (RL 95/46/EG: DSRL). Die Kommission nahm dabei jedoch eine abwartende Haltung ein. Anstatt selbst die Initiative eines Rechtsaktes zu ergreifen, zog sie es vor, den Mitgliedstaaten zu empfehlen, die Datenschutzkonvention des Europarates zu ratifizieren (s. unten B. I 2) b)). Was auf den ersten Blick merkwürdig erscheint, spiegelt in Wirklichkeit die unterschiedlichen Ausgangspunkte des Parlaments und der Kommission wieder. Während für die Kommission der Gemeinsame Markt eine wirtschaftspolitische Handlungsvoraussetzung und -zweck war,[49] betrachtete das Parlament die Datenverarbeitung aus der Perspektive ihrer möglichen Folgen für die Rechte der Einzelnen.[50]
Diese Ambivalenz lässt sich auch aus der schwerfälligen Überschrift ableiten: Im Unterschied zu den nationalen Gesetzen und zur Konvention des Europarates ist nicht nur vom Datenschutz die Rede. In einem Atemzug wird neben dem „Schutz natürlicher Personen" auch der „freie Datenverkehr" erwähnt.[51] Auch die Zwecksetzung der Richtlinie erwähnt beide Aspekte: Die Schaffung des Gemeinsamen Markts (Art. 1 Abs. 2; Erwägungsgründen 5, 7, 8, 9) und Gewährung des Grundrechtsschutzes (Art. 1 Abs. 1; Erwägungsgründen 1, 2, 3, 10).
In diesem Regelungs-Spagat spiegelt sich der die Beratungen des Rates begleitende Kompetenzstreit wieder. Da derzeit keine Norm des EGV der Gemeinschaft ausdrücklich die Zuständigkeit zuwies, den Umgang mit personenbezogenen Daten zu regeln, hätte eine europäische Regelung in diesem Bereich an sich scheitern sollen. Darüber hinaus war auch der Bezug zu den Grundrechten nicht

[49] Vgl. die Politikfelder der EG, welche die Informationsgesellschaft betreffen, in: *Kloepfer/Neun*, Rechtsfragen der europäischen Informationsgesellschaft, EuR 2000, S. 514-525
[50] *Simitis, S.*, Die EU-Datenschutzrichtlinie-Stillstand oder Anreiz?, NJW 1997, 281; *ders*, in Damman-Simitis, SRL-*Simitis*, Einleitung, Rn. 1; *Burkert, H.*, Internationale Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, Rn.42.; *Abel, R.B.*, Geschichte des Datenschutzrechts, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, Rn. 45.
[51] Damman-Simitis, DSRL-*Simitis*, Einleitung, Rn. 4.

unproblematisch: Wie das Gutachten 2/94 des EuGH[52] deutlich hervorhob, fehlt der EG eine allgemeine Menschenrechtszuständigkeit.
Inwiefern Datenverarbeitung und insbesondere inter-mitgliedstaatliche Datenübermittlungen Bestandteil des Gemeinsamen Marktes sind (I) und inwiefern dieser eines grundrechtlichen Schutzes bedarf (II) wird nachfolgend dargestellt.

I. Data Flows in einem gemeinsamen Markt

Die Schaffung eines europäischen Binnenmarkts durch die Verschmelzung der nationalen Märkte (Art. 3 c; 14 EGV) betrifft auch den Sektor der Datenverarbeitung. Die Infrastruktur der Telekommunikationsdienste ist ihrem Wesen nach, der Raumüberwindung einschließlich der grenzüberschreitenden Bewegung von Daten angelegt.[53]
Der Datenverkehr fällt unter den Tatbestand der gemeinschaftsrechtlichen Grundfreiheiten. Erstens, kommt der freie Warenverkehr (Art. 28 EGV) in Betracht, da unter dem Begriff der „Waren" auch die Träger von Informationen zu verstehen sind. Erfasst sind neben den eher traditionellen Zeitungen, Zeitschriften, Büchern, Audio- und Videokassetten, auch alle auf Computerdisketten oder anderem technischen Material gespeicherten Informationen. Zweitens, garantiert ein freier Dienstleistungsverkehr (Art.49 EGV) die Freiheit der Verbreitung von Informationen, die entgeltlich und nicht lediglich akzessorisch zum materiellen Träger übermittelt werden, z.B. eine künstlerische Aufführung oder eine Rundfunksendung oder sonstiger elektronische Punkt zu Punkt Übermittlungen über Telekommunikationsnetze. Drittens, wird die Freizügigkeit (Art. 39 EGV) der Arbeitnehmer gewährleistet, welche in der Informationsbranche, einschließlich aller kulturellen und journalistischen Tätigkeiten, beschäftigt sind. Viertens, ist den in der Informationsbranche Selbständigen (Presse, Verleger, Rundfunk- und Filmunternehmen, Erbringer von online Diensten, Wirtschaftsinformationsdienste etc.), das Recht der freien Niederlassung gewährt (Art. 43, 48 EGV).[54]
Das ungestörte Funktionieren des Binnenmarkts (Art. 14 Abs.2 EGV) ist aufgrund der Unterschiedlichkeit der Datenschutzregelungen der Mitgliedsstaaten verwehrt. Diese könnte ein Hindernis zur vollen Gewährleistung der (informationellen) Grundfreiheiten bewirken und Wettbewerbsverzerrungen hervorrufen. Insofern stellt Datenschutz eine Beschränkung der informationellen Grundfreiheiten der EGV dar. Um innerstaatlich weiter bestehen zu dürfen, muss diese Beschränkung gemäß dem die Grundfreiheiten strukturierenden Gemeinschaftsrecht gerechtfertigt sein. Soweit die in Art. 30 und 46 EGV vorgeschriebenen Voraussetzungen nicht vorliegen, müssen die vom EuGH erarbeiteten „zwingenden Erfordernisse bzw. Gründe des Allgemeininteresses" gegeben sein.[55] Dazu kann der Datenschutz gezählt werden. Dies ergibt sich z.B. auch aus dem Fall *Alpine Investments*[56], wo es um ein Verbot der Verarbeitung personenbezogener Daten für unerbetene Werbeanrufe zum Absatz von Finanzdienstleistungen ging, was den Tatbestand eines Eingriffs in die Dienstleistungsfreiheit erfüllte. Zum „Schutz des Rufes des nationalen Finanzmarktes" und „der Kapitalanleger" hielt der EuGH diese Beschränkung für gerechtfertigt. Obwohl das Gericht selbst nicht von Datenschutz sprach, lässt sich das in diesem Falle das bejahte zwingende Erfordernis des Allgemeininteresses als Datenschutz im Gewand des Verbraucherschutzes verstehen.[57]

---

[52] Slg. 1996, S. I-1763.
[53] *Ellger, R.*, Datenschutz im grenzüberschreitenten Datenverkehr, a.o.O. (Fn. 6), S. 54-59.
[54] Grabitz/Hilf-*Brühann*, München 1999, Richtlinie 95/46, Vorbem. A 30, Rn. 11-14.
[55] Rs. 120/78, Slg.1979, 649 (Cassis de Dijon).
[56] Rs. C-348/93, auch abgedrückt in: NJW 1995, 2541ff.
[57] Grabitz/Hilf-*Brühann*, Richtlinie 95/46, Vorbem. A30, Rn. 29; vgl. *Weichert, T.*, Datenschutz als Verbraucherschutz, DuD 2001, 264; Dass Rechtfertigungsgründe den jeweiligen aktuellen Präferenzen entsprechen, betont u.a. Mayer: *Mayer, F.*, Die Warenverkehrsfreiheit im Europarecht- eine Rekonstruktion, Walter Hallstein-Institut für Europäisches Verfassungsrecht Paper 1/04, http://www.berlin.de/warenverkehr.htm , S. 5 Fn 23, (EuR 2003, S. 797).

Falls ein Interesse als ein zwingendes Erfordernisse in diesem Sinne gewertet wird, kommt eine Rechtsangleichung in Betracht[58]. Die Funktion einer solchen Rechtsangleichung liegt darin, dieses Allgemeininteresse auf Gemeinschaftsebene zu behandeln und zu schützen und zugleich eine für alle Mitgliedstaaten gleichermaßen geltende Ausnahme von den Grundfreiheiten zu schaffen. Als passende Rechtsgrundlage bietet sich Art. 95 EGV an.

II. Datenschutz als Grundrecht

Bis vor kurzem verfügten die EU und ihr Kern, die EG, über keinen Grundrechtskatalog.[59] Der EuGH hat jedoch im Wege der Rechtsfortbildung Grundrechte als allgemeine Rechtsgrundsätze in die Rechtsordnung der Europäischen Gemeinschaften eingeordnet. Für die Legitimation und Einbindung der europäischen Hoheitsgewalt in einen Verfassungsverbund war dies unentbehrlich.[60] Einerseits hat sich der EuGH auf die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten gestützt, sowie auf die EMRK und andere völkerrechtliche Verträge über Grund- und Menschenrechte, denen die Mitgliedstaaten beigetreten sind. Hierbei gelten weder die Verfassungsüberlieferungen der Mitgliedstaaten noch die völkerrechtliche Verträge unmittelbar als europäisches Recht, sondern sind als Rechtserkenntnisquellen zu begreifen.[61] Andererseits hat das geschriebene Verfassungsrecht der EU selbst diese Legitimation gebilligt (Art. 6 Abs. 2 EUV).[62]

1) Entwicklung zum eigenständigen Schutzbereich

Mehrmals haben sich der EuGH und das EG mit Datenschutzthemen auseinandergesetzt, wenn auch der in Frage kommende Tatbestand nicht unter einem „Grundrecht auf informationelle Selbstbestimmung“ subsumiert wurden, sondern unter dem eher traditionellen Recht auf Achtung der Privatsphäre, dem Wohnungsgrundrecht und dem Recht auf rechtliches Gehör.
Dass der Schutzbereich eines Rechts auf Datenschutz ursprünglich nicht klar von den Schutzbereichen anderer Grundrechte zu trennen war, ist allerdings keine Besonderheit des europäischen Rechts. An dieser Stelle sei nicht nur an das vom deutschen Bundesverfassungsgericht anerkannte Recht auf informationelle Selbstbestimmung als Konkretisierung des Allgemeinen Persönlichkeitsrechts i.S.d. Art. 2 Abs. 1 GG erinnert, sondern auch an das italienische *diritto alla riservatezza*, welches je nach Auffassung entweder aus dem Kommunikationsgrundrecht gem. Art. 15 Cost., aus dem Recht auf Meinungsfreiheit nach Art. 21 Cost. oder aus der allgemeinen Grundrechtsbestimmung i.S.d. Art. 2 Cost. abgeleitet wird.[63] Als weiteres Beispiel zählt das amerikanische *right to privacy*, welches der *Supreme Court* in der grundlegenden *Griswold* Entscheidung[64] aus den „*penumbra zones*“ mehrerer Grundrechte, den I, IV, V, IX *Amendments*, herrührt.

---

[58] Es bestehet daher ein Zusammenhang zwischen Anwendungsbereich der Warenverkehrsfreiheit und Regelungskompetenz: s. *Mayer, F.*, a.o.O. (Fn. 57), S. 15 (EuR 2003, S. 810).
[59] Die Charta der Grundrechte der Europäischen Union wurde beim Rat von Nizza am 7. Dezember 2000 unterzeichnet.
[60] *Pernice, I.*, Gemeinschaftsverfassung und Grundrechtsschutz, Grundlagen, Bestand und Perspektiven, NJW 1990, 2410.
[61] *Streinz, R.*, Europarecht, 5. Aufl., Heidelberg 2001, Rn. 358
[62] Statt allen, *Zuleeg,* Zum Verhältnis nationaler und europäischer Grundrechte, EuGRZ 2000, S. 511.
[63] Der Reihenfolge nach: *Pace, A.*, Nuove frontiere della libertà di “comunicare riservatamente”..?, Giurisprudenza costituzionale 1992, 746; *Cerri, A.*, Libertà negativa di manifestazione del pensiero e di comunicazione, Giurisprudenza costituzionale 1974, 618; *Giampiccolo,* La tutela giuridica della persona umana e il cd. diritto alla riservatezza, Rivista trimestrale di diritto e procedura civile 1958, 465-466.
[64] Vgl. *Baldassarre, A.*, Privacy e costituzione, Roma 1974, S. 322.

2) Die Entwicklung des grundrechtlichen Datenschutzes durch Rechtsprechung des EUGHs

Schon beim ersten Gemeinschaftsgrundrechte bejahenden Urteil des EuGHs ging es um eine Datenschutzthematik. In der Rs. 29/69 (*Stauder*[65]) war Streitgegenstand, ob Gutscheine, welche an Sozialhilfeempfänger zum Kauf von Butter zu herabgesetzten Preisen ausgegeben wurden, anonymisiert werden müssen. Der EuGH urteilte, dass hinsichtlich der einschlägigen Kommissionsentscheidung die am wenigsten belastende Auslegung für den Betroffenen vorzuziehen sei. Folglich kann die „Rs. *Stauder* unter Berücksichtigung heutiger Datenschutzmaßstäbe (Zweckbindungsgrundsatz, Prinzip der Datenanonymität), als Ausgangspunkt zur Entwicklung eines Rechts auf informationelle Selbstbestimmung im Gemeinschaftsrecht angesehen“ werden.[66]
Oftmals war das europäische Beamtenrecht Anlass dafür, offene Fragen im Datenschutzrecht zu beantworten. Im Fall *Baltsavias* (T-39/93 und T-553/93)[67] wurde die Kommission zum Ersatz des immateriellen Schadens verurteilt, der dem Kläger durch das Vorhandensein nicht gestatteter Parallelakte entstanden ist. Einschlägige Rechtsnorm war hier Art. 26 des Beamtenstatuts. Als unmittelbar betroffen wurde kein Grundrecht angesprochen.
Dazu im Gegensatz stehend hat der EuGH in der Rs. *X/Kommission* (C-404-92)[68] unmittelbar Bezug auf Art. 8 EMRK genommen. Bei der Einstellungsuntersuchung eines Beamtenbewerbers seien Untersuchungen auf bestimmte gesundheitliche Risiken gegen dessen Willen (z.B. verdeckter Aids-Test) nicht zulässig. Sie verletzen das Recht auf Achtung des Privatlebens i.S.d. Art. 8 EMRK, welches (im Sinne einer Rechtserkenntnisquelle) über Art. 6 Abs. 2 EUV für die europäische Rechtsordnung maßgeblich ist.
Dementsprechend wurde auch in anderen Fällen der Anwendungsbereich des Art. 8 EMRK i.V.m. Art. 6 Abs. 2 EUV als eröffnet angesehen. Eine Verletzung wurde jedoch verneint, wenn nach Meinung des EuGHs das gemeinschaftsrechtliche Allgemeinwohl überwog.[69]
In der Entscheidung *Stanley-Adams*[70] (Rs. 145/85) erkannte das EuGH implizit an, dass personenbezogene Daten unter die Geheimnispflicht der Kommissionsbediensteten i.S.d. Art. *214 a.F EGV* (Art. 284 n.F. EGV) fällt. Früher war der Vertraulichkeitsschutz des Schriftverkehrs zwischen einem Anwalt und seinem Mandant im Fall *Am&S*[71] gewährt worden.
Des weiteren ist auf die auf Anlass der exekutiven Befugnisse der Kommission erlassenen Urteile (VO 17/62) Bezug zu nehmen. Am Prüfstein stand die Schaffung der Informationen durch die Kommission im Bereich des Wettbewerbsrechts, wobei es auch um die Geltung der europäischen Grundrechte für juristische Personen ging. Während im Fall *National Panasonic*[72] (Rs.136/79) eine Verletzung des Recht auf rechtliches Gehör eines Unternehmens für möglich gehalten wurde, weigerte sich der EuGH in Rs. *Hoechst* (Rs.46/87, 227/88) das Grundrecht auf Unverletzlichkeit der Wohnung einer juristischen Person zu gewähren. Jüngst hat sich die Rechtsprechung jedoch in dieser Hinsicht gewandelt. Im Fall *Roquette*[73] dehnte der EuGH, dem EGMR folgend, den Schutzbereich dieses Rechts dergestalt aus, dass er nunmehr auch Geschäftsräume umfasst.
Bezüglich der von der Kommission erlangten Informationen wurde des weiteren in der Rs. C-67/92[74] ein Beweisverwertungsverbot für nationale Behörden innerhalb nationaler Wettbewerbsverfahren bejaht.

---

65 Slg. 1969, 419ff.
66 *Dressel, C.O.*, Die gemeinschaftsrechtliche Harmonisierung des europäischen Datenschutzrechts, München 1995, S. 210.
67 Slg. ÖD 1995 I-A, S. 233ff.
68 Slg. 1994, II-4780 ff.
69 *K/Kommission*, T-176/94; *Gill/Kommission*, T-90/95; *Gaspari/Parlament*, T-66/98; *N/Kommission*, T-273/94.
70 Slg. 1985, S. 3539.
71 Slg. 1982, S. 1575.
72 Slg. 1980, S. 2033ff.
73 Rs. C-94/00, EuGRZ 2003, 35ff.
74 *Direccion General de Defensa de la Competencia/AEBP*, in EuZW 1992, S.671.

Insgesamt kann man daraus schlussfolgern, dass sich die Maßnahmen der Gemeinschaftsorgane bzw. die Auslegung des Gemeinschaftsrechts auch schon vor Inkrafttreten der DSRL am grundrechtlichen Datenschutz zu orientieren hatten.

III. Die Kompetenzfrage zwischen Binnenmarktorientierter Rechtsangleichung und Grundrechtsschutz

Erkennt man den Datenschutz als rechtfertigendes „zwingendes Erfordernis" an, bietet sich *Art. 100a EGV* (Art. 95 EGV) als der richtige Anknüpfungspunkt für eine gemeinschaftliche Harmonisierung an (s.o. I). Im Gegensatz zu Art. *235 a.F. EGV* (Art. 308 n.F.), welcher im Rahmen der Beratungen als alternative Rechtsgrundlage in Betracht und eigentlich in der Systematik des Gründungsvertrags auch nur als ultima ratio[75] verstanden wird, fordert Art. 95 EGV als Quorum keine Einstimmigkeit, sondern lediglich eine qualifizierte Mehrheit. Damit reduziert sich die Risiken eines Kompromisszwanges und eines Vetoboykotts.[76]
Dennoch ist die Anknüpfung an Art. 95 EGV dem Wortlaut nach nicht unproblematisch. Die binnenmarktfinale Rechtsangleichung nach Art. 95 EGV setzt voraus, dass unterschiedliche Regelungen der Mitgliedsstaaten zu Hindernissen des Binnenmarktes und damit der Marktfreiheit werden. Wie bereits festgestellt wurde, liegt das besondere am Datenschutz jedoch gerade darin, dass er nicht nur ein „zwingendes Erfordernis" i.S.d. *Cassis*-Rechtssprechung darstellt, sondern darüber hinaus auch Grundrechtscharakter aufweist. Während die Datenschutzrichtlinie, sofern sie lediglich als Harmonisierungsmaßnahme verstanden wird , eindeutig von Art. 95 EGV gedeckt wird, könnte sie, als Grundrechtskonkretisierung aufgrund des Prinzips der Einzelermächtigung (Art. 5, 7 EGV, und dessen Bestätigung durch den EuGH im Gutachten 2/94) als kompetenzlose Maßnahme ungültig sein. Das zur Suche der zutreffenden Kompetenz bzw. Rechtsgrundlage üblicherweise angewandte Kriterium, d.h. der aus dem Zweck und Inhalt der Regelung zu entnehmende Schwerpunkt, könnte sich in diesem Fall als nicht befriedigend erweisen. Dem Titel der DSRL folgend sowie ihrem Art. 1 nach, ist Zweck der Richtlinie sowohl der Grundrechtsschutz („der Schutz der Grundrechte und insbesondere das Recht auf Schutz der Privatsphäre"), als auch der Freie Datenverkehr. Einige der zahlreichen Erwägungsgründen (1, 2, 3, 10) konzentrieren sich auf den ersten, andere (5, 7, 8, 9) auf den zweiten Aspekt.
Auch die bisher vor dem EuGH vorgelegten Fälle bestätigen diese Widersprüchlichkeit. Obwohl die DSRL nie Gegenstand einer Nichtigkeitsklage kraft Unzuständigkeit i.S.d. Art. 230 EGV war, stellte sich die Kompetenzfrage im Rahmen eines Vorabentscheidungsverfahrens (vgl. unten B II 3 d).[77] Bemerkenswert ist hierbei, dass auf die Kompetenzproblematik lediglich der Schlussantrag des Generalanwalts Tizzanos eingeht. Nach ihm liegt der Schwerpunkt der DSRL in der Herstellung des Binnenmarktes. Die Richter des EuGHs betonten zwar ausdrücklich die Grundrechtsrelevanz der DSRL, enthielten sich jedoch jeglicher Stellungnahme hinsichtlich der Kompetenzgrundlage und gingen damit stillschweigend von der Gültigkeit der DSRL aus.
Diese vermeintliche Widersprüchlichkeit würde sich jedoch auflösen, wenn man bedenkt, dass sich die Regelungsziele des Grundrechtsschutzes und der Binnenmarktrealisierung nicht gegenseitig ausschließen. Sie sind keine kontradiktorischen Konzepte.[78]
Begründen lässt sich diese Auffassung damit, dass Verwirklichung des Binnenmarktes kein rein wirtschaftliches Anliegen ist, da sich „die Rechtsangleichung ... trotz ihrer marktfunktionalen Zielbindung als genuine Gemeinschaftsgesetzgebung mit [auch] sog. nicht-ökonomischen Regelungszielen dar[stellt]."[79] Der im *Art. 100a Abs. 3 a. F.* verankerte Hinweis auf Verbraucher-,

---

[75] *Opperman, T.*, Europarecht, 2. Aufl., München 1999, Rn. 524.
[76] Damman/Simitis, DSRL-*Simitis*, Baden-Baden 1997, Einleitung, Rn. 5. *Simitis* definiert der Kompetenzstreit als ein „verhüllter Versuch, die Union davon abzuhalten, gemeinsame Datenschutzregelungen aufzustellen" und die Auseinandersetzung über den richtigen Anknüpfungspunkt als Verlagerung solcher Kompetenzstreit sieht.
[77] EuGH, Urteil vom 20.5.2003, Rs. C-465/00; C-138/01 und C-139/01, EuGRZ 2003, 232ff.
[78] Vgl. *Ridola, P.*, Diritti di libertà e mercato nella "costituzione europea", Quaderni costituzionali 2000, 31ff.
[79] *Müller-Graff*, Die Rechtsangleichung zur Verwirklichung des Binnenmarktes, EuR 1989, 134.

Umwelt- und Gesundheitsschutz deutet daraufhin, dass sich der Akzent auf die Lebensbedingungen des Einzelnen verschoben hat.[80] Obwohl die Harmonisierung nach Art. 95 EGV marktfunktional begründet ist, deckt sich ihr Regelungsinhalt oft mit dem bisherigen Kernbereich staatlicher Rechtsetzung. Überlegungen über Kompetenzabgrenzung allein erweisen sich somit als zu kurz greifend, um die Inhaltsgestaltung einer Rechtsangleichungsmaßnahme zu beurteilen.[81] Hierauf deutet auch die jüngst erlassene *Schmidberger*-Entscheidung,[82] wonach eine Maßnahme zum „Schutz der Grundrechte" als „zwingendes Erfordernis" die Binnenmarktsfreiheit zu begrenzen vermag und somit eine extensive Anwendung von Art. 95 EGV begründen könnte.[83]

B. Rechtsentwicklung und Rechtsvergleichung bei der Datenschutzrichtlinie

Für die DSRL lässt sich feststellen, wie der Inhalt der europäischen Datenschutzregelung einer bestimmten historischen Entwicklung folgt und wie sich daraus die grundrechtliche Dimension des Datenschutzes ergibt. Insofern ist der Behauptung zuzustimmen, dass die „Union [durch die DSRL] erstmals im Bereich der Grund- und Freiheitsrechte gesetzgeberisch"[84] tätig wurde.
Die Richtlinie ist wegen ihrer Flexibilität das typische Instrument der Rechtsangleichung[85]. Durch sie wird die Kompetenz der Mitgliedstaaten zur autonomen Rechtssetzung eingeschränkt und ihnen gleichzeitig die Wahl der Mittel überlassen, so dass die jeweiligen nationalen Besonderheiten berücksichtigt werden können. Einen solchen „Spielraum" misst den Mitgliedstaaten auch die DSRL bei (Erwägungsgrund Nr. 9), wobei ein möglichst „hohes Schutzniveau zu erreichen ist" (Erwägungsgrund Nr. 10). Da eine Harmonisierung keine Vereinheitlichung ist, wurde auch hier vermutet, dass Auslegung bzw. Umsetzung der Richtlinie sich hauptsächlich nach der jeweils eigenen nationalen Rechtstradition richten würden und die ursprüngliche Regelungsvielfalt in einem für den Binnenmarkt unerträglichen Maß weiter bestehen könnte.[86] Im Nachhinein hat sich diese Gefahr jedoch als nicht erheblich erwiesen,[87] so dass die Spannung zwischen europäischer Regelungseinheit und nationaler Regelungsvielfalt im konkreten Fall der DSRL durch die Umsetzung sowie mittels einer progressiven prozeduralen Harmonisierung (s.u.), ihre „praktische Konkordanz"[88] finden konnte.
Nationale Regelungen spielen jedoch nicht nur bei der Umsetzung eine wichtige Rolle, sondern vielmehr auch bei der davor liegenden Entstehung der angleichenden Regelung. Rechtsvergleichung ist für die Vorbereitung und Verfassung einer Richtlinie i.S.d. Art. 95 EGV unentbehrlich, was nicht zuletzt dazu beitragen soll, dass die europäische juristische Kultur einen Wandel vom Positivismus zum Rechtsvergleich erfährt.[89]
Gerade bei der DSRL waren „unterschiedliche juristische Ansätze und verschiedenartige Rechtskulturen auf einen Nenner zu bringen."[90] Die DSRL setzt sich nämlich aus einer konsistenten Kombination wesentlicher Elemente der verschiedensten nationalen Datenschutzgesetze zusammen, welche sich wiederum auf das „europäisch geprägte nationale Recht"[91] auswirken.

---

80 Damman/Simitis, DSRL-*Simitis*, Einleitung Rn. 6.
81 *Müller-Graff*, a.o.O. (Fn. 79), 134.
82 EuGH, Urteil vom 12.6.2003, Rs. C-112/00, EuZW 2003, 592.
83 *Pernice/Kanitz*, a.o.O. (Fn. 3), S. 17 Fn. 61
84 *Burkert, H.*, a.o.O. (Fn. 50), Rn.45.
85 *Opperman, T.*, a.o.O. (Fn. 75) , Rn. 1229.
86 Damman-Simitis, DSRL-*Simitis*, Einleitung, Rn. 5; allgemein zur Harmonisierung, *della Cananea, G.*, L'Unione europea, Bari 2003, S. 51-52.
87 KOM (2003) 265 endg., Erster Bericht über die Durchführung der Datenschutzrichtlinie.
88 Die bekannte Formel Hesses wird hier in einem anderen Kontext als dem ursprünglichen (dem der Grundrechtsabwägung) angewandt.
89 *della Cananea, G.*, a.o.O. (Fn. 86), S. 173.; wie oben erwähnt, soll nach Häberle Rechtsvergleichung „die fünfte Auslegungsmethode" werden: *Häberle, P.*, Grundrechtsgeltung und Grundrechtsinterpretation, a.o.O. (Fn. 4), 916.
90 *Abel, R.B.*, Geschichte des Datenschutzes, a.o.O. (Fn. 50), Rn. 46.
91 *Opperman*, a.o.O. (Fn. 75), Rn. 1229.

Die Vielheit der Datenschutzkonzepte, die in der DSRL nebeneinander bestehen, läßt sich nicht nur räumlich (jedes Datenschutzkonzept gilt auf dem Territorium eines jeden Mitgliedstaates), sondern auch zeitlich bejahen.
Die DSRL und deren nationale Anpassung der lässt sich der sogn. „dritten Generation" der Datenschutzgesetze zugeordnet.[92] Daher finden sich in ihr sowohl einige antizipierte Elemente der nachfolgenden vierten Generation (Stichwort: „Modernisierung der Datenschutzgesetze") voraus, andererseits sind Elemente der ersten, sowie der zweiten Generation in der DSRL als Niederschlag zu finden (s.u. I). Ein Blick auf die Entwicklung der Datenschutzgesetzgebung wird zeigen, wie eng nationale und internationale Lösungen verbunden sind. Rechtshistorische und rechtsvergleichende Perspektiven stützen sich gegenseitig.

I. Die Generationen der Datenschutzgesetze

Wie oben erwähnt, ist es in der (vor allem deutschen) Literatur üblich, zwischen verschiedenen Generationen der Datenschutzgesetze zu unterscheiden. Der die dritte Generation der Datenschutzgesetze konkretisierenden DSRL wird ein eigenständiger Teil gewidmet (s. u. II). Folgend werden die der DSRL vor- bzw. nachkommende Periode näher dargestellt.

1) Erste Generation: Regelungsansätze

Auslöser der ersten Generation ist die Großrechner Technologie (vgl. Teil 1 A I). Anfang der 70er Jahren wurden das hessische (HDSG, 1970) sowie das schwedische Datenschutzgesetz erlassen. 1977 und 1978 folgten das deutsche und das französische Datenschutzgesetz.
Alle genannten Datenschutzgesetze wiesen die Gemeinsamkeit auf, dass kein Gesetzgeber auf ein ausführliches, über lange Jahre hinweg aufgearbeitetes Fallmaterial, einschließlich richterlicher Entscheidungen, zurückgreifen konnte. Daher war die legislative Aufgabe mit einem ungewöhnlich hohen Maß an Unsicherheitsfaktoren belastet. Die Gesetzgeber mussten Regelungsformen bevorzugen, die den Nachteil eines nur unscharf abgrenzbaren Regelungsgegenstandes durch ein Höchstmaß an Flexibilität ausglichen.[93] Da die Lösungsansätze sich nicht einheitlich entwickelten, lassen sich zwei Regelungsmodelle unterscheiden. Ein drittes Modell, das des bereichsspezifischen Ansatzes, haben die USA aufgenommen. Auf dessen Besonderheiten wird im weiteren Verlauf (Teil 3 C) näher eingegangen.

a) Der globale Ansatz

Der deutsche sowie der österreichische Gesetzgeber hatten ein global angelegtes Modell ausgewählt. Solche Regelungen sind insofern „global" zu verstehen, indem grundsätzlich jeder, der personenbezogene Daten verarbeiten möchte, sie beachten soll. Folglich sind die Kernvorschriften solcher Gesetze sehr allgemein formuliert. Das „Informationsdefizit des Gesetzgebers verbirgt sich hinter einer Vielzahl von Generalklauseln, deren Dehnbarkeit das am ehesten geeignete Mittel ist, eine möglichst anpassungsfähige Regelung zu erzielen."[94] Darüber hinaus wurde ein „Selbsteinschätzungsmodell" befürwortet. Dieses legt die Kriterien der Rechtmäßigkeit für den Verantwortlichen fest und beabsichtigte, dass dieser die Umsetzung des Gesetzes durchführt, und überlässt es ihm, die Rechtmäßigkeit des Verarbeitungsvorgangs einzuschätzen.[95] Im Gegensatz zum nächsten Ansatz, spielt bei diesem Modell die institutionalisierte und zentralisierte Kontrolle eine eher untergeordnete Rolle.

---

92 Obwohl alle Autoren die Geschichte des Datenschutzes periodisieren, sind die jeweilige Periodisierungen nicht immer identisch, vgl. *Abel, R.B.,* Geschichte des Datenschutzrechts, a.o.O. (Fn. 50), Rn. 45.; Simitis u.a, BDSG-*Simitis*, Einleitung, Rn. 134; *Brühann*, Die Anforderungen der Europäischen Datenschutzrichtlinie, in: Bäumler/Mutius (Hrsg.) Datenschutzgesetze der dritten Generation, Neuwied 1999, S.12.
93 Simitis u.a, BDSG-*Simitis*, Einleitung, Rn. 113.
94 Simitis u.a, BDSG-*Simitis*, Einleitung, Rn. 114
95 *Burkert*, a.o.O. (Fn.50), Rn. 46.

Der Nachteil eines globalen Ansatzes liegt jedoch in der Durchlässigkeit der geschaffenen rechtlichen Infrastruktur. In rechtspolitischer Hinsicht führt ein exzessiver Gebrauch von Generalklauseln zu einer Abdankung des Gesetzgebers und einer machtergreifenden Interpretationsherrschaft der datenverarbeitenden Verwaltung bzw. Privatinstitutionen.[96]

b) Lizenzmodell

Den umgekehrten Weg hat der schwedische Gesetzgeber genommen. In der Heimat der Ombudsstellen sowie der Verwaltungsöffentlichkeit hat er sich für ein Lizenzmodell entschieden.[97] Da er das gesetzgeberische Informationsdefizit nicht überspringen konnte, hat er das Verarbeitungsverfahren nicht an detaillierte Bedingungen geknüpft, sondern stattdessen eine Kontrollinstanz eingerichtet.

Der Schwerpunkt liegt hier bei einem Verfahren, das dem Verantwortlichen zur Offenlegung der Verarbeitungsziele und Verarbeitungsmodalitäten zwingt. Die Erklärungen durch den Verantwortlichen über Art und Weise der Verarbeitung werden mit einem formalen Akt anerkannt oder abgelehnt. Eine solche Genehmigungspflicht ermöglicht es der Kontrollinstanz konsequent und zielbewusst zu reagieren und gleichzeitig den mangelhaften Wissenstand des Gesetzgebers zu kompensieren. Andererseits zieht das Lizensierungsmodell ein Übermaß an Bürokratisierung nach sich.[98]

c) Verbindung verschiedener Ansätze

Nicht jedes Gesetz entspricht einem der beiden Regelungsmodelle. So hat der französische Gesetzgeber versucht, verschiedene Ansätze miteinander zu verbinden. Wenn auch die Einrichtung einer besonderen Kontrollinstanz (*CNIL: Commission Nationale de l'Informatique et des Libertés)* für ein Lizensmodell spricht, ist die Genehmigung nicht das einzige und entscheidende Regelungsmittel. Für nicht-öffentliche Stellen wird vielmehr lediglich eine Anmeldung vorgesehen, so dass sich der Schwerpunkt auf zahlreiche materielle Vorgaben zur Verarbeitung verschiebt.[99]

d) Datenschutz und Informationsfreiheit

Aus einigen der ersten Datenschutzgesetze (z.B. aus dem hessischen sowie dem schwedischen, nicht aber aus dem BDSG) ist zu entnehmen, inwiefern Datenschutz eine informationsrechtliche Angelegenheit ist. Der Umgang mit personenbezogenen Daten wird hierbei zusammen mit dem die Existenz einer demokratischen Gesellschaft unmittelbar berührenden sog. „Informationsgleichgewicht" behandelt.[100] Während der hessische Gesetzgeber sich gegen einen Informationsvorsprung der Regierung gegenüber dem Parlament wehrte, sicherte das schwedische Datenschutzgesetz den freien Zugang zu staatlichen Informationen.

Obwohl dieser Zusammenhang zwischen zwei eng miteinander verbundenen Fragenbereichen später aufgelöst wurde, ist heutzutage die Abstimmung mit den Regeln zur Informationsfreiheit in einem schlüssigen Konzept des Datenschutzes zu einer informationsrechtlichen Grundaufgabe geworden.[101]

2) Zweite Generation: verfassungsrechtliche Erheblichkeit. Internationale Instrumente

Die „zweite Generation" der Datenschutzgesetze ist einerseits durch die verfassungsrechtliche Relevanz des Datenschutzes auf der nationalen Ebene,[102] andererseits durch die erste internationale Regelung gekennzeichnet.[103] Zum Ersten sei hier nicht nur an die Bestimmungen der portugiesischen

---

96 *Simitis, S.*, a.o.O. (Fn. 16), S. 21-3.

97 *Burkert, H.*, a.o.O. (Fn. 50), Rn. 17, 67; Simitis u.a, BDSG-*Simitis*, Einleitung, Rn. 115, 125.

98 *Ellger, R.*, Datenschutz im grenzüberschreitenden Datenverkehr, a.o.O. (Fn. 6), S. 421.

99 Simitis u.a, BDSG-*Simitis*, Einleitung, Rn. 118.

100 *Sokol, B.*, Informationszugang und Datenschutz, in: Roßnagel (Hrsg.), Handbuch des Datenschutzrechts, München 2003, Rn. 6.; Simitis u.a, BDSG-*Simitis*, Einleitung, Rn. 21

101 *Burkert, H.*, a.o.O. (Fn. 83), Rn.69; *Sokol, B.*, a.o.O. (Fn. 100), Rn. 1-3.

102 Statt allen, *Bäumler*, Datenschutzgesetze, in Bäumler/Mutius (Hrsg.), Datenschutzgesetze der dritten Generation, Neuwied, 1999, S.3

103 Simitis u.a., BDSG-*Simitis*, Einleitung, Rn. 121.

(Art. 35) sowie der spanischen (Art. 18 n.4) Verfassung erinnert, die aus den Jahren 1977 bzw. 1978 stammen. Vielmehr verdient auch die richterliche Entwicklung und Präzisierung dieser grundrechtserheblichen Rechtspositionen, insbesondere die 1983 erlassene Volkszählungsentscheidung des BVerfG eine nähere Betrachtung (2a). Zweitens ist die Entwicklung in der OECD (2b.) sowie im Europarat (2c.) von besonderer Relevanz. Beide Organisationen haben erkannt, dass der grenzüberschreitende Datenverkehr eingeschränkt werden könne, wenn das jeweilige Datenschuztniveau des Sender- und Empfängerlandes allzu unterschiedlich ausfällt.
Zwischen nationalen und internationalen Lösungen besteht eine kaum zu unterschätzende Interdependenz. Die Arbeiten in den internationalen Einrichtungen erleichterten die Definition des Datenschutzes auf einzelstaatlicher Ebene, denn „sie hielten immer vor Augen, dass nationale Lösungen erforderlich waren, um sich nicht zu isolieren, dass diese nationale Lösungen der nationalen Abstimmung bedurften und dass aber zugleich aus dem Bestand anderer nationalen Lösungen Lösungsmodule für die eigenen nationalen Lösungen zur Verfügung standen“.[104]

a) Das Volkszählungsentscheidung des BVerfG[105]

.

i) Vor der Entscheidung: eine „offene Gesellschaft der Verfassungsinterpreten“

Oftmals findet man in der Literatur die mehr oder weniger ironische Behauptung, dass das sog. Volkszählungsurteil die „Bergpredigt“ des Bundesverfassungsgerichts zum Thema Datenschutz sei.[106] In jüngster Zeit wurde diese Entscheidung zunehmend kritisch bewertet.[107] Trotzdem ist und bleibt sie ein Meilenstein in der Geschichte des Datenschutzrechts – auch außerhalb Deutschlands. Welche Auswirkungen die Datenverarbeitung für die Freiheitsrechte der Einzelnen hat, war der deutschen „Gesellschaft der Verfassungsinterpreten“[108] schon recht frühzeitig bewusst.
Unter dem geschärften Blick der deutschen Öffentlichkeit fand sich das Volkszählungsgesetz von 1983 (VZG), welches deutlich den Anspruch der staatlichen Politik auf Rationalität und Planungsmäßigkeit verkörperte, im Brennpunkt öffentlicher Kritik. Die durch statistische Erhebungen gewonnenen Angaben sollten es staatlichen Stellen ermöglichen, rein spekulative Erwägungen durch einen sachkundigen und rationalen Entscheidungsprozeß zu ersetzen.[109] Mit der Volkszählung „wandelte sich eine bis dahin nur individuelle Erfahrung in ein kollektives Erlebnis: … Jeder Bürger sah[] sich Punkt für Punkt mit den gleichen Informationsanforderungen konfrontiert“. Insofern erlangte die für 1983

---

[104] *Burkert, H.*, a.o.O. (Fn. 50), Rn. 18.

[105] Bevor die wesentlichen Aspekte dieser Entscheidung erörtert werden, möchten wir einem möglichen methodischen Einwand begegnen und zwar, dass es für das Verständnis eines „europäischen“ Datenschutzrechts irreführend sein könnte, hauptsächlich auf die Perspektive der deutschen Rechtsordnung Bezug zu nehmen. Es kann in der Tat nicht geleugnet werden, dass ein Grundrechtsschutz auf europäischer Ebene eine Neutralisierung der in den mitgliedstaatlichen Traditionen verankerten Rechtsbesonderheiten nach sich zieht. (s. *Ridola, P.,* Diritti di libertà e mercato, (Fn. 78), S. 30 sowie *ders.*, La Carta dei diritti fondamentali, (Fn. 3), S. 100). So hat der EuGH im Fall *Grogan* die nach der irischen Verfassung nicht gestattete Abtreibung durch die Anwendung der Dienstleistungs-Grundfreiheit „neutralisiert“. Auf der andere Seite, jedoch, ist der Bezug auf mitgliedstaatliche Rechtstraditionen im Grundrechtsbereich selbst in der EUV vorgesehen (Art. 6 Abs. 2), wobei entscheidend ist, dass es sich dabei um eine „gemeinsame Verfassungsüberlieferung der Mietgliedstaaten“ handelt.
Anders als der Schutz pränatalen Lebens kann der Schutz des Einzelnen bei der Verarbeitung personenbezogener Daten als eine gemeinsame Tendenz der Rechtsordnungen der Mitgliedstaaten gesehen werden. Von den spanischen sowie portugiesischen Verfassungen war schon die Rede. Hinzu kommt das österreichische Verfassungsgesetz sowie die Entscheidungen nationaler Obergerichte bzw. Verfassungsgerichte (z.B. hat die italienische *Corte Costituzionale* in der Entscheidung n. 38/1973 das *diritto alla riservatezza* als *inviolabile* anerkannt). Daraus ergibt sich, dass die Betrachtung des Volkszählungsurteils des BVerfG hier keinen Schwerpunkt auf die deutsche Rechtsordnung setzen möchte. Vielmehr drückt diese Entscheidung eine den Mitgliedstaaten gemeinsame Entwicklung aus: Der Schutz der Bürger vor zunehmenden Gefahren der Informations- und Risikogesellschaft.

[106] Vgl. u.a., *Ladeur, K.H.,* Datenschutz- vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, DuD 2000, 12; *Trute, H.H.,* a.o.O. (Fn. 48), Rn. 7.

[107] *Ladeur*, a.o.O. (Fn. 106), S. 12.

[108] Im Sinne Häberles: *Häberle, P.*, Verfassung als öffentlicher Prozess, 2. Aufl., Berlin 1998, S. 155ff.

[109] *Simitis, S.,* Die Entscheidung des Bundesverfassungsgericht zur Volkszählung 10 Jahre danach, KritV 1994, 121.

geplante Volkszählung ein Symbolwert.[110] Vor dem BVerfG gingen 1310 Verfassungsbeschwerden ein, eine Anzahl, die weder davor noch später übertroffen wurde. Beschwerdeführer gehörten zu den unterschiedlichsten sozialen Gruppierungen. Alle beklagten die durch das VZG 1983 vorgeschriebenen „Totalerhebung" als Verletzung ihres Allgemeinen Persönlichkeitsrechts an. Zusätzlich machten auch Datenschutzbeauftragte auf die unzulässige Verknüpfung zu statistischen und administrativen Zwecke aufmerksam (§ 9 VZG).[111]
Vor diesem Hintergrund überrascht es daher nicht, dass der BVerfG bewusst darauf verzichtete, sich ausschließlich zum VZG zu äußern, was dem vorgelegten Beschwerdegegenstand nicht völlig entsprach. Da solch erhebliche Anteile der Bevölkerung ihre „Furcht vor einer unkontrollierten Persönlichkeitserfassung" derart eindeutig artikulierten, setzte sich das Gericht auch mit den allgemeinen verfassungsrechtlichen Anforderungen auseinander, die sich an die Verarbeitung personenbezogener Daten stellen. Die Bedeutung dieses Urteils reicht deshalb über den konkreten Tatbestand (Verfassungswidrigkeit der gesetzlichen vorgeschriebenen Koppelung statistischer und administrativen Zwecke) hinaus. Mit seinen Grundsatzaussagen zeichnete das BVerfG vielmehr die Leitlinien an hand deren alle künftigen Datenverarbeitungsverfahren verbindlich zu messen seien.[112] Nachfolgend sollen die wichtigsten Vorgaben der BVerfG dargestellt werden.

ii) Datenschutz ist Grundrechtsschutz

Als erstes wurde dem Datenschutz Verfassungsrang eingeräumt.[113] Kann der einzelne das Wissen möglicher Kommunikationspartner nicht überschauen, wird er in seiner Freiheit eingeschränkt. Die Ausübung seiner Grundrechte wird ihm erschwert. Der darin zu Tage tretende Bezug zwischen Daten- und Grundrechtsschutz, sollte auch im Rahmen der oben bereits aufgeworfnen Kompetenzfrage der DSRL nicht unbeachtet bleiben. Vergegenwärtigt man sich die Eindeutigkeit dieser Aussage des Bundesverfassungsgerichts, erscheint eine Einordnung der DSRL als eine lediglich unter dem Blickwinkel „Hemmnis zum Binnenmarkt" getätigte Maßnahme wenig überzeugend.
Des weiteren leistet Datenschutz einen funktionellen Beitrag zum Schutz demokratischer Mitwirkungsfähigkeit des Bürgers in dem Sinne dass „Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[114]

iii) Kennzeichen nationaler Spezialität und europäischer Konvergenz

Unter den weiteren Vorgaben der Volkszählungsentscheidung können einige als besondere Ausgestaltung des deutschen Datenschutzes verstanden werden. Andere hingegen verkörpern Anforderungen, welche eine rechtsordnungsunspezifische Gültigkeit beanspruchen könnten.
Auf der einen Seite steht z.B. die Formulierung eines „Recht auf informationelle Selbstbestimmung" (RiS) als Konkretisierung des Allgemeinen Persönlichkeitsrechts i.S.d. Art. 1 Abs. I GG und Art. 2 Abs. I GG. Einer der Richter musste hierbei sogar um „Verständnis für den nicht so schönen Begriff" bitten.[115] Der Entscheidung zufolge ist sein Inhalt „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[116] Durch die Entwicklung des RiS hat das BVerfG die sog. Sphärentheorie stillschweigend fallen gelassen. Nach ihr lässt sich der Handlungsraum eines jeden Menschen in Sphären aufteilen.[117] Personenbezogene Daten der Intimsphäre, genießen danach einen weitaus stärkeren Schutz, als Daten, die eher zur sozialen

---

110 Simitis u.a., BDSG-*Simitis*, Einleitung, Rn. 28.
111 *Simitis, S.,* Die informationelle Selbstbestimmung, Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1998, 398.
112 Simitis u.a., BDSG-*Simitis*, Einleitung, Rn. 29;
113 Zu den ursprünglichen verfassungsrechtlichen Problemen bezüglich der Einführung eines Grundrechts auf Datenschutz s. *Klöpfer, M.*, Datenschutz als Grundrecht, Königstein 1980.
114 BVerfGE 65, 1, S. 43.
115 *Benda, E.,* Das Recht auf informationelle Selbstbestimmung und die Rechtssprechung des BVerfG zum Datenschutz, DuD 1984, 87.
116 BVerfGE 65, 1, S. 43.
117 vgl. *Podlech,* Art. 2 Abs. I, in: AK GG, Bd. 1, Neuwied 1989, Rn. 35.; *Benda, E.*, a.o.O. (Fn.115), S. 88.

Sphäre des Einzelnen gehören. In der Volkszählungsentscheidung hingegen postulierte das BVerfG, dass es „kein belangloses" Datum gibt.[118] Was die „sensible" Natur eines Datums ausmacht ist nicht die engere oder weitere Sphäre der Persönlichkeit, der es zuzurechnen ist. Es kommt vielmehr entscheidend auf die Nutzbarkeit bzw. Verwertungsmöglichkeit der Daten an. In den Mittelpunkt der Betrachtung rückt somit der Zweck, zu dem das Datum erhoben wurde und für den es verwertet wird. Dies ist nicht nur aus einer reinen juristischen Perspektive von Bedeutung. Zusammen mit der Sphärentheorie wurde ebenso ihr soziologisches Menschenbild, das eines isolierten Individuums verbunden mit der strickten Trennung zwischen einem privatem und einem öffentlichen Bereich des Bürgers, abgewiesen. Das BVerfG erkannte nunmehr implizit an, dass menschliche Personalität sich mit einem sozialen Bezug durch Kommunikation im Habermas'schen Sinne bildet: „Privatheit ist keine Sache des isoliert gedachten Individuums, die durch Kommunikation mit anderen (bzw.) einem Sozialbezug verloren geht. Privatheit ist eine mögliche Eigenschaft des Umgangs mit anderen".[119]
Daneben decken sich einige der vom BVerfG klar formulierten Programmsätze mit Kernelementen der internationalen Datenschutzregelung. Hierunter fallen insbesondere das Zweckbindungsprinzip sowie die Aufforderung nach bereichsspezifischen Regelungen, welche beide den Verwendungszusammenhangs der Daten begrenzen sollen und die generellen Aussagen der bis dahin geltenden vagen Generalklauseln ersetzten.[120] Des weiteren wird auf die Unabdingbarkeit einer unabhängigen Kontrolle hingewiesen, welche nicht nur die Transparenz der Datenverarbeitungsvorgänge und die Verwirklichung der rechtspolitischen Ziele der Datenschutzes gewährleisten soll. Vielmehr wird auch eine unabhängige, speziell dafür eingerichtete Instanz in Form eines Datenschutzbeauftragten zur prozeduralen Vorbedingung eines wirksamen Schutzes der Betroffenen.[121]

(iv) Interpretationsmodelle des (grundrechtsrelevanten) Datenschutzes

Für das Verständnis der Vielschichtigkeit eines auf europäischer Ebene verankerten „Grundrecht[s] auf Datenschutz" erscheint die Auseinandersetzung der deutschen Rechtssprechung und Literatur zum RiS von erheblichem Nutzen. Der in der deutschen Grundrechtsdogmatik gefestigte Unterschied zwischen einer subjektivrechtlichen und einer objektivrechtlichen Dimension der Grundrechte sowie deren Koexistenz lässt sich bei der Entwicklung des europäischen Datenschutzrechts besonders deutlich beobachten.

(v) Minimalistische Subjektivrechtliche Dimension

Einige,[122] teilweise auch „Minimalisten" genannt,[123] verstehen das im Volkszählungsurteil begründete Recht auf informationelle Selbstbestimmung als eine Konkretisierung des allgemeinen Persönlichkeitsrechtes und gehen daher auch von dessen völligen Einschränkbarkeit zum Zwecke des Allgemeinwohls aus.[124] Nach ihnen könne man dem RiS eine Reihe von „Gegenprinzipien" gegenüberstellen. So wird z.B. eine staatliche „Informationsvorsorge" allgemein aus dem Sozialstaatsprinzip nach Art. 20 Abs. 1 und 28 Abs. 1 GG abgeleitet.[125] Ebenfalls wurde ein „Grundrecht auf Sicherheit" formuliert,[126] welches sowohl ein s*tatus positivus libertatis* im Sinne Jellineks als auch eine Schutzpflicht des Staates fundieren soll.

---

[118] BVerfGE 65, 1, S.45
[119] *Podlech*, a.o.O (Fn. 117), Rn. 38
[120] BVerfGE 65, 1, S. 44-45.
[121] BVerfGE 65, 1, S. 46.
[122] *Vogelsang, K.*, Grundrecht auf informationelle Selbstbestimmung?, Baden- Baden 1987, S. 190ff; *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984, S.101ff; *Isensee, J.*, Das Grundrecht auf Sicherheit, Berlin New York 1983, S.21ff.
[123] Bzw. Reduktionisten, vgl. *Donos, P.K.*, a.o.O. (Fn. 7), S.74.
[124] BVerfGE 65, 1, S.44.
[125] *Scholz/Pitschas*, a.o.O. (Fn. 122), S. 101 ff.; 132 ff.
[126] *Isensee, J.*, a.o.O. (Fn. 122), S. 21, 27 ff.

Im nicht öffentlichen Bereich kollidiert das RiS eher mit einem aus Art. 5 Abs. 1 abgeleiteten Grundrecht auf Informationsfreiheit[127]. Dieses wird als das Pendant des Prinzips freier Marktwirtschaft in der Informationsbranche betrachtet.
Beklagt wird jedoch, dass, sollte die Verarbeitung personenbezogener Daten als Unterfall des allgemeinen Persönlichkeitsrechts und dadurch lediglich unter dem Eingriff-Schranken Schema verstanden werden, könnte dies die Regelungsperspektive beträchtlich reduzieren.[128] Die Datenverarbeitungsprozesse und ihren Folgen würden als ein „rein individuelle[s] Problem" empfunden, für dessen Lösung lediglich die Grundsätze zur Anwendung kämen, die bei der rechtlichen Bewertung von Eingriffen in individuelle Rechtspositionen zu beachten sind.
Hiernach wird ein Datenschutzgesetz als Auffanggesetz verstanden, das nur anlässlich eines festgestellten Eingriffs als Konkretisierung des Gesetzvorbehalts betätigt werden soll.
Darüber hinaus setzt das Eingriff-Schranken Modell voraus, dass der Interpret die oben genannte Sphärentheorie akzeptiert hat, von der sich das BVerfG aber gerade abgewandt hatte.
Folglich wird den „Minimalisten" vorgeworfen, dass sie einen zu geringen Kontakt zu den Sozialwissenschaften suchen und somit einen allzu beschränkten Begriff der Kommunikation und Information annehmen. Ferner haben sie den Sinn und Zweck einer Datenschutzregelung innerhalb einer Informationsgesellschaft missverstanden und unterschätzt (ausführlicher s. u. (vi)).
Letztlich verbürge sich hinter ihrem Argumentationsmuster ein „Abwägungsopportunismus". Nach Luhmann lässt sich dieser gerade dadurch kennzeichnen, dass im Rahmen der abstrakten juristischen Abwägung üblicherweise alle strukturelle Fragen und faktisch-soziale Verhältnisse außer acht gelassen, also schlecht einfach getilgt werden.[129]
Eine solche Rhetorik des Abwägungsdenkens findet jedoch gerade in einigen Passagen der Volkszählungsentscheidung ihre Unterstützung. Da Selbstbestimmung nach dem BVerfG „Funktionsbedingung" einer Demokratie ist und personenbezogene Informationen zum „Abbild sozialer Realität" werden, löst sich die Unterscheidung zwischen Schutzbereich und Schranken auf. Anders als die meisten andere Grundrechten ist der Staat beim RiS schon auf der Ebene des Normbereichs selbst als Verfügungsberechtigter präsent.[130] Das „Allgemeininteresse" bekommt damit das Potential einer Art von „Übergeneralklausel". Deren Elastizität vermag prinzipiell jede von öffentlichen Stellen eingesetzte Verarbeitungskonstellation mit Berufung auf deren Rationalität und Effizienz rechtfertigen.[131]

(vi) Objektivrechtliche Dimension: der Prozedurale Datenschutz

Einer zweiten Gruppe der Interpreten zufolge, hat die Kritik gegen das herkömmliche Angriffsabwehrdenken bei dem RiS in den letzen Jahren mehr und mehr Zustimmung gefunden. Die Akzentverlagerung der elektronischen Kommunikation im privaten Sektor hat dazu beigetragen, dass die objektiv-rechtliche Dimension des RiS, insbesondere der Schutzpflicht des Staates, besondere Bedeutung erlangte.[132] Der Rechtsstaat nimmt die dem einzelnen und seiner Freiheit gegenüber obliegende Schutzpflicht durch den Erlass von Verfahrens- und Organisationsregeln[133] wahr, da ein wirksamer Schutz der Grundrechte im klassischen *status negativus* prozedurale Ergänzungen der materiellrechtlichen Position erfordert. Eingreifende Verfahrens- und Organisationsregeln legitimieren sich dadurch, dass sie ein Gespräch zwischen Verwaltung und Bürger sowie zwischen Bürgern untereinander ermöglichen und somit zum Grundrechtsschutz beitragen. Der einzelne muss eine faire Chance haben, durch seine Meinungs- und Willensbildung das Ergebnis zu beeinflussen.[134] Insofern

---

127 *Ehmann, H.*, I principi del diritto tedesco in materia di trattamento dei dati personali con riguardo alla direttiva comunitaria del 24 ottobre 1995, Contratto e Impresa / Europa 1997, S. 900.
128 Simitis u.a., BDSG-*Simitis*, Einleitung, Rn. 26.
129 So *Donos, P.K.*, a.o.O. (Fn 7), S. 81.
130 *Ladeur, K.*, a.o.O. (Fn. 106), S. 13.
131 *Donos, P.K.*, a.o.O. (Fn. 7), S. 73; Simitis u.a., in BDSG-*Simitis*, Rn. 44-45.
132 *Trute, H.H.*, a.o.O. (Fn. 48), Rn 46; *Ladeur, K.*, a.o.O. (Fn. 106), S. 15.
133 *Denninger, E.*, Staatliche Hilfe zur Grundrechtsausübung, durch Verfahren, Organisation und Finanzierung, in Isensee / Kirchof (Hrsg.), Handbuch des Staatsrechts, Bd.5, Heidelberg 1992, Rn. 5.
134 *Denninger, E.*, Staatliche Hilfe zur Grundrechtsausübung, a.o.O. (Fn. 133), Rn. 27-28.

können diejenige Strukturen „grundrechtsgeboten“ sein, die für die Herstellung eines Kommunikationszusammenhangs prozedural bzw. organisatorisch unentbehrlich sind und deren Versäumen damit zum Misserfolg einer rationalen Kommunikation führen würde.[135]
Im Rahmen dieser Perspektive ist auch Datenschutz ein prozedurales Recht, welches den Freiheitsschutz abhängig vom umfassenden Verfahren macht. Hauptziel des Datenschutzes als prozedurales Recht ist, den Inhalt der informationellen Selbstbestimmung durch Prozeduralisierung zu gewährleisten.[136] Der Gesetzgeber sieht von einer unmittelbaren und ausführlichen Regulierung des sozialen Verhaltens ab und lässt durch institutionalisierte Verfahren und Organisation die auftretenden Konflikte von den Betroffenen selbst lösen. Passendes Stichwort: Wandel von der Erfüllungsverantwortung zur Gewährleistungsverantwortung.[137]
Die Einführung des Datenschutzrechts markierte auch einen Wandel der bis dahin hauptsächlich wohlfahrtsstaatlichen Aufgaben zur vermehrten hoheitlichen Präventivtätigkeit.[138] Anstatt der isoliert betrachteten Daten, rückte der Verwendungszusammenhang der Datenverarbeitung zunehmend in den Vordergrund. Durch Zweckbindung wurde der Datenverarbeitungsprozess stets berechenbar und für den Betroffenen damit transparent und nachvollziehbar.[139] Beeinträchtigt, dem BVerfG folgend, die Unkenntnis über das Wissen anderer die Möglichkeiten der Selbsteinschätzung der einzelnen und dadurch ihre Verhaltensfreiheit, dann ist Transparenz der Erhebungs- und Verarbeitungszusammenhänge das gebotene Instrument zum Schutz der Selbstbestimmung. Insoweit werden Unterrichtungs- und, zur Ermöglichung einer nachträglichen Kenntnisnahme, Benachrichtigungspflichten im öffentlichen sowie im privaten Bereich erforderlich. Darüber hinaus ist als strukturelle und prozedurale Kompensation der Defizite an Rechtswahrnehmungsmöglichkeiten der Einzelnen die Einrichtung unabhängiger und hinreichend wirksame Kontrollstellen erforderlich. Diese Anforderungen haben sowohl eine die Kenntnisnahmemöglichkeit der Betroffenen sichernde individuelle, als auch eine allgemeine, auf die Transparenz der Rechtsordnung abzielende Dimension.[140]

b) OECDs Guidelines

1980 hat die OECD die „*Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data*“ verabschiedet. Beim Erlaß der *Guidelines* stützte man sich auf Art. 1c, 3a und 5b der OECD-Konvention. Nach Art. 1c, möchte die OECD eine Politik fördern, die zur Ausweitung des Welthandels beiträgt. Es liegt somit nahe, dass die Freiheit von grenzüberschreitenden Datenflüssen als notwendige Bedingung der modernen, international verflochtenen Weltwirtschaft und nicht der Schutz der Persönlichkeitssphäre des Betroffenen im Vordergrund steht.[141] Datenschutz wird somit primär als wirtschaftspolitisches Mittel verstanden.
Wie auch in der Konvention des Europarates finden sich in den OECDs *Guidelines* die wesentlichen Prinzipien des Datenschutzes, wie die der Datenqualität, der Datensicherheit, der eingeschränkten Erfassung, der Zweckbestimmung, der Transparenz und der Beteiligung des einzelnen. Vergleichbar mit der Konvention des Europarates sind sie sowohl im öffentlichen als auch im privaten Sektor anwendbar. Die Wirkung der *Guidelines* ist allerdings aus zwei Gründen beschränkt. Erstens besteht gegenüber den Mitgliedstaaten keine durchsetzbare Verpflichtung, die *Guidelines* in nationales Recht umzusetzen. Zweitens steht es den Mitgliedstaaten frei, die Ausnahmen von den genannten Grundsätzen festzulegen (Art. 3 a).[142]
Eine Annahme von Empfehlungen der OECD blieb jedoch für die betroffenen Staaten völkerrechtlich nicht ohne Folgen: Es entstand die Verpflichtung, ein nichtwidersprüchliches Verhalten in anderen

---

135 *Denninger, E.*,Staatliche Hilfe zur Grundrechtsausübung, a.o.O. (Fn. 133), Rn. 26, 29.
136 *Donos, P.K.*, a.o.O. (Fn. 7), S. 131.
137 *Trute, H.H.*, a.o.O. (Fn. 48), Rn. 48, 50; *Ladeur, K.*, a.o.O. (Fn. 106), S.16.
138 *Grimm, D.*, Ursprung und Wandel der Verfassung, in Isensee/Kirchof (Hrsg.), Handbuch des Staatsrechts, Bd.1, Heidelberg 2003, Rn. 27
139 Simitis u.a., BDSG-*Simitis*, Rn. 37; *ders.*, Die informationelle Selbstbestimmung, a. o.O. (Fn. 111), S. 402; *Donos, P.K.*, a.o.O. (Fn. 7), S. 127-131.
140 *Trute, H.H.*, a.o.O. (Fn. 48), Rn. 33.
141 *Ellger, R.*, Datenschutz im grenzüberschreitenden Datenverkehr, a.o.O. (Fn. 6), S. 515.
142 *Wuermeling, U.*, Handelshemmnis Datenschutz, Köln Berlin Bonn München 2002, S. 8.

internationalen Foren zu zeigen, sofern diese Staaten den Guidelines zugestimmt und sich nicht enthalten haben.[143]

c) Konvention des Europarates

1981 kommt die Konvention des Europarates „zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten" (Nr.108) zustande. Der Hauptunterschied zur Initiative der OECD liegt darin, dass für den Europarat Datenschutz ein Aspekt des Schutzes von Menschenrechten ist und daher unter dem Blickwinkel von Art. 8 EMRK betrachtet wird.[144]

Die Konvention enthält zahlreiche Impulse, die einerseits Ansatzpunkte für nationale Regelungen bereitstellen (die Konvention ist ein sog. *non self executing treaty*), andererseits ein Mindestmaß an Übereinstimmung zwischen diesen Regelungen sichern sollen (die Konvention, anders als die OECDs *Guidelines*, bindet die Mitgliedstaaten). Dieses Mindestmaß besteht aus dem „harten Kern"[145] des Datenschutzes und stimmt grundsätzlich mit den Verarbeitungsgrundsätzen der OECD überein. Sonderregelungen gelten für „sensitive" Daten (Art. 6), wobei deren Aufzählung nicht abschließend ist. Der Anwendungsbereich der Konvention ist erstmals auf die automatisierte Verarbeitung begrenzt (Art.1 i.V.m. Art. 3 Abs. 2 Buch c).

Die Annahme einer Mindestregelung durch alle Mitgliedsstaaten, die den Datenaustausch ermöglicht, macht allerdings Kollisionsnormen nicht überflüssig. Genau daran fehlt es jedoch in der Konvention.[146] Ebenso fehlt ein Hinweis auf eine unabhängige Datenschutzbehörde. Beide Punkte hätten nachgeholt werden können und müssen. Geschehen ist dies erst durch die Datenschutzrichtlinie, also im Rahmen der sogn. „dritten Generation" der Datenschutzgesetzgebung (s.u. II 2 d ii und Teil 3 A).[147]

3) Vierte Generation: „Modernisierte" Konzepte des Datenschutzes

Der letzte Zeitraum der Geschichte des Datenschutzes spiegelt sich in dem Begriff „Modernisierung des Datenschutzes" wieder. Um den jüngsten globalen Entwicklungen der Informationsbranche zu begegnen, hat man passende „Konzepte" des Datenschutzes formulieren müssen. Gegenüber den 70er Jahren hat sich der historische Kontext in den späten Neunzigern und zum Beginn des 21. Jahrhunderts erheblich verändert. Die Territorialstaaten erscheinen immer weniger als ein Leviathan: Gegenüber dem globalen Netz sind sie zunehmend mit Ohnmacht konfrontiert. Die Steuerungsschwäche der nationalen Gesetzgeber zeigt sich besonders im Bereich des Datenschutzes, wenn man ihn der obigen Ausführung folgend vor allem als Bestandteil der präventiven Staatstätigkeit versteht.[148] Da mögliche Schadensquellen vielfältiger und versteckter sind als tatsächliche Schädigungen, empfindet vor allem der Präventionsstaat einen großen Informationsbedarf., was eine gesetzliche *ex ante* Steuerung der Datenverarbeitung erheblich erschwert.[149] Der System- bzw. Selbstdatenschutz sowie der Selbstregulierung lassen sich in diesem Kontext als Versuche betrachten die Informations-, Regelungs- und Vollzugsdefizite zu überwinden.

a) Systemdatenschutz

Unter Systemdatenschutz versteht man „die Menge der Rechtsregeln, die Vorgänge der Informationserhebung und Verarbeitung unabhängig davon …[regelt], ob im Einzelfall Interessen der Betroffenen berührt sind oder nicht und diese so …[ordnet], dass die Gesamtheit der rechtlich geregelten Informationsvorgänge keine sozialschädlichen Folgen herbeiführen".[150] In neuerer Zeit sind Konzepte des Systemdatenschutzes in den Vordergrund der datenschutzrechtlichen Diskussion gerückt. Nahezu alle davon erheben den Anspruch, Datenschutz und Datensicherheit in die Struktur von Datenverarbeitungssysteme zu integrieren und damit effektiven Datenschutz nicht nur davon

---

143 *Burkert, H.*, a.o.O. (Fn. 50), Rn. 18.
144 *Wuermeling, U.*, a.o.O. (Fn. 142), S. 9.
145 *Simitis u.a., Simitis/* Einleitung, Rn. 143.
146 *Burkert, H.*, a.o.O. (Fn. 50), Rn. 9.
147 Vgl. 1. Zusatzprotokoll zur Konvention Nr. 108, vom 8.11.2001
148 *Grimm, D.*, a.o.O. (Fn. 138), Rn. 71
149 *Ladeur, K.*, a.o.O. (Fn. 106), S. 16
150 Nach Podlechs Definition vgl. *Hoffmann, B.*, a.o.O. (Fn. 10), S. 24.

abhängen zu lassen, dass Menschen sich an Rechtsregeln über den zulässigen Umfang der Verarbeitung von personenbezogenen Daten halten oder die ihnen zustehenden Rechte kennen und ausüben.[151] Als Beispiel kann die technische Systemgestaltung nach den Prinzipien der Datenvermeidung und Anonymisierung sowie der Anwendung der sog. *Privacy enhancing technologies* genannt werden.

b) Selbstdatenschutz

Die Wende der Staatsaufgaben in unserer Risikogesellschaft bedeutet auch, dass es unzureichend ist, die Erfüllung staatlicher Schutzpflichten allein staatlich implementierter und kontrollierter Verfahren zu überlassen. Der Schwerpunkt verschiebt sich vielmehr auf die Gewährleistung und Verstärkung privater Selbstschutzmöglichkeiten. Der Staat hat auch mittelbar dafür zu sorgen, dass Private dazu beitragen, ein adäquates Schutzniveau zu garantieren. Soweit dies durch private Eigenvorsorge erreicht werden kann, könnte sich (subsidiärer) staatlicher Schutz auch erübrigen. Die Veränderung der Gefährdungslagen stärkt den Zusammenhang von Freiheit und Selbstverantwortung durch geeignete Vorkehrungen ein.[152] Gewährleistungsverantwortung des Staates ist hier als Infrastrukturverantwortung zu begreifen: Der Staat muss dem Bürger die infrastrukturelle Voraussetzungen bieten, damit er seine Eigenverantwortung auch erfüllen kann.[153]
Zu einer solchen Gewährungsinfrastruktur zählen, unter anderem, die selbstbestimmte Nutzung von technischen und organisatorischen Schutzinstrumenten und einfach zu bedienende Tools wie Steganographie, Anonymisierung, Pseudonimität, P3P, Opt in und Opt out.[154]

c) Selbstregulierung

Als weitere Form und „dritte Säule" der staatlichen Gewährleistungsverantwortung im Bereich des Datenschutzes lässt sich die Selbstregulierung zählen.[155] Ähnlich dem System- und Selbstdatenschutz, erweisen sich Selbstregulierungslösungen zunehmend als eine grundrechtsfreundliche und dezentrale Form des Datenschutzes. Regelmäßig ist Selbstregulierung in einem staatlichen Ordnungsrahmen eingefügt und soll dadurch dem Prinzip der Kooperation zwischen Staat und Gesellschaft entsprechen.[156] Einige Autoren reden dabei von einer „arbeitsteiligen Gemeinwohlkonkretisierung durch Staat und Private",[157] wobei der Gesetzgeber nach dem Demokratie- und Wesentlichkeitsprinzip die essentiellen grundrechtsrelevanten Entscheidungen selbst erfasst und deren Konkretisierung privaten Akteuren anvertraut.
Nach anderer Auffassung stellt Selbstregulierung ein Wandel des Verfassungsstaates dar, der sich in dieser Hinsicht vor allem durch eine entfallende Kontrolle durch das verfassungsmäßige Gesetz kennzeichnet.[158] Die mit dem strukturellen Wandel zum „paktierendem Staat" verbunden demokratischen und rechtsstaatlichen Kosten liegen auf der Hand.
Als Ergänzungen der Selbstregulierung sowie als Beispiele einer neuen Modellierung des Datenschutzes sind ferner sogn. Datenschutzaudits oder Evaluationsverfahren zu nennen.[159] *Ex-post* Evaluationsverfahren erweisen sich vor allem dann als sinnvoll und notwendig, wenn zum Zeitpunkt einer (ansonsten alternative vorzunehmenden) Legislativtätigkeit keine zur Umsetzung gesetzlicher Zielvorstellungen ausreichenden Kenntnisse der Ursache-Wirkungszusammenhänge verfügbar sind. Der Schwerpunkt des Datenschutzes wäre daher bei den Regeln für die Datenverknüpfung nach bestimmten Fragestellungen intensiver zu setzen. Zum Beispiel könnten Behörde verpflichtet werden,

---

[151] *Dix, A.,* Konzepte des Systemdatenschutzes, in: Roßnagel A. (Hrsg.), Handbuch Datenschutzrecht München 2003, Rn. 1.; *Roßnagel/Pfitzmann/Garstka,* Modernisierung des Datenschutzes, DuD 2001, S. 254.
[152] *Trute, H.H.,* a.o.O. (Fn. 48), Rn. 50-51. *Roßnagel, A.,* Konzepte des Selbstdatenschutzes, in: Roßnagel A. (Hrsg.), Handbuch Datenschutzrecht München 2003, Rn. 17-19.
[153] *Roßnagel, A.*, Konzepte des Selbstdatenschutzes, a.o.O. (Fn. 152) Rn. 21
[154] *Roßnagel/Pfitzmann/Garstka,* a.o.O. (Fn. 151), S. 255.
[155] *Trute, H.H.,* a.o.O. (Fn. 48), Rn.53; *Roßnagel, A.,* Konzepte der Selbstregulierung, in Roßnagel A. (Hrsg.), Handbuch Datenschutzrecht München 2003, Rn. 22.
[156] *Roßnagel, A.*, Konzepte der Selbstregulierung, a.o.O. (Fn. 155), Rn. 21.
[157] So *Roßnagel, A.*, Konzepte der Selbstregulierung, a.o.O. (Fn. 155), Rn.21.
[158] *Grimm, D.,* a.o.O. (Fn. 138), Rn.79-86.
[159] *Ladeur, K.,* a.o.O. (Fn. 106), S. 17.

Datenverbindungen nach bestimmten Voraussetzungen durchzuführen, die erst im Nachhinein evaluiert und ggf. bestätigt oder abgelehnt werden könnten. In der Privatwirtschaft werden Evaluationsstellen unter dem Begriff des Datenschutzaudit begriffen. Zu den Zielen eines Datenschutzaudits zählt erstens die Hilfe bei der Gewährleistung des Datenschutzes, indem die Kontrolle des Datenschutzaudits als Ergänzung (aber nicht Ersetzung) der behördlichen Datenschutzkontrolle erfasst wird. Zweitens soll ein Datenschutzaudit zu einer ständigen Verbesserung des Datenschutzes und der Datensicherung beitragen, wenn es nicht gebotene Datenschutzanstrengungen der Unternehmen zu Marktanreize verwandelt. Darauf knüpft, drittens, die Stärkung der Wahrnehmung des Datenschutzes als Wettbewerbsvorteil, indem Wirtschaft und Verwaltung Datenschutz als ein Qualitätsmerkmal für Vertrauensbeziehungen zu Kunden und Bürger empfinden. Schließlich, soll das Datenschutzaudit ein Lernprozess des Datenschutzmanagementsystems fördern.[160]

d) Datenschutz als Property Right

Die normativen Betonung einer Strategie der Selbstregulierung hat auch nicht zu unterschätzende theoretische Folgen. Gerade Befürworter der Selbstregulierung haben in den letzten Jahren immer häufiger auf weitere Modelle und Argumentationsmuster der ökonomischen Analyse des Rechts zurückgegriffen. Nach ihnen ist das Verhalten von Gesellschaften, Gruppen und Organisationen auf individuelles Rationalverhalten zurückzuführen. Individuen werden mit bestimmten aber beliebigen Präferenzfunktionen und Ausgangsgüter versehen. Das Ziel aller Handlungen liegt im Konsum knapper Güter, die prinzipiell gegeneinander substituierbar sind und daher unter dem Gesichtspunkt von Kosten und Nutzen analysiert werden können.[161] Kritisierst wurde dieser Ansatz vor allem deshalb, weil er den Menschen als *homo oeconomicus* zu einem rationalen, nutzenmaximierenden Bedürfnisträger reduziert, der mit anderen Menschen lediglich Tauschgeschäfte betreibt. Ferner seien im Bereich des Persönlichkeitsrechts die jeweils in Betracht kommenden Handlungen kaum ersetzbar.

Anfang der 80er Jahren ist Posners Untersuchung[162] des *right to privacy* daher bei Juristen außerhalb der USA auch auf keine begeisterte Gefolgschaft getroffen.[163] Nichtsdestoweniger wurde bemerkt, dass die Praxis der Rechtssprechung oftmals Ansprüche gerade deswegen abgelehnt hat, weil sie zu kostspielig waren. Umgekehrt wurde Rechtschutz vor allem für diejenigen Persönlichkeitselemente gesichert, welche vermarktbar sind (z.B. das Recht am eigenen Namen, Bild oder am Betriebsgeheimnis).[164]

Der Begriff des „Property rights" kann vielleicht am besten mit „absolutes Recht des Einzelnen" anstatt mit „Eigentumsrecht" übersetzt werden. Somit erscheint es nicht inkompatible, das absolute Recht des Einzelnen auf informationelle Selbstbestimmung als property right im Sinne Posners zu begreifen[165], obwohl Datenschutz unter traditioneller Anschauung nicht als eigentumsähnliches Recht an eigenen Daten, sondern vielmehr als prozeduraler Grundrechtsschutz verstanden wird.[166] Ein „Dateneigentum" widerspräche auch den Annahmen der sozialwissenschaftlichen Theorien Luhmanns und Habermas, da es die ihnen zugrunde liegende Kommunikationsstruktur einer demokratischen Gesellschaft verkennt.

Was sich in der jüngsten Zeit verändert hat und das Verständnis des Datenschutzes betrifft, ist die zunehmende Vermarktung personenbezogener Daten. Als ökonomischen Gütern wird ihnen nunmehr ein Marktwert zugeschrieben. Es wird plädiert, dass öffentliche Stellen ihre Datenbanken auf einem freien Markt verkaufen sollen, da ein freier Informationszugang zu Marktpreisen positive Externalitäten für die globale Wirtschaft haben würde.[167] Paradoxerweise verhilft das Fehlverständnis der „property

---

160 *Roßnagel, A.*, Datenschutzaudit, in Roßnagel A. (Hrsg.), Handbuch Datenschutzrecht München 2003, Rn. 5-8.

161 *Eger/Nagel/Weise,* Effizienz und Menschenwürde, Ein Gegensatz?, in: Ott/Schäfer (Hrsg.), Ökonomische Probleme des Zivilrechts, Berlin Heidelberg 1991, S. 19.

162 *Posner, R.*, The Economics of Justice, Cambridge London 1993, Kapitel 9 bis 11.

163 So *Maglio, M.*, An Economic Analysis of the Right to privacy, CRi 2003, 104.

164 *Kohl, H.*, Das allgemeine Persönlichkeitsrecht, als Ausdruck oder Grenze des Effizienzdenkens im Zivilrecht?, in: Ott/Schäfer (Hrsg.), Ökonomische Probleme des Zivilrechts, Berlin Heidelberg 1991, S. 45.

165 *Posner, R A.*, Economic Analysis of Law, 6. Aufl., New York 2003, S. 32ff.

166 Simitis u.a., BDSG-*Simitis*, Einleitung, Rn.26.

167 *Zeno-Zencovich, V.*, Uso a fini privati dei dati personali in mano pubblica, Diritto dell'informazione e dell'informatica 2003, 197, welcher den Richtlinienentwurf KOM (2002) 207 endg. kommentiert.

rights“ als Eigentumsrechte und eine Verwechslung des methodischen Ansatzes (der Ökonomik) mit dem Gegenstandsbereich (der Wirtschaft) diesem Ansatz jüngst zu einer vermehrten Aufmerksamkeit. Inwiefern die ökonomische Analyse des Rechts ein Auslegungsinstrument der Grundrechte sein kann, wird bestritten. Wenn man sie ihrer auch nicht ausschließlich bedient, vermag sie doch dem Juristen helfen, eine Rechtsfolgenabschätzung vorzunehmen (sogn. positive ökonomische Analyse[168]), indem er die Anreize und Sanktionen feststellen kann, welche das menschliche Handeln innerhalb eines bestimmten Sachverhalts beeinflussen.[169]
Geht man einen Schritt weiter und verbindet man den *property rights* Ansatz mit einer am Effizienzkriterium orientierten normativen Auslegung des Datenschutzrechts, eröffnet sich die Chance einer stärkeren Flexibilisierung des Datenschutzrechts, da vermehrt auf die Einwilligung des Betroffen abgestellt werden kann.[170] In dem Maße, dass Transaktionskosten vernachlässigt werden können, sollte das Recht den Individuen ermöglicht auf Datenschutzrechte zu verzichten bzw. sich „abkaufen“ zu lassen, um eine effizienteren Allokation der Ressource Information zu ermöglichen.[171] So können personenbezogene Daten z.B. für die Ausarbeitung von Marketingstrategien oder die Herstellung neuer Produkte verwendet werden, was durch das Recht nicht prinzipiell negativ bewertet werden sollte.[172]
Selbstregulierung spielt unter diesem Blickwinkel eine zentrale Rolle als Form der Kompensation von Schutz- und Nutzungsinteressen. Ähnlich wie beim Systemschutz, ist Selbstregulierung eng mit dem Konzept des Selbstschutzes verknüpft, da „Selbstschutz auch in erster Linie gesellschaftlich durch Konventionen selbst zu organisieren ist.“[173] Daneben könnte der Staat durch begrenzte Interventionen zur privaten Selbstregulierung anregen.[174]

II. Die Datenschutzrichtlinie: Ausdruck der dritten Generation

In der dritten Generation der Datenschutzgesetze nimmt die supranationale Gesetzgebung eine zentrale Rolle ein, und die Verflechtung zwischen internationalen und nationalen Instrumenten gewinnt eine weitere Dimension. Die Spannung zwischen nationaler Vielheit und europäischer Einheit der Regelungen findet in der auf eine Harmonisierung abzielenden DSRL ein (Zwischen-) Gleichgewicht. Dieses ist allerdings nicht in der DSRL „versteinert“, sondern ist vielmehr dynamisch, im Sinne einer prozeduralen Anpassungsfähigkeit (s.u. 3), zu verstehen.
Was die inhaltliche Neuerungen betrifft, ist der Versuch zu betonen, sowohl die Verhandlungsposition des Einzelnen zu stärken als auch seine Dispositionsfreiheit in einem gewissen Umfang einzuschränken. Als Beispiele dafür kann man die Einführung einer verschuldensunabhängigen Gefährdungshaftung, sowie die für den Verantwortlichen als öffentlich-rechtliche Pflichten konzipierte Unbeschränkbarkeit der Ausübung bestimmter Rechte der Betroffenen nennen.[175] So sind in der Datenschutzrichtlinie Prinzipien der Qualität, der Zweckbindung, der Richtigkeit der Daten (Art. 6 DSRL), sowie der Information des Betroffenen (Art.10-11 DSRL) nicht als Rechte des Betroffenen eingeordnet, worauf er verzichten könnte, sondern als Verpflichtungen der Verantwortlichen formuliert.

---

168 *Posner, R.*A., a.o.O. (Fn. 165), S. 24ff.
169 *Maglio, M.*, a.o.O. (Fn. 163), S. 108.
170 *Maglio, M.*, a.o.O. (Fn. 163), S. 103-4.
171 Vgl. das grundlegende *Coase Theorem,*: *Coase, R.H.*, The Problem of social cost, in: Posner/Parisi (Hrsg.) Economic Foundations of private Law, Cheltenham Northampton 2002, S. 215-6.
172 *Ladeur, K,* a.o.O. (Fn. 106), S. 19
173 *Ladeur, K.*, a.o.O. (Fn. 106), S. 19
174 Es wurde bemerkt, dass, von eigentumsrechtlichen Vorstellungen abgesehen, Selbstregulierung eine große Bedeutung in denjenigen Sachbereichen beigemessen wird, die ohnehin auf eine Staatsferne Autonomie ausgerichtet sein müssen. Medien, Wissenschaft und Religionsausübung sind treffende Beispiele, vgl. *Trute, H.H.*, a.o.O. (Fn. 48), Rn. 55.
175 *Brühann, U.*, Die Anforderungen der europäischen Datenschutzrichtlinie, a.o.O. (Fn. 92), S.12.; *Burkert, H.*, a.o.O. (Fn. 50), Rn. 45.

1) Supranationalität der Regelung

Nach Art. 249 Abs. 3 EGV ist eine Richtlinie für jeden Mitgliedstaat, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Normgebern die Wahl der Form und Mittel zur Verfolgung dieses Ziels. Insoweit erscheint der Unterschied zwischen der DSRL und der Konvention des Europarates nicht wesentlich. Als *non self-executing treaty* wendet sich die Konvention ausschließlich an seine Vertragsstaaten. Da sie zu seiner Wirksamkeit im innerstaatlichen Recht der Umsetzung in das Recht der jeweiligen Mitgliedstaaten bedarf, ist sie kein unmittelbar anwendungsfähiger Vertrag.
Allerdings sind nach der Rechtssprechung des EuGH ebenso die EG-Richtlinien unmittelbar anwendbar, wenn ihre in Frage stehenden Vorschriften hinreichend genau sind und die Umsetzungsfrist abgelaufen ist bzw. die Umsetzung fehlerhaft war. Daher können einige Bestimmungen der Richtlinie (beispielsweise diejenigen, die den Einzelnen weitere Rechte einräumen) wohl Ansprüche der Bürger gegen einen Mitgliedstaat begründen, der seiner Umsetzungspflicht nicht bzw. fehlerhaft nachgekommen ist.[176]
Darüber hinaus sind die Durchsetzungsmechanismen des Gemeinschaftsrechts kurz zu erwähnen, welche sich von denen des Völkerrechts, einschließlich des Rechts des Europarates, erheblich unterscheiden. Für die Verletzung des Umsetzungsgebots der Konvention ist lediglich die Suspendierung oder Beendigung eines mehrseitigen Vertrages vorgesehen (Art. 60 Abs. 2 Wiener Übereinkommen; Art. 12 Abs. 2 Ü 108). Im Gegensatz dazu wirken die Sanktionsmöglichkeiten des Gemeinschaftsrechts tiefer. Nach Art. 268-269 EGV steht der Kommission oder einem Mitgliedsstaat Klagebefugnis vor dem EuGH zu, wenn sie der Ansicht sind, dass ein anderer Mitgliedsstaat eine Verpflichtung aus dem EGV nicht eingehalten hat.
Nicht weniger wichtig ist der durch das Urteil *Francovich* eingeräumte Schadensersatzanspruch des Einzelnen gegen einen Mitgliedstaat, welcher vor den nationalen Gerichten geltend gemacht wird.

2) Inhalte einer harmonisierten Regelung

a) Informationelle Selbstbestimmung vs. Privatheit

Es wurde bereits erwähnt, dass die EG-Datenschutzrichtlinie die zentralen Elemente der vorherigen Generationen der nationalen Datenschutzgesetze miteinander kombiniert. Wie diese Kombination konkret erfolgte, soll nachfolgend umrissen werden.
Dazu ist zunächst auf das geschützte Rechtsgut einzugehen. So hat das deutsche Datenschutzrecht mit dem Recht auf informationelle Selbstbestimmung den Weg eines spezifischen informationsrechtlichen Ansatzes genommen. Ein solcher war bisher den anderen Mitgliedsstaaten der EG fremd. Wie bei der Konvention Nr. 108 war deren Schwerpunkt in der Gewährleistung des „*droit à la vie privée*“ bzw. des „*right to privacy*“ gelegen, in deutlicher Anlehnung an der Achtung des Privatlebens i.S.d. Art. 8 EMRK.[177] Der Grundgedanke der Verfechter des Rechts auf informationelle Selbstbestimmung sowie des BDSG ist dadurch gekennzeichnet, dass wegen der vielfältigen Verwendungen und Verknüpfungen, die die EDV ermöglicht, auch offenbar belanglose personenbezogene Daten gänzlich in den rechtlichen Schutz einzubeziehen sind. Hingegen knüpft die DSRL an Art. 6 der Datenschutzkonvention an und fordert für sog. *sensible* Datenarten (Informationen über Rasse, ethische Herkunft, Meinungen/Überzeugungen aus dem Bereich von Religion, Philosophie und Politik sowie über seine Gesundheit und Sexualleben) einen intensiveren Schutz (Art. 8 DSRL). Dahinten steht ein der Sphärentheorie ähnlicher Gedanke, wonach sich das jeweilige Schutzniveaus nach den „besonderen“ Dimensionen der Persönlichkeitsentfaltung sowie deren „besonderen“, schmerzlich erfahrbaren Gefährdungen in den jeweils verschiedenen psycho-sozialen Bereichen orientiert.

b) Verbot mit Erlaubnisvorbehalt

Dem deutschen Datenschutzkonzept entsprechend wurde in der DSRL das sog. Verbot mit gesetzlichen Erlaubnisvorbehalt (vgl. §4 Abs. 1 BDSG) aufgenommen, das den übrigen

[176] *Ellger, R.*, Konvergenz oder Konflikt bei der Harmonisierung des Datenschutzes in Europa?, CR 1994, 561.
[177] *Rüpke, G.*, Aspekte zur Entwicklung eines EU-Datenschutzrechts, ZRP 1995, 186.

Mitgliedsstaaten wenig bekannt ist. Nach Art. 5 Abs. 1 und DSRL ist die Verarbeitung personenbezogener Daten nur dann zulässig, wenn bestimmte materiell-rechtliche Voraussetzung erfüllt sind (z.B. die Einwilligung des Betroffenen, überwiegendes Interesse durch den Verantwortlichen, überwiegendes öffentliches Interesse).
Damit besteht im Ausgangspunkt zugunsten der „betroffenen Person", auf die sich eine Information bezieht, eine Vermutung gegen die Zulässigkeit jeglicher Datenverarbeitung. Es wird von dem Verarbeiter erwartet, dass er seine Tätigkeit immer nach einem Erlaubnistatbestand legitimiert. Charakteristisch für das „Recht auf informationelle Selbstbestimmung" ist gerade dieser systematische und generelle Vorrang des Rechts des Betroffenen.[178] Allerdings erscheint eine solche Transposition des deutschen Abwägungsmodell ins Europarecht ohne gleichzeitige Annahme der dem BDSG eigenen deutlichen Unterscheidung zwischen öffentlichem und privatem Bereich problematisch. Zwar wurde zwischen den beiden Sektoren auch in mehreren anderen nationalen Datenschutzgesetzen sowie in der Konvention des Europarates nicht differenziert, doch enthielten diese kein allgemeines Verarbeitungsverbot. Schwer hinnehmbar erscheint somit ein grundsätzlicher Niveauverlust privatwirtschaftlicher/beruflicher Verarbeitungsfreiheit, der ebenso unter den Anwendungsbereich einiger Grundrechte fällt (Art. 12, 14, 5 Abs. 1 GG).[179]

c) Meldepflicht

Die Regelung der Meldepflichten ist ein klares Beispiel für die Aufnahme und Kombination vorgefundener nationaler Regelungselemente in der Richtlinie.[180] Die Meldepflicht hatte in ihren verschiedenen Varianten (bloße Meldung, vorherige bzw. nachträgliche Genehmigung) auch schon zum Regelungsbestand der Datenschutzgesetze der ersten Generation gehört (s. o. B I 1 b) und c)).
Die DSRL stellt einen subtilen Mechanismus bereit (Art. 18, 20 DSRL), in welchem die Vorabmeldung bei der Kontrollinstanz zur Regel wird. Zugleich wird den Mitgliedstaaten ein Optionsrecht gewährt: Sie dürfen die das französische Recht kennzeichnende Meldepflicht durch die für das deutsche Recht typische Bestellung eines betrieblichen Beauftragten für den Datenschutz ersetzen.[181]

d) Verarbeitungskontrolle

In einer möglichst effizienten Verarbeitungskontrolle liegt ein Stützpfeiler der DSRL. Der Ansatz orientiert sich ohne Durchbrechung an den bislang existierenden Vorbildern.[182] Individuelle (i) und institutionelle Kontrolle (ii) ergänzen einander dabei.

i) Individuelle Verarbeitungskontrolle

Genauso wie die nationalen Rechtordnungen und die Konvention des Europarates stellt die DSRL das Auskunftsrecht in den Mittelpunkt und verknüpft es mit dem Recht des Betroffenen, eine Löschung, Sperrung oder Berichtigung unvollständiger oder unrichtiger Daten zu verlangen. Jedoch präzisiert die DSRL den Mindestinhalt der Auskunft durch die Herkunft der Daten (Art. 12 a), und ergänzt die allgemein anerkannten Rechte um zwei weitere: Ein Widerspruchsrecht (Art. 14) und das Recht nicht einer Entscheidung unterworfen zu werden, die sich allein auf die automatisierte Erstellung eines Verhaltensprofils stützt. Wenn einerseits die Konkretisierung und Erweiterung der Konvention Nr. 108 durch die DSRL betont wird, bereut man andererseits die weit reichenden und akribischen Ausnahmen zu diesen Vorschriften,[183] welche eine allgemeine positive Beurteilung abschwächen.[184]

---

178 Damman-Simitis, DSRL-*Simitis*, Einleitung, Rn. 11; *Rüpke, G.*, a.o.O. (Fn. 177), 187
179 *Rüpke, G.*, a.o.O. (Fn. 177), 187.
180 *Burkert, H.*, a.o.O. (Fn. 50), Rn. 52.
181 *Königshofen, T.*, Betriebliche Datenschutzbeauftragte, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, Rn. 14; Damman-Simitis, BDSG-*Simitis*, Einleitung, Rn. 12.
182 *Simitis, S.*, a.o.O. (Fn. 50), S. 286.
183 Grabitz/Hilf-*Brühann*, Richtlinie95/46, Vorbem. A 30, Rn. 64-66.
184 Damman-Simitis, DSRL-*Simitis*, Einleitung, Rn. 37.

ii) Institutionelle Verarbeitungskontrolle

1983 hatte die Volkszählungsentscheidung die Einrichtung einer unabhängigen Kontrollinstanz als verfassungsrechtlichen Auftrag erkannt.[185] Genauso unabdingbar erscheint diese Vorgabe bei der DSRL (Art. 28, Erwägungsgrund 62). Allerdings verlangt jene Unabhängigkeit keine institutionelle Trennung von der öffentlichen Verwaltung, so wie es die Kommission vorgeschlagen hatte, sondern lediglich eine funktionale Trennung, so wie es der Rat zugebilligt hatte.[186] Wenn auch den Mitgliedstaaten nicht die Verpflichtung auferlegt wird, alle in Art. 28 Abs. 3 erwähnten Rechte zu übernehmen, sieht die DSRL neben Untersuchungs- und Einwirkungsbefugnissen ein Klagerecht der Kontrollinstanz vor.

Die Vorschriften der DSRL über die Kontrollinstanz haben sich erheblich auf das nationale Organisationsrecht ausgewirkt.

Beispielsweise war in Italien die bis dahin unbekannte Einrichtung eines Datenschutzbeauftragten Folge der Umsetzung der DSRL. Dies hat die wissenschaftliche Diskussion über die verfassungsrechtliche Stellung der sog. *autorità indipendenti* fortgeführt.

Dass die jeweils nationalen und die europäische Rechtsordnung in einem wechselseitigen Verhältnis stehen wird von einem breiten Schrifttum vertreten.[187] Nicht nur werden die zwei mit einander verflochtenen Ebenen als eine übergreifende *public arena*[188] verstanden, wo die vollziehende Gewalt ebenso eine *multilevel* Struktur hat.[189] Vielmehr wird die Befugnis des Datenschutzbeauftragten, Rechtsverordnungen zu erlassen, direkt aus der DSRL abgeleitet, ohne dass eine innerstaatliche Norm dazu erforderlich ist. Der italienische Datenschutzbeauftragte wird somit als ein *ente autarchico europeo* (autonome europäische Anstalt) betrachtet.[190] Es liegt nah, dass solche Thesen bzw. Modelle deutliche Parallelen zu der These des Verfassungsverbunds aufweisen, welcher die gestufte Verfassungsstruktur und die Einheit der durch die nationalen Verfassungen und durch den Unionsvertrag konstituierten Ordnung ausdrückt.[191]

Was das deutsche Verwaltungsrecht betrifft, entspricht die Einrichtung des Amtes des Bundesdatenschutzbeauftragten (BfD), sowie seine Ausstattung, seine Untersuchungs- und Einwirkungsbefugnisse den europäischen Anforderungen bereits vor Verabschiedung der Richtlinie.[192] Die institutionelle Kontrolle des Datenschutzes in Deutschland setzt sich allerdings aus mehreren Einrichtungen zusammen. Neben dem BfD sind die Landesbeauftragten und die Aufsichtsbehörden, welche den Datenschutz bei den Behörden der Landesverwaltungen bzw. im privaten Bereich kontrollieren, zu erwähnen. Über diese sog. Fremdkontrolle hinaus, werden Formen der Selbstkontrolle durch betriebliche und behördliche Datenschutzbeauftragte realisiert.[193] Gerade aber im Hinblick auf die Unabhängigkeit der betrieblichen Datenschutzbeauftragten (§ 4f BDSG 2001) sowie auf die

---

185 *Heil, H.,* Bundesbeauftragter für den Datenschutz, in: Büllesbach (Hrsg.), Datenverkehr ohne Datenschutz? Köln 1999, Rn. 20.

186 *Hillenbrand-Beck,* Aufsichtsbehörden, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 817ff., München 200, Rn. 25-27.

187 *Cassese, S.*, L' Arena Pubblica, Nuovi paradigmi per lo Stato, Rivista Trimestrale di diritto pubblico 2001, S. 601ff; *Franchini, C.,* I principi dell' organizzazione amministrativa comunitaria, Rivista Trimestrale di diritto pubblico 2002, S. 651ff.; *della Cananea, G.,* a.o.O. (Fn. 86), S. 33-61, 141-179; *Chiti, M.,* Diritto amministrativo europeo, Milano 1999, S. 118-127; *Merusi, F.*,Democrazia e autorità indipendenti, Bologna 2000, S. 75-76; *Merusi/Passaro,* Autorità Indipendenti, in: Enciclopedia del diritto, Milano 2002, S. 186-187.

188 *Cassese, S.,* L' Arena Pubblica, a.o.O. (Fn. 187), S 643-649. Das Konzept der *Public Arena* ist dadurch gekennzeichnet, dass Privaten (natürlichen sowie juristischen Personen) dermaßen Beteiligungs- sowie Mitwirkungsrechte eingeräumt werden, dass die Trennung zwischen dem öffentlichen und dem privaten Bereich verschwimmen soll.

189 *Franchini, C.*, a.o.O. (Fn. 187), S. 675-679, *Cassese, S.,* L' Arena Pubblica, a.o.O. (Fn. 187), S. 645-647.

190 *Merusi, F.,* a.o.O. (Fn. 187), S. 75; *Merusi/Passaro,* a.o.O. (Fn. 187), S. 186.

191 *Pernice, I.,* Die dritte Gewalt im europäischen Verfassungsverbund, EuR 1996, 27, *ders.* Europäisches und nationales Verfassungsrecht, VVDStRL (2003) 60, 172-176; Für den nicht-deustchsprachigen Leser scheint diese Übersetzung des Begriffes des multilevel constitutionalism vom Deutschen (Verfassungsverbund) ins Englische die Gefahr eines Missverständnisses zu bergen, insbesondere dann, wenn dieser Begriff hierarchisch verstanden wird, vgl. z.B. *della Cananea, G.,* a.o.O (Fn. 86), S. 65.

192 *Heil, H.,* Bundesbeauftragter für den Datenschutz, a.o.O (Fn. 185), Rn. 83.

193*Heil, H.,* Bundesbeauftragter für den Datenschutz,a.o.O. (Fn. 185), Rn. 3-9; *Hillenbrand-Beck,* a.o.O. (Fn. 186), Rn. 2-4.; *Abel, R.B.,* Behördliche Datenschutzbeauftragte, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, Rn.1-3.; *Büllesbach, A.,* Konzeption und Funktion des Datenschutzbeauftragten vor dem Hintergrund der EG Richtlinie und der Novellierung des BDSG, RDV 2001, 4.

Einwirkungsmöglichkeit der Aufsichtsbehörde (§ 38 BDSG) wurde jedoch deren ungenügende Ausgestaltungen als „offenkundige Verstöße“ gegen die DSRL angesehen.[194]

3) Harmonisierung durch Verfahren

Die DSRL förderte eine der bis dahin wenigen gemeinschaftlichen Harmonisierungen im Bereich des öffentlichen Rechts.[195] Der Erlaß der DSRL stellte jedoch nicht das Ende der Harmonisierung dar. Was *Brühann* im Bezug auf die DSRL behauptet, gilt allgemein für jede Harmonisierung nach dem Gemeinschaftsrecht (was wiederum eine Besonderheit der europäischen Integration ist): Jede Richtlinie i.S.d. Art. 95 EGV „setzt einen Prozeß fortschreitender Harmonisierung in Gang“. Sowohl die DSRL als auch das allgemeine Gemeinschaftsrecht „stellen eine Reihe von Verfahren zur Verfügung, mit denen die Harmonisierungstiefe schrittweise entsprechend der Notwendigkeit vergrößert werden kann“[196]. Auf diese Vielfalt von Verfahren wird hier kurz eingegangen.

a) Selbstregulierung

Der Herausforderung einer „Modernisierung“ des Datenschutzes und den Vorstellungen des niederländischen, britischen und irischen Rechts entsprechend, fördert Art. 27 DSRL die Ausarbeitung von Verhaltensregeln durch Berufsverbände. Insofern enthält schon die DSRL einen Ansatz, welchen die nachfolgende sog. vierte Generation der Datenschutzgesetze stärker betonen wird.

Dabei handelt es sich um sog. *soft law*, das die DSRL in den spezifischen Arbeitsbereichen implementieren will.[197] Es werden nicht nur Verhaltensregeln vorgesehen, deren Anwendungsbereich auf die einzelnen Mitgliedstaaten beschränkt ist (Art. 27 Abs. 2), sondern auch „gemeinschaftliche Verhaltensregeln“ (Art. 27 Abs. 3). Berufsverbände sollen Entwürfe für gemeinschaftliche Verhaltensregeln der Art. 29-Gruppe (s. u. b)) für eine Überprüfung unterbreiten. Die Art. 29-Gruppe prüft die Entwürfe am Maßstab der zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Vorschriften. Sobald die Gruppe sich positiv ausgedrückt hat, wird die Kommission ermächtigt, Verhaltensregelungen zu veröffentlichen.

Obwohl die zunehmende Bedeutung der gemeinschaftlichen Verhaltensregelungen im Hinblick auf die Harmonisierung im Binnenmarkt in der Literatur betont wird,[198] haben nach Auffassung der Kommission zu wenige Einrichtungen sektorale Verhaltenskodizes vorgelegt.[199] Die Förderung der Selbstregulierung bleibt daher eine der zentralen datenschutzrechtliches Anliegen der Kommission. Darunter fällt auch die im Jahr 2002 an die europäischen Sozialpartner gerichteten Konsultationspapiere und deren darin enthaltene Empfehlung, einen Arbeitnehmerdatenschutz über Art. 137 Abs.2 EGV zu schaffen.[200]

---

194 Simitis u.a., BDSG-*Simitis*, Einleitung, Rn. 102. Die Aufsichtsbehörde werden als „Papiertiger beschrieben“ von *von Lewinski, K.*, Formelles und informelles Handeln der datenschutzrechtlichen Aufsichtsbehörden, RDV 2001, 275-276. *Contra, von Schmeling, M.,* Vom Papiertiger zu Sonderordnungsbehörde, DuD 2002, 352-353, Simitis u.a., BDSG-*Walz*, § 38, Rn. 39. Dass die Datenschutzbehörde eher durch die Öffentlichkeitsarbeit als durch Anordnungsbefugnisse Wirkung erzielen, behauptet *Bull*, Öffentlichkeitsarbeit unter gerichtlicher Kontrolle, SS. 421-423.

195 *Opperman, T.,* a.o.O. (Fn. 75), Rn. 1259. Die Harmonisierung im Bereich des öffentlichen Rechts hat inzwischen einen relativen Impuls durch die Errichtung eines „Raumes der Freiheit, der Sicherheit und des Rechts“ bekommen, insbesondere in den Politikbereiche die dem Titel IV EGV zugeordnet wurden.

196 Grabitz/Hilf-*Brühann*, Richtlinie 95/46, Vorbem. A 30, Rn. 53.

197 *Abel, R.B.*, Umsetzung der Selbstregulierung im Datenschutz: Probleme und Lösungen, RDV 2003, 12-13.; *Heil, H.*, Datenschutz durch Selbstregulierung-Der europäische Ansatz, DuD 2001, 131.

198 Grabitz/Hilf-*Brühann*, Richtlinie 95/46, Vorbem. A 30, Rn. 54; Dammann-Simitis, DSRL-*Dammann*, Art. 27, Rn. 10; *Heil, H.*, Datenschutz durch Selbstregulierung, a.o.O. (Fn. 197), 131.

199 KOM (2003) 265 endg., S. 28. Entwürfe für gemeinschaftliche Verhaltensregeln haben FEDMA (Federation of European Direct Marketing Associations), IATA (International Air Transport Association) und AESE (Association of Executive Search Consultants) unterbreitet, vgl. *Heil, H.*, Datenschutz durch Selbstregulierung, a.o.O. (Fn. 197), 131.

200 KOM (2003) 265 endg., SS. 5, 29. Sei es daran erinnert, dass es bisher auf nationaler Ebene nicht gelungen ist, eine bereichsspezifische Regelung zum Arbeitnehmerdatenschutz zu erlassen, vgl. Simitis u.a., BDSG-*Simitis*, Einleitung, Rn. 42.

b) Die Art. 29-Datenschutzgruppe

Immer häufiger wird auf eine Netz-Struktur der europäischen Verwaltung hingewiesen, welche aus den (mehr oder weniger) unabhängigen Einrichtungen der Mitgliedsstaaten und den Agenturen der EG/EU besteht.[201] Um die Flexibilität der Umsetzung des Gemeinschaftsrechts, sowie die Wirksamkeit der Harmonisierung zu fördern und den Mitgliedstaaten den erforderliche Spielraum beizubehalten, werden strukturelle Veränderungen der traditionellen vollziehenden Gewalt durchgeführt. Gleichzeitig erfolgen solche Umwandlungen sowohl auf der Ebene der Mitgliedsstaaten als auch auf europäischer Ebene, welche aufeinander wirken. Dies zeigt, meiner Meinung nach, dass das Netz-Modell mit dem Modell des Verfassungsverbunds kompatibel ist.

Wenn auch die Art. 29-Datenschutzgruppe (sowie der einzurichtende Europäische Datenschutzbeauftragte) nicht den europäischen Agenturen zugeordnet wird, kann ein solches Gremium als der ursprüngliche Kern eines Netzes zwischen den nationalen Datenschutzbeauftragten angesehen werden.

Art. 29 DSRL legt fest, dass eine Datenschutzgruppe einzusetzen ist und „schafft damit auf der Ebene des sekundären Gemeinschaftsrechts eine neue Institution."[202] Art 29 (der die Zusammensetzung dieser Gruppe und Geschäftsordnungsfragen bestimmt) sowie Art. 30 (der die Aufgaben der Gruppe und ihr Verfahren nach außen regelt) sind materiell keine an die Mitgliedstaaten gerichtete Richtlinien, die in einzelstaatliches Recht umzusetzen sind, sondern Entscheidungen i.S.d. Art. 249 Abs. 4 EGV, die für ihre Regelungsadressaten unmittelbar verbindlich sind.[203]

Die Gruppe setzt sich aus Vertretern der unabhängigen Kontrollstellen der Mitgliedstaaten sowie einem Vertreter der Kommission zusammen und ermöglicht somit ihre laufende Zusammenarbeit auf der Ebene der Gemeinschaft. Sie ist aber keine den nationalen Kontrollstellen übergeordnete Instanz. Sowohl die Kommission als auch der Rat haben absichtlich keine supranationale Intervention in die innerstaatliche Kontrolltätigkeit einführen wollen.[204]

Die Art. 29-Gruppe ist ein Forum der EG, in dem die nationalen Erfahrungen ausgetauscht, bestehende Datenschutzdefizite aufgezeigt und neue Tendenzen festgestellt bzw. gefördert und neue Regelungen entwickelt werden sollen. Weiterhin ist sie ein beratendes Organ der Kommission bei allen datenschutzrelevanten Gemeinschaftsvorhaben (Art. 30 Abs. 1 c). Daher verkörpert sie die Verbindung zwischen einer unverändert nationalen Kontrolle und der in der DSRL materialisierten supranationalen Verantwortung für einen effizienten Datenschutz.[205]

Dem Verständnis der Harmonisierung als kontinuierlichen Prozess entsprechend, zählt zu den Aufgaben der Gruppe die Prüfung aller Fragen anlässlich der Umsetzung der DSRL „um zu [ihrer] einheitlichen Anwendung beizutragen" (Art. 30 Abs. 1 a); Erwägungsgrund Nr. 65). Die Personalunion, die daraus besteht, dass die in den Mitgliedstaaten eingerichteten Kontrollinstanzen zugleich Mitglieder der Art-29 Gruppe sind, trägt mittelbar zur Einheitlichkeit der Anwendung der Richtlinie bei. Jede innerstaatliche Stelle ist nämlich dazu veranlasst, im nationalen Bereich die gemeinsame Auffassung ihrer jeweiligen Maßnahmen zugrunde zu legen, was denkbare nationale Unterschiede bei der Auslegung bzw. Durchführung der DSRL mildern soll.

Dieser Harmonisierungsfunktion ist sich die Kommission weitgehend bewusst. In ihrem Bericht zur Umsetzung sieht sie die künftige Arbeit der Art. 29-Gruppe, neben den Initiativen der Kommission selbst, als ein wirkungsvolles Mittel, um fehlerhafte Umsetzungen der DSRL zu korrigieren.[206]

Ein zusätzliches Mittel für die Zusammenarbeit der nationalen Datenschutzbeauftragten ist in der europäischen Amtshilfen nach Art. 28 Abs. 6 der DSRL zu sehen.

---

201 *Cassese, S.*, Gli Stati nella rete internazionale dei poteri pubblici, Rivista Trimestrale di diritto pubblico 1999, 325-329; *Chiti, E.* , Le agenzie europee, Padova 2002, 38-39.

202 *Ehmann/Ehrlich*, EG-Datenschutzrichtlinie, Köln 1999, Art. 29, Rn. 1.

203 Dammann-Simitis, DSRL-*Dammann*, Art. 29, Rn. 2.

204 Dammann-Simitis, DSRL-*Simitis*, Einleitung, Rn. 41.

205 Dammann-Simitis, DSRL-*Simitis* Rn. 41., *Heil, H.*, Bundesbeauftragter für den datenschutz, a.o.O. (Fn. 185), Rn. 84.; *Heil, H.*, Die Artikel 29-Datenschutzgruppe, DuD 1999, 471.

206 KOM (2003) 265 endg., SS. 26-27.

d) Entscheidungen durch die Kommission

Art. 25 Abs. 4 sowie Art. 26 Abs. 4 erteilen der Kommission die Befugnis, Entscheidungen im Bereich der Übermittlung personenbezogener Daten in Drittländer zu erlassen, welche für alle Mitgliedstaaten verbindlich sind und deshalb zur einheitlichen Durchführung der Richtlinie beitragen (ausführlicher siehe unten Teil 3 B III).

e) Vorabentscheidungsverfahren

Nach dem EGV entscheidet der EuGH im Wege der Vorabentscheidung über die Gültigkeit und die Auslegung sekundären Gemeinschaftsrechts (Art. 234 Abs. 2 b)), d.h. auch über Gültigkeit und Auslegung der DSRL. Bekanntlich trägt das Vorabentscheidungsverfahren zur einheitlichen Anwendung des Gemeinschaftsrechts durch die Mitgliedsstaaten bei. Bisher hat der EuGH lediglich drei Rechtssachen über die Auslegung der DSRL entschieden.

Im Fall *Fisher* (C-369-98)[207] handelte es sich um das integrierte Verwaltungs- und Kontrollsystem für bestimmte gemeinschaftliche Beihilfereglungen. Um Beihilfen für eine bestimmte Fläche zu bekommen hatte Herr *Fisher* beim englischen Wirtschaftsministerium einige Daten über die frühere Bewirtschaftung der Höfe beantragt. Diese wurden ihm auf Grund der Vertraulichkeit verweigert. Rechtlich ging es um die Auslegung des Art. 7 Buchstabe l) über eine der Zulässigkeitsvoraussetzungen für die Datenverarbeitung. Nach dieser Norm ist eine Verarbeitung zulässig, wenn die Verarbeitung zur Verwirklichung eines berechtigten Interesses des für die Verarbeitung Verantwortlichen bzw. eines Dritten, „sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person … überwiegen." Der EuGH hat die Abwägung zwischen Vertraulichkeit und Aktenzugang zugunsten des Letzteren entschieden, da die „Weitergabe der Daten an *Fisher* kein Interesse des Inhabers der Daten beeinträchtigt".

Auch der zweite Fall (C-465/00, C-138/01, C-139-01[208]) wurde im Wege einer Abwägung entschieden. Diesmal stand dem Interesse auf Schutz personenbezogener Daten das öffentliche Interesse an der Kontrolle der Bezüge öffentlicher Funktionäre gegenüber (Art. 6 Abs. 1 c) i.V.m. Art. 7 c), e) DSRL). Nach einem österreichischen Verfassungsgesetz müssen Angaben bezüglich das eine bestimmte Grenze überschreitende Einkommen von Arbeitnehmern öffentlicher Unternehmen bzw. Behörden erhoben werden, die unter namentlicher Nennung des Betroffenen in einem Bericht des Rechnungshofes aufzunehmen sind, welcher auch veröffentlicht wird. Diese Entscheidung ist aus mehren Gründen bemerkenswert.

Erstens wird das Vorabentscheidungsverfahren von dem österreichischen Verfassungshof eingeleitet, was, im Gegensatz zum BVerfG und zur italienischen Corte Costituzionale, sein Selbstverständnis als Gericht letzter Instanz i.S.d. Art. 234 EGV bestätigt.

Zweitens wird der Anwendungsbereich der Richtlinie, der sich nach Art. 3 DSRL mit dem Anwendungsbereich des Gemeinschaftsrechts deckt, tendenziell weit verstanden. Darunter falle auch die Kontrolltätigkeit des österreichischen Rechnungshofes, der die individualisierten Bezüge öffentlicher Funktionäre offen legt. Im Einklang mit seiner früheren Rechtssprechung urteilte der EuGH, dass die DSRL auf Sachverhalte anwendbar ist, bei denen kein unmittelbarer Zusammenhang mit der Ausübung der durch den EG-Vertrag garantierten Grundfreiheiten (hier Art. 39 EGV) besteht.[209]

Drittens wurde den österreicherischen Gerichten vom EuGH aufgetragen die von Art. 6 Abs. 1 c) i.V.m. Art. 7 c), e) DSRL aufgeworfene Abwägungsfrage jeweils unter Berücksichtigung der Kriterien der EGMR-Rechtsprechung zu lösen. Von einem strikten Kooperationsverhältnis zwischen EGMR und EuGH ausgehend bezieht sich letztere direkt auf Art.8 EMRK (Recht auf Achtung der Privatsphäre). Explizit wurde angeordnet, die Bestimmungen der DSRL im Lichte der Grundrechte

---

[207] Abgedruckt in EuGRZ 2001, SS. 32ff.

[208] Abgedruckt in RDV 2003, SS. 231ff.

[209] Trotz der gegenteiligen Auffassung des Genaralanwaltes Tizzano, wonach die Erhebung bzw. Verarbeitung personenbezogener Daten durch den Rechnungshof der effizienten Verwaltung öffentlicher Mittel diene, d.h. einer „öffentlichen Kontrolltätigkeit, die von den österreichschen Stellen aufgrund einer selbstständigen politisch-institutionellen Entscheidung vorgesehen und (mit Verfassungsrang) geregelt wurde", EuGRZ 2003, S. 90.

auszulegen. Grundrechte gehören zu den gemeinschaftsrechtlichen allgemeinen Rechtsgrundsätzen, welche in Art. 6 Abs. 2 EUV aufgenommen wurden. Es muss daher festgestellt werden, ob die österreichische Regelung einen Eingriff in die Privatsphäre des Betroffenen darstellt und ob ein solcher Eingriff gegebenenfalls gerechtfertigt ist. Um dies zu prüfen, wird ohne weiteres an Art. 8 EMRK sowie an die einschlägige Rechtssprechung des EGMR angeknüpft. Die Eröffnung des Anwendungsbereichs wird nach den jüngsten Entscheidungen[210] auch dann bejaht, wenn die erhobenen, personenbezogenen Daten nicht der strikten Privatsphäre des Betroffenen zuzuordnen sind. Art. 8 EMRK ist daher auch in diesem Fall, wo es um Daten über die beruflichen Einkünfte Einzelner geht, anwendbar. Darüber hinaus wird der bislang durch die Rechtssprechung des EGMR entwickelte Begriff „Notwendigkeit in einer demokratischen Gesellschaft" nach wie vor herangezogen. Deutlich wird bemerkt, dass, obwohl kein Hinweis zu den Art. 52 Abs. 3 und 53 der Charta der Grundrechte gemacht wird, der EuGH diese Bestimmungen *de facto* anwendet.[211]
Dennoch, auch wenn verschleierte Hinweise des EuGH nicht fehlen, löst dieser die Abwägungsfrage nicht selbst, sondern überantwortet sie dem zuständigen innerstaatlichen „europäischen" Richter.[212] Die Frage, inwiefern die Veröffentlichung der Namen jeglicher Arbeitnehmer in Verbindung mit deren Einkünften für eine sparsame und sachgerechte Verwendung öffentlicher Mittel durch die Verwaltung notwendig ist, müssen die nationalen Gerichte beantworten. Denen obliegt eine richtlinienkonforme Auslegung der nationalen Vorschriften, welche an eine grundrechtskonforme Auslegung der Richtlinie orientiert ist. „Sollten die vorlegenden Gerichte die … nationale Regelung für unvereinbar mit Art. 8 EMRK halten, so kann diese Regelung auch nicht dem Erfordernis der Verhältnismäßigkeit nach Art. 6 Abs.1 c) und Art. 7 c), e) DSRL genügen."
Letztlich bestätigt der EuGH, dass die hier in Frage kommenden Artikel der DSRL der Voraussetzung zur unmittelbaren Anwendbarkeit erfüllen, so dass „sich der Einzelne vor den nationalen Gerichten auf sie berufen kann, um die Anwendung entgegenstehender Vorschriften des innerstaatlichen Rechts zu verhindern."
Eine interessante Konstellation ergab sich ebenso aus dem dritten Fall (C-101/01, *Lindquist*)*. Der Beklagten, Frau Lindqvist, wurde vorgeworfen, gegen die schwedischen Rechtsvorschriften über den Schutz personenbezogener Daten verstoßen zu haben, indem sie auf ihrer Internetwebsite personenbezogene Daten über eine Reihe von Personen veröffentlichte, die wie sie ehrenamtlich in einer Gemeinde der protestantischen Kirche von Schweden tätig seien. Zum Kern des Disputes wurden hier die Fragen, inwieweit Datenübermittlungen über das Internet dem Anwendungsbereich der DSRL, unterfallen und wie das (Grund)recht auf Schutz personenbezogener Daten mit dem Grundrecht auf Meinungsfreiheit abzuwägen ist.
Nachdem der EuGH, seiner vorherigen Rechtssprechung folgend, einen breiten Anwendungsbereich der DSRL bejahte, musste er feststellen, dass die spezifische Norm für Datenübermittlung in Drittländer (Art. 25 DSRL, s. ausführlich unten Teil 3 B) im vorliegenden Fall nicht einschlägig ist. Zum Zeitpunkt der Handlung waren auch die bereichspezifischen Normen hinsichtlich des Datenschutzes im Falle elektronischer Kommunikation (RL 2002/58/EG) noch nicht in Kraft getreten und die strikte Anwendung der allgemeinen Regelung des Art. 25 DSRL hätte zu einer völligen Blockade der Datenströme im Internet führen können.
Bezüglich des Konflikts zwischen den kollidierenden Grundrechten (wobei für Fr. Lindqvist neben der Meinungsfreiheit auch die Religionsfreiheit in Betrachtung kommt), deutet der EuGH auf eine „mildere"** Auslegung der DSRL. Insbesondere wies er die nationalen Gerichte darauf hin, dass „Behörden und Gerichte der Mitgliedstaaten nicht nur ihr nationales Recht im Einklang mit der

---

210 EGMR, Urteile Amann/Schweiz vom 16.2.2000 und Rotaru/Rumänien vom 4.5.2000)

211 *Denicoló/Palermo*, La riservatezza ...senza riserve, nota a sentenza cause riunite C-465/00, C-138/01, C-139/01, Diritto Pubblico Comparato ed Europeo 2003, 1258

212 *Pernice, I.*, Der dritte Gewalt, a.o.O. (Fn. 192), S. 33ff.

* abrufbar unter: http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=de&Submit=Suchen&docrequire=alldocs&numaff=C-101%2F01&datefs=&datefe=&nomusuel=&domaine=

** Die Metapher eines „milden" Rechts wurde in der italienischen Literatur von Zagrebelsky eingeführt, um die Eigenschaft des Verfassungsrechts zur Zeit einer pluralistischen Demokratie, welche den Positivismus überholt hat, auszudrücken: S. *Zagrebelsky, V.*, Il diritto mite, Torino 1992.

Richtlinie 95/46 auszulegen [haben], sondern auch, dass sie sich [dabei] nicht auf eine Auslegung dieser Richtlinie stützen [dürfen], die mit den durch die Gemeinschaftsrechtsordnung geschützten Grundrechten…kollidiert". Somit ist eine sorgfältige Verhältnismäßigkeitsprüfung vonnöten, wobei „insbesondere die Dauer der Zuwiderhandlung gegen die die Richtlinie 95/46 durchführenden Vorschriften" zu berücksichtigen ist. Da Fr. Lindquist die fraglichen Seiten „sofort" wieder entfernte, als sie erfuhr, dass sie von einigen ihrer Kollegen missbilligt wurden, ist es voraussehbar, dass die gegen Fr. Lindqvist auf den ersten Blick „übermäßige" Geldstrafe erheblich reduziert wird.

f) Bereichsspezifische Regelungen

Die Ausarbeitung von sektorspezifischen Verarbeitungsregeln neben einem allgemeinen Datenschutzgesetz war von Anfang an ein Hauptanliegen des Datenschutzes. Bereichspezifische Regeln zu formulieren, war 1983 gerade eine der Vorgaben der Volkszählungsentscheidung. Hierdurch kann man sich mit den konkreten Verarbeitungszusammenhängen befassen und für den Bürger besser verständliche Normen schaffen, was hingegen Generalklauseln weniger ermöglichen (s. o. I 1 a).[213]
Eine Vertiefung der Harmonisierung kann daher die EG/EU durch bereichspezifische Regelungen erlangen.[214] Als Beispiel gilt die RL 97/66/EG im Bereich der Telekommunikation, welche schon durch die RL 2002/58/EG[215] für die gesamte elektronische Kommunikation ersetzt worden ist.

Teil 3: Die Drittländerregelung der DSRL

Der Prozess der Globalisierung ist irreversibel.[216] Die Anzahl multinationaler Konzerne wächst und weltweite Datennetze sowie moderne Informations- und kommunikationstechnologien vereinfachen den Datenaustausch auf internationaler Ebene. Im Rahmen internationaler Arbeitsteilung suchen nationale Unternehmen vermehrt die Zusammenarbeit mit ausländischen Firmen zur gemeinsamen Produktion, Leistungserbringung oder Funktionsübernahme. Die Ursachen hierfür sind vielfältig: Erhaltung der Wettbewerbsfähigkeit, Erhöhung der Produktivität, Optimierung der Kosten, Ausnutzung von Standortvorteilen, Synergieeffekte oder die Eröffnung neuer Märkte.[217] In diesem Kontext werden Informationen zunehmend zum strategischen Wettbewerbsfaktor.[218] Hinzu kommt die stets zunehmende Bedeutung des *Electronic Business.*
In einem Unternehmen fallen die unterschiedlichsten Datenverarbeitungen und -übermittlungen an: Kundendaten, Daten von Lieferanten und Geschäftspartnern sowie Arbeitnehmerdaten.[219] Im Internet hingegen sammeln sich die Datenspuren eines jeden *surfers*.
Während das Anliegen des Arbeitnehmerdatenschutzes im Konzern seit längerem diskutiert wird, ohne dass dabei eine befriedigende Lösung gefunden wurde,[220] ist der Kundendatenschutz gerade für Unternehmen zum neuen Thema geworden. Es wird behauptet: *„Privacy is essential for electronic commerce to flourish",*[221] „Datenschutz und Datensicherheit sind Bestandteile einer modernen und wertorientierten Managementphilosophie"[222]; auch sollen „für Manager finanzielle Belohnungen" für die „Umsetzung

213 Simitis u.a., BDSG-*Simitis*, Einleitung, Rn. 45-48.
214 Grabitz/Hilf-*Brühann*, Richtlinie 95/46, Vorbem. A 30, Rn. 58.
215 Abl. 2002 L 201/37.
216 *Beck, U.*, Che cos'é la globalizzazione, Roma 1999, S. 24.
217 *Eul/Gödefroid*, Übermittlung personenbezogener Daten ins Ausland nach Ablauf der Umsetzungsfrist der EG-Datenschutzrichtlinie, RDV 1998, 185.
218 *Büllesbach, A.*, Datenschutz im Konzern, in: Roßnagel (Hrsg.), Handbuch des Datenschutzrechts, München 2003, Rn.1
219 *Büllesbach, A.*, Datenschutz im Konzern, a.o.O. (Fn. 218), Rn. 5-48.
220 *Däubler, W.*, Grenzüberschreitender Datenschutz-Handlungsmöglichkeiten des Betriebsrats, RDV 1998, 97-99; *ders.*, Übermittlung von Arbeitnehmerdaten ins Ausland, in: Büllesbach (Hrsg.), Datenverkehr ohne Datenschutz?, Köln 1999, S. 77-80; *Klug, C.*, Globaler Arbeitnehmerdatenschtz, SS.112-114.
221 *Wellbery, B.*, The U.S. Side of Privacy, in: Büllesbach (Hrsg.), Datenverkehr ohne Datenschutz?, Köln 1999, S. 168.
222 *Büllesbach, A.*, Datenschutzsfragen der internationalen Vertriebsdatenverarbeitung, in: Büllesbach (Hrsg.), Datenverkehr ohne Datenschutz?, Köln 1999, S.66.; *ders.* Datenschutz im Konzern, a.o.O. (Fn. 218), Rn.72.

des Datenschutzes im Konzern“[223] vorgesehen werden. Solche Aussagen sind ein Beleg dafür, dass Konsumentendatenschutz von der Industrie zunehmend als Wettbewerbsfaktor betrachtet wird und zum Objekt ökonomischer Entscheidung wird. Dieser Entwicklung liegt offenbar eine „Verkaufslogik“[224] zugrunde, die ähnlich wie beim Umweltschutz dazu führt, Datenschutz und Sicherheit als integrale Bestandteile von Produkten, Dienstleistungen und Geschäftsprozessen zu begreifen.
Offenbar sind hierbei, neben einem ökonomisch orientierten Verständnis des Datenschutzes (s. o. I 3 d), Konzepte der Selbstschutz- bzw. der Selbstregulierung spürbar (s. o. I 3 b und c) Dies soll aber nicht überraschen, denn es spiegelt das wesentliche Merkmal der Globalisierung wieder: Der Nationalstaat ist nicht mehr durch seine Souveränität untermauert. Im Raum weltweiter und offener Netze kann kein (demokratischer Rechts-) Staat eine unbegrenzte Vollzugshoheit hinsichtlich seiner Gesetze durchsetzen.[225]
Wenn der Nationalstaat aber eher ohnmächtig ist, kann der supranationale Gesetzgeber für eine gewisse Abhilfe sorgen. Die Rolle der DSRL darf in diesem Zusammenhang nicht unterschätzt werden. Zwar beansprucht sie keine globale Geltung, doch ist sie als eine der „modernsten“[226] internationalen Datenschutzregelungen.[227] Nicht nur hat sie zum ersten Mal Kollisionsregeln vorgesehen (A), sondern auch eine im Vergleich zu den Instrumenten des OECDs und des Europarates klarere Regelung bezüglich des Datenexports getroffen (B). Diese sog. Drittländerregelung hat aus wirtschaftspolitischen Gründen einen erheblichen Einfluss auf das amerikanische Konzept des Datenschutzes gehabt (C), bis sie von der jüngsten internationalen geopolitischen Situation in Frage gestellt wurde (D).

A. Kollisionsregeln

Bei grenzüberschreitenden Tatbeständen ist es unabdingbar, das anwendbare Recht festzustellen, was gerade Aufgabe des internationalen Privatrechts ist. Obwohl die im IPR erforderlichen „Auslandsberührung“ in der technischen Natur der Datenübermittlung schon angelegt ist, steckte das Kollisionsrecht des Datenschutzes bis vor kurzem noch „in den Kinderschuhen.“[228] Bezüglich des zu wählenden Anknüpfungspunktes standen verschiedene zur Auswahl: Zunächst ließe sich an das Recht des Aufenthaltsorts des Betroffenen oder an das Recht des Orts, wo die Datenverarbeitung stattfindet anknüpfen. Ferner könnte das Recht des angerufenen Gerichts oder des höheren Schutzniveaus gewählt werden.
Was beispielsweise das deutsche Recht anbelangt, wird Datenschutz als Bestandteil der Wirtschaftsordnung verstanden, was sich auch aus der Kontrolltätigkeit der Aufsichtsbehörde, sowie aus den Sanktionen in Form der Straf- und Bußgeldtatbeständen ergibt. Somit ist Datenschutz „zwingendes Recht“ i.S.d. Art. 34 EGBGB, welches alle Verarbeitungen umfasst, die auf deutschem Territorium vorgenommen werden.[229]
Mit dieser im Wege der Auslegung erreichten Lösung stimmt grundsätzlich die Kollisionsregel i.S.d. Art. 4 DSRL überein. Die Regelung unterscheidet zwischen Sachverhalten, die mehr als einen Mitgliedsstaat betreffen (Abs.1 a) und b)) und Sachverhalten, die sich (mindestens) zwischen einem Mitgliedstaat und dem eines Drittstaates abspielen (Abs. 1 c und Abs. 2).
Als maßgeblichen Anknüpfungspunkt sieht die Richtlinie den Ort der Niederlassung des Verantwortlichen der Verarbeitung vor. Daher sind die zur Umsetzung der Richtlinie erlassenen

---

[223] *Schrecker, I.,* Problematik der Umsetzung der EG-Richtlinie in einer Multi-Nationalen Kartenorganisation, in: Büllesbach (Hrsg.), Datenverkehr ohne Datenschutz?, Köln 1999, S. 164-165.
[224] *Büllesbach, A.,* Datenschutzfragen der internationalen Vertriebsdatenverarbeitung, a.o.O. (Fn. 222), S. 67.
[225] *Beck, U.,* a.o.O. (Fn. 216), S. 21-26; *Baldassarre, A.,* Globalizzazione contro Democrazia, Bari 2002, S. 261-271; *Roßnagel, A.*, Globale Datennetze: Ohnmacht des Staates, Selbstschutz der Bürger, ZRP 1997, 27.
[226] Nach der oben dargestellten Periodisierung der Datenschutzgesetzgebung könnte die Drittländerregelung als ein Versuch der “dritten” Generation angesehen werden, mit gesetzgeberischen Instrumenten die Herausforderungen der Globalisierung entgegen zu kommen.
[227] *Wuermeling, U.,* a.o.O. (Fn. 142), S. 212.
[228] *Däubler,* Übermittlung von Arbeitnehmerdaten ins Ausland, a.o.O. (Fn. 220), S. 74.
[229] *Däubler,* Übermittlung von Arbeitnehmerdaten ins Ausland, a.o.O. (Fn. 220), S. 75.

Vorschriften von jedem Mitgliedsstaat auf alle Vorgänge anzuwenden, die innerhalb der Tätigkeit von Niederlassungen ausgeführt werden, die sich in seinem Hoheitsgebiet befinden (Art. 4 Abs. 1 S. 1). Nur scheinbar entscheidet sich die Richtlinie für ein Sitzlandsprinzip, da die Richtlinie nicht auf den Sitz der Zentrale abstellt, sondern auf den Ort der Niederlassung, in deren Rahmen die jeweilige Verarbeitung stattfindet. Letztlich bewirkt dies eine Anknüpfung an das Territorialitätsprinzip.[230]
Die Bedeutung einer Kollisionsnorm zwischen den Mitgliedstaaten ist beispielsweise beim Arbeitnehmerdatenschutz zu sehen. Eine Besonderheit der deutschen Rechtsordnung ist der Betriebsrat, der durch Ausübung seiner Mitbestimmungs- bzw. Beteiligungsrechte auch eine wichtige Datenschutzfunktion hat (vgl. §§ 75 Abs. 2; 80 Abs. 1; 90; 87 Abs.1; 94 Abs.1; 94 Abs. 2; 95 Abs.1 BetrVG).[231] Ist nun das deutsche Datenschutzrecht anwendbar, dann sollen die datenschutzrelevanten Beteiligungsrechte des Betriebsrates gewahrt bleiben.
Für den Fall, dass der Verantwortliche nicht im Gebiet der Gemeinschaft niedergelassen ist, kommt das Recht eines Mitgliedsstaates dann zur Anwendung, wenn der Verantwortliche zum Zwecke der Verarbeitung personenbezogener Daten auf Mittel zurückgreift, die sich im Hoheitsgebiet des betreffenden Mitgliedsstaats befinden (Art. 4 Abs. 1 c) DSRL). Dadurch soll verhindert werden, dass Verarbeiter erfolgreich in sog. „Datenoasen" flüchten, d.h. dass sie sich durch Verlegung ihrer Niederlassung in einem Drittstaat der Anwendung des harmonisierten Datenschutzrechts entziehen.[232]
Ein automatisiertes Mittel i.S. dieser Regelung ist z.B. ein physisch innerhalb eines Mitgliedsstaats gelegenes EDV-System, durch das Informationsdienstleistungen angeboten oder über welches z.B. Warenbestellungen auf elektronischem Wege entgegengenommen werden.[233] Ausgenommen ist der Fall der bloßen „Durchfuhr durch das EG-Gebiet", das besonders die Anwendung der modernen Übertragungstechnik betrifft und hierbei für packetvermittelnde Dienste wie das Internet gilt (vgl. o. Fall Lindquist, Teil 2 B II 3 e) Hierbei handelt es sich um lediglich übertragungsbedingte Zwischenspeicherungen, welche nicht eine Anwendbarkeit des mitgliedstaatlichen Datenschutzrechts durch das Territorialitätsprinzips auslösen sollen.[234]
Darüber hinaus muss der im Drittland niedergelassene Verantwortliche nach Art. 4 Abs. 2 einen sog. Inlandsvertreter im Hoheitsgebiet des Mitgliedstaates bestellen, welcher die Aufgabe hat, die praktische Umsetzung des als anwendbar befundenen Recht des Mitgliedstaates zu sichern.[235]

B. Internationaler Datentransfer

I. Verhältnis von Art. 25 zu Art. 26 DSRL

Mit der Drittländerregelung bleibt die DSRL ihren Prämissen treu.[236] Danach haben die Betroffenen auch dann Anspruch auf den Schutz ihrer Grundrechte, wenn ihre Daten in einem Staat, der nicht Mitglied der EU ist, übermittelt und danach verarbeitet werden.
Nach der Grundregel des Art. 25 DSRL ist die Übermittlung in ein Drittland grundsätzlich nicht erlaubt,[237] wenn dieses kein „angemessenes" Schutzniveau gewährleistet. Die Angemessenheit richtet sich nach Art. 25 Abs. 2 „unter Berücksichtigung aller Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen." Konkret werden neben der Art der Daten auch die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das

---

230 Dammann-Simitis, DSRL-*Dammann,* Art.4, Rn. 2. Von einem *abgeschwächtesn Sitzlandsprinzip* spricht dagegen *Wuermeling, U.*, a.o.O. (Fn. 142), S. 76
231 *Gola/Klug,* a.o.O. (Fn. 29), S. 175; *Klug,* Globaler Arbeitnehmerdatenschutz, Ausstrahlungswirkung der EG-Datenschutzrichtlinie auf Drittländer am Beispiel der USA, RDV 1999, S. 113-114; *Roßmann,* Grundlagen der EDV-Mitbestimmung, Ansätze einer kollektivrechtlichen Datenschutzrechts, DuD 2002, S. 286-288.
232 *Wuermeling, U.*, a.o.O. (Fn.142), S. 77; Dammann-Simitis, DSRL-*Dammann,* Art. 4, Rn. 6.
233 Dammann-Simitis, DSRL-*Dammann,*, Art. 4, Rn. 6.
234 *Wuermeling, U.*, a.o.O. (Fn. 142), S. 80.
235 Dammann-Simitis, DSRL-*Dammann,* Art. 4, Rn. 10.
236 Dammann-Simitis, DSRL- *Simitis,* Einleitung, Rn. 27.
237 Nach *Dammann* ist die in Art. 25 enthaltene Norm keine Erlaubnisnorm, sondern eine Verbotsnorm, in Dammann-Simitis, DSRL-*Dammann,* Art. 25, Rn.4.

Endbestimmungsland, die im Herkunftsland und dem betreffenden Drittland geltenden allgemeinen oder bereichsspezifischen Rechtsnormen, sowie die dort beachteten Standesregeln und Sicherheitsmaßnahmen berücksichtigt. Die Ausnahmen, nach denen ein Datentransfer auch dann in ein Drittland ohne angemessenes Schutzniveau vorgenommen werden kann, sind im Art. 26 aufgelistet. Dazu, neben den Übermittlungen, die einem öffentlichen Interesse bzw. einem lebenswichtigen Interesse der Betroffenen dienen (Art. 26 Abs. 1 d),e), zählen die Fallgruppen der Einwilligung des Betroffenen, sowie der Vertragserfüllung bzw. Vertragsanbahnung (Art. 26 Abs. 1 a),b),c)).
Die Struktur dieser Bestimmungen vermittelt jedoch einen falschen Eindruck von der Übermittlungsrealität.[238] Nicht Art. 25 ist der Regelfall, sonder Art. 26 Abs. 1 a) bis c). D.h., erst wenn die Übermittlung weder von der Einwilligung der Betroffenen, noch für den Ablauf einer vertraglichen Beziehung erforderlich ist, ist festzustellen, ob das Empfängerland über adäquate Schutzvorkehrungen verfügt. Dies trägt dem Umstand Rechnung, dass es bei Alltagsgeschäften viel zu aufwendig ist, über die Existenz adäquater Anforderungen nachzudenken. Der Transfer wird unabhängig davon durchgeführt, inwiefern der Datenschutz im Empfängerland gewährleistet wird, unabhängig davon, ob es um Warenbestellungen, Vertragsverhandlungen, Geldüberweisungen, Hotelbuchungen, Kontoeröffnungen, Kranken- oder Haftpflichtversicherungen geht. Entscheidend ist alleinig das Einverständnis der Betroffenen oder die jeweils abzuwickelnde vertragliche Beziehung.

II. Standardsvertragsklauseln

Obwohl die in Art. 26 vorgesehenen Ausnahmen vielschichtige Fallkonstellationen des Datenaustausches mit Drittländern abdecken, kann es nach wie vor Bereiche geben, in denen keine der vorerwähnten Ausnahmen einschlägig ist. Als Beispielsfälle sind gerade international operierende Konzerne zu nennen, die Daten von Kunden und Beschäftigten zentral verarbeiten.[239] Die DSRL sieht kein Konzernprivileg vor, d.h., dass jede Übermittlung von personenbezogenen Daten an eine Tochtergesellschaft im Ausland wie eine Übermittlung an jeden anderen Dritten behandelt wird and daher bei einem niedrigerem Datenschutzniveau in einem Drittsaat grundsätzlich unzulässig ist.[240]
Einen weiteren Ausnahmefall sieht jedoch Art. 26 Abs. 2 vor: Sollte der für die Verarbeitung Verantwortliche „ausreichende Garantien“ bieten, dann darf ein Mitgliedsstaat die in Betracht kommende Übermittlung genehmigen. Als besonders geeignete Form einer Garantie gemäß Art. 26 Abs. 2 erscheinen Vertragsklauseln, die inhaltlich so entworfen sind, dass sie die Privatsphäre der Betroffenen ausreichend zu schützen vermögen.
Art. 26 Abs. 4 stellt ein förmliches Verfahren bereit, in dem festgestellt werden kann, welche Vertragsklauseln ausreichende Garantien i.S.d. Art. 26 Abs. 2 bieten.[241] Dieses Verfahren weist auf das Ausschussverfahren des Art. 31 Abs. 2 hin, wonach die Mitgliedsstaaten im Ausschuss bzw. im Rat an der Entscheidung teilnehmen können (der Ausschuss des Art. 30 setzt sich aus Vertretern der Mitgliedsstaaten zusammen. Sollte die von ihm abgelieferte Stellungnahme nicht mit den Maßnahmen der Kommission überstimmen, befasst sich der Rat mit der Angelegenheit). Auf Initiative der Kommission wird das Verfahren eingeleitet.
Das Interesse der Unternehmen an der Anerkennung von Standardvertragsklauseln durch eine Entscheidung der Kommission war aus Gründen der Rechtssicherheit und Kostenoptimierung groß. Initiativen der Internationalen Handelskammer, des Britischen Industrieverbandes, des Bankenverbands sowie die *lobbying* Aktion einzelner großer Unternehmen veranlassten die Kommission zum Erlass zweier Entscheidungen.[242] Neben allgemeinen Standardvertragsklauseln[243] wurden auch

---

238 *Simitis, S.,* Der Datentransfer von Daten in Drittländer, ein Streit ohne Ende?, in: Büllesbach (Hrsg.), Datenverkehr ohne Datenschutz?, Köln 1999, S. 180.
239 *Jakob, J.,* Datenübermittlungen in Drittländer nach der EU-Richtlinie, ein Streit ohne Ende?, SS. 177ff., in Büllesbach (Hrsg.), Datenverkehr ohne Datenschutz?, Köln 1999, S. 27.
240 *Büllesbach, A.,* Datenschutzfragen der internationalen Vetriebsdatenverarbeitung, a.o.O. (Fn. 222), S. 60.; *Gola/Klug,* a.o.O. (Fn. 29), S. 170.
241 *Ehmann/Helfrich,* a.o.O. (Fn. 202), Art. 26, Rn. 20-21.
242 *Eul/Godefroid,* a.o.O. (Fn. 217), S. 191-192.; *Schrecker, I.,* a.o.O. (Fn. 223), S. 161-162.
243 Entscheidung der Kommission Nr. 2001/497/EG, Abl. L 181/19ff.

welche spezifisch für den Bereich der Auftragsverarbeitung[244] festgestellt. Nach den genannten Enzscheidungen, wird dem Adäquanzerfordernis der Art. 25, 26 DSRL auf alle Fälle dann entsprochen, wenn sich der Importeur nach Übermittlung der Daten dazu verpflichtet, einen ausreichenden Datenschutz zu gewährleisten, wozu er hauptsächlich die nachfolgend genannten Punkte berücksichtigen muss. Zunächst muss die Garantieerklärung eine Drittbegünstigungsregelung zugunsten der jeweils betroffenen Person enthalten, welche eine gesamtschuldnerische Haftung des Datenexporteurs und -importeurs mit Möglichkeit eines Innenregresses begründet. Ferner wird eine den Betroffenen begünstigende Gerichtsstandsklausel verlangt. Auch der Datenimporteur eine Überprüfung seiner Schutzpflichten durch eine unabhängige Stelle zu ermöglichen.
In der europäischen und insbesondere deutschen Literatur wird diesbezüglich die Auffassung vertreten, dass bei Datenübermittlungen in Drittstaaten Vertragslösungen kein Ersatz für angemessene, gesetzliche Datenschutzregelungen sind.[245]
Erstens fehlt es bei Vertragsklauseln an Kontrollmöglichkeiten. Nationale Aufsichtsbehörde können nicht kontrollieren, ob der Datenschutzvertrag im Ausland auch wirklich eingehalten wird.[246] Dies würde nämlich auf einen Eingriff in fremde Souveränitätsrechte hinauslaufen, so dass entsprechende Kompetenzerweiterungen nur auf völkerrechtlicher Basis, also durch Abschluss eines Verwaltungsabkommens zulässig wären.
Zweitens weist die Rechtsform „Vertrag" einige Schwächen auf. Der Vertrag wird zwischen dem Datenexporteur und dem Datenimporteur geschlossen, wobei der Betroffene ein begünstigter Dritter ist. Eine solche Form des Vertrags zugunsten Dritter i.S.d. § 328 BGB bzw. Art. 1411 *codice civile* ist aber der *common law* Rechtsfamilie, wozu u.a. die USA zählen, unbekannt. Darüber hinaus kann der Vertrag „über die Köpfe der Betroffenen" hinweg verändert oder gar aufgehoben werden.
Schließlich ist es durchaus nachvollziehbar, dass die im Ausland gespeicherten Daten, deren Übermittlung an andere Private im Rahmen einer Sekundärnutzung ausgeschlossen ist, dem Zugriff der dortigen Behörden unterliegen.

III. Feststellung der Angemessenheit durch die Kommission

Aufgrund der Unbestimmtheit des Begriffes „angemessenes" Schutzniveau" i.S.d. Art. 25 DSRL, ist es leicht möglich, dass es in den Mitgliedsstaaten zu einer unterschiedlich schutzintensiven Auslegung kommt. Die Richtlinie schreibt deshalb ein Verfahren zur Garantie einer harmonisierten Praxis vor. Die Kommission kann nach Art. 25 Abs. 4 feststellen, dass kein angemessenes Schutzniveau vorliegt. Hingegen ist nach Art. 25 Abs. 6 eine positive Feststellung der Angemessenheit möglich. Darüber hinaus ermächtigt Art. 25 Abs. 5 die Kommission dazu, Verhandlungen mit Drittländern zu führen, um die gemäß Abs. 4 getroffene negative Entscheidung zu verbessern. Offizielle Bestätigungen der Angemessenheit des Datenschutzniveaus eines Drittlandes liegen bisher für Ungarn, der Schweiz, Kanada, Argentinien und Guernsey vor.[247] Für die U.S.A. wurde eine besondere Lösung gefunden (s. u. C).
Die Feststellung ist kein autonomes Übermittlungsverbot bzw. -gebot, sondern bewirkt eine zwingende Auslegung der Drittländervorschrift, welche demgemäß für die Mitgliedsstaaten verbindlich ist. Sie gilt

---

244 Entscheidung der Kommission Nr. 2002/16/EG, Abl. L 6/52ff.
245 *Ellger, R.*, Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem neuen Europäischen Datenschutzrechts, RabelsZ 1996, S. 761-767; *Däubler, W.*, Übermittlung von Arbeitnehmerdaten ins Ausland, a.o.O. (Fn. 220), S. 83-85.
246 Bemerkenswert ist ohnehin der Fall Citibank-Bahnkard: hierbei hat sich durch Vertrag die Citibank Tochterunternehmen in den USA damit einverstanden erklärt, daß die zuständige deutsche Datenschutzaufsichtsbehörde, d.h. der Berliner Datenschutzbeauftragte oder ein von ihm beauftragter Vertreter, z.B. eine amerikanische Wirtschaftsprüfungsgesellschaft, in seinem Namen Kontrollen vor Ort durchführen (§ 10 II des Vertrages), s. unter www.datenschutz-berlin.de/doc/int/konf/18/bahn_de.htm
247 Entscheidungen Nr.2000/519/EG, Nr. 2000/518/EG, Nr.2002/2/EG, Nr.2003/1731/EG, Nr.2003/EG abrufbar unter http://europa.eu.int/comm/internal_market/privacy/adequacy_de.htm

nach Art. 10 EGV für alle staatlichen Organe. In Zweifelsfällen steht der Rechtsweg zum EuGH mittels eines Vorabentscheidungsverfahrens offen.[248]
Dadurch hat sich die europäische Kommission den Primat für die Außenbeziehung gesichert.[249] Den Verhandlungen der Kommission könnte ein Abkommen der Gemeinschaft mit dem Drittstaat folgen, in welchem sich der Drittstaat zur Sicherung bestimmter Schutzvorkehrungen verpflichtet, die eine positive Beurteilung des Schutzniveaus ermöglichen. Die Kompetenz zum Abschluss eines solchen Übereinkommens liegt insoweit bei der Gemeinschaft. Gemäß der AETR Rechtssprechung des EuGH hat die Gemeinschaft durch den Erlass der DSRL von ihrer inneren Normsetzungsbefugnis i.S.d. Art. 95 EGV Gebrauch gemacht. Damit hindert sie die Mitgliedsstaaten ihrerseits in diesem Bereich auf völkerrechtlicher Ebene mit Drittstaaten einen Vertrag abzuschließen. Als Kompetenzgrundlage ist Art. 25 Abs. 5 DSRL daher rein deklaratorischer Natur.[250] Bedenklich ist hier aber, dass durch einen Akt des Sekundärrechts eine Organkompetenz an die Kommission zugewiesen wird, nämlich die Verhandlungskompetenz für völkerrechtliche Verträge, was die in Art. 300 EGV Abs. 1 festgeschriebenen Zuständigkeitsverteilung zwischen Kommission und Rat aushöhlt.[251]

C. Ein „sicherer Hafen“ für USA-Unternehmen

Schon während der Vorbereitung der DSRL hatten die USA Kritik an der Drittländerregelung geübt. Diese bewirke eine Ausstrahlungswirkung bzw. eine Extraterritorialität der DSRL, welche dem völkerrechtlichen Interventionsverbot zuwiderlaufe. Dieser Streit spitzte sich nach dem Erlass der DSRL zu. Die EG hätte Datenschutz als wirtschaftspolitisches Mittel benutzt. Im Beurteilungsspielraum der Angemessenheitsprüfung würde dazu gerade einladen, jegliche politische Zielsetzungen in die Feststellung der Angemessenheit einfließen zu lassen. Damit könnte der Datenschutz als Druckmittel in Verhandlungen über politische Fragen dienen, obwohl diese in gar keinem sachlichen Zusammenhang zum Regelungszweck der DSRL stehen.[252]
Die Kommission und der Rat spürten von Anfang an, dass jede Bestrebung, die Verwendung personenbezogener Daten weltweit an vorgegebene Voraussetzungen zu knüpfen, auf weltweitem Widerstand stieß. Die Auswahl einer „Angemessenheitsformel“ statt der bis dahin üblichen „Äquivalenzformel“ manifestiert gerade ihre Kompromissbereitschaft zur Milderung einer voraussehbarer Drittländerobstruktion.[253]
Selbst die USA waren bislang als ein Drittland ohne angemessenes Datenschutzniveau eingestuft. Daher verhandelten sie seit 1998 mit der Kommission, um eine positive Feststellung nach Art. 25 Abs. 6 DSRL zu erreichen. Dieser transatlantische Dialog wurde jedoch in einigen Punkten durchaus kontrovers geführt. Dabei stützten sich die verschiedenen Ansätze insbesondere auf die Diskrepanz der jeweiligen Rechtssysteme, welche auf politisch-kulturelle Unterschiede beruhen.[254]
Zum einen betrachtet die amerikanische Grundrechtsdoktrin die Auswirkung von Grundrechten auf privatrechtliche Beziehungen sowie die damit verbundenen staatlichen Schutzpflichten eher mit Zurückhaltung. Gleichzeitig genießt das Kommunikationsgrundrecht i.S.d. *First Amendment* tendenziell auch bei kommerziellen Aktivitäten einen höheren Schutz.

---

248 *Wuermeling, U.*, a.o.O. (Fn. 142), S. 138.
249 *Burkert, H.*, a.o.O. (Fn. 84), Rn. 64.
250 *Stein, T.*, Transnationale Datenübermittlung und die Kompetenz der Europäischen Gemeinschaft zum Abschluß eines internationalen Abkommen zum Datenschutz mit Dritten Staaten, in: Festschrift für Arndt, Heidelberg 2001, S. 527.; *Cremona, M.*, External Relations and Exernal Competence: The Emergence of an Integrated Policy, in: Craig/de Bùrca (Hrsg.), The Evolution of EU Law, Oxford 1999, S. 138-152.
251 *Stein, T.*, a.o.O. (Fn. 250), S. 528.
252 *Wuermeling, U.*, a.o.O. (Fn. 142), S. 211.
253 *Simitis*, Damman/Simitis/Einleitung, Rn. 28.
254 *Klug, C.*, Persönlichkeitsschutz beim Datentransfer in die USA-Die Safe-Harbor-Lösung, RDV 2000, 213; *Burkert, H.*, a.o.O. (Fn. 50), Rn. 87; *Wellberry, B.*, a.o.O. (Fn. 221), S. 169-173; *Schwarz, P.*, Die neuesten Entwicklungen im amerikanischen Datenschutz, RDV 1989, 153ff; *ders.* The Computer in German and American Constitutional Law: towards an american right of informational self-determination, American Journal comparative Law 1989, 676-686; *Walz, S.*, Buchbesprechungen (zu Schwarz/Reidenberg, Data Privacy Law), DuD 1998, 180-181.; *Baldassarre, A.*, Privacy e Costituzione, a.o.O. (Fn. 64) insb. S. 322-353.

Zweitens ist das zum *common law* gehörende amerikanische Recht größtenteils durch Fallrecht und eher äußerst detailliert verfassten Gesetzesregelungen geprägt, welche sich eher an einer den Einzelfall lösenden Formulierung orientieren. Hierin liegt der wesentliche Unterschied zu dem Kodifikationsgedanken der kontinentaleuropäischen *civil law*. In den Vereinigten Staaten wurde 1974 der *Privacy Act* verabschidet, welcher jedoch ausschließlich für den öffentlichen Bereich gilt. Für die Privatwirtschaft gilt stattdessen eine Reihe spezialgesetzlicher Regelungen, die sowohl vom *federal Congress* als auch von den Einzelstaaten erlassen wurden. Darüber hinaus haben Unternehmen sogn. p*rivacy codes* vereinbart, wobei häufig die OECD-Richtlinien als Grundlage für die Selbstregulierung herangezogen werden. Dieser *bottom-up* Ansatz steht im Gegensatz zum europäischen *top-down* Ansatz einer gesetzlichen Regelung.[255]
Dieser Systemunterschiedlichkeit entsprechend lehnten die USA die Schaffung eines allgemeinen Datenschutzgesetzes ab und schlugen als Äquivalent den als Selbstregulierungsinstrument konzipierten „Safe Harbor" vor. Dabei handelt es sich um sieben *Principles*, welche durch 15 *FAQs*[256] ergänzt werden, auf deren Einhaltung sich US-Unternehmen freiwillig verpflichten sollen, falls sie personenbezogenen Daten aus der EU bekommen und verarbeiten.
Es wird davon ausgegangen, dass die Unternehmen, welche sich an die vom „safe Harbor" verlangten Vorgaben halten, über ein angemessenes Datenschutzniveau i.S.d. Art. 25 DSRL verfügen. Eines dieser Kriterien ist z.B. dass im Fall einer erbetenen Einwilligung nicht die bisher üblichen *opt-out* Klauseln sondern *opt-in* Klauseln zu verwenden sind, so dass eine Untätigkeit nicht wie bisher einer informierten Einwilligung gleichkommt. Des weiteren ist die Errichtung einer unabhängigen Stelle zur Gewährleistung eines schnellen Beschwerdeverfahrens zu nennen. Hierdurch sollen Streitfragen gelöst und Schadenersatzverpflichtungen ausgesprochen werden. Ferner hat eine weitere unabhängige Instanz zu prüfen, ob jeweiligen Unternehmen die sich aus dem „safe Harbor" Programm ergebenden Verpflichtungen auch einhalten.[257]
Obwohl das Europäische Parlament anregte, dass die Kommission ihre Genehmigung des „safe Harbor" Systems von der Funktionsfähigkeit aller seiner Bestandteile und von der Bekräftigung dieser Funktionsfähigkeit durch die US-Behörde abhängig macht und obwohl die Art. 29-Gruppe auch eine kritische Stellungnahme zum „safe Harbor"-Entwurf veröffentlicht, u.a. hinsichtlich des Auskunftsrechts der Betroffenen und der Durchsetzung der sieben allgemeinen Prinzipien (s.o.), traf die Kommission trotzdem eine Entscheidung nach Art. 25 Abs. 6 DSRL.[258]

D. Der Fall: die Übermittlung von Fluggastdatensätzen an die USA

I. Die Zesur des 11. 9. 2001

Die Ereignisse des 11.9.2001 deuten auf einen Wendepunkt in der jüngsten Geschichte. Dass die breite Öffentlichkeit diese durch ein bloßes Datum bezeichnete spiegelt in bemerkenswerter Weise ihre sprachliche Unfassbarkeit wieder.[259]
Für den Datenschutz ist vor allem die innenpolitische Reaktion in den USA von Bedeutung[260], welche aufgrund des außenpolitischen Gewichts der Vereinigten Staaten eine erhebliche Ausstrahlungswirkung

---

255 *Wellberry, B.*, a.o.O. (Fn. 221), S. 169.
256 Frequently Asked Questions.
257 vgl. *Dammann*, Safe Harbor-neue Elemente im internationalen Datenschutz, in: Simon/Weiß (Hrsg.), „Zur Autonomie des Individuums" Liber Amicorum Spiros Simitis, Baden Baden 2000, S. 22.
258 Entscheidung 2000/520/EG, Abl. 2000 L 215/7.
259 Derrida, hält dass die Ereignisse des 11.09.04 sind wohl im Heideggers Sinne zu verstehen als ein *Ereignis*, welcher zugleich Gegenstand einer Ein-eignung bzw. einer Ent-eignung ist. Das Konzept bleibt auf den ersten Eindruck unbegreiflich: „Le télégramme d'une métonymie- un nom, un chiffre-accuse l'inqualifiable en reconnaissant qu'on ne reconnassaît pas: on ne connaît même pas, on ne sais plus encore qualifier, on ne sais pas de quoi on parle, " in: Derrida/Habermas, *Le Concept du 11 septembre*, Paris 2004, S. 134-135.
260 Vgl. *Lanchester, F.*, Gli Stati Uniti e l'11 settembre 2001, unter: http://associazionedeicostituzionalisti.it/dibattiti/vicendeinternazionali/lanchester.htm; *ders.* La Corte Suprema e

entfalten.[261] So wurde dem Präsident die umfangreichsten Befugnisse seit der Bürgerkriegzeit zugeteilt.[262]
Wie oben dargestellt war bis dahin das Anliegen des Datentransfers zwischen der EU und den USA eher wirtschaftspolitischer Natur. Nun hat sich der Schwerpunkt jedoch verstärkt auf Sicherheitsinteressen verlagert.

II. Zugriff der USA auf PNR und Handlungen der Kommission

Als Reaktion auf die Ereignisse des 11. September 2001 erließen die Vereinigten Staaten ihrem Selbstverständnis folgend,[263] Rechtsvorschriften, welche Fluggesellschaften in ihrem Hoheitsgebiet dazu verpflichten, den US-Behörden personenbezogene Daten über einreisende oder ausreisende Fluggäste und Besatzungsmitglieder zu übermitteln.[264] Insbesondere müssen die Fluggesellschaften dem US Bureau of Customs and Border Protection (US CBS) bei Flügen in oder durch die USA elektronischen Zugang zu den im sogenannten Passenger Name Record (PNR) enthaltenen Fluggastdaten verschaffen. Für diejenigen Fluggesellschaften, welche diesen Forderungen nicht nachkommen, drohen hohe Geldstrafen oder sogar der Entzug der Landerechte, und deren Passagiere müssen mit Verspätungen bei der Ankunft in den USA rechnen.[265] Die US-Regierung hat das Inkrafttreten der neuen Vorschriften verschoben, sich letztendlich aber geweigert, die Verhängung von Strafen gegen Fluggesellschaften über den 5. März 2004 hinaus auszusetzen. Daher sind Fluggastdatensätzen mehrerer großer europäischer Fluggesellschaften seitdem den amerikanischen Behörden zugänglich.[266]
Das europäische Parlament hat in zwei Entschließungen[267] die Kommission gebeten, Maßnahmen im Hinblick auf die Übermittlung von PNR-Daten an die USA zu ergreifen und dabei der europäischen Bedenken Rechnung zu tragen. Mangels der Gewährleistung eines befriedigenden Datenschutzstandards durch die USA lag es für die europäische Kommission nahe, die Gespräche mit den USA vorläufig zu beenden und ein Einschreiten gegen den fortdauernden Datentransfer anzudrohen. Allerdings wollte es die Kommission zu keiner „Machtprobe" kommen lassen.[268] In einer im Dezember 2003 erlassenen Mitteilung bestand sie darauf, ein „sektorübergreifendes EU-Datenschutzkonzept" zu entwickeln, wobei sich eine Konkordanz mehrerer Interessen ergeben soll: Die Bekämpfung von Terrorismus, der Grenzschutz, das Datenschutzrecht, „die generellen Beziehungen zwischen der EU und den USA", aber auch die Sicherheit und der Komfort von Fluggästen sowie die Notwendigkeit für die Fluggesellschaften, Rechtsvorschriften zu annehmbaren Kosten einzuhalten. Nicht vergessen ist ebenso, dass diese Themen einen „weltweiten" Umfang haben, so dass sie in einem möglichst breiten internationalen Rahmen eine Lösung finden müssen.

---

l'emergenza, unter: http://www.associazionedeicostituzionalisti.it/dibattiti/vicendeinternazionali/lanchester_20040906.html ; *Band/Kennedy*, The USA-Patriot Act, Cri 2002.

261 *Kovaks, C.,* US-European Relations from the Twentieth to the Twenty-first Century, European Foreign Affairs Review 2003, S. 448-451; *Croci, O.,* A closer Look at the changing of Transatlantic Relationship, European Foreign Affairs Review 2003, S. 469-471. Für Deutschland s. *Rublak,* Terrosirmusbekämpfungsgesetz: neue Befugnisse für die Sicherheitsbehörden, DuD 2002, 202ff, sowie *Pernice I.M.*, Die Telekommunikations-Uberwachungsverordnung (TKÜV), DuD 2002, S. 207ff.

262 *Lanchester, F.,* a.o.O. (Fn. 260) ; *Kovaks, C.,* a.o.O. (Fn. 260), S. 448.

263 Derrida, a.o.O. (Fn. 259), S. 146: „Il reste que les Etas-Unis ont le pouvoir d'accréditer auprès du monde une autoprèsentation: ils reprèsent l'ultime unité présumée de la force et du droit, de la plus grand force et du discours du droit".

264 Title 49, United State Code, section 44909(c)(8); Title 19, Code of Federal Regulations, section 122.49b; Vgl. KOM (2003) 826, endg., S.3; Art. 29-Gruppe, WP 87, S. 2 abrufbar unter http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_de.pdf

265 Von dem bevorstehenden sog. Computer Assisted Passenger Pre-Screening System (CAPPS II) ist hier nicht die Rede. Dieses System sammelt Datenbestände von privaten Unternehmen, um sie zu vergleichen. Am Ende des Prüfungsprozeßes entsteht eine Risikoprognose für den betreffenden Passagier. Ihm wird entweder grünes, oranges oder rotes Licht erteilt. Je nachdem, was für Licht angezeigt wird, darf der Passagier das Flugzeug betreten oder nicht. Vgl. *Schröder, C.,* a.o.O. (Fn. 1), S. 289.

266 Z.B. Lufthansa, nicht aber Austrian Airlines und Alitalia, vgl. *Schröder, C.,* a.o.O. (Fn. 1), S. 287.

267 P5_TA(2003)0097 vom März 2003; P5_TA(2003)0429 vom Oktober 2003

268 Vgl. KOM (2003) 826, endg., S.6.

Hauptkomponenten eines solchen sektorübergreifenden Datenschutzkonzeptes der Kommission sind: Erstens, die Schaffung eines Rechtsrahmens für bestehende PNR-Übermittlungen an die USA, der die Form einer Entscheidung gemäß Art.25 Abs. 6 DSRL zusammen mit einem „einfachen" bilateralen Abkommen zwischen der EU und den USA erhalten soll; zweitens, eine vollständige, genaue und rechtzeitige Unterrichtung der Passagiere; drittens, die *Pull*-Übermittlungsmethode (Verfahren, bei dem die US-Behörden direkten Zugang zu den Datenbanken der Fluggesellschaften haben) soll durch eine *Push*-Übermittlungsmethode (Verfahren, bei dem die Fluggesellschaften die Daten auswählen und an die US-Behörden übermitteln) ersetzt werden; viertens, eine spezifische und einheitliche EU-Position zur Verwendung von Passagierdaten zum Zwecke der Flugsicherheit und des Grenzschutzes zu entwickeln und einen multilateralen Rahmen für die Übermittlung von PNR-Daten innerhalb der ICAO zu schaffen.[269]
Diesen Prämissen folgend haben im Mai 2004 zum einem die Kommission eine Angemessenheitsentscheidung i.S.d. Art. 25 Abs. 6 getroffen[270] und zum anderem der Ministerrat den Abschluss eines bilateralen Abkommens beschlossen.[271] Die inhaltliche Ausgestaltung beider Akte blieb jedoch nicht ohne Beanstandung seitens anderer europäischer Organe, insbesondere des Europäischen Parlaments, dessen Kritik nachfolgend skizziert wird.

III. Bedenken hinsichtlich des Gemeinschaftsrechts

Grundlage der Angemessenheitsentscheidung sowie des bilateralen Abkommens ist eine trotz jüngster Veröffentlichung im *Federal Register*[272] an sich nicht bindende Verpflichtungserklärung des *Department of Homeland Security (DHS), Custom Border Protection (CBP).* Dass beide auf diese Verpflichtungserklärung verweisenden Rechtsakte (die Entscheidung der Kommission sowie das Abkommen) gegen die grundrechtskonform ausgelegte DSRL sowie das Primärrecht verstoßen könnten, behaupten sowohl das Europäische Parlament[273] als auch der Art. 29-Arbeitsgruppe.[274]
In der Tat hat die Kommission in ihrer Verhandlungen mit dem *DHS* einige der geäußerten Bedenken berücksichtigt, beispielsweise in Bezug auf die sog. sensiblen Daten sowie die Geltendmachung der Rechte der Betroffenen und die Dauer der Speicherung. Die Relevanz sensibler Daten (Art. 8 DSRL) in diesem Bereich lässt sich dadurch zeigen, dass dazu u.a. Gesundheitsdaten, Daten über die Essensauswahl (Koscher oder Hindu), oder Daten, welche Rückschlüsse auf die Religionszugehörigkeit erlauben (etwa wie „*pilgrim fare*", „*missionary*", „*clergy*") gehören. Das *CBP* hat sich verpflichtet, solche Daten nicht zu verwenden und entsprechende Filtersysteme einzuführen. Was die Rechte der Betroffenen (Artt. 10 bis 12 DSRL) anbelangt, sollen künftig die im amerikanischen Informationsfreiheitsgesetz (*FOIA*: *Freedom of Information Act*) enthaltenen Informations- und Auskunftsansprüche unabhängig von der Staatsangehörigkeit bzw. des dauerhaften Wohnsitzes zur Geltung kommen. Bezüglich der Speicherungsdauer wurde die ursprüngliche 50 Jahre Frist (!) auf 3,5 Jahren reduziert, obwohl eine Verlängerung bis zu 8 Jahre möglich sein soll, was wiederum über der Erforderlichkeitsvoraussetzung i.S.d. Art. 6 Abs. 1 d) und e) hinausgehen kann.

1) Grundrechtskonform ausgelegte DSRL

Allerdings erscheint die Angemessenheitsentscheidung der Kommission den bisherigen Schutzstandard der DSRL immer noch zu unterminieren. Sieht man die Entscheidung der Kommission als Durchfüh-

269 KOM (2003) 826, endg., S.4-5.
270 K (2004) 1924, Abl. 2004 L 235/11
271 Abl. 2004 L 183/83
272 Die Veröffentlichung erfolgte am 9 July 2004, s. Federal Register/Vol. 69, No. 131/Friday, July 9, 2004/ Notices.
273 B5-0156/2004, European Parliament resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) tranferred to the US Bureau of Customs and Border Protection
274 Art.29-Gruppe, WP 87, SS.7-14, abrufbar unter
http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_de.pdf; *Schröder, C.*, a.o.O. (Fn. 1), S. 287-288.

rungsakt der DSRL an, muss sie die in der DSRL festgelegten Maßstäbe einhalten. Auch müssen die einschlägigen Normen der DSRL (Art. 25 Abs. 1 und 2) grundrechtskonform ausgelegt werden,[275] so dass ein Verstoß der Entscheidung gegen das Grundrecht auf den Schutz der Privatsphäre mittelbar gegeben sein kann. Kommt Art. 8 EMRK und die einschlägige Rechtssprechung des EuGHs in Betracht, dann könnte die Einschränkung des Rechts der Betroffenen über das hinausgehen, was in einer „demokratischen Gesellschaft" notwendig ist. In diesem Zusammenhang wird auf folgende Gesichtspunkte hingewiesen.

Zum ersten könnte die systematische Übermittlung personenbezogener Daten an US-Behörden der Anforderung der Zweckbestimmung (Art. 25 Abs. 2) nicht nachkommen. Zweck der Erhebung ist es nämlich, den Luftfahrttransport operationell zu erleichtern, und nicht Informationen an Behörden der Gefahrenabwehr und Strafverfolgung weiterzuleiten.

Zum zweiten ist die vorgesehene Weiterübermittlung durch das *CBP* an andere- auch ausländische staatliche Behörde bedenklich. Zwar soll die Übermittlung auf Zwecke der Terrorismusbekämpfung und Strafverfolgung begrenzt sein, dem *CBP* werden aber erhebliche Entscheidungsbefugnisse eingeräumt. Diese Behörde wird bei jeglicher Weitergabe als „Eigentümer" der Daten betrachtet, der „im Rahmen seines Ermessens" die Übermittlung personenbezogener Daten an andere staatliche Stellen genehmigt. Als Garantie gegen den Missbrauch dieser Befugnis wird lediglich vorgesehen, dass das CBP „*judiciously*" handeln soll (§§ 28-32 der Verpflichtungserklärung).

Drittens ist es fraglich, inwiefern der Kontrollmechanismus den Anforderungen der Unabhängigkeit bzw. Effektivität der Kontrollinstanzen entspricht (Art. 25 Abs. 2 HS 2 DSRL). Als Kontrollstellen werden nämlich nur das *CBP* selbst und das *DHS Privacy Office* bezeichnet. Letzteres vertritt zwar ein Beamter des *DHS*, dieser ist vom *DHS* jedoch in organisatorischer Hinsicht autonom. An ihm können direkt sowie durch die mitgliedstaatlichen Datenschutzbehörden Beschwerden Einzelner eingereicht werden. Als Sanktion ist allerdings lediglich eine Mitteilung der von Fall zu Fall getroffenen Schlussfolgerungen vorgesehen. Keine bemerkenswerte abschreckende Wirkung mag der jährlichen Bericht an den (amerikanischen) Kongress entwickeln. Die Beteiligung europäischer Organe an der Kontrolltätigkeit erfolgt stattdessen nur mittelbar. Mindestens einmal im Jahr wird die Umsetzung der Verpflichtungserklärung von dem *CBP* und *DHS* zusammen mit der europäischen Kommission und gegebenenfalls mitgliedstaatlichen Behörden überprüft (§ 42). Ferner ermöglicht es Art. 3 der Angemessenheitsentscheidung in besonderen, restriktiv formulierten Tatbeständen den zuständigen staatlichen Instanzen, die Datenübermittlung an das *CBP* auszusetzen.

2) Kompetenz

Schließlich könnte gerade die Kompetenz der Kommission zum Erlass einer Entscheidung gemäß Art. 25 Abs. 6 in diesem Fall problematisch sein. Dabei handelt sich um die Weiterleitung personenbezogener Daten zum Zweck der Strafverfolgung bzw. der Ausübung von Exekutivbefugnissen zum Schutz der öffentlichen Sicherheit und Ordnung. Bei diesem Datenzugriff liegt das Besondere lediglich darin, dass es sich um einen außereuropäischen Hoheitsakt handelt.[276] Ein Drittstaat verfügt über Datenbestände von europäischen Privatunternehmen, die somit „quasi zu ihrem verlängerten Arm" werden. Im Ergebnis ist hierbei das Politikfeld der internationalen Zusammenarbeit bei Verbrechensbekämpfung, also ein Bereich außerhalb des Gemeinschaftsrechts, berührt. Außerhalb des Gemeinschaftsrechts ist jedoch eine Ausübung der in Art. 25 Abs. 6 DSRL gewährten Kompetenz nicht gestattet (Art. 3 Abs. 2 DSRL).

Nicht anderes gilt für die Vertretungsbefugnis zum Abschluss eines bilateralen bzw. multilateralen Abkommens (Art. 300 Abs. 1 EGV). Die Zusammenarbeit zur Verbrechensbekämpfung gehört bisher zur sog. dritten Säule der Union, so dass man sich nicht auf Art. 300 EGV, sondern auf Art. 38 EUV berufen müsste.

---

[275] Anders als Schröder und der EuGH prüfen wir die Übermittlung von PNR zu CBS allein am Maßstab des Art. 25 DSRL, welche als *lex specialis* für die Übermittlung personenbezogener Daten ins Ausland anzusehen sind.

[276] *Schröder, C.*, a.o.O. (Fn. 1), S. 288.

3) „Legaler Rahmen“

Genügt Art. 25 Abs. 6 DSRL als Rechtsgrundlage nicht, bewahrheitet sich die Kritik des Europäischen Parlaments. Hiernach soll die Überprüfung der Entscheidung an europäischen Grundrechten durch den üblichen Verweis an Art. 8 EMRK nicht nur hinsichtlich der üblichen Verhältnismäßigkeit erfolgen („Notwendig[keit] …in einer demokratischen Gesellschaft“), sondern auch hinsichtlich des Gesetzesvorbehalts, denn es könnte am „vorsehbaren“ Gesetz i.S.d. EMRK fehlen.[277]
Art und Maß der Grundrechtsbeschränkung werden lediglich durch die Verpflichtungserklärungen bestimmt, welche erst auf eine spätere Rechtssetzung deutet, diese aber noch nicht selbst enthält. Damit fehlt ihr aber gerade die Qualität einer Rechtsnorm.
Innerhalb der Systematik der Europäischen Rechtsordnung erscheint dieser Bezug zum Gesetzesvorbehalt von großer Interesse, gerade weil die im nationalen Verfassungsrecht typische Garantie des Gesetzesvorbehalts kein direktes Parallel im Europarecht findet (nicht von ungefähr prüft der EuGH die europäische Grundrechte nicht am Maßstab des Gesetzesvorbehalt), was sich voraussichtlich erst nach dem Inkrafttreten der europäischen Verfassung (Art. I-32 Abs. 1 UAbs. 1; Art. I-33 i.V.m. Art. II-52 Abs.1 VE) ändern wird.
In diesem Kontext lässt sich nachvollziehen, dass der Beschluss des Ministerrates über den Abschluss eines völkerrechtlichen Vertrages zwischen der EG und den Vereinigten Staaten über die Übermittlung von PNR, gefasst wurde, um einen „legalen Rahmen“ zu schaffen.[278]
Dafür verweist dieser Beschluss aber gerade auf den Inhalt der Angemessenheitsentscheidung, („*Air carriers (..) shall process PNR data (..) strictly in accordance with the Decision*“), was die vorgetragenen Bedenken nicht ausgeräumt hat, denn durch diesen Verweis hat das Abkommen die Verpflichtungserklärung lediglich mittelbar inkorporiert, welche nach wie vor der alleinige substantielle Maßstab einer Grundrechtsbeschränkung darstellt.
Seiner Einschätzung folgend hat das Europäische Parlament erstmals ein Gutachtenverfahren nach Art. 300 Abs. 6 EGV eingeleiten, um den EuGH mit der Frage zu befassen, inwiefern das bevorstehenden Abkommens mit Primärrecht in Einklang zu bringen ist. Unter anderem wurde der EuGH auch darüber unterrichtet, ob das internationale Abkommen nicht dem Parlament zur Zustimmung hätte vorgelegt werden müssen, da Normen der DSRL betroffen waren.[279] Mittlerweile ist das Gutachtenverfahren jedoch gegenstandslos geworden, da das Abkommen bereits vom Rat beschlossen wurde. Somit hat im Juni 2004 der damalige Präsident des Europäischen Parlaments nach Empfehlung der *Legal committee* und der *Conference of Presidents* entschlossen, eine Nichtigkeitsklage sowohl gegen das Abkommens als auch gegen die Entscheidung zu erheben. In seinem Brief an den EuGH finden sich folgende Worte: „*While naturally accepting that the US Administration is perfectly free to exercise its sovereign right to protect its own homeland both the EU and the US must guard against a new form of creeping extraterritoriality. (..) This decision reflects (..) the need to defend European citizens' fundamental rights and freedoms.*[280]“

Teil 4 : Schengen, Europol und unionsinterne Datenverarbeitungen (Von der DSRL nicht erfaßt)

Nach Art. 3 Abs. 2 1. Spiegelstrich DSRL ist die Anwendung der DSRL auf Datenverarbeitungen, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, ausgeschlossen. Als Beispiel werden Tätigkeiten gemäß dem Titel VI EUV genannt. 1995 handelte es sich dabei um die polizeiliche und justizielle Zusammenarbeit in Strafsachen. Des weiteren wird eine Anwendung für Verarbeitungen

---

277 Als solches genügt auch eine von der Exekutiven verfassten Rechtsnormen welche für den Normadressaten „vorseherbar“ i.S.d. Bestimmtheitsgebotes sein muss.
278 Abl. 2004 L 183/83.
279 Vgl. Pressemitteilung der Kommission unter
http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/650&format=HTML&
280 Vgl. www.statewatch.org/news/2004/jun/21-ep-court-pnr.htm

ausgeschlossen, welche die „öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich“ betreffen. Letztere Regelung hat zur Folge, dass sich im Falle einer Ausweitung des Anwendungsbereichs des Gemeinschaftsrechts der Anwendungsbereich der Richtlinie sich nicht automatisch darauf erstreckt, sondern die aufgelisteten Gebiete ausgeklammert bleiben.[281]
Ebensowenig ist die DSRL auf den internen, durch europäische Organe bzw. Einrichtungen erfolgten Umgang mit personenbezogenen Angaben anwendbar. Die Regelungsbestrebungen der DSRL beziehen sich lediglich auf Verarbeitungsabläufe in den Mitgliedsstaaten, die die Richtlinie umzusetzen haben.
Nicht von ungefähr hatte die Kommission schon 1990 neben dem Vorschlag zur DSRL weitere ergänzende Vorschläge veröffentlicht. Einer davon zielte auf einen Beschluss über die Geltung der DSRL im gesamten öffentlichen Bereich der Mitgliedsstaaten ab.[282] Eine zusätzliche Verpflichtung der Mitgliedsstaaten, die Umsetzung der Richtlinie im gesamten öffentlichen Bereich zu vollziehen, hätte das Problem der beschränkten Richtlinienkompetenz der EU lösen können. Der Rat lehnte diesen Vorschlag jedoch ab.[283]
Eine weitere Initiative betraf die Anwendung der Richtlinie auf die Institutionen der Europäischen Union als solche.[284] Dieser Weg wurde erst nach Verabschiedung der DSRL konsequent eingeschlagen. Beide Aspekte weisen Besonderheiten auf, auf welche näher eingegangen wird..

A. Polizeiliche und Justizielle Zusammenarbeit

Dass es im Bereich der sog. dritten Säule der EU an Transparenz und demokratischer Legitimation fehlt, ist wohl bekannt. Die äußerst geringe Einwirkungsmöglichkeit des Europäischen Parlaments, sowie die begrenzte Zuständigkeit des EuGH rufen Bedenken bezüglich der Verwirklichung der Demokratie- und Rechtsstaatsprinzipien hervor.
Die im Bereich der polizeilichen und justiziellen Zusammenarbeit durchgeführten Datenverarbeitungen stellen schon potentielle Eingriffe in das Recht auf informationelle Selbstbestimmung der Einzelnen dar.[285] Die Gegenmeinung, dass die Zusammenarbeit in der PJZS als internationale Kooperation keine „Durchgriffswirkung“ entfaltet, erklärt bzw. rechtfertigt den Umstand, dass der Rechtsweg zum EuGH in der dritten Säule nicht für jeden eröffnet ist, der eine Verletzung seiner Rechte aufgrund einer Handlung eines „europäischen Organs“ geltend macht.[286] Ein Verzicht auf effektive Grundrechtsbindung und gerichtliche Kontrolle droht hier zum „Skandal ersten Ranges“ zu werden.[287] Daher ist, von dem Inkrafttreten einer europäischen Verfassung abgesehen, eine schnellstmögliche bindende Grundrechte-Charta äußerst wünschenswert.
Inzwischen müssen gemäß Art. 6 Abs. 2 EUV die EMRK (Art. 8 und 13), sowie die durch die Verfassungsüberlieferungen der Mitgliedstaaten entwickelten Grundrechte als Maßstab gelten.
Bei Schengen und Europol erscheinen datenschutzrechtliche Fragen besonders wichtig zu sein. Darüber hinaus hat das vom 11.9.2001 veranlasste *political impetus*[288] im Bereich der polizeilichen und justiziellen Kooperation zum Erlass neuer Maßnahmen geführt (europäischer Haftbefehl,[289] Abkommen zwischen EU und USA über Auslieferung sowie über Rechtshilfe in Strafsachen,[290]

---

281 Simitis-Dammann, DSRL-*Dammann*, Art. 3, Rn. 6.
282 KOM (90) 314, endg.
283 Vgl. *Wuermeling, U.*, a.o.O. (Fn. 142), S. 19.
284 KOM (90) 314, endg.
285 *Baldus, M.*, Transnationales Polizeirecht, Baden- Baden 2001, S. 258, 261.
286 *Gleß/Zeitler*, Die Europäische Union, in: Gleß/Grote/Heine (Hrsg.), Justizielle Einbindung und Kontrolle von Europol, Bd.1, Freiburg in Bresgau, 2001, S. 618.
287 *Pernice, I.*, Eine Grundrechte-Charta für die Europäische Union, DVBl. 2000, S. 855.
288 *Mitsilegas, V.*, The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data, European Foreign Affairs Review 2003, 516.; *Gilmore,B.*, The Twin Towers and the Third Pillar, Some Secutity Agenda Developments, WP 2003/7 EUI, abrufbar unter http://webdb.iue.it/FMPro , S. 2-4.
289 Abl. 2002 L 190/1
290 Abl. 2003 L 181/25-27ff.-34ff.

Abkommen zwischen Europol und den USA über die Übermittlung personenbezogener Daten[291]), welche datenschutzrechtlich nicht unproblematisch sind.

I. Rechtsakte, Ziele und Aufgaben

1) Schengen

Die zur Abschaffung der Grenzkontrollen abgeschlossenen Schengen-Abkommen[292] sind multilateral zustande gekommene völkerrechtliche Verträge und funktionelles Nebensrecht zum Unionsrecht (vgl. Art. 140, 134, 142 SDÜ).[293]
Datenschutzrechtliche Relevanz haben unter den sog. Ausgleichsmaßnahmen sowohl die Vorschriften über eine stärkere Zusammenarbeit im Binnengrenzgebiet (Art. 39-47 SDÜ) als auch das Schengener Informationssystem (SIS; Art. 92-119 SDÜ). Kernstück des SIS ist die Vernetzung der polizeilichen Datenbanken der Schengen-Mitgliedsstaaten. Hierfür wurde in Straßburg ein Zentralrechner und in allen Mitgliedsstaaten ein nationaler Zentralrechner mit identischem Datensatz installiert.
Durch ein Protokoll zum Amsterdamer Vertrag wurde die Einbeziehung des sog. Schengen-Besitzstandes in den rechtlichen Rahmen der EU vorgesehen. Praktisch sollte die Einbeziehung durch einen Beschluss des Rates erfolgen, der über die Zuordnung der jeweiligen Bestimmungen des Schengen-Besitzstandes unter den passenden Rechtsgrundlagen im Titel IV EGV bzw. Titel VI EUV entscheiden sollte (Art. 2 Abs. 2 Protokoll). Der Rat hat zwar zwei Beschlüsse erlassen,[294] eine Zuordnung der Vorschriften über das SIS unterblieb jedoch bisher, so dass die Auffangnorm zur Anwendung kam, nach der die nicht zugeordneten Bestimmungen unter den EUV fallen sollten (Art. 2 Abs. 1 Protokoll).[295]
Diese Aufspaltung zwischen dem EGV und dem EUV und die damit verbundenen unterschiedlichen Handlungsmöglichkeiten und Justiziabilitätsvoraussetzungen wurden als zunehmende Komplexität des Schengen-Rechts einstimmig kritisiert.[296]In Bezug auf die Datenschutzrelevanten Vorschriften wäre deren gesamte Zuordnung unter dem EGV wünschenswert gewesen. Als Rechtsgrundlage stünden Art.95 sowie Art.286 EGV zur Verfügung,[297] doch werden die meisten Normen gem. Art. 2 Abs.1 Protokoll, mit Ausnahme der Art. 126 Nr. 3 und Art. 127, dem EUV zugeordnet.
Innerhalb des Jahres 2006 soll die Inbetriebnahme eines SIS zweiter Generation (SIS II) realisiert werden. Sowohl technische Anforderungen als auch der Beitritt neuer Staaten werden als Grund für den Aufbau des SIS II genannt.[298] Künftig wird der Zugang zu den Datenbeständen des SIS II sowohl Europol als auch Eurojust erlaubt sein.[299]

---

291 Doc. 13689/02 Europol 82, 4 Nov. 2002.
292 BGBl. 1993 II, 1013.
293 *Di Fabio, U.*, Die „Dritte Säule" der Union, DÖV 1997, S. 92.
294 Abl. 1999 L 176/1, 17.
295 Vgl. *Thym, D.*, The Schengen Law: a Challenge for Legal Accountability in the European Union, ELJ 2002, 227, 241; *Pallaro, P.*, Libertà della persona e trattamento dei dati personali nell'Unione Europea, Milano 2002, S. 273.
296 *Labayle, H.*, Un espace de liberté de sécurité et de justice, Revue trimestrale de droit européen 1997, 843; *Kuijper,PJ.*, Some legal problems associated with the communitarization of policy on visas, asylum and immigration under the Amsterdam Treaty and incorporation of the Schengen Acquis, CMLR 2000, 366; *Thym, D.*, a.o.O. (Fn. 295), S. 221; *Monar, J.*, Die Entwicklung des "Raumes der Freiheit der Sicherheit und des Rechts", Perspektiven nach dem Vertrag von Amsterdam und dem Europäischem Rat von Tampere, Integration 2000, 22; *Merli, F.*, Der Raum der Freiheit der Sicherheit und des Rechts und die Osterweiterung der Europäischen Union, eine Einführung, in: Merli (Hrsg.) Der Raum der Freiheit der Sicherheit und des Rechts und die Osterweiterung der Europäischen Union, Dresden 2001, S. 23.
297 *Pallaro, P.*, a.o.O. (Fn. 295), S. 270.
298 *Schengen Joint Supervisory Authority*, Report January 2002-December 2003, S.14. abrufbar unter http://www.garanteprivacy.it
299 Vorschlag des Präsidium, 9408/3/02 vom 6 November 2002; vgl. *Schengen Joint Supervisory Authority*, Report January 2002-December 2003, S.14.

2) Europol

Auch für die Errichtung Europols wurde 1995 der völkerrechtliche Vertrag als Instrument gewählt. Die dazu verwendete Rechtsgrundlage war schon im ursprünglichen EUV (*Art. K.3 a.F. EUV*) enthalten,[300] sodass der Aufbau Europols auf einer „quasi-verfassungsrechtlichen" Grundlage beruht.[301] Allerdings ist Europol keine Institution der EU, sondern eine eigenständige internationale Organisation, deren Ziel die Verbesserung der polizeilichen Zusammenarbeit zwischen den Mitgliedsstaaten ist (Art. 2 Abs. 1 EuropolÜ). Seine Aufgaben sind bisher[302] vor allem auf Informationssammlung und –analyse, sowie auf die Erleichterung des Informationsaustausches zwischen den Mitgliedstaaten (Art. 3 Abs.1 EuropolÜ) beschränkt. Inzwischen wurde der Kompetenzbereich Europols zur Verhütung bzw. Bekämpfung des Terrorismus und des illegalen Drogenhandels ausgeweitet. Zuletzt hat der Rat der Europäischen Union die materiellen Kompetenzen Europols unter dem Eindruck der Terroranschläge vom 11. September 2001 noch einmal mit Wirkung zum 1. Januar 2002 erheblich erweitert,[303] sodass die Behörde nunmehr für „nahezu alle Formen internationaler Kriminalität zuständig ist."[304]

II. Verfassungsrechtlich relevante Datenschutzfragen

1) Gesetzesvorbehalt

Sowohl das SDÜ als auch das EuropolÜ schreiben den jeweiligen Mitgliedstaaten vor, datenschutzrechtliche Maßnahmen zu treffen, die zumindest dem Datenschutzstandard der Konvention des Europarates Nr. 108 entsprechen (Art. 117, 126 SDÜ[305]; Art. 14 EuropolÜ). Damit konnte das SiS in einem Mitgliedsstaat nur nach tatsächlicher Umsetzung der Konvention in betreib genommen werden.
Problematisch bleibt dabei jedoch, dass gerade das SDÜ und das Europol-Abkommen einige zentrale Bestimmungen enthalten, welche aufgrund ihrer weiten Fassung dem Gebot der Bestimmtheit des Gesetzes nicht gerecht werden[306].

a) Schengen

Art. 46 SDÜ erlaubt beispielsweise jeder Vertragspartei einer anderen Vertragspartei Informationen mitzuteilen, die für den Empfänger zur Unterstützung „bei der Bekämpfung zukünftiger Straftaten" von Bedeutung sein können. Hierbei ist das für die traditionelle Amtshilfe erforderliche „Ersuchen im Einzelfall" überflüssig.[307]

---

300 Abl. 1995 C 316/1.

301 *Di Fabio, U.*, a.o.O. (Fn. 293), S. 97.

302 Obwohl Europol durch den Rechtsakt des Rates vom 28.11.2002 die Befugnis erhalten hat, an gemeinsamen Ermittlungsgruppen teilzunehmen, bleibt es Europol verwehrt Zwangsmaßnahme jeglicher Art durchzuführen (Art. 3a), Abl. 2002 C 312/1. In dem Entwurf des Konvents für eine europäische Verfassung sind sog. „operative" Aufgaben für Europol vorgesehen, vgl CONV 850/03, Art. III-177 Abs. 3 VE sowie der Schlußbericht der Gruppe X CONV 426/02, S. 18; zur Ambivalenz des Konzeptes „operative Aufgaben" vgl. *Di Martino, A.,* Schengen, Europol und der Raum der Freiheit, der Sicherheit und des Rechts in der Verfassung der EU, WHP 13/03, S. 21 unter http://www.whi-berlin.de .

303 Abl. 2001 C 362/1.

304 *Ellermann, J.*, Vom Sammler zum Jäger-Europol auf dem Weg zu einem „europäischen FBI"?, Zeus 2002, 564.

305 Mangels einer solchen Regelung konnte bis dem Jahr 1997 das SDÜ in Italien nicht zur Anwendung kommen, vgl. *Galetta, D.U.*, La cooperazione fra le polizie e il SIS, in: Losano (Hrsg.), La legge italiana sulla privacy-Bilancio dei primi cinque anni, Bari 2002, S. 210.

306 Eine Bezugnahme auf den Gesetzesvorbehalt erscheint gerade im Bereich des SDÜ sowie des EuropolÜ angebracht, da innerstaatliche Gesetze zur Ratifizierung beider Abkommen erforderlich waren. Als einschlägiger Prüfungsmaßstab gelten die Anforderungen der EMRK.

307 *Denninger, E.*, Das Recht auf informationelle Selbstbestimmung und innere Sicherheit, in: Schöler (Hrsg.), Informationsgesellschaft oder Überwachungsstaat?, Opladen, 1986, S. 152-153. Nach seiner Auffassung sollte statt der Amtshilfe vielmehr von „Informationshilfe" die Rede sein.; *Lavranos, N.*, Datenschutz in Europa, Am Beispiel der Datenschutzrichtlinie, des SIS und Europol, DuD 1996, 405.

Eine solche zur Bekämpfung aller „künftigen Straftaten“ gestattete Speicherung personenbezogener Daten erscheint recht deutlich im Konflikt mit dem Verhältnismäßigkeitsprinzip zu stehen.[308]
Sollten dem SIS II auch Europol und Eurojust beitreten, wird eine nähere Bestimmung ihrer Aufgaben sowohl vom EP als auch von der gemeinsamen Kontrollinstanz Schengens (GKI) als erforderlich angesehen.[309]
Schwierigkeiten könnten ebenso bei der Datenverantwortlichkeit für die Ausschreibung zur Festnahme von Personen zur Auslieferung entstehen.[310] Nach Art. 64 SDÜ ist eine solche Ausschreibung gem. Art. 95 SDÜ einem Ersuchen um vorläufige Festnahme gleichzusetzen, die nahezu automatisch erfolgen könnte. Dieser Automatismus ist deswegen so bedenklich, weil von der ausschreibenden Justizbehörde zunächst etwas Unmögliches verlangt. Sie hat sich gem. Art. 95 Abs. 2 SDÜ darüber zu vergewissern, ob die Festnahme nach dem Recht aller ersuchten Vertragsparteien zulässig ist. Dies führt *de facto* zur Verlagerung der Verantwortlichkeit auf die nationalen Zentralstellen, die SIRENEN, welche die Daten eingeben. Hierbei geht es vor allem um einen Schutz vor Daten, welche „automatisiert [und] in falschen Händen zu einem gefährlichen Werkzeug gegen den Bürger werden können.“[311]
Konkret hat der Betrieb des SIS in Deutschland zur Eingabe der Daten abgelehnter Asylbewerber, als unerwünschte Personen geführt, was vom französischen *Conseil d'Etat* beanstandet wurde. In dieser von einem französischen Gericht vorgenommenen Rechtsmäßigkeitsüberprüfung einer Handlung deutscher Behörden kann ein Beispiel einer sich im europäischen Verfassungsverbund entwickelnden „horizontalen Dimension“ angesehen werden.[312]
Ferner verweigerten spanische Behörden, aufgrund einer Eintragung im SIS, die Aufenthaltsgenehmigung für aus Drittländer ausreisende Familienangehörigen von Unionsbürgern, was die Kommission dazu veranlasste, ein Vertragsverletzungsverfahren einleiten zu wollen.[313]

b) Europäischer Haftbefehl; Transatlantische Abkommen über Auslieferung und Rechtshilfe

Das Inkrafttreten des Rahmenbeschlusses des Rates über den europäischen Haftbefehl hat die oben erwähnten Bedenken, wie das europäische Parlament betonte,[314] nicht weniger erheblich gemacht. Die jeweilige Justizbehörde kann gesuchte Personen im SIS ausschreiben, wobei auf Art. 95 SDÜ verwiesen wird (Art. 9 Abs. 2 und 3 des Rahmenbeschlusses). Diese werden vom festnehmenden in Gewahrsam genommen und an den ausschreibenden Staat übergeben. Ein sonst übliches Auslieferungsverfahren erübrigt sich damit in diesem Fall.
In transatlantischer Hinsicht kommen die Bestimmungen des gemäß Art. 38 i.V.m. 24 EUV abgeschlossenen Abkommens zwischen EU und USA über die Auslieferung in Betracht.[315]
Ähnliche Einwände lassen sich gegen die breite Formulierung einiger Bestimmungen des Abkommens über Rechtshilfe in Strafsachen[316] zwischen der USA und der EU vorbringen. Die vereinfachte Identifizierung durch Bankangaben sowie die umfangreiche Voraussetzungen der Übermittlungstatbestände

---

308 *Rossi, L.S.,* La protezione dei dati personali negli accordi di Schengen, in: Nascimbene (Hrsg.), Da Schengen a Maastricht, Milano 1995, S. 179; *Missorici, M.,* Banche dati e tutela della riservatezza, Rivista internazionale diritti dell'uomo 1996, 69.

309 Empfehlung des EPs zum SIS II nr. 2003/2180 abrufbar unter http://escher.drt.garanteprivacy.it/garante/doc.jsp?ID=423364; *Schengen Joint Supervisory Authority*, a.o.O. (Fn. 298), S. 23

310 *Schomburg, W.,* Datenschutz im internationalen Rechtshilfeverkehr in Strafsachen, in: Büllesbach (Hrsg.), Datenverkehr ohne Datenschutz?, Köln 1999, S. 144.

311 *Schomburg, W.,* a.o.O. (Fn. 310), S. 145.

312 *Di Martino, A.,* a.o.O. (Fn. 302), S. 29 und 34. Die angesprochene Entscheidungen sind: *Conseil d'Etat*, Urteile vom 9.6.1999, Rs. 190384 (Forabosco) sowie Rs. N. 198344 (Hamssaoui), darüber *Guild, E.*, Moving the borders of Europe, S. 30-31, unter http://www.jur.kun.nl/cmr/articles/oratieEG.pdf

313 Dok. IP/02/940 vom 27.06.02, unter http://www.europa.eu.int/rapid/pressReleasesAction.do?reference=IP/02/940&format=HTML&aged=1&language=EN&guiLanguage=en

314 Empfehlung des EPs zum SIS II nr. 2003/2180 abrufbar unter http://escher.drt.garanteprivacy.it/garante/doc.jsp?ID=423364; zum Grundrechtsschutz in Zusammenhang mit dem europäischen Haftbefehl vgl. *Lugato, M.,* La tutela dei diritti fondamentali rispetto al mandato di arresto europeo, Rivista diritto internazionale 2003, S. 39-42.

315 Abl. 2004 L 181/27.

316 Abl. 2004 L 181/34.

(Art. 4 Abs. 1 a) und Art. 9 Abs. 1 d) und e)) werden nicht nur in der Literatur kritisiert.[317] Vielmehr haben sich sowohl nationale Parlamente als auch das Europäische Parlament Bedenken gegen die Breite der Tatbestände ausgesprochen, doch wurde ihnen mangels Mitwirkungsbefugnis keine Einflussmöglichkeit eingeräumt. Die Unterzeichnung des Abkommens durch den Rat musste als *fait accompli* akzeptiert werden.[318]

c) Europol

Gegen das Gebot der Bestimmtheit des Gesetzes könnten auch einige Bestimmungen des EuropolÜ verstoßen. So erlaubt Art. 8 Abs. 1 Nr. 2 EuropolÜ die Verarbeitung von Daten über Personen, „bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie Straftaten begehen werden", was bedenken hinsichtlich der geforderten Konkretheit der Gefahr hervorruft.[319]

Darüber hinaus wird der tangierte Personenkreis in Art. 10 Abs. 1 S. 1 um potentielle Zeugen und Opfer, um Kontakt und Begleitpersonen, sowie um potentielle Informanten beachtlich ausgedehnt. Aufgrund dieser Unschärfe könnte praktisch jede Person erfaßt werden, sofern Anknüpfungspunkte bestehen, durch die Europol die Befugnis erhält, bei vielfältigen Personengruppen Nachforschungen vorzunehmen und im polizeilichen „Vorfeld" tätig zu werden.[320]

Dass die Unbestimmtheit des Anwendungsbereichs ein wiederkehrendes Thema ist, beweist auch die Diskussion um das gemäß Art.26 EuropolÜ geschlossene Abkommen zwischen Europol und den USA über die Übermittlung personenbezogener Daten.[321] Hierbei fehlt es an einer genauen Beschreibung der übermittlungsfähigen personenbezogenen Daten („any information relating to an identifiable natural person" Art. 2 a), Art. 6), sowie der Empfängerbehörde in den USA („any competent state or local authority" , Art. 7) und des Zieles der Übermittlung („any offence", Art. 7).

Ebenfalls wird den USA erlaubt personenbezogener Daten in unbegrenztem Umfang und kontinuierlich (*onward transmission*) an Drittländer bzw. Einrichtungen weiterzugeben (Art. 7 Abs. 3). Dazu reicht eine allgemeine, im voraus abgegebene Einwilligung des übermittelnden Mitgliedstaates bzw. Europols aus. Da den Mitgliedstaaten und Europol selbst eine *onward transmission* nicht möglich ist, erscheint es fragwürdig, warum ihnen eine solche mittelbare Befugnis, durch Handlungen der USA, verliehen wurde.

Da SIS II auch für Europol zugänglich sein wird, erhält die USA somit über Europol mittelbar auch einen Zugriff zu den im SIS II enthaltenen Informationen, welche z.B. Daten über Ausländer und Asylbewerber umfassen.

2) Rechtsschutz

Gegen rechtswidrige Verarbeitungen bieten beide, das SDÜ und die EuropolÜ, Rechtsschutzmöglichkeiten. Jedoch ist die Effektivität dieses Schutzes unterschiedlich. Bevor die wesentlichen Merkmale jedes Systems näher beschrieben werden, erscheint es von Interesse, einige Gemeinsamkeiten zu betonen.

Erstens sehen beide Abkommen (Art. 111 SDÜ, Art. 19 Abs. 1 EuropolÜ) vor, dass jede Person das Recht hat, eine Klage auf Auskunftserteilung, Berichtigung, Löschung oder Schadensersatz „im Mitgliedsstaat ihrer Wahl" zu erheben.[322] Wenn diese Ansprüche für den Einzelnen auch nicht einfach

---

317 *Mitsilegas, V.*, a.o.O. (Fn. 288), S. 526-532.

318 *Mitsilegas, V.*, a.o.O. (Fn. 288), S. 526.

319 *Weichert, T.*, Europol-Konvention und Datenschutz, DuD 1995, S. 454

320 *Weichert, T.*, Europol-Konvention und Datenschutz, a.o.O. (Fn. 318), S. 454; *Galetta, D.U.*, a.o.O. (Fn. 305), S. 210.

321 *Lavranos, N.*, Europol and the fight against Terrorism, European Foreign Affairs Review 2003, S. 267-269; *Mitsilegas, V.*, a.o.O. (Fn. 288), S. 519-522. Vor dem Abschluß dieses Abkommens hatte die EU ausnahmsweise einzelne Transfers (Art. 2 Abs.2 des Ratesbeschlußes über die Übermittlung personenbezogener Daten zu Drittländer, Abl. 1999 C 88/1) sowie eine *onward transmission* Europols Data zu Drittländer bzw. Einrichtungen erlaubt (Abl. 2002 C 76/1).

322 Im Anwendungsbereich des EuropolÜ könnte aber der Schadensersatzanspruch in dem Mitgliedstaat geltend gemacht werden, wo der Schaden wegen unzulässiger Verarbeitung entstanden ist, sollte die Verantwortlichkeit bei dem Mitgliedstaat und nicht bei Europol liegen (Art. 38 Nr.1 EuropolÜ)

durchsetzten sind, könnte eine solche Möglichkeit des *forum shopping* die Harmonisierung des Datenschutzes in den Mitgliedsstaaten vorantreiben.[323]
Zweitens wurde im Jahr 2000 vom Rat[324] eine unabhängige Datenschutzgeschäftsstelle für die gemeinsamen Kontrollinstanzen eingerichtet, welche mit dem SDÜ und dem EuropolÜ (sowie dem Übereinkommen über den Einsatz der Informationstechnologie im Zollbereich) geschaffen wurde. Diese Stelle nimmt die administrativen Aufgaben des jeweiligen Sekretariats wahr, wodurch die Unabhängigkeit der Kontrollen gestärkt werden sollte.[325] Das SDÜ und das EuropolÜ haben beide eine „Gemeinsame Kontrollinstanz" eingerichtet, welche sich aus „zwei Vertretern der jeweiligen nationalen Kontrollinstanzen" zusammensetzt (Art. 115 SDÜ, Art. 24 EuropolÜ).
Demnach kann hier Ähnliche angemerkt werden wie bei der DSRL: Die Personalunion der auf nationaler und auf europäischer Ebene tätigen Kontrolleure kann eine harmonisierende Funktion der nationalen Datenschutzregelungen entfalten.
Schließlich ist auf die drei Abkommen mit den USA hinzuweisen. Sowohl bei den EU-Abkommen über Auslieferung und über Rechtshilfe als auch bei dem Europol-Abkommen über Datenübermittlungen ist nicht von einer institutionellen Datenverarbeitungskontrolle die Rede. Die derzeit verfügbaren und nicht erwähnten Kontrollen werden für unzureichend gehalten.[326]

a) Schengen

Das SDÜ enthält sowohl allgemeine (Art 126-127 SDÜ) als auch für das SIS spezielle Datenschutzvorschriften (Art. 102-118 SDÜ). Hiernach sind die bekannten Datenschutzgrundsätze einzuhalten. Darüber hinaus haben Betroffene ein Recht auf Auskunft, Berichtigung falscher Daten und Löschung unrechtsmäßig gespeicherter Daten sowie auf Schadensersatz. Diese Ansprüche können in jedem Vertragsstaat vor dem jeweils zuständigen Gericht geltend gemacht werden. Außerdem können sich Betroffene an die Datenschutzkontrollbehörden wenden. Dies entspricht dem Stand der polizeilichen Zusammenarbeit in Europa, deren justizielle Einbindung auf nationaler Ebene erfolgt.[327]
Grundsätzlich sind die nationalen Gerichte berufen, sowohl die Rechtsmäßigkeit der grenzüberschreitenden als auch der innerstaatlichen Polizeitätigkeit zu überprüfen.
Bereits zu Anfang wurde mangels einer supranationalen justiziellen Kontrolle die grenzüberschreitenden Polizeizusammenarbeit negativ beurteilt.[328] In der Zwischenzeit haben die Mitgliedstaaten durch Art. 35 EUV, fakultativ einen Rechtsweg in Form der Nichtigkeitsklage und des Vorabentscheidungsverfahrens zugänglich gemacht. Ein direkter Individualrechtsschutz ist bisher, auch in dem Entwurf für die künftige europäische Verfassung, nur unter engen Voraussetzungen vorgesehen, wobei eine europäische Beschwerde gegen Grundrechtsverletzungen nicht eingeführt wurde.[329]

b) Europol

Ist der Datenschutzstandard für das SDÜ nicht völlig befriedigend, bleibt das EuropolÜ „weit hinter dem SDÜ" zurück.[330] Die Literatur der 90er Jahre war sich darüber relativ einig.[331]

---

323 *Pallaro, P.*, a.o.O. (Fn. 295), S. 290, 342.; *Gleß/Zeitler*, a.o.O. (Fn. 286), S.612.
324 Ratsbeschluß 641/2000/GAI
325 *Thym, D.* a.o.O. (Fn. 295), S. 239.
326 *Lavranos, N.*, Europol and the Fight against Terrorism, a.o.O (Fn. 320), S. 269-270; *Mitsilegas, V.*, a.o.O. (Fn. 288), S. 522, 530.
327 *Gleß/Zeitler*, S. 613; *Ellermann, J.*, a.o.O. (Fn. 304), 572-574.
328 *Gleß/Zeitler*, a.o.O. (Fn. 288), S. 613, Fn. 377.
329 Als Folge einer Abschaffung der Säulenstruktur hat der Verfassungsentwurf die Justiziabilität durch den EuGH uniformiert, so dass spezielle Bestimmungen zum Vorabentscheidungsverfahren wie der bisherige Art. 68 EGV sowie Art. 35 EUV nicht mehr bestehen. Was die individuelle Nichtigkeitsklage betrifft, hat der Europäische Konvent die sog. Pflaumann-Formel teilweise erweitert, indem künftig der Einzelne auch gegen ihn unmittelbar und individuell betreffende „Handlungen" sowie gegen umsetzungsfreie Rechtsakte mit Verordnungscharakter einschreiten darf (Art. III-270 Abs. 4 VE), dazu *Mayer, F.*, Individualrechtsschutz im europäischen Verfassungsrecht, Walter Hallstein Institut für europäisches Verfassungsrecht Paper 9/04, http://www.whi-berlin.de/rechtsschutz.htm , S.7ss (DVBl. 2004, 610ff.).
330 *Weichert, T.*, Europol-Konvention und Datenschutz, a.o.O. (Fn. 318), S. 455.

Erstens richtete sich die Kritik[332] gegen die den Europol-Bediensteten durch das jüngst geänderte Immunitätsprotokoll[333] eingeräumte Immunität. Zweitens wird die Durchsetzung der Betroffenenrechte durch ein unzulängliches Verfahren (Art. 19 EuropolÜ) erschwert, welches neben einem direkten, gegenüber Europol wahrzunehmenden Auskunftsanspruch bezüglich der Speicherung und Verarbeitung der personenbezogenen Europol-Daten, auch ermöglicht eine bloß mittelbare Auskunftserteilung vorzusehen. Darüber hinaus kann Europol die Durchsetzung des Auskunftsanspruchs mit Ausübung eines gerichtlich nicht überprüfbaren Vetorechts hemmen. Lediglich die GKI kann sich mit der Zweidrittelmehrheit ihrer Mitglieder über dieses hinwegsetzten kann.[334]
Die durchaus bekannte Kritik von *Frowein/Kirsch*[335], die gemäß Art. 6 und 13 EMRK eine hinreichende Unabhängigkeit für die in die Verwaltungsstruktur Europols eingebundene GKI verneinte, ist nach Einrichtung der Datenschutz-Geschäftsstelle teilweise entkräftet.
Die Überwachung der Einhaltung nationaler Vorschriften über die Zulässigkeit der Eingabe und des Abrufs personenbezogener Daten liegt grundsätzlich bei den nationalen Gerichten. Diesen verbleibt jedoch aufgrund der Unverletzlichkeit der Archive Europols (Art. 3 Immunitätsprotokoll), der Immunität der Bediensteten außerhalb gemeinsamer Ermittlungsgruppen (Art. 5 Immunitätsprotokoll), sowie der Rechtskraftwirkung einer Entscheidung der GKI nur eine geringfügige Kontrollmöglichkeit.[336]
Was die Zuständigkeit des EuGH betrifft, wurde schon 1996 ein Protokoll über die Auslegung des EuropolÜ beschlossen. Die Unterzeichnung steht allerdings jedem Mitgliedsstaat frei (Art. 2 Abs.1). Hiernach konnte der EuGH nur im Wege eines Vorabentscheidungsverfahrens entscheiden (Art. 1 Abs. 1). Eine weitere Auslegungskompetenz des EuGHs ergibt sich aus den Erklärungen der Mitgliedstaaten zu Art. 40 Abs. 2 EuropolÜ, wonach Mitgliedsstaaten dem EuGH systematisch Streitigkeiten über die Auslegung bzw. die Anwendung der EuropolÜ vorlegen sollten.
Wie beim Schengen-Recht gewährt der EuGH bzw. EuG auch hinsichtlich des EuropolÜ keinen direkten Individualrechtsschutz in Form eines Beschwerdeverfahrens.

3) Parlamentarische Kontrolle

Ähnliche Bemerkungen gelten hier für die paramentarische Kontrolle, der Durchführug des SDÜ und EuropolÜ, wobei aufgrund seiner gegenwärtigen (und möglicherweise auch künftigen) Aufgaben Europols vor allem die Problematik des letzteren thematisiert wird.[337] Um das Demokratiedefizit in der dritten Säule zu überwinden ist eine Verstärkung der parlamentarischen Kontrolle wünschenswert. Diese könnte sowohl auf der Ebene des Europäischen Parlaments, als auch auf der Ebene der nationalen Parlamente erfolgen. Nach Art. 39 EUV steht dem Europäischen Parlament eine Beteiligung in Form der Anhörung zu. Gemäß Abs. 3 kann es Anfragen und Empfehlungen an den Rat richten, was bisher vor allem durch den Ausschuss Bürgerrechte stattfand. Sollte jedoch der Verfassungsentwurf in Kraft treten, werden die Beteiligungsrechte des Parlaments in zweifacher Hinsicht verstärkt. Erstens wird Europol sowohl durch das Europäischen Parlament als auch durch die mitgliedstaatlichen Parlamente überwacht (Art. III-177 Abs. 2 UAbs. 2 VE). Zweitens wird das Mitentscheidungsverfahren zum normalen Rechtssetzungsverfahren der EU.[338]

---

331 *Werner, U.*, Schengen und Europol, CR 1997, S. 36; *Lavranos, N.*, Datenschutz in Europa, a.o.O. (Fn. 307), S. 405.
332 *Hölscheid/Schotten*, Immunität für Europol-Bedienstete, - Normalfall oder Sündefall?, NJW 1999, S. 2854-2855.
333 Abl. 1997 C 221/2. Das Änderungsprotokoll hat die Immunität für Amtshandlungen bei Teilnahme an gemeinsamen Ermittlungsgruppen aufgehoben: Abl. 2002 C 312/1.
334 Vgl. *Weichert, T.*, Europol-Konvention und Datenschutz, a.o.O. (Fn. 318), S. 456.; *Schomburg, W.*, a.o.O. (Fn. 310), S. 151-152.
335 *Frowein/Kirsch*, Der Rechtsschutz gegen Europol, JZ 1998, 594-597.
336 *Frowein/Kirsch*, a.o.O. (Fn. 334), S. 591; *Grote, R.*, Folgerungen für die rechtsstaatliche Einbindung der grenzüberschreitenden Verbrechungsbekämpfung und –aufklärung durch Europol, in: Gleß/Grote/Heine (Hrsg.), Justizielle Einbindung und Kontrolle von Europol, Bd.2, Freiburg in Bresgau, 2001, S. 612.
337 *Baldus, M.*, Europol und Demokratieprinzip, ZRP 1997, S. 288-289; *Petri, T.*, Die Verwirklichung des „Rechtsstaats"prinzip bei Europol, KritV 1998, 451-452.
338 CONV. 850/03, Art. I-33 i.V.m. III-302 VE.

Die Mitwirkungsrechte der nationalen Parlamente sollen ferner durch das Protokoll über die Subsidiarität sowie durch das Protokoll über die Rolle der nationalen Parlamente gesichert werden.
Inzwischen könnte die Kontrollfunktion des Europäischen Parlaments zumindest hinsichtlich des Haushaltes realisiert werden. Dies wäre z.B. der Fall, wenn das Budget des SIS II dem EG-Haushalts zugeschrieben würde.[339]
Was Europol betrifft, sieht Art. 34 EuropolÜ einen jährlichen Bericht des Rates an das Europäische Parlament hinsichtlich der Tätigkeit Europols vor. Für eine gewisse Überwachung auf nationaler Ebene sorgt Art. 43, indem er den Rat verpflichtet, einstimmig Änderungen des Europol-Übereinkommen den Mitgliedstaaten zur Annahme nach den jeweiligen verfassungsrechtlichen Vorschriften vorzuschlagen. Dies bedeutet ein Ratifikationserfordernis durch die nationalstaatlichen Parlamente, was das Europäische Parlament als allzu langwierig gehalten hat.[340] Daher hat es für die Ersetzung des EuropolÜ durch einen Beschluß i.S.d. Art. 34 Abs. 2 c) EUV plädiert. In einem solchen Fall könnte das Europäische Parlament bei einer Verletzung seiner Rechte den EuGH anrufen, welcher wiederum sich nicht nur über die Auslegung sondern auch für oder gegen die Gültigkeit des Beschlusses aussprechen könnte. Im Gegensatz zum Übereinkommen ist der Beschluss, wenn er auch in den Mitgliedsstaaten nicht unmittelbar wirksam ist, auch ohne eine Ratifikation durch die nationalstaatlichen Parlamente völkerrechtlich verpflichtend.
Am Beispiel Europols lässt sich daher das Dilemma der dritten Säule der Union beispielhaft betrachten.[341] Die einzelnen Mitgliedstaaten möchten auf ihre originäre Dispositionsgewalt im Bereich der polizeilichen und justiziellen Zusammenarbeit nicht verzichten. Gleichwohl wollen die Mitgliedstatten sie bis zu einem gewissen Maße auf europäischer Ebene integrieren. Sollen dem Europäischen Parlament substantielle Mitwirkungsrechte eingeräumt werden, würde dies dazu führen, dass der intergouvernementale Charakter von Europol und damit die „Souveränität" der Nationalstaaten weiter relativiert wird. Resultat dieser Zwischenlösung ist ein unter Effizienzgesichtspunkten eher als umständlich zu beurteilendes Verfahren, welches zur Änderung des EuropolÜ einer Ratifikation durch alle einzelnen nationalen Parlamente erfordert.

B. Europäische Organe und Einrichtungen

Für das Selbstverständnis der Union war wichtig, zusätzlich zum Umgang mit personenbezogenen Angaben in den Mitgliedstaaten auch die unionsinternen Datenverarbeitung zu regeln. Das Fehlen eines Schutzes personenbezogener Daten sei mit dem Engagement der Union für die Wahrung der Grundrechte nicht vereinbar.[342] Die Union ist aus vielschichtigen Gründen (z.B. der statistischen Erhebungen und Subventionskontrolle) auf höchst unterschiedliche Daten angewiesen, welche überwiegend aus den Mitgliedstaaten kommen Darüber hinaus sind die personenbezogenen Daten der eigenen Beschäftigen zu zählen.
Deshalb gab die Kommission 1990 eine Erklärung[343] ab, wonach sie sich selbst verpflichtete, die erforderlichen Vorschläge zur Sicherstellung des Datenschutzes in den Gemeinschaftsorganen und –einrichtungen zu machen und geeignete Maßnahmen zu ergreifen. Der Rat schloss sich dieser Absicht in einer gemeinsamen Erklärung anlässlich der Verabschiedung der Richtlinie an.[344] Dies geschah auch vor dem Hintergrund der EuGH-Rechtssprechung zum Schutz der Privatsphäre (s. o. Teil 2 A II).
Die Entscheidung, bloß eine unverbindliche Erklärung abzugeben und auf einen eventuell später eintretenden Rechtsschutz durch Richterrecht des EuGHs zu warten, ist geradezu prädestiniert zu einer systematischen Unausgewogenheit zu führen.[345] Daher hat die Regierungskonferenz in Amsterdam von

339 *Thym, D.*, a.o.O. (Fn. 295), S. 228.
340 Bericht des europäischen Parlaments, PE 31 1.028, SS. 9, 15.
341 *Ellermann, J.*, a.o.O. (Fn. 304), S. 578.
342 Dammann-Simitis, DSRL-*Einleitung*, Rn. 52.
343 KOM (90) 314 endg., 16.
344 Am 24.7.1995 abgegebene Presseerklärung des Rates 9012/95, Presse 226-G.
345 Grabitz-Hilf-*Brühann*, Richtlinie 95/46, A 30 Vorbem., Rn. 70.

1997, den Forderungen des Europäischen Parlaments, der europäischen Datenschutz-Kontrollinstanzen, sowie des Schrifttums entsprechend, einen Datenschutzartikel im EGV aufgenommen (I.). Auf dessen Grundlage ist der Europäische Datenschutzbeauftragte eingerichtet worden (II.).

I. Art. 286 EGV

Als neuer „Datenschutzartikel" des EGV bestimmt Art. 286, dass die datenschutzrechtlichen Rechtsakte der Gemeinschaft auch auf die Organe und Einrichtungen der Gemeinschaft Anwendung finden (Abs.1). Durch Rat und Parlament soll eine unabhängige Kontrollinstanz errichtet werden, welche die Anwendung dieser Rechtsakte überwacht (Abs. 2 S. 1). Der Rat und die Kommission sind dazu ermächtigt, erforderlichenfalls weitere einschlägige Vorschriften zu erlassen. (Abs. 2 S. 2).
Art. 286 Abs.1 verweist auf die „Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten". Hierbei handelt es sich um eine dynamische Verweisung auf den jeweiligen Bestand der datenschutzrechtlichen Rechtsakte der europäischen Gemeinschaft, vor allem auf die DSRL.[346] Diese könnte entweder als eine inkorporierende oder als eine geltungserweiternde Verweisung verstanden werden. Im ersten Fall bedeutet die Inkorporierung des materiellen Gehalts der verwiesenen Norm in die Verweisungsnorm, dass die resultierende Regelung die Ranghöhe und Geltungskraft der Verweisungsnorm besitzt, also selbst zum Primärrecht wird.[347] Im zweiten Fall erweitert sich lediglich der Geltungsbereich des gemeinschaftlichen Datenschutzrechts, ohne dass sich sein Rang als sekundäres Gemeinschaftsrecht ändert. Sollte man in Art. 286 Abs.1 EGV eine inkorporierende Verweisung sehen, dann stünde die Datenschutzregelung für Gemeinschaftsorgane im Range des primären Gemeinschaftsrechts und könnte nicht auf ihre Grundrechtskonformität überprüft werden.[348] Daher wird die zweite Alternative der ersten vorgezogen und von einer geltungserweiternden Verweisung ausgegangen.[349]
Wird Art. 286 Abs. 1 EGV als Verweisungsnorm verstanden, so kann in der von den Mitgliedsstaaten im Rahmen des Vertragsänderungsverfahrens vorgenommenen Reform aufgrund der dynamischen Verweisung auf sekundäres Datenschutzrecht eine Verlagerung von Rechtssetzungsbefugnissen zu den Organen der EG gesehen werden.[350]
Des weiteren könnte damit auch eine dogmatisch neue, in Art. 249 EGV nicht aufgelistete Rechtsaktsform ins Leben gerufen worden sein, nämlich eine (auch) an die Gemeinschaft gerichtete Richtlinie,[351] da die Verweisungsobjekte ihren sekundärrechtlichen Rang beibehalten und lediglich ihr Anwendungsbereich und Regelungsadressat verändert wurde. Damit wäre Art. 286 Abs. 1 auch eine spezielle Ausnahmebestimmung zu Art. 249 Abs. 3. Eine Umsetzung dieses Rechtsakts durch die Gemeinschaft hätte selbstverständlich keine „umsetzende" Funktion, da es sich bei der DSRL bereits um Gemeinschaftsrecht handelt. Vielmehr würde eine solche Transposition ein im Verhältnis Bürger-Gemeinschaft unmittelbar anwendbares Recht herstellen. Da nach der Rechtsprechung des EuGHs allgemeine Rechtsnormen für jegliche Umsetzungsakte verwendet werden müssen,[352] wäre in diesem Fall die Rechtsform einer Verordnung zu verwenden.

---

346 *Haratsch, A.*, Verweisungstechnik und gemeinschaftsgerichtete EG-Richtlinie, Anmerkungen zum neuen Datenschutzartikel des EG-Vertrages, EuR 2000, S .44.
347 Vgl. für die italienische Literatur *Crisafulli, V.*, Lezioni di diritto costituzionale, Bd. 2, Le fonti normative, Padova 1993, S. 201-204.
348 *Haratsch, A.*, a.o.O. (Fn. 345), S. 45. Voraussetzung dafür ist, dass keine Hierarchie zwischen den allgemeinen Rechtsgrundsätzen des Gemeinschaftsrechts einschließlich der Grundrechte und dem sonstigen primären Gemeinschaftsrecht besteht, s. *Opperman, T.*, a.o.O. (Fn. 75), Rn. 488. Anderer Meinung ist z.B. Tizzano: nach ihm haben Grundrechte aber ´nicht alle Normen der Gründungsverträge Verfassungsqualität und daher einen höheren Rang (*Tizzano, A.*, La gerarchia delle norme comunitarie, Diritto dell'Unione Europea 1996, 61). Die ausdrückliche Formulierung des Grundrechts auf Schutz personenbezogener Daten im Art. II-8 des Verfassungsentwurfs soll dieses Dilemma gelöst haben.
349 *Haratsch, A.*, a.o.O. (Fn. 345), S.45.
350 *Haratsch, A.*, a.o.O. (Fn. 345), S. 52.
351 *Haratsch, A.*, a.o.O. (Fn. 345), S.52.
352 *Streinz, R.*, a.o.O. (Fn. 61) Rn. 391.

Von der Ermächtigungsgrundlage des Art. 286 Abs. 2 EGV Gebrauch machend wurde somit 2001 im Wege des Mitbestimmungsverfahrens die „Verordnung des Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr“ (VO Nr.45/2001/EG[353]) erlassen.
Obwohl eine ähnliche Entwicklung wie beim Recht auf Dokumentenzugang wünschenswert gewesen wäre,[354] um das Datenschutzrecht im Bereich aller „Säulen“ der Union zu gewähren, beschränkt Art. 3 den Anwendungsbereich der Verordnung auf Tätigkeiten innerhalb des Gemeinschaftsrechts. Miteinbezogen werden die Organe der Gemeinschaft (EP; Rat; Kommission; EuGH; Rechnungshof), die durch den EGV, den EGKS-V, den EURATOM-V (EZB; EIB; AdR) sowie die durch das Sekundärrecht geschaffenen Einrichtungen (die sog. Agenturen). Über die konsolidierten Datenschutzgrundsätze und Rechte der Betroffenen hinaus sieht die Verordnung die vor, dass jedes Organ bzw. jede Einrichtung eine Person zum unabhängigen behördlichen Datenschutzbeauftragten der jeweiligen Institution ernennt (Art. 24).

II. Europäischer Datenschutzbeauftragte

Sich auf Art. 286 Abs. 2 S. 1 stützend sieht die Verordnung die Einsetzung eines „unabhängigen“ Europäischen Datenschutzbeauftragten vor (Art. 41). Die Stelle wurde im September 2002 öffentlich ausgeschrieben[355] und im Dezember 2003 besetzt.[356] Besondere Garantien sollen die Unabhängigkeit der Kontrollstelle gewährleisten.[357] Diese Bestimmungen betreffen insbesondere die Ernennung (durch das Europäische Parlament und den Rat (Art. 41 Abs. 1)), die Amtsenthebung (vom Gerichtshof, auf Antrag des EP, des Rates oder der Kommission (Art. 42 Abs. 5)), die Dauer seiner Amtszeit (fünf Jahre, nur eine Wiederernennung zulässig (Art. 42 Abs. 1 und 2)) und das Verbot Weisungen entgegenzunehmen (Art. 44).
Ob der Europäische Datenschutzbeauftragte, dem Vorschlag der Kommission gemäß vergleichbar, zum Bürgerbeauftragten zu gestalten war, wurde im Europäischen Parlament intensiv diskutiert.[358] Trotz des finanziell motivierten Widerspruchs des Haushaltsausschusses wurde der Kommissionsvorschlag, dem sich der federführende Ausschuss angeschlossen hatte, durch einen gemeinsamen Beschluss akzeptiert.[359]
Unter seine Aufgaben fällt u.a. die Beratung der Organe bzw. Einrichtungen der Gemeinschaft bei Datenschutzfragen (Art. 46 d)), sowie die Bearbeitung von Beschwerden (Art. 46 a)). Aufgrund einer Beschwerde oder auch von sich aus kann der Datenschutzbeauftragte Untersuchungen durchführen (Art. 46 b)), wofür ihm eine Reihe von Befugnissen zugebilligt werden. Ihm ist Zugang zu Informationen und Räumlichkeiten zu gewähren und er ist befugt eigene Schlussfolgerungen aus seinen Untersuchungen zu ziehen sowie Anordnungen gegen die für die Verarbeitung verantwortliche Einrichtung bzw. Organ zu erlassen. Darüber hinaus hat er Klagebefugnis vor dem EuGH und kann anhängigen Verfahren beitreten (Art. 47 h) und i)).
Beschwerden können beim Europäischen Datenschutzbeauftragter auch dann eingereicht werden, wenn bereits ein Rechtsbehelf beim EuGH eingelegt wurde (Art. 32 Abs. 2). Alle bei einem Organ bzw. einer Einrichtung beschäftigten Personen können beim Datenschutzbeauftragten eine Beschwerde wegen Verletzung der Bestimmungen der Verordnung einreichen, ohne dass zuvor der Dienstweg beschritten werden muss und ohne dass man als Arbeitnehmer anschließend „benachteiligt“ wird (Art. 33). Es ist voraussehbar, dass sich diese Tätigkeit, im Hinblick auf die große Menge personenbezogener (davon vor allem viele sensible) Daten, welche die Organe und Einrichtungen der

353 Abl. 2001 L 8/1.
354 *Pallaro, P.*, a.o.O. (Fn. 295), S. 232.
355 Abl. 2002 C 224 A/1
356 Abl. 2004 L 12/47
357 Vgl. *Gola/Klug*, a.o.O. (Fn. 29), S. 29; Bericht zum Europäischen Datenschutzbeauftragter, RDV 2003, 33
358 *Brühann, U.*, Sektorspezifischer Datenschutz in Europa, DuD 2002, 360.
359 Beschluß Nr. 1247/2002/EG des EP, des Rates und der Kommission, Abl. 2002 L 183.

Gemeinschaft über ihre Beschäftigten verarbeiten, für den Datenschutzbeauftragten als zeitraubend erweisen wird.[360]
Schließlich ist die Rolle des Europäischen Datenschutzbeauftragten in den Netzen der europäischen Zusammenarbeit zu betonen.[361] Zum einem arbeitet er mit den nationalen Aufsichtsbehörden zusammen, um die jeweiligen Aufgaben zu erfüllen, insbesondere durch Austausch aller einschlägigen Informationen, durch die Aufforderung an eine nationale Stelle, ihre Befugnisse auszuüben oder durch die Reaktion auf eine Aufforderung von einer solchen Stelle (Art. 46 fi)). Darüber hinaus nimmt er an den Tätigkeiten der Art. 29-Gruppe teil, was eine vertikale neben der horizontalen Zusammenarbeit ermöglichen soll (Art. 46 g)).[362]
Schließlich ist der europäische Datenschuzbeauftragte der wichtigste Knoten eines Netzes der Datenschutzbehörden auf europäische Ebene, welches Stellen wie die AGi Schengens und Europols miteinbezieht (s. o.).

Schlussbetrachtung

Im Hinblick auf in den Teilen 1 bis 4 erfolgten Ausführungen, erscheint eine Verankerung des Grundrechts auf Datenschutz in der künftigen europäischen Verfassung (Art. I-50, II-8 VE) als vorläufiger Höhepunkt der europäischen Datenschutzrechtsentwicklung.
Zwar ist der Wortlaut beider Artikel teilweise identisch, doch kann darin nicht nur eine bloße Wiederholung gesehen werden. Die Einordnung des Art. I-50 VE unter den Titel des „Demokratischen Lebens der Union“ und des Art. II-8 VE unter den Titel der „Freiheiten“ der Grundrechtscharta spiegelt vielmehr die vielseitigen Funktionen des Datenschutzes wieder

Art. II-8 VE, worauf auch die Geheimhaltungspflichten der Gemeinschaftsbedienstete gestützt werden,[363] wurde als *„a summary of the very essence of the Directive 95/46 CE“*[364] angesehen. In dieser Vorschrift kommen sowohl die abwehrrechtliche als auch die objektiv-rechtliche Dimension des „Rechts auf Schutz personenbezogener Daten“ zum Ausdruck. Was den abwehrrechtlichen Aspekt (Art. II-8 Abs.1 VE) anbelangt, gelten für das Recht auf Schutz personenbezogener Daten die gerade nicht nur die allgemeinen Einschränkungs- bzw. Auslegungsgrundsätze der Art. II-52 und II-53 VE, sondern das spezielle Erfordernis, dass eine einschränkende Maßnahme auf einem Gesetz beruhen muss, welches selbst jeder Person das Recht gewährt „Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken“ (Art. II-8 Abs. 2 S. 2).
Im Vergleich zu den traditionellen Grundrechtskatalogen gewinnt die objektiv-rechtliche Dimension zunehmend an Bedeutung[365] (Art. II-8 Abs. 2 und 3 VE). Die grundlegenden Prinzipien des Datenschutzes werden ausdrücklich als Schutzpflicht der Union formuliert, welche das erforderliche Verfahren und Organisation, vor allem eine „unabhängige Stelle“, bereitzustellen hat. Der nach der h.M. schon im Volkszählungsurteil des BVerfG implizite Ansatz eines „prozeduralen Datenschutzes“ wird damit in der europäischen Verfassung ausdrücklich verankert.

---

360 Bericht zum Europäischen Datenschutzbeauftragter, RDV 2003, S.33.
361 Zu den „europäischen Netzen“ vgl. *Cassese, S.,* Gli Stati nella rete internazionale dei poteri pubblici, a.o.O. (Fn. 201), S. 325-329; *Chiti, E.* , Le agenzie europee, a.o. O. (Fn. 201), S. 38-39.
362 *Pallaro, P.*, a.o.O. (Fn. 295), S. 232.
S. 254.
363 Grabitz/Hilf-*Pernice/Mayer*, nach Art. 6 EUV, Rn.98.
364 *Hustinx, P.*, Art. 8 of the Charter: Fundamental Data Protection and the interaction with directives 95/46/EC and 97/66/EC, in: EMR –Institut für europäisches Medienrecht (Hrsg.), Nizza-Die Grundrechte-charta, Baden-Baden 2001, S. 92.
365 *Pernice, I,* Eine Grundrechte-Charta, a.o.O. (Fn. 287), S. 856; *Ridola, P.*, La carta dei diritti fondamentali, a.o.O. (Fn. 3), S. 109.

Aus einer theoretischen Perspektive betracht ist Art. I-50 VE nicht weniger von Interesse. Sollte man mit Habermas in einem freien kommunikativen Handeln die erforderliche Voraussetzung für eine individuelle und soziale sowie bewusste und echte Entfaltung der Person im Verfassungsstaat sehen und den Datenschutz als ein Mittel für die Schaffung solcher Kommunikationsräume verstehen, wird Datenschutz auch zur „Funktionsbedingung … eines freiheitlichen demokratischen Gemeinwesens."[366] Welchen Einfluss diese Aussage des Bundesverfassdungsgerichts und der dahinter stehenden soziologischen Auffassung auf das EU-Recht hat, lässt sich auch daran erkennen, dass in der europäischen Verfassung der Datenschutz i.S.d. Art. I-50 VE das „demokratische Leben der Union" fördern soll.

Diese demokratisch-partizipative Funktion[367] des Art. 1-50 VE, zusammen mit dem objektiven Wertegehalt des Art. II-8 VE erscheinen als europaweit konsensfähig und vermögen somit als gemeinsamer Wertekanon die Verfassungsintegration voranzutreiben.[368]

Über diese Überlegungen grundrechtstheoretischer Natur hinaus, hat die Aufnahme eines Grundrechts auf Datenschutz in der europäischen Verfassung mit Geltung für alle „Organe, Einrichtungen, Ämter und Agenturen" (Art. II-51 VE) im Falle ihres Inkrafttretens weitreichende praktische Konsequenzen. Erstens würden die für die drei Säulen der Union unterschiedlichen Grundrechtsniveaus nicht mehr bestehen, so dass Defizite der dritten Säule in Bezug auf das Rechtsstaats- bzw. das Demokratieprinzip jedenfalls für den Bereich des Datenschutzes kaum mehr bestünden (Teil IV).

Zweitens, würde die Außen- und Organkompetenz zum Abschluß von völkerrechtlichen Verträge, welche Auswirkungen auf Grundrechte haben, in Zusammenhang mit der Abschaffung der Säulenstruktur[369] an Bestimmtheit gewinnen. Problemen, wie beim PNR-Fall, könnten von Anfang an vermieden werden (Teil III).

Drittens, werden die gegenseitigen Auswirkungen zwischen den im Verfassungsverbund verschränkten nationalen bzw. europäischen Ebenen weiter fortschreiten. Das Kooperationsverhältnis zwischen den Gerichten der Mitgliedstaaten und dem mit umfassender Kompetenz versehenen EuGH sowie das Netz unabhängiger Kontrollinstanzen würden langfristig zu gegenseitigen Anpassungen und Harmonisierungen führen (vgl. entsprechende Stellen im Teil 2 B 3 und Teil 4 A II 2). Hierbei würden sowohl die vertikale (zwischen der EU und den Mitgliedstaaten) als auch die horizontale Perspektive (zwischen den Mitgliedstaaten unter einander) in Betracht kommen. Eine entscheidende Rolle käme dann dem europäischen Datenschutzbeauftragten zu, welcher erst vor kurzem die in der EURODAC-Verordnung[370] vorgesehene Kontrollinstanz ersetzt hat und künftig auch die Aufgaben der Schengener und Europol GKI (gemeinsamen Kontrollinstanzen) übernehmen könnte.

Zum Abschluss eine eher rechtspolitische Anmerkung: Die jüngsten internationalen Ereignisse haben Anlass zum Nachdenken gegeben, ob sich die EU dem steigenden amerikanischen Drück auf verstärkte militärische und polizeiliche Unterstützung dauerhaft widersetzen kann. Mit Unterzeichnung der Abkommen zur Rechtshilfe in Strafsachen und zum Datenaustausch blieb der Bereich des Datenschutzes nicht unberührt. Inwiefern eine als „Rechtsgemeinschaft"[371] verstandene Europäische Union, einen effektiven Datenschutz zu gewährleisten vermag, bleibt daher abzuwarten.

---

366 So das BVerG im Volkszählungsurteil: " Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechende Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesen ist", NJW 1984, S. 422.

367 *Ridola, P.,* Libertà e diritti nello sviluppo storico del costituzionalismo, in: Nania/Ridola (Hrsg.), I diritti costituzionali, Torino 2002.

368 *Pernice, I.,* Eine Grundrechte-Charta, a.o.O. (Fn. 287), S. 849; *Ridola, P.,* La carta dei diritti fondamentali, a.o.O. (Fn. 3), S. 91; *ders.* Libertà e diritti, a.o.O. (Fn. 367), S. 52-55.

369 Dem Verfassungsentwurf nach wird die Säulenstruktur abgeschafft und der Union eine eigene Rechtspersönlichkeit eingeräumt, s. CONV 850/03 I-6, sowie CONV 426/02, SS.2-3. und *Labayle, H.,* WG X- WD 3, SS.4-5.

370 VO 2725/2000/EG, Abl. 2000 L 316/1, dazu *Pallaro, P.,* a.o.O. (Fn. 295), S. 320-322.

371 *Hallsteins* „Credo", vgl. *Pernice, I.,* Walter Hallstein-Erbe und Verpflichtung, WHI-Paper 7/01, S. 2 unter http://www.whi-berlin.de/pernice-hallstein.htm; *Opperman, T.,* a.o.O. (Fn. 75), Rn. 469; *della Cananea, G.,* a.o.O. (Fn. 86), S. 174-178.