Zu ausgewählten Herausforderungen des Datenschutzrechts

Bericht der Generalberichterstatterin

Astrid Epiney

Dieser Beitrag wurde erstmals wie folgt veröffentlicht:
***Astrid Epiney,* Zu ausgewählten Herausforderungen des Datenschutzrechts, in: Astrid Epiney/Sarah Theuerkauf (Hrsg.), Datenschutz in Europa und die Schweiz / La protection des données en Europe et la Suisse, Zürich 2006, S. 1-44. Es ist möglich, dass die Druckversion – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript geringfügige Modifikationen enthält.**

I. Einleitung

Die Diskussionen anlässlich dieser 27. Internationalen Konferenz der Datenschutzbeauftragten – die zudem vielfach auch in parallel stattfindenden Sessionen stattfanden – waren so vielschichtig und berührten so viele Themata, dass es im Rahmen dieses Generalberichts weder möglich noch sinnvoll ist, die Diskussionen auch nur annähernd zusammenfassen zu wollen. Allerdings – und dies ist angesichts der Vielfalt der angesprochenen Themata außerordentlich bemerkenswert – kehrten einige Grundprobleme und auch Grundanliegen des Datenschutzes bzw. des Datenschutzrechts unter verschiedenen Vorzeichen und in unterschiedlichen Zusammenhängen immer wieder. Zu nennen sind hier im Wesentlichen drei Kategorien datenschutzrechtlicher Probleme, die aber auch miteinander verbunden sind:

- Stellenwert des Datenschutzes;
- Ausgewählte Probleme des datenschutzrechtlichen Standards;
- Rechtliche Absicherung datenschutzrechtlicher Garantien.

Im Folgenden geht es auf dieser Grundlage und ausgehend von den Diskussionen an dieser Tagung darum, einige der wichtigsten derzeitigen Herausforderungen in den drei angesprochenen Problemkreisen zu skizzieren und zu versuchen, einige Perspektiven für die Zukunft zu entwickeln.

II. Stellenwert des Datenschutzes

Das Anliegen des Datenschutzes – das insgesamt ein relativ junges Politik- und Rechtsgebiet ist[1] – ist in den letzten Jahren in der öffentlichen Wahrnehmung sowie in der politischen Diskussion wohl etwas in den Hintergrund getreten[2].

> Während sich etwa in den 80er Jahren noch weite Kreise der Bevölkerung gegen Volkszählungen an sich wandten, werden heute z.B. neue Maßnahmen zur Bekämpfung des Terrorismus oder die Einführung neuer Instrumente der (internationalen) polizeilichen Zusammenarbeit kaum und allenfalls am Rande unter datenschutzrechtlichen Gesichtspunkten diskutiert.

Über die Ursachen dieses Verlusts an Stellenwert nicht in der nationalen, sondern auch in der internationalen Diskussion mag man trefflich streiten, und es dürfte schwierig sein, hier verlässliche Aussagen zu treffen. Gleichwohl sei die Behauptung gewagt, dass dieser relative Verlust auch an öffentlicher und politischer Aufmerksamkeit wohl auf zwei gegenläufigen Tendenzen bzw. Entwicklungen beruht:

- Einerseits sind –zumindest in zahlreichen Staaten und auf der Ebene einiger gewichtiger internationaler Gremien und Organisationen – datenschutzrechtliche Anliegen gewissermaßen zum *courant normal* geworden; es ist teilweise unbestritten, dass datenschutzrechtliche Aspekte zu berücksichtigenund in die entsprechenden Politiken, Gesetzgebungsprojekte und die Rechtsanwendung einzufließen haben.
- Andererseits dürften aber auch im Laufe der Jahre andere Anliegen eher schleichend mehr in den Vordergrund gerückt sein, so dass datenschutzrechtlichen Aspekten im Vergleich zu anderen (öffentlichen) Interessen – wie etwa Kriminalitäts- oder Terrorismusbekämpfung oder wirtschaftliche Entwicklung – häufig weniger Gewicht beigemessen wird.

Es dürfte – wie bereits angedeutet – äußerst schwierig sein, das genaue Gewicht dieser zumindest teilweise gegenläufigen Tendenzen zu bewerten. Jedenfalls aber sind sie Anlass dafür, nochmals die Hintergründe datenschutzrechtlicher Regelungen in Erinnerung zu rufen: Persönlichkeitsschutz auf der einen (1.) und Verfolgung öffentlicher Interessen (2.) auf der anderen Seite, auf deren Grundlage dann eine kurze Bewertung des Stellenwerts des Datenschutzes aus rechtlicher Sicht vorgenommen werden kann (3.).

1. Datenschutz als besonderer Teil des Schutzes der Persönlichkeit

Datenschutzrechtliche Regelungen sind (auch) vor dem Hintergrund zu sehen, dass der Datenschutz ein Teilgehalt des Rechts auf Schutz der Privatsphäre und der Persönlichkeit ist. Eine Reihe internationaler und regionaler Menschenrechtsabkommen enthalten denn auch allgemeine Garantien des Schutzes der Privatsphäre.

---

[1] Zur Entwicklung des Datenschutzrechts auf nationaler und internationaler Ebene etwa *Spiros Simitis,* in: Spiros Simitis (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., 2003, Einleitung, Rz. 1 ff., 112 ff.; *Walter Rudolf,* Datenschutz in Europa, ZEuS 2003, 217 ff.

[2] Mehrere Beiträge wiesen auf diesen Befund hin. Vgl. z.B. *Herbert Burkert*, Globalization – Strategies for Data Protection, 3, 6 f. (zitiert nach Manuskript).

Auf internationaler Ebene wurde der Schutz der Privatsphäre erstmals in der Allgemeinen Erklärung der Menschenrechte (AEMR) vom 10.12.1948[3] erwähnt[4]. Im Übrigen verankert Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPBPR) vom 19.12.1966[5], der inzwischen von 154 Staaten ratifiziert wurde[6] und für diese bindendes Völkerrecht ist, den Schutz der Privatsphäre nahezu wortgleich mit Art. 12 der Allgemeinen Erklärung der Menschenrechte[7]. Insgesamt ist damit davon auszugehen, dass ein völkergewohnheitsrechtlich verankertes Recht auf Schutz der Privatsphäre besteht. Regional wird die Privatsphäre außerdem durch Art. 8[8] der Europäischen Menschenrechtskonvention (EMRK) vom 4.11.1950 und Art. 11[9] der amerikanischen Menschenrechtskonvention vom 22.11.1969 garantiert.

Insbesondere der Europäische Gerichtshof für Menschenrechte (EGMR) und die mit dem Inkrafttreten des 11. Zusatzprotokolls 1998 abgeschaffte Europäische Kommission für Menschenrechte (EKMR) haben zahlreiche wegweisende Entscheidungen zum Schutz der Privatsphäre und insbesondere auch zum Datenschutz gefällt[10]. Datenschutz bzw. das Recht der Einzelnen darauf, dass sie betreffende Daten nicht gespeichert und verwertet werden, wird dabei als spezifischer Teilbereich des Rechts auf Achtung der Privatsphäre (Art. 8 EMRK) angesehen[11].

---

3 Art. 12 AEMR: „No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Dt. Übersetzung: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jedermann hat Anspruch auf rechtlichen Schutz gegen derartige Eingriffe oder Beeinträchtigungen."

4 Vgl. hierzu *Rudolf*, ZEuS 2003 (Fn.), 217 (222); ausführlich auch *Rudolf Gridl*, Datenschutz in globalen Telekommunikationssystemen – eine völker- und europarechtliche Analyse der vom internationalen Datenschutzrecht vorgegebenen Rahmenbedingungen, 1999, 168 ff.

5 Art. 17 IPBPR: „1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." Dt. Übersetzung: „(1) Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. (2) Jedermann hat Anspruch auf rechtlichen Schutz gegen derartige Eingriffe oder Beeinträchtigungen."

6 Der Stand der Ratifizierungen kann im Internet unter http://www.ohchr.org/english/countries/ratification/4.htm abgerufen werden.

7 Zur Bedeutung des IPBPR für den Datenschutz ausführlich *Gridl,* Datenschutz in globalen Kommunikationssystemen (Fn.), 157 ff. unter Berücksichtigung der Praxis des Menschenrechtsausschusses.

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

9 „1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks."

10 Vgl. dazu *Jens Meyer-Ladewig*, Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Handkommentar, 2003, Art. 8, Rz. 11 ff; *Christoph Grabenwarter*, Europäische Menschenrechtskonvention, 2005, § 22, Rz. 9, 23, 32, 36, m.w.N.

11 *Stephan Breitenmoser*, Der Schutz der Privatsphäre nach Art. 8 EMRK, 1986, 245; ausführlich zur Bedeutung der EMRK für den Datenschutz *Gridl,* Datenschutz in globalen Kommunikationssystemen (Fn.), 107 ff.; *René Detlev Matz,* Europol. Datenschutz und Individualrechtsschutz im Hinblick auf die Anforderungen der EMRK, 2003, 108 ff.; unter Berücksichtigung der Praxis des EuGH, die sich ihrerseits durch Art. 8 EMRK „inspiriert", *Johanna Kübler,* Die Säulen der Europäischen Union: einheitliche

> Der Schutzbereich des Art. 8 Abs. 1 EMRK umfasst danach die Erhebung und Speicherung personenbezogener Daten sowie ihre Verwertung und Übermittlung. Eingeschlossen sind damit auch etwa die Aufnahme in ein Register oder polizeiliche bzw. hoheitliche Überwachung[12]. Einschlägig ist Art. 8 Abs. 1 EMRK aber auch bei der Weitergabe von die Privatsphäre betreffenden Informationen[13], und aus dieser Bestimmung kann jedenfalls bei höchstpersönlichen Daten ein Recht auf Einsichtnahme in Datensammlungen abgeleitet werden[14]. Vieles spricht dafür, dass aus Art. 8 Abs. 1 EMRK zudem eine Schutzpflicht der Vertragsstaaten dergestalt abgeleitet werden kann, dass durch geeignete, insbesondere gesetzgeberische Maßnahmen sicherzustellen ist, dass Private Informationen anderer Privater nicht missbräuchlich erheben, speichern oder verwenden[15]; dem nationalen Gesetzgeber ist hier jedoch ein weiter Gestaltungsspielraum einzuräumen.

Allerdings kann die Garantie des Art. 8 Abs. 1 EMRK nach Art. 8 Abs. 2 EMRK auch eingeschränkt werden, wobei diese Bestimmung jedoch enge Voraussetzungen vorsieht[16]:

- Zunächst muss der Eingriff in einer gesetzlichen Grundlage vorgesehen sein.
- Weiter darf eine Einschränkung des in Art. 8 EMRK verankerten Rechts nur aus bestimmten Gründen erfolgen, wobei in unserem Zusammenhang insbesondere die nationale oder öffentliche Sicherheit, die Aufrechterhaltung der Ordnung, die Verhütung von Straftaten sowie der Schutz der Rechte und Freiheiten anderer von Bedeutung ist.
- Schließlich muss der Grundsatz der Verhältnismäßigkeit gewahrt werden.

In neuerer Zeit wird das Recht auf den Schutz personenbezogener Daten häufig von dem Recht auf Achtung des Privat- und Familienlebens getrennt und in einer eigenen Norm verankert. Hingewiesen sei hier beispielhaft auf die auf ihrer Tagung in Nizza von den Staats- und Regierungschefs der Mitgliedstaaten der EU am 7.12.2000 feierlich proklamierte Europäische Grundrechtecharta[17]. Deren Art. 8 enthält ein Recht auf Schutz personenbezogener Daten. Im Einzelnen hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten; solche Daten dürften nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Personen oder beruhend auf einer gesetzlichen Grundlage verarbeitet werden. Jeder Person wird das Recht eingeräumt, Auskunft über die sie betreffenden Daten zu erhalten und ggf. die Berichtigung der Daten zu

---

Grundrechte? – Zur Grundrechtsdivergenz zwischen der ersten und dritten Säule am Beispiel des Datenschutzes, 2002, 32 ff., jeweils m.w.N.

12 Aus der Rechtsprechung etwa EKMR, Entscheidung vom 6.10.1982, EuGRZ 1983, 410 (X/Vereinigtes Königreich); EGMR, Urteil vom 6.9.1978, EuGRZ 1979, 278 (Klass u.a./Deutschland); EGMR, Urt. vom 26.3.1987, Serie A, Bd. 116, § 48 (Leander/Schweden); EGMR, Urt. vom 2.8.1984, EuGRZ 1984, 17 ff. (Malone/Großbritannien); EGMR, Urteile vom 24.4.1990, Serie A, Bd. 176 A und 176 B (Kruslin und Huvig/Frankreich); EGMR, Urteil vom 16.12.19990, Serie A, Bd. 251 A und 251 B (Niemitz/Deutschland); EGMR, Urteil vom 25.6.1997, Rec. des Arrêts et Décisions 1997 III, 1005 ff. (Halford/Vereinigtes Königreich); EGMR, Urteil vom 4.5.2000, Application no. 28341/95 (Rotaru/Rumänien); EGMR, Urteil vom 16.2.2000, Application no 27798/95 (Amann/Schweiz).

13 EGMR, Urt. vom 26.2.1997, Rep. of Judgements and Decisions 1997 I, 323 ff. (Z/Finnland).

14 EGMR, Urt. vom 7.7.1989, Serie A, Bd. 60 (Gaskin/Großbritannien). Zur Problematik *Gridl,* Datenschutz in globalen Kommunikationssystemen (Fn.), 135 ff.

15 Vgl. in Bezug auf Schutzpflichten EGMR, Urt. vom 26.3.1985, Serie A, Bd. 91 (X u. Y/Niederlande). I. Erg. wie hier in Bezug auf datenschutzrechtliche Fragestellungen *Gridl,* Datenschutz in globalen Kommunikationssystemen (Fn.), 139 ff.

16 Ausführlich zu diesen Anforderungen *Matz,* Europol (Fn.), 124 ff.

17 Zur Bedeutung der Charta für den Datenschutz etwa *Rudolf*, ZEuS 2003 (Fn.), 217 (227).

erwirken. Die Einhaltung dieser Vorschriften ist von einer unabhängigen Stelle zu überwachen. Die Charta hat bis auf weiteres keine unmittelbare Rechtswirkung, soll aber Teil II der geplanten EU-Verfassung[18] bilden.

> Die Aufnahme des Datenschutzes in die Grundrechtecharta folgt der europaweiten Tendenz, dem informationellen Selbstbestimmungsrecht Verfassungsrang einzuräumen. Bereits jetzt haben datenschutzrechtlich relevante Bestimmungen in Deutschland, Österreich, Portugal, Spanien und den Niederlanden Verfassungsrang.[19]

Zusammenfassend kann damit festgehalten werden, dass das Recht des Einzelnen auf den Schutz personenbezogener Daten ein Grund- bzw. Menschenrecht darstellt, das nur unter Beachtung der bei Grundrechtsbeeinträchtigungen allgemein einschlägigen Voraussetzungen eingeschränkt werden kann. Dieses Recht richtet sich als unmittelbar anwendbares Abwehrrecht zunächst gegen Staaten bzw. die hoheitliche Gewalt; vieles spricht aber dafür, aus der objektiven Dimension der Grundrechte auch Schutzpflichten der Staaten bzw. Organisationen abzuleiten, die diese dazu verpflichten, angemessene (gesetzgeberische) Vorkehrungen gegen (übermäßige) Beeinträchtigungen dieses Rechts durch Private zu treffen[20].

2. Datenschutz als öffentliches Interesse in einem demokratischen Rechtsstaat

M.E. wird gelegentlich zu wenig beachtet, dass Datenschutz über den Schutz der Persönlichkeit – also ein Recht des Einzelnen, auf das er damit grundsätzlich auch verzichten kann – auch ein eminent öffentliches und vielfach verfassungsrechtlich verankertes Interesse darstellt. Denn ein demokratischer Rechtsstaat kann nur funktionieren, wenn Staat und Private nicht die Befugnis haben, beliebige personenbezogene Daten nach Gutdünken zu erheben und zu verwerten, wird doch damit der Bürger nicht (mehr) als eigenverantwortliche Person, die nach freiem Willen Teil am politischen Willensbildungsprozess hat, wahrgenommen.
Diese Charakterisierung des Datenschutzes als eigenständiges öffentliches Interesse impliziert auch und gerade, dass der Datenschutz nicht nur dann zu gewährleisten ist, wenn Einzelne dies verlangen, sondern dass eine objektivrechtliche Pflicht der Staaten besteht, einen hinreichenden Schutz zu garantieren. Weiter bedeutet dieser Ansatz, dass die Einwilligung der Betroffenen in die Erhebung und Verarbeitung ihrer persönlichen Daten nicht in jedem Fall ausreichend sein kann, um diese zu „legalisieren".

---

18 Im Internet abrufbar unter http://europa.eu.int/eur-lex/lex/de/index.htm. Der Entwurf findet sich zudem im ABl. C 310 v. 16.12.2004, 1.

19 Weitere Ausführungen bei *Peter Schaar*, Datenschutz im Internet – Die Grundlagen, 2002, Rz. 91 ff.

20 Hierzu EGMR, Urt. vom 26.3.1985, Serie A, Bd. 91 (X u. Y/Niederlande). I. Erg. wie hier in Bezug auf datenschutzrechtliche Fragestellungen *Gridl,* Datenschutz in globalen Kommunikationssystemen (Fn.), 139 ff.

3. Schlussfolgerung: Datenschutz als Grundrecht und verfassungsrechtliches Schutzgut

Vor dem Hintergrund des skizzierten Stellenwerts des Datenschutzes in zahlreichen Verfassungen sind die Datenschutzgesetze nicht nur „sinnvolle“ Gesetze, die zu einem bestimmten Zeitpunkt opportun waren und aufgrund der gegebenen politischen Mehrheiten entsprechend verabschiedet wurden, so dass sie auch wieder abgeschafft werden könnten; vielmehr ist die Datenschutzgesetzgebung in zahlreichen Staaten sowie in der EU als Umsetzung eines völker- und verfassungsrechtlichen Auftrages, dem verbindlicher Charakter zukommt, anzusehen. Damit steht die Datenschutzgesetzgebung als solche nicht etwa zur Disposition des Gesetzgebers, sondern sie ist grundsätzlich aufrechtzuerhalten. Dies bedeutet zwar nicht, dass Modifikationen ausgeschlossen wären; diese dürfen jedoch den jeweils völker- und verfassungsrechtlich geforderten Mindeststandard nicht unterschreiten.
M.E. ist es zentral, diesen verfassungsrechtlichen Status' des Datenschutzes zu betonen; auch kann auf dieser Grundlage seine (allgemeine) rechtliche Tragweite in den verschiedenen Rechtsordnungen durchaus (teilweise sogar recht weitgehend) konkretisiert werden. Gleichwohl sind darüber hinaus noch spezifische Vorgaben für einzelne Bereiche notwendig, die die allgemeinen Kriterien und Anforderungen – die den jedenfalls zu beachtenden Rahmen abgeben – im Hinblick auf die konkreten Problemstellungen einer Lösung zuführen können. Zwei ausgewählte Bereiche seien dabei im Folgenden beispielhaft etwas näher betrachtet.

III. Ausgewählte Probleme des datenschutzrechtlichen Standards

Verschiedene Berichte und Diskussionen an der Tagung berührten in der einen oder anderen Weise zwei große Themenblöcke, nämlich Fragen des Datenschutzes im Rahmen (internationaler) polizeilicher Zusammenarbeit und Verbrechens- sowie Terrorismusbekämpfung (1.) einerseits und die sich dem Datenschutz im Zuge der rasanten technologischen Entwicklungen stellenden neuen Probleme bzw. Herausforderungen (2.). Es kann im Folgenden selbstverständlich nicht darum gehen, diese beiden Themenbereiche umfassend und erschöpfend zu erörtern; vielmehr sollen (teilweise auch nur beispielhaft) die sich hier stellenden Herausforderungen aufgezeigt und mögliche Lösungsansätze bzw. Perspektiven entwickelt werden, die wiederum teilweise im Zusammenhang mit den unter IV. zu betrachtenden Aspekten der rechtlichen Absicherung datenschutzrechtlicher Standards stehen.

1. Datenschutz und (internationale) Sicherheit

An sich ist der Themenkomplex Datenschutz und öffentliche Sicherheit kein neues Thema: Schon seit mehreren Jahrzehnten ist bekannt, dass das Interesse der Sicherheitskräfte an einer effektiven und effizienten Bekämpfung der Kriminalität in Konflikt geraten kann mit dem Recht der Einzelnen auf den Schutz ihrer personenbezogener Daten. Gleichwohl rechtfertigt es sich, diese Thematik hier aufzugreifen, dies aus mindestens zwei Gründen:

- Zunächst dürften sich in diesem Bereich in den letzten Jahren die Gewichte etwas verschoben haben: Neue, zumindest in ihrem Ausmaß bislang kaum bekannte Bedrohungen der öffentlichen Sicherheit durch organisierte Kriminalität und insbesondere terroristische Attentate führen dazu, dass das öffentliche Interesse an effektivem Schutz der öffentlichen Sicherheit ein viel stärkeres Gewicht erhält als dies vor einigen Jahren noch denkbar war und datenschutzrechtliche Bedenken bzw. Anliegen die Gefahr laufen, in den Hintergrund gedrängt zu werden. Aufgeworfen wird damit die Frage, ob und inwieweit ein effektiver und effizienter Schutz der öffentlichen Sicherheit mit der hinreichenden Beachtung datenschutzrechtlicher Anforderungen in Einklang gebracht werden kann.
- Zweitens hat sich die internationale polizeiliche und teilweise auch justitielle Zusammenarbeit in den letzten Jahren sehr schnell entwickelt und intensiviert und damit ein Ausmaß angenommen, das bis vor kurzem aufgrund der hier oft herrschenden souveräntitätspolitischen Vorbehalte kaum denkbar war. Da die internationale (polizeiliche und justitielle) Zusammenarbeit aber häufig mit dem Austausch von (personenbezogenen) Daten einhergeht, stellt sich die Frage, auf welche Weise und inwieweit aus rechtlicher Sicht datenschutzrechtliche Garantien gewährleistet werden sollen.

Im Folgenden soll diesen beiden zentralen Themenkomplexen – die auch in einigen Beiträgen zur Tagung angesprochen wurden[21] – nachgegangen werden, wobei die Probleme aber nur beispielhaft in Bezug auf bestimmte Rechtsentwicklungen und nicht umfassend erörtert werden können.

a) Zum Spannungsverhältnis zwischen dem Schutz öffentlicher Sicherheit und datenschutzrechtlichen Anforderungen

Im Zuge drohender terroristischer Anschläge haben zahlreiche Staaten Gesetzgebungsentwürfe entwickelt oder verabschiedet, die die innere Sicherheit verstärken sollen. Im Einzelnen unterscheiden sich diese Entwürfe teilweise deutlich, so dass es hier nicht darum gehen kann, einzelne nationale Entwürfe auf den Prüfstand zu stellen.

---

[21] Vgl. insbesondere *Klaus-R. Kalk,* Sind Datenschutz und der Kampf gegen den Terrorismus miteinander vereinbar?; *Ann Cavoukian,* The New Breed of Practical Privacy: an Evolution; *Gus Hosein,* Strategies for Privacy Protection in the face of Terrorism.

Beispielhaft sei hier aber kurz auf die Diskussion in der Schweiz verwiesen[22]: Derzeit diskutiert wird eine Revision des Gesetzes zur Wahrung der inneren Sicherheit. Der Entwurf des Bundesamts für Polizei, der allerdings vom Bundesrat (noch) nicht angenommen worden ist, sieht insbesondere folgende Maßnahmen vor: Strafprozessuale Zwangsmaßnahmen (wie insbesondere Telefon- und Mailverkehrüberwachung, Abhören von Wohnungen und Einholen von Informationen bei Banken) sollen ohne Einleitung eines Strafverfahrens möglich sein. Voraussetzung soll nur sein, dass „bestimmte aktuelle Tatsachen (…)" den „konkreten Verdacht" begründen, dass von den Betroffenen eine die Überwachung rechtfertigende Gefährdung der Sicherheit ausgeht und die Lagebeurteilung auf andere Art „aussichtslos oder unverhältnismäßig erschwert" wäre. Bemerkenswert ist, dass auch Telefon- und Mailverbindungen Dritter überwacht werden können, wenn der Verdacht besteht, dass die Anschlüsse durch eine die Sicherheit gefährdende Person benutzt werden. Auch dem Berufsgeheimnis unterstehende Personen (wie Ärzte oder Anwälte) können grundsätzlich überwacht werden. Vorgesehen sind weiter verdeckte Untersuchungen von Wohnungen, Fahrzeugen oder anderen Räumen, der Einsatz von Richtmikrophonen, Wanzen und weiteren technischen Mitteln, Leibesvisitationen (auch unter Verschleierung der Gründe), die Beschaffung elektronisch gespeicherter Daten, das Eindringen in gesicherte Datenverarbeitungssysteme oder der Einsatz von mit einer Legende ausgestatteten Personen. Zur Erkennung oder Abwehr einer konkreten Terrorgefahr sind sämtliche Behörden und Amtsstellen des Bundes und der Kantone sowie weitere Organisationen und Anstalten, die öffentliche Aufgaben wahrnehmen, zur Auskunftserteilung verpflichtet, wobei amtliche Geheimhaltungspflichten außer Kraft gesetzt werden.
Zur Anordnung dieser Maßnahmen ist grundsätzlich das Bundesamt zuständig, teilweise ist aber eine Genehmigung durch eine vom Bundesrat gewählte unabhängige „Fachkommission" notwendig. Auskunfts- oder Einsichtsrechte für Betroffene sind nicht vorgesehen.
Diese Maßnahmen sind in verschiedener Hinsicht bedenklich:
- Erstens sind die Eingriffsvoraussetzungen denkbar unscharf umschrieben, so dass die Voraussetzungen für das Persönlichkeitsrecht ggf. sehr weitgehend beeinträchtigende Maßnahmen nicht klar umschrieben sind.
- Zweitens ist das Fehlen richterlicher Genehmigung zu beanstanden; die Entscheidung zur Durchführung der Maßnahmen ist sehr exekutivlastig.
- Drittens und mit dem vorherigen Punkt in engem Zusammenhang stehend ist darauf hinzuweisen, dass die geplanten Maßnahmen präventivre Natur sind und außerhalb eines Strafverfahrens auch gegen Personen ergriffen werden können, gegen die kein konkreter Verdacht auf strafbares Verhalten besteht.
- Schließlich steht das völlig fehlende Auskunfts-, Einsichts- und Berichtigungsrecht der Betroffenen in diametralem Gegensatz zu grundlegenden datenschutzrechtlichen Anforderungen.

Vielmehr soll die Problematik ausgehend von den entsprechenden Bestrebungen auf der Ebene der Europäischen Union erörtert werden, womit dann auch die hier auf der Grundlage verfassungsrechtlichen Grundentscheidungen zu beachtenden Leitlinien formuliert werden können[23].

Ausgangspunkt der Bestrebungen der EU im Hinblick auf den Erlass spezifischer Maßnahmen zur Terrorismusbekämpfung war das sog. Haager Programm[24], in dem der Europäische Rat im Anschluss an die bisherigen Bemühungen der Zusammenarbeit in der EU und unter dem Eindruck der Anschläge vom 11.9.2001 in den USA und vom 11.3.2004 in Madrid die Prioritäten für die Tätigkeit der Union im Hinblick auf die Sicherstellung der öffentlichen Sicherheit und der Bekämpfung der (internationalen) Kriminalität sowie des Terrorismus formuliert.

Im Zentrum des Haager Programms stehen der Einbezug biometrischer Identifikatoren in den Reisedokumenten, Visa, Aufenthaltstiteln und Reisepässen, der verbesserte Austausch von strafverfolgungsrelevanten Informationen zwischen den Mitgliedstaaten sowie ein gemeinsames Konzept

22 Vgl. NZZ vom 19.8.2005, S. 13.

23 Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, ABl. 20045 C 53, 1.

24 Vgl. insoweit unten III.1.c).

zur Verwendung von Passagierdaten für die Zwecke der Grenz- und Luftverkehrssicherheit sowie für Strafverfolgungszwecke.
Das Haager Programm – das im Juni 2005 vom Europäischen Rat bekräftigt wurde[25] – bildete dann die Grundlage für den Aktionsplan der Kommission vom 17. Juni 2005, in dem diese ein Paket konkreter Maßnahmen, einschließlich eines Zeitplans für deren Erlass bzw. Umsetzung formulierte. Die Schwerpunkte liegen hier in erster Linie – neben der allgemeinen Vertiefung der Zusammenarbeit – auf der Bekämpfung der Terrorismusfinanzierung und der Einführung verschiedener Überwachungsinstrumente, wie etwa die noch zu erörternde Vorratsspeicherung von Telekommunikationsdaten.
Der Vollständigkeit halber sei in diesem Zusammenhang auch noch auf die Erklärung des Europäischen Rates zum Kampf gegen den Terrorismus vom 25.3.2004 hingewiesen, in dem unter dem Eindruck der Anschläge in Madrid vom 11.3.2004 versichert wird, dass alles getan werden solle, um im Einklang mit den Grundprinzipien der Union, der Satzung der Vereinten Nationen und den Verpflichtungen im Rahmen der Resolution 1373/2001 des Sicherheitsrates alle Formen des Terrorismus zu bekämpfen. An konkreten Maßnahmen werden insbesondere Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter, der Austausch von Informationen über die Verurteilung wegen terroristischer Straftaten, die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten, die Einführung des Europol-Informationssystems sowie die Fertigstellung von SIS II erwähnt.

Auf dieser Grundlage wurden eine Reihe von Maßnahmen vorgeschlagen bzw. verabschiedet, die durchweg auch Aspekte des Datenschutzes betreffen. Im Folgenden sollen beispielhaft die Vorratsspeicherung von Telekommunikationsdaten und der Informationsaustausch zwischen nationalen Strafverfolgungsbehörden herausgegriffen werden.

aa) Vorratsspeicherung von Telekommunikationsverkehrsdaten

Auf Initiative von Großbritannien, Frankreich, Irland und Schweden wurde ein Entwurf für einen auf Art. 31 Abs. 1 lit. c) und Art. 34 Abs. 2 lit. b EUV gestützten Vorschlag eines Rahmenbeschlusses über die Vorratsspeicherung von Telekommunikationsdaten eingebracht[26], der vom Europäischen Parlament insgesamt sehr kritisch aufgenommen wurde[27]. Der Rat befasste sich mit der Initiative im Juni 2005 und formulierte einen Vorschlag für einen entsprechenden Rahmenbeschluss[28], dessen Eckpunkte wie folgt zusammengefasst werden können:

- Der Rahmenbeschluss soll nur auf sog. Kommunikationsdaten anwendbar sein, worunter Verkehrs- und Standortdaten i.S.d. Art. 2 RL 2002/58[29], Nutzer- und Teilnehmerdaten zu verstehen sind. Unter die beiden letzteren fallen persönliche Daten einer natürlichen oder juristischen Person, die einen öffentlich zugänglichen

---

25 Nachweis?

26 Vgl. Ratsdokument 8958/04 vom 28.4.2004. Hierzu die Bemerkungen m.w.N. bei *Peter Gola/Christoph Klug,* Die Entwicklung des Datenschutzrechts in den Jahren 2004/2005, NJW 2005, 2434 (2439).

27 Vgl. Stellungnahme des EP vom 7.6.2005. Hingewiesen wurde insbesondere auf die nach Ansicht des EP unzutreffende Rechtsgrundlage (statt der Dritten Säule sei Art. 95 EGV einschlägig) sowie die Unverhältnismäßigkeit des vorgeschlagenen Rahmenbeschlusses und seine Unvereinbarkeit mit Art. 8 EMRK.

28 Vgl. Ratsdokument 10609/05 vom 29.6.2005.

29 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 v. 31.07.2002, 37.

elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt oder abonniert hat. Der Rahmenbeschluss soll keine Anwendung auf die Inhalte der Kommunikation finden (Art. 1, 2 des Entwurfs).

- Art. 3 des Entwurfs enthält eine Mindestliste der zu speichernden Daten, insbesondere zur Rückverfolgung der Quelle und des Ziels sowie der Kommunikationsart erforderliche Daten.
- Art. 4 i.V.m. Art. 8 des Entwurfs legt die Fristen für die Vorratsspeicherung fest: Grundsätzlich sind die Daten während 12 Monaten (ab Erzeugung) zu speichern; eine Ausdehnung auf 48 Monate ist möglich (aber durch die Mitgliedstaaten nicht zwingend vorzusehen), wenn dies eine verhältnismäßige Maßnahme innerhalb einer demokratischen Gesellschaft ist. Umgekehrt können die Mitgliedstaaten den Zeitraum der Speicherung auf sechs Monate reduzieren, wenn eine längere Speicherung für den betreffenden Mitgliedstaat nicht akzeptabel ist. Unter ganz besonderen Umständen (wenn die betreffenden Daten üblicherweise für weniger als sieben Tage für kommerzielle Zwecke gespeichert werden) kann ein Mitgliedstaat ausnahmsweise eine Speicherung für weniger als sechs Monate vorsehen.
- Art. 5 des Entwurfs verweist auf die Maßgeblichkeit der RL 95/46[30] und der RL 2002/58 und gibt den Mitgliedstaaten auf, geeignete Sicherheitsvorkehrungen zu treffen und dafür zu sorgen, dass die Daten nach Ablauf der Speicherzeit gelöscht werden.
- Art. 6 des Entwurfs regelt den Zugang zu den gespeicherten Daten, wobei folgende Aspekte von Bedeutung sind:
  - Der Zugang von Behörden ist nur für „specified, explicit and legitimate pruposes“ von Fall zu Fall zulässig, wobei aber das nationale Recht maßgeblich ist.
  - Das Verfahren für den Zugang ist durch nationales Recht zu regeln.
  - Der Zugang ist unter Beachtung des Verhältnismäßigkeitsgrundsatzes zu gewähren.
  - Der Rechtsweg ist entsprechend der RL 95/46 zu gewähren, was auch den Rechtsschutz der Betroffenen einschließt.
- Art. 7 des Entwurfs gibt den Mitgliedstaaten auf, entsprechend den einschlägigen gemeinschaftlichen Regelungen im Bereich der justiziellen Zusammenarbeit in Strafsachen die nach dem Rahmenbeschluss gespeicherten Daten anderen Mitgliedstaaten zu kommunizieren, womit die Verbindung zu dem sogleich zu behandelnden Informationsaustausch zwischen nationalen Strafverfolgungsbehörden hergestellt wird.

Der Rahmenbeschluss soll noch im Jahr 2005 verabschiedet werden, wobei sich die Diskussion auf die Liste der zu speichernden Kommunikationsdaten, die Ausnahmen zu den

---

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

Vorratsfristen, Kosten und Nutzen der Vorratsspeicherung sowie die Datensicherheit konzentrieren soll.

bb) Informationsaustausch zwischen nationalen Strafverfolgungsbehörden

Hier sind insbesondere drei geplante Rechtsakte von Bedeutung:

- Der Vorschlag für einen Rahmenbeschluss des Rates über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafverfahren[31] zielt letztlich auf eine Vereinfachung (bzw. besser Abschaffung in dem durch den Rahmenbeschluss gedeckten Bereich und Ersetzung durch das in dem Vorschlag vorgesehene Verfahren) der Rechtshilfe. Ihr Grundprinzip ist demjenigen des Europäischen Haftbefehls nachgebildet[32] und geht dahin, dass die europäische Beweisanordnung – worunter eine von einer zuständigen Behörde eines Mitgliedstaats erlassene justizielle Entscheidung, die die Erlangung von Sachen, Schriftstücken und Daten anordnet, zu verstehen ist – von jedem anderen Mitgliedstaat ohne erneute Rechtmäßigkeitsprüfung nach dem Grundsatz der gegenseitigen Anerkennung zu vollziehen ist. Allerdings sind bestimmte Bereiche ausgenommen (Art. 3). Somit soll es der Rahmenbeschluss erlauben, in allen Strafverfahren eine Beweisanordnung zu erlassen mit der Folge, dass der „Vollstreckungsstaat" die geforderten Schriftstücke, Daten oder sonstige Beweisstücke ohne nähere Prüfung (insbesondere der doppelten Strafbarkeit) zu übermitteln hat, wenn die Voraussetzungen des Art. 16 des Vorschlags vorliegen, es also insbesondere um eine im Katalog aufgeführte Straftat geht, wobei diese Tatbestände teilweise sehr weit und wenig präzise gefasst sind (z.B. Beteiligung an einer kriminellen Vereinigung, Rassismus und Fremdenfeindlichkeit) und die Liste im Übrigen sehr lang ist. Der „Anordnungsstaat" kann die erlangten Beweisstücke verwenden, ohne sich um die Art und Weise der Erlangung der Beweise kümmern zu müssen. Darüber hinaus können personenbezogene Daten auch für sonstige justizielle oder verwaltungsbehördliche Verfahren, die mit den Verfahren, für die eine Europäische Beweisanordnung erlassen wurde, unmittelbar zusammenhängen, oder zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit verwendet werden, womit das ansonsten in der Rechtshilfe zur Anwendung kommende Spezialitätsprinzip nicht unerheblich verwässert werden dürfte.
- Eine Initiative Schwedens vom November 2004[33] zielt auf die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten (insbesondere in Bezug auf

---

31 KOM 2003, 688 endg.

32 Zu diesem bzw. dessen Entwurf aus rechtsstaatlicher Sicht sehr kritisch *Bernd Schünemann,* Europäischer Haftbefehl und EU-Verfassungsentwurf auf schiefer Ebene, ZRP 2003, 185 ff.

33 Vgl. ABl. 2004 C 281, 5 ff.

schwerwiegende Straftaten einschließlich terroristischer Handlungen) ab. Sie ist auf die polizeiliche Zusammenarbeit beschränkt und enthält eine Verpflichtung der Mitgliedstaaten, Informationen und Erkenntnisse im Besitz der nationalen Strafverfolgungsbehörden anderen Mitgliedstaaten auf Ersuchen zur Verfügung zu stellen (nach Art. 8 kann der Austausch aber auch spontan erfolgen). Diese Verpflichtung bezieht sich auf Straftaten, die nach den Rechtsvorschriften des ersuchenden Mitgliedstaats mit einer Freiheitsstrafe im Höchstmaß von mindestens 12 Monaten bedroht sind, wobei die Mitgliedstaaten auch darüber hinaus den Informationsaustausch vorsehen können. Bei einer sehr langen Liste von Straftaten (die sich weitgehend mit derjenigen des Vorschlags über die Europäische Beweisanordnung deckt) müssen die Mitgliedstaaten die Informationen und Erkenntnisse innerhalb von 12 Stunden übermitteln (können). Art. 6 des Vorschlags betrifft die Zulässigkeit des Austauschs von personenbezogenen Informationen und Erkenntnissen: Dieser Austausch ist unter eher weit gefassten Voraussetzungen zulässig (Verdacht, eine Straftat des Katalogs begangen zu haben oder zukünftig zu begehen oder Bestehen von konkreten Gründen für die Annahme, dass der Austausch von Informationen oder Erkenntnissen notwendiger Bestandteil der strafrechtlichen oder nachrichtendienstlichen Ermittlung zur Aufdeckung der in der Liste enthaltenen Straftaten, zu ihrer Verhütung oder zur Durchführung von Ermittlungen darstellt, Identifizierung der unter die vorherigen Kategorien fallenden Personen). Die Verwendung personenbezogener Daten ist in paralleler Weise wie in dem Vorschlag zur Europäischen Beweisanordnung geregelt.

- Schließlich ist der Vorschlag der Kommission für einen Beschluss des Rates über den Informationsaustausch und die Zusammenarbeit betreffend terroristische Straftaten[34] zu nennen. Dieser auf Art. 29, 30 Abs. 1, 31, 34 Abs. 2 lit. c) EUV gestützte Vorschlag sieht einen sich auf alle Phasen des Strafverfahrens erstreckenden Austausch von Informationen betreffend Ermittlungen, strafrechtliche Verfolgungen oder Verurteilungen wegen terroristischer Straftaten[35] vor. Bestimmte, in Art. 2 Abs. 4 aufgeführte Informationen sind spontan an Europol und Eurojust gemäß den innerstaatlichen Vorschriften zu übermitteln; im Übrigen ist gemäß den innerstaatlichen Rechtsvorschriften eine Übermittlung an Behörden anderer Mitgliedstaaten sicherzustellen.

b) Insbesondere: Datenschutz: und Schengener Informationssystem (SIS)

---

34 KOM 2004, 221 endg.

35 Wobei auf die Definition in den Art. 1-3 des Rahmenbeschlusses 2002/475/JI des Rates zur Terrorismusbekämpfung (ABl. 2002 L 164, 3) Bezug genommen wird.

Spezielle datenschutzrechtliche Probleme im Zusammenhang mit der internationalen Sicherheit stellen sich bei der Einrichtung von internationalen Datenbanken im Hinblick auf die Bekämpfung von Kriminalität. Dieser Problemkreis soll anhand des im Rahmen der EU bestehenden Schengener Informationssystems (SIS) aufgezeigt werden. Das SIS ist eine umfassende Datenbank zum Zwecke der Personen- und Sachfahndung[36]. Zielsetzung des SIS, das nach dem Wegfall der Grenzkontrollen als notwendige „Ersatzmaßnahme" konzipiert wurde[37], ist die Verbesserung der Verbrechensbekämpfung in den Schengen-Staaten mittels eines bis dahin nicht existierenden grenzüberschreitenden Sicherheitssystems[38].

Die Vorschriften über das SIS finden sich in Titel IV (Art. 92 ff.) des Schengener Durchführungsübereinkommens (SDÜ).
Nach Art. 92 SDÜ besteht das SIS aus einem nationalen Teil (National Schengen Information System, N-SIS), den jede Vertragspartei in eigener Verantwortung und auf eigene Kosten errichtet und unterhält (Art. 119 Abs. 2 SDÜ), und einer „technischen Unterstützungseinheit" (Central Schengen Information System, C-SIS), einem Zentralrechner, der der Online-Übermittlung der Informationen an die nationalen Bestände dient[39]. Diese Zentrale ist in Straßburg errichtet worden[40]. Sie steht in gemeinsamer Verantwortung und wird gemeinsam finanziert[41]. Ihre Aufgabe ist es vor allem, einen inhaltlich identischen Bestand an Daten zu gewährleisten (Art. 92 Abs. 3 SDÜ).
Derzeit wird das SIS von 15 Staaten eingesetzt, wobei mit Island und Norwegen auch zwei Nicht-EU-Mitgliedstaaten beteiligt sind. Großbritannien und Irland sind seit 2004 teilweise eingebunden, und auch die neuen EU-Mitgliedstaaten sollen bis 2007 an das System angeschlossen werden. So entsteht ein Fahndungsraum mit 27 Mitgliedstaaten und rund 450 Millionen Einwohnern[42]. Mittlerweile gilt das SIS jedoch als technisch veraltet; zudem können nicht mehr als 18 Staaten technisch angebunden werden.[43] Daher ist geplant, es bis Mitte 2007 durch eine zweite Generation, das sog. SIS II, zu ersetzen[44].

Mit Blick auf die hier im Vordergrund stehende Problemstellung sei in erster Linie auf folgende Charakteristika des SIS hingewiesen[45]:

- Die Ausschreibung und Speicherung der Daten erfolgt nach nationalem Recht, wobei allerdings die Vorgaben des SDÜ zu beachten sind (Art. 104 SDÜ). Diese enthalten in

---

36 *Ruth Wehner*, 4. Kapitel: Die polizeiliche Zusammenarbeit zwischen den Schengen-Staaten unter besonderer Berücksichtigung des SIS, in: Alberto Achermann/Roland Bieber/Astrid Epiney/Ruth Wehner, Schengen und die Folgen – Der Abbau der Grenzkontrollen in Europa, 1995, 129 (133); *Rainer Oberleitner*, Schengen und Europol – Kriminalitätsbekämpfung in einem Europa der inneren Sicherheit, 1998, 74.

37 Zu diesem Ansatz *Hans Claudius Taschner*, Schengen – Die Übereinkommen zum Abbau der Personengrenzkontrollen an den Binnengrenzen von EU-Staaten, 1997, 43.

38 *Astrid Epiney/Annekathrin Meier/Sarah Theuerkauf*, „Schengen": Ein neuer Prüfstein für die Schweiz, Plädoyer 2005, 38 (42).

39 *Wehner*, in: Schengen und die Folgen (Fn.), 129 (133 ff.).

40 *Nikolaos Lavranos*, Datenschutz in Europa – am Beispiel der Datenschutzrichtlinien, des Schengen Information System (SIS) und Europol, DuD 1996, 400 (403).

41 *Taschner*, Schengen (Fn.), 43.

42 *Epiney/Meier/Theuerkauf*, Plädoyer 2005 (Fn.), 38 (43).

43 Vgl. Rz. 2 des Beschlusses 2001/886/JI des Rates vom 6.12.2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II), Amtsblatt L 328 v. 13.12.2001, 1; bzw. Rz. 2 der VO (EG) 2424/2001 des Rates vom 6.12.2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 328 v. 13.12.2001, 4.

44 Vgl. auch den Bericht der Kommission über die Entwicklung des SIS II, KOM/2001/0720 endg. sowie die Mitteilung der Kommission an den Rat und das Europäische Parlament über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) und mögliche Synergien mit einem künftigen Visa-Informationssystem (VIS), KOM/2003/0771 endg.

45 Es ist hier hingegen nicht der Ort, im Einzelnen die Funktionsweise des SIS zu erläutern. Vgl. umfassend zu diesem System im Zusammenhang mit datenschutzrechtlichen Garantien etwa *Oberleitner,* Schengen und Europol (Fn.), 74 ff.; *Viethen,* Datenschutz als Aufgabe der EG (Fn.), 52 ff.

Art. 92 ff. SDÜ insbesondere die Datenkategorien sowie die Angaben, die über Personen gespeichert werden dürfen. Bemerkenswert ist hier insbesondere, dass bestimmte Kategorien, so insbesondere diejenige zur verdeckten Registrierung (Art. 99 SDÜ), sehr offen formuliert sind.

- Die ausschreibende Vertragspartei ist auch für die Richtigkeit und Aktualität der Daten verantwortlich (Art. 105 SDÜ, für die Änderung, Ergänzung, Berichtigung oder Löschung s. Art. 106 SDÜ).
- Art. 112, 113 enthalten Vorschriften über die maximale Speicherdauer: Danach dürfen die zur Personenfahndung im SIS aufgenommenen Daten nicht länger als für den verfolgten Zweck erforderlich gespeichert werden. Spätestens drei Jahre nach ihrer Einspeicherung ist dies zu überprüfen. Für alle anderen Daten bestimmt Art. 113 SDÜ die maximalen Speicherfristen, die je nach betroffenem Gegenstand drei bis zehn Jahre betragen. Gelöschte Daten bleiben noch ein Jahr in der technischen Unterstützungseinheit C-SIS gespeichert (Art. 113 Abs. 2 SDÜ).
- Das Zugriffsrecht auf das SIS ist relativ weit gehalten; insbesondere haben alle Grenzkontrollbeamten und alle Polizeistationen im Schengen-Raum einen umfassenden Zugriff (Art. 101 SDÜ).
- Nach Art. 102 SDÜ unterliegt die Nutzung der im SIS gespeicherten Daten einer Zweckbindung, so dass die Daten nur für die der jeweiligen Ausschreibung entsprechenden Zwecke genutzt werden dürfen (Art. 102 SDÜ).
- Das SDÜ enthält auch Rechte Betroffener, so insbesondere das Recht, die Kontrollinstanzen zu ersuchen, die zu seiner eigenen Person im SIS gespeicherten Daten sowie deren Nutzung überprüfen zu lassen (Art. 114 Abs. 2 SDÜ), einen Auskunftsanspruch über die zu seiner Person gespeicherten Daten, der nach nationalem Recht geltend zu machen ist, aber unter gewissen Voraussetzungen zu verweigern ist (Art. 109 SDÜ), und einen Anspruch auf Berichtigung unrichtiger Daten bzw. Löschung unrechtmäßig gespeicherter Daten (Art. 110 SDÜ).

c) Schlussfolgerung

Versucht man vor dem Hintergrund der Grundprinzipien des Datenschutzes eine notwendigerweise vorläufige und partielle (da neben dem Datenschutz auch noch andere Aspekte eine Rolle spielen) Bewertung der skizzierten Bestrebungen in der EU auf dem Gebiet der Kriminalitäts- und Terrorismusbekämpfung, so erscheinen zwei Aspekte von besonderer Bedeutung:

- Was die einzelnen Maßnahmen betrifft, so fällt in Bezug auf die geplante Vorratsspeicherung von Telekommunikationsdaten auf, dass hier eine Unmenge von Daten eben „auf Vorrat“ zu speichern ist. Ob und inwieweit diese Maßnahme – die

einen nicht unerheblichen Eingriff in die Privatsphäre der Betroffenen darstellt – aber tatsächlich geeignet und erforderlich ist, um die Zielsetzung des Rahmenbeschlusses (Bekämpfung von Terrorismus und organisierter Kriminalität) zu erreichen, bleibt offen. Hinzuweisen ist insbesondere – angesichts des Volumens der gespeicherten Daten – auf die Unmöglichkeit, die Daten wirklich alle zu evaluieren; im Übrigen dürfte es den wirklich mit der Maßnahme anvisierten Personen möglich sein, die Speicherung zu umgehen (etwa durch Benutzung verschiedener Telephone, den Rückgriff auf öffentliche Fernsprecher oder die Änderung der Mailadressen). Vor diesem Hintergrund dürfte die Vereinbarkeit des geplanten Rahmenbeschlusses mit Art. 8 EMRK mehr als zweifelhaft sein.

In Bezug auf die in Aussicht gestellten Maßnahmen zum Informationsaustausch bzw. zur Informationsübermittlung und Sicherstellung von Beweisen ist – wie schon teilweise angedeutet – bemerkenswert, dass für eine in Teilen sehr offen formulierte Liste von Straftaten ein justizieller oder polizeilicher „Informationsaustausch" zu gewähren ist, der vollumfänglich auf dem Prinzip der „gegenseitigen Anerkennung" – ein Grundsatz, der im Zusammenhang mit den Grundfreiheiten entwickelt wurde – beruht. Dieser Ansatz führt insofern zu (potentiell) bedenklichen Resultaten, als damit die justiziellen oder polizeilichen Behörden in einem Mitgliedstaat zu Beweisstücken oder Erkenntnissen kommen können, die nach dem Recht des Herkunftsstaats der Beweisstücke oder Erkenntnisse entweder nicht übermittelt werden dürfen oder sich gar – aufgrund der offenen Formulierung der Tatbestände – auf Straftaten beziehen, die im Herkunftsstaat nicht strafbar sind. Aber auch umgekehrt kann durch diese Verpflichtung zur Informations- und Beweisstückübermittlung der Empfangsstaat zu Erkenntnissen oder Beweisstücken kommen, die er nach seinem nationalen Recht nicht hätte erheben dürfen.

- Nimmt man nun die vorgesehene Vorratsspeicherung von Daten und die geplanten Pflichten zur Übermittlung von Beweisstücken und Erkenntnissen zusammen, so erweitert sich der potentielle Bezugspunkt der Übermittlungspflichten ganz erheblich, ohne dass jedoch die Grundsätze für die Erhebung von Beweisstücken oder Erkenntnissen und die hier zum Zuge kommenden spezifischen datenschutzrechtlichen Prinzipien merklich angeglichen werden; insbesondere findet die RL 95/46 im Bereich der „Dritten Säule" keine Anwendung. Es bleibt fraglich, ob und inwieweit eine Internationalisierung der Informationserhebung und des Informationsaustauschs ohne eine in gleichem Ausmaß erfolgende Internationalisierung der Rechte der Betroffenen und des Datenschutzes rechtsstaatlichen Grundanliegen zu genügen vermag[46].

[46] Hingewiesen sei in diesem Zusammenhang auch auf die Ausführungen von *Thilo Weichert,* Datenschutz bei föderaler Polizeikooperation in Deutschland – und in Europa, 3 (zitiert nach den Folien), der davon spricht dass es eine „rasante Entwicklung" bei Befugnissen und Einführung von Informationssystemen zur Bekämpfung von Terrorismus und (internationaler) Kriminalität gebe, die nicht von einer „rasanten Entwicklung" in den Bereichen Rechtsschutz, Datenschutz und Kontrolle begleitet werde.

- Dieser Befund wird durch einen Blick auf die speziell bei „internationalisierten Datenbanken“ (wie dem SIS) entstehenden Problemen bestätigt: Dieses System „internationalisiert“ zwar den Zugriff auf die dort gespeicherten Daten; die Voraussetzungen für die Speicherung sowie die Rechte der Betroffenen sind jedoch nur ansatzweise und zudem teilweise in sehr offener Form „harmonisiert“. Dies impliziert, dass Personen Zugriff auf Daten haben, die nach ihrem nationalen Recht gar nicht hätten gespeichert werden dürfen, wird doch die Erhebung der zu speichernden Daten sowie die Zulässigkeit der Ausschreibung nur lückenhaft geregelt, sieht man einmal von den allerdings teilweise sehr offen formulierten Datenkategorien ab. Auch wird bei den Rechten der Betroffenen auf das nationale Recht verwiesen. Insgesamt wird damit die Frage aufgeworfen, ob eine Internationalisierung der Datenspeicherung und des Datenzugriffs nicht mit einer vollumfänglichen oder zumindest weitgehenden Internationalisierung der Rechte der Betroffenen und der datenschutzrechtlichen Standards einhergehen müsste.

Als Schlussfolgerung aus dieser notwendigerweise knappen (und auch lückenhaften[47]) Bestandsaufnahme und Bewertung der polizeilichen und justiziellen Zusammenarbeit in der EU drängen sich m.E. im Hinblick auf die Sicherstellung von Belangen des Datenschutzes folgende Anliegen auf, die hier nur stichwortartig erwähnt werden können:

- Im selben Ausmaß, wie internationale Zusammenarbeit im Hinblick auf den Austausch von Daten eingeführt wird, sind die datenschutzrechtlichen Grundsätze anzugleichen. Dies impliziert letztlich ein einheitliches Datenschutzrecht in den Mitgliedstaaten, und nicht – wie sie heute immer noch besteht – eine Vielzahl unterschiedlicher Vorschriften, die zudem teilweise offen formuliert und lückenhaft sind, für die verschiedenen Instrumente.
- Bei der Definition dieser Standards ist insbesondere auf die Wahrung der Zweckbindung die der Erforderlichkeit zu achten; weiter sind die Beteiligungs- und Betroffenenrechte nach vereinheitlichten Standards zu gewährleisten.
- Die Wahrung der datenschutzrechtlichen Anforderungen ist durch die Einrichtung eines unabhängigen Kontrollverfahrens, durchgeführt durch eine unabhängige Stelle, sicherzustellen.

2. Aktualität der anerkannten datenschutzrechtlichen Grundsätze angesichts neuer technologischer Entwicklungen

Ein weiterer Aspekt, der in den Diskussionen an dieser Konferenz in der einen oder anderen Form immer wieder problematisiert wurde, ist die Frage, ob und inwieweit die bestehenden

[47] Konnten doch eine Reihe von Instrumenten auf EU-Ebene nicht beleuchtet werden, so etwa der Datenaustausch in Arbeitsgruppen oder im Rahmen von Europol.

(nationalen und internationalen) datenschutzrechtlichen Regeln und Grundsätze den Herausforderungen der sehr raschen technologischen Entwicklungen Rechnung zu tragen vermögen[48]. Hier drängen sich aus meiner Sicht – ausgehend von den Diskussionen – in erster Linie zwei Bemerkungen auf:

- Erstens besteht keinerlei Anlass, die datenschutzrechtlichen Grundsätze angesichts der technologischen Entwicklungen zu relativieren, im Gegenteil: Aufgrund dieser Entwicklungen sind heute Eingriffe und Gefahren – sowohl von staatlicher als auch von privater Seite – möglich, die noch vor wenigen Jahren undenkbar waren und die letztlich die Grundanliegen des Datenschutzes (Schutz des Persönlichkeitsrechts der Betroffenen, öffentliches Interesse[49]) herausfordern. Beispielhaft sei etwa auf die Speicherkapazitäten oder die sinkende Kontrolle über die eigene Kommunikation hingewiesen. Insofern ist nachdrücklich zu betonen, dass die sich in den letzten rund 30 Jahren herausgebildeten und durch Praxis und Rechtsprechung präzisierten datenschutzrechtlichen Grundsätze auch dann umfassend zu gewährleisten sind, wenn es um durch neue technologische Entwicklungen ermöglichte Eingriffe geht, auch wenn dies gelegentlich auf Schwierigkeiten stoßen mag[50].

  Es ist daher nachdrücklich zu fordern, dass die effektive Beachtung der zentralen datenschutzrechtlichen Grundsätze auch im Zeitalter der „Informationsgesellschaft" sichergestellt wird. Von besonderer Bedeutung sind dabei folgende Grundsätze:
  - Grundsatz der Gesetzmäßigkeit;
  - Grundsatz der Richtigkeit der Daten;
  - Grundsatz der Zweckbindung;
  - Grundsatz der Verhältnismäßigkeit;
  - Grundsatz der Transparenz;
  - Grundsatz der Beteiligung und Zugangsrecht der Betroffenen;
  - Grundsatz der Datensicherheit;
  - Grundsatz der unabhängigen Kontrolle.

- Zweitens – und damit in engem Zusammenhang stehend – impliziert diese Maßgeblichkeit „traditioneller" datenschutzrechtlicher Grundsätze, dass sie im Hinblick auf die sich stellenden technologischen Herausforderungen operationalisiert werden (müssen), m.a.W.: Der Bedeutungsgehalt der jeweiligen Grundsätze ist konkret in Bezug zu den sich stellenden technischen Möglichkeiten und setzen und entsprechend im Hinblick auf die dadurch aufgeworfenen Probleme zu konkretisieren. Diese Konkretisierung hat natürlich zunächst auf nationaler Ebene zu erfolgen, ist aber supra- und international zu koordinieren, worauf sogleich einzugehen sein wird[51].

---

48 Vgl. hierzu etwa die Bemerkungen bei *Emilio Aced Félez*, The Future of Private Data in Private Companies, in Bezug auf private Gesellschaften; *Yves Poullet/Jean-Marc Dinant,* Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, T-PD (2004) final, in Bezug auf die Frage der Anpassung der Konvention des Europarates angesichts der technischen Entwicklungen. S. auch den *John Karat/Clare-Marie Karat/Carolyn Brodie/Jinjuan Feng,* Privacy in Information Technology: Designing to Enable Privacy Policy Management in Organizations.

49 Hierzu oben II.

50 Zur Frage der rechtlichen Absicherung noch unten IV.

51 Unten IV.

Jedenfalls ist zu fordern, dass geeignete Präzisierungen vorgenommen werden und diese implementiert werden, um den technologischen Entwicklungen Rechnung tragen zu können[52]. Zu denken ist hier an einige Anpassungen der grundlegenden rechtlichen Vorgaben, die sich aber – angesichts der nach wie vor aktuellen datenschutzrechtlichen Prinzipien – insgesamt in Grenzen halten dürften. Eher im Vordergrund stehen dürfte die Entwicklung spezifischer technischer Vorkehrungen, die in sehr unterschiedlichen Bereichen – so auch etwa in Firmen und Banken, in denen möglicherweise eine Vielzahl von Mitarbeitenden mit sensiblen Daten in Berührung kommen[53] – relevant werden können[54].

IV. Rechtliche Absicherung datenschutzrechtlicher Garantien

1. Kontrollmechanismen

Das Datenschutzrecht hat im Laufe der Jahre eine Reihe institutioneller Mechanismen entwickelt, die die Einhaltung datenschutzrechtlicher Garantien rechtlich absichern sollen. Selbstverständlich sind diese Garantien in den verschiedenen Staaten jeweils unterschiedlich ausgestaltet; gleichwohl haben sich gewisse Grundsätze entwickelt, die in der einen oder anderen Form in die meisten nationalen und internationalen datenschutzrechtlichen Instrumenten Eingang gefunden haben, wobei folgende von besonderer Bedeutung sind, die jedoch in diesem Zusammenhang nur stichwortartig zu erwähnen sind:

- Zugangs-, Auskunfts-, Berichtigungs- und Löschungsrechte der Betroffenen;
- Meldepflichten;
- Einrichtung von Kontrollinstanzen;
- Sanktionen;
- gerichtlicher Zugang für Betroffene.

Diese Rechte und Mechanismen sind nach wie vor von zentraler Bedeutung und jedenfalls aufrechtzuerhalten bzw. (teilweise) einzuführen und zu präzisieren.

Allerdings erscheinen sie aus mindestens drei Gründen nicht ausreichend:

- Erstens sind sie vom Ansatz her eher reaktiver Natur: Sie greifen im Wesentlichen erst dann, wenn Daten bereits erhoben, gespeichert und teilweise genutzt worden sind. Dies erscheint jedoch schon insofern unzureichend, als gerade das bereits erwähnte Verhältnismäßigkeitsprinzip davon ausgeht, dass bereits die Erhebung der Daten nur dann erfolgen soll bzw. darf, wenn dies zur Verfolgung des angestrebten Zwecks

---

52 Dies impliziert dann auch eine internationale Zusammenarbeit im Hinblick auf den Transfer entsprechenden technischen *know hows*, vgl. *Herbert Burkert*, Globalization – Strategies for Data Protection, 12 f. (zitiert nach Manuskript).

53 Zu diesem Problem etwa das Interview mit dem Eidgenössischen Datenschutzbeauftragten *Hanspeter Thür*, NZZ am Sonntag vom 3.7.2005, 31.

54 S. zur Durchführung auch noch die Ausführungen unten IV.1.

geeignet, erforderlich und angemessen ist. Weiter und damit in engem Zusammenhang stehend ist nicht zu verkennen, dass allein der Umstand, dass persönliche Daten vorhanden sind, eine Gefahr ihres Missbrauchs mit sich bringt, so dass mit Nachdruck daran zu erinnern ist, dass bereits die Erhebung und Speicherung persönlicher Daten nur in den skizzierten engen Grenzen ermöglicht werden soll. Insofern sollten datenschutzrechtliche Kontrollmechanismen auch vorbeugend ansetzen.

- Zweitens stellen sie in erster Linie auf das Interesse der Einzelnen an der Nichtbeeinträchtigung ihres Rechts auf Achtung der Privatsphäre ab, während der Aspekt des Datenschutzes als öffentliches Interesse nur am Rande (nämlich im Rahmen der Aufgabenumschreibung von Kontrollinstanzen und bei den Meldepflichten) berücksichtigt wird.
- Drittens schließlich bleiben einige der Kontrollinstrumente teilweise (wobei hier natürlich je nach Ausgestaltung große Variationen festzustellen sind) ineffektiv, da maßgeblich auf die Geltendmachung der Rechte von Betroffenen abgestellt wird, die häufig aus verschiedenen Gründen „überfordert“ sind, und allenfalls eingerichtete Kontrollinstanzen häufig in personeller und finanzieller Hinsicht weit unterdotiert sind, so dass sie ihre Aufgaben kaum wahrnehmen können und insbesondere eine eher umfassende Kontrolle, die unabhängig von an die Kontrollstellen herangetragenen konkreten Problemen erfolgt, kaum möglich ist.

Vor diesem Hintergrund drängt es sich m.E. auf, weitere Kontrollmechanismen bzw. einen Ausbau der bestehenden in Betracht zu ziehen, wobei die genannten Schwächen der derzeitigen Mechanismen den Ausgangspunkt der Überlegungen darstellen; der effektiven Durchsetzung des Anliegens des Datenschutzes in seiner Dimension als öffentliches Interesse soll im Übrigen besondere Aufmerksamkeit geschenkt werden. Konkret erscheinen insbesondere folgende Mechanismen als erwägenswert:

- Auf der Ebene der Rechtsetzung könnte eine Datenschutzvereinbarkeitsprüfung sicherstellen, dass (bestimmte) neue gesetzgeberische Instrumente tatsächlich die datenschutzrechtlichen Mindestanforderungen erfüllen. M.a.W. wäre bei der Neuregelung datenschutzrelevanter Gesetzgebungsvorlagen – wobei dieser Begriff bzw. die Ermittlung der Datenschutzrelevanz noch zu präzisieren wäre und auch in Erwägung gezogen werden könnte, diese Prüfung auf Antrag bestimmter Stellen oder Gremien durchzuführen – jeweils ein Verfahren durchzuführen, das (unter Einbezug unabhängiger Kontrollinstanzen) die Auswirkungen des Projekts auf datenschutzrelevante Anliegen prüft. Der Gesetzgeber müsste sodann zumindest insoweit in die Pflicht genommen werden, als er die Ergebnisse dieser Prüfung materiell zu berücksichtigen hätte. Eine solche Datenschutzvereinbarkeitsprüfung ermöglichte eine umfassende Würdigung der diesbezüglichen Aspekte gesetzgeberischer Vorhaben und trüge damit dazu bei, dass Anliegen des Datenschutzes im Gesetzgebungsverfahren

ausreichend berücksichtigt werden und nicht angesichts anderer, durchaus möglicherweise gerechtfertigter Prioritäten „untergehen".

- Weiter und damit in engem Zusammenhang stehend sollten neue Kommunikationstechnologien – wobei dieser Begriff und damit der materielle Anwendungsbereich des hier formulierten Postulats noch zu präzisieren wäre – vor ihrer Einführung (geschehe sie nun auf staatlicher oder auf privater Ebene) insofern auf ihre Vereinbarkeit mit datenschutzrechtlichen Anforderungen geprüft werden, als die Anwendung der jeweiligen Technologie nicht einen datenschutzrechtlichen Mindeststandard unterschreiten dürfte. M.a.W. müssten die Technologien so ausgestaltet sein, dass die grundlegenden datenschutzrechtlichen Prinzipien gewahrt werden. Damit wäre es möglich, im Vorfeld des Inverkehrbringens neuer Technologien ihre datenschutzrechtliche Vereinbarkeit zu untersuchen und damit vorbeugend zu verhindern, dass unvereinbare Technologien benutzt werden. Im Übrigen ist zu erwarten, dass sich auch die Technik im Falle der Existenz eines solchen Verfahrens schon bei der Entwicklung der Technologien auf diese Anforderungen einstellen würde. Die Heranziehung des Vorbeuge- oder Vorsorgegedankens in diesem Zusammenhang ist auch und gerade insofern ebenso sinnvoll wie notwendig, als nur auf diese Weise verhindert werden kann, dass in Bezug auf Belange des Datenschutzes „unsichere Technologien" zur Anwendung gelangen, deren Folgen und Auswirkungen man dann kaum noch abschätzen kann.

  Dabei wäre es hier insbesondere denkbar, dass – im Ansatz ähnlich wie die sog. „neue Konzeption" der EG im Bereich der Harmonisierung technischer Vorschriften und Normen zur Verwirklichung des Binnenmarkts[55] – private Normungsorganisationen beauftragt werden, die technischen Anforderungen in Normen zu präzisieren, die notwendig sind, um die oben erwähnten[56] grundlegenden datenschutzrechtlichen Mindestanforderungen einzuhalten. Auf diese Weise könnte einerseits erreicht werden, dass die durch den demokratisch legitimierten Gesetzgeber formulierten Vorgaben auch maßgeblich sind, andererseits aber auch sichergestellt werden, dass die technischen Anforderungen durch unter Einbezug des hier auch bei Privaten vorhandenen Sachverstands definiert werden.
- Ebenfalls in Bezug auf die Kontrolle ist in Erwägung zu ziehen, für bestimmte Unternehmen und bestimmte staatliche Stellen regelmäßige sog. Audits vorzusehen, die nach einem genau festzulegenden Verfahren unter Einbezug externer unabhängiger Experten die Überprüfung der Einhaltung der datenschutzrechtlichen Anforderungen zu sicherstellen können.

---

55 Hierzu nur, m.w.N., *Astrid Epiney/Hanspeter Pfenninger*, Auswirkungen eines Beitritts zur Europäischen Union auf das schweizerische Umweltrecht – das Problem der Umweltnormung, in: Thomas Cottier/Alwin Kopse (Hrsg.), Der Beitritt der Schweiz zur EU. Brennpunkte und Auswirkungen, 1998, 949 (951 ff.).

56 Oben III.2.

- Schließlich ist in Erwägung zu ziehen, nicht nur Betroffenen Klagerechte im Falle der (möglichen) Verletzung ihrer Rechte einzuräumen, sondern auch ausgewählten Nichtregierungsorganisationen – die dann einer Art Akkreditierung bedürften – die Legitimation zur Klage im Falle der Verletzung (bestimmter) datenschutzrechtlicher Grundsätze durch den Staat und Private einzuräumen. Auf diese Weise würde die Effektivität der datenschutzrechtlichen Regelungen verstärkt, und mit der Akkreditierung könnte sichergestellt werden, dass die Organisationen auch in der Lage sind, dieses Recht tatsächlich wahrzunehmen. Entsprechende flankierende Maßnahmen – insbesondere auch auf der Ebene der Kosten – könnten sicherstellen, dass ein solches Klagerecht nicht „missbraucht" würde.

Es ist selbstverständlich nicht zu verkennen, dass die Einführung solcher Mechanismen eine Reihe von Problemen aufwerfen würde, die von ihrem Anwendungsbereich über ihre Kontrolle bis hin zu dem im Einzelnen zu durchlaufenden Verfahren reichen. Gleichwohl lohnte es sich nach der hier vertretenen Ansicht, sie im Einzelnen zu prüfen, unter Einbezug der noch zu erarbeitenden konkreten Ausgestaltung, die sich selbstverständlich in die jeweilige Rechtsordnung einbetten müsste. Nur auf diese Weise dürfte nämlich sichergestellt werden können, dass datenschutzrechtliche Belange nicht Gefahr laufen, im Zuge der wechselnden politischen Prioritätensetzung (zu) viel an Gewicht und an Beachtung verlieren, was der Durchsetzung des Datenschutzes als öffentliches Interesse diametral entgegenliefe.

2. Rechtliche Absicherung datenschutzrechtlicher Garantien auf internationaler Ebene

Zum Schluss sei noch auf die Ebene der rechtlichen Absicherung datenschutzrechtlicher Garantien eingegangen. Bislang sind insbesondere folgende datenschutzrechtlichen Instrumente auf den verschiedenen internationalen und supranationalen Ebenen zu verzeichnen:

- Auf universeller Ebene sind insbesondere die von der Generalversammlung der Vereinten Nationen am 4.12.1990 angenommenen Richtlinien betreffend personenbezogene Daten in automatisierten Dateien[57] von Bedeutung[58]. Die Richtlinien enthalten allgemeine Grundsätze, die bei der nationalen Gesetzgebung in den Mitgliedstaaten der Vereinten Nationen berücksichtigt werden sollen[59]. Ziel der

[57] „*Guidelines for the Regulation of Computerized Personal Data Files*", Doc. E/CN.4/1990/72, angenommen durch die Generalversammlung in der Resolution 45/95 vom 4.12.1990. Im Internet abrufbar unter http://www.unhchr.ch/html/menu3/b/71.htm. Eine deutsche Version ist erhältlich unter http://www.datenschutz-berlin.de/recht/int/uno/gl_pbdde.htm.

[58] Vgl. zu diesen Richtlinien *Gridl,* Datenschutz in globalen Kommunikationssystemen (Fn.), 182 ff.; zur Entstehungsgeschichte und zum Entwurf *Reinhard Ellger,* Der Datenschutz im grenzüberschreitenden Datenverkehr, 1990, 564 ff. Die Rolle der Vereinten Nationen im Zusammenhang mit dem Datenschutz wurde auch an der Konferenz angesprochen, so insbesondere von *Maria Vicien-Milburn,* The United Nations and Personal Data Protection.

[59] Diese sollen auch auf personenbezogene Daten in den Dateien Internationaler Organisationen angewandt werden.

Richtlinien ist in erster Linie, den Datenschutzgedanken zu verbreiten und Impulse für die Rechtsetzung in den Mitgliedstaaten der Vereinten Nationen zu geben, die noch nicht über geeignete rechtliche Instrumente verfügen. Allerdings entfalten diese als solche völkerrechtlich keine Bindungswirkung, d.h. eine Pflicht zur tatsächlichen Umsetzung in innerstaatliches Recht besteht hier nicht[60]. Ihre Bedeutung bleibt damit – da die Voraussetzungen für ihre Anerkennung als Völkergewohnheitsrecht nicht vorliegen dürften – auf die Rolle eines bloßen rechtspolitischen Anhaltspunktes beschränkt[61], was auch insofern zu bedauern ist, als sie inhaltlich die zu beachtenden datenschutzrechtlichen Anforderungen in recht klarer Weise umschreiben.

- Am 23.9.1980 erließ der Rat der OECD Leitlinien für den Schutz der Privatsphäre und grenzüberschreitende Ströme personenbezogener Daten[62]. Diese sind jedoch völkerrechtlich nicht verbindlich und verpflichten daher auch nicht die OECD-Mitgliedstaaten zu einer Umsetzung in innerstaatliches Recht[63]. Inhaltlich zielen zielen die OECD-Leitlinien insgesamt eher auf die Liberalisierung des grenzüberschreitenden Datentransfers als auf den Schutz subjektiver Persönlichkeitsrechte ab; Datenschutzregelungen werden in erster Linie als potentielle Hindernisse des internationalen Datenaustauschs angesehen[64]. Zudem sind die Formulierungen der Leitlinien in weiten Teilen recht vage gehalten, so dass ihnen kaum präzise Vorgaben entnommen werden können und ihre Effektivität letztlich entscheidend von der „Umsetzungswilligkeit“ der Mitgliedstaaten abhängt. Diese Offenheit hat auf der anderen Seite aber auch den Vorteil, dass die Leitlinien auch im Zuge technologischer Weiterentwicklungen durchaus aktuell bleiben. Auch ist nicht zu verkennen, dass die Leitlinien einen – wenn auch nur geringen – Beitrag zur Harmonisierung der Rechtsordnungen der OECD-Mitgliedstaaten – insbesondere der europäischen Staaten – in Bezug auf den Schutz personenbezogener Daten geleistet und damit die Entwicklung des europäischen Datenschutzrechts mit beeinflusst haben.

---

60 *Reinhard Ellger*, Die Entwicklung des Datenschutzrechts in der Europäischen Union, in: Rolf H. Weber/Daniel Thürer/Roger Zäch (Hrsg.). Datenschutz im europäischen Umfeld, 1995, 1 (29); *Schaar*, Datenschutz im Internet (Fn.), Rz. 79; *Alexander Viethen*, Datenschutz als Aufgabe der EG – Bestandsaufnahme des datenschutzspezifischen Sekundärrechts und Analyse anhand der Kompetenzordnung des EG-Vertrages, 2003, 27; *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr (Fn.), 566; *Gridl*, Datenschutz in globalen Telekommunikationssystemen (Fn.), 183.

61 *Viethen*, Datenschutz als Aufgabe der EG (Fn.), 27.

62 „OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“; diese sind im Internet abrufbar unter http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html sowie unter http://www1.oecd.org/publications/e-book/9302011E.PDF. Eine deutsche Zusammenfassung ist erhältlich unter http://www.oecd.org/dataoecd/16/7/15589558.pdf. Zur Entstehungsgeschichte der Richtlinien: *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr (Fn.), 513 f.; *Burkert,* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.3, B, II, 1 (Fn.), Rz. 23.

63 *Ellger*, in: Datenschutz im europäischen Umfeld (Fn.), 1 (29); *Lavranos*, DuD 1996 (Fn.), 400 (401), m.w.N.

64 *Viethen*, Datenschutz als Aufgabe der EG (Fn.), 24; s. auch die eher kritischen Bemerkungen zu den Leitlinien vor diesem Hintergrund bei *Ellger,* Datenschutz im grenzüberschreitenden Datenverkehr (Fn.), 530 f.

- Weiter ist auf die Konvention Nr. 108 zum Schutz des Einzelnen im Hinblick auf die automatische Verarbeitung personenbezogener Daten[65] vom 28.1.1981 hinzuweisen[66]. Sie formuliert einen datenschutzrechtlichen Mindeststandard, der für alle Mitgliedstaaten verbindlich ist. Die Konvention trat am 1.10.1985 nach Hinterlegung der gemäß Art. 22 Abs. 2 erforderlichen fünf Ratifizierungsurkunden[67] in Kraft. Die Konvention ist die wichtigste – gleichzeitig erste und einzige rechtsverbindliche – völkerrechtliche Regelung im Bereich des Datenschutzes[68].

  Als sog. „offener Vertrag“[69] steht die DSK unter bestimmten formellen Voraussetzungen auch Nicht-Mitgliedern des Europarates zum Beitritt offen (vgl. Art. 23 DSK); bewusst wurde daher auf die offizielle Bezeichnung „Europäische Konvention“ verzichtet[70]. Bis heute[71] haben 32 Staaten die DSK ratifiziert; weitere sechs Staaten haben sie unterzeichnet[72]. Alle sind jedoch Mitglieder des Europarates, so dass das Konzept der „offenen“ Konvention hier offensichtlich nicht von Erfolg gekrönt war.
  Am 15.6.1999 wurde der Konventionstext in Hinblick auf einen möglichen Beitritt der Europäischen Gemeinschaften (EG) erweitert.[73] Am 8.11.2001 wurde die DSK durch das Zusatzprotokoll Nr. 181[74] ergänzt, das im Juli 2004 in Kraft getreten ist.

  Es ist hier nicht der Ort, ausführlich auf die Konvention einzugehen. Immerhin sei aber darauf hingewiesen[75], dass sie als erste internationale Konvention Regelungen zum Datenschutz enthält, die ihre Vertragsstaaten unmittelbar verpflichten. Gerade die Entwicklung in mittel- und osteuropäischen Staaten wurde durch die DSK und die nachfolgenden bereichsspezifischen Empfehlungen des Europarats entscheidend

---

65 Diese ist unter www.conventions.coe.int/ im Internet abrufbar. Eine deutsche Übersetzung ist abgedruckt in EuGRZ 1981, 378.

66 Der Europarat entfaltet aber auch weitere Aktivitäten auf diesem Gebiet, insbesondere durch den Erlass von Empfehlungen. Die Rolle des Europarates wurde denn auch auf der Konferenz diskutiert, vgl. insbesondere *Roberto Lamponi,* Le rôle du Conseil de l'Europe dans le respect du droit à la protection des données personnelles et de la vie privée.

67 Anfangs verlief der Ratifizierungsprozess etwas schleppend. Die ersten fünf Ratifizierungen erfolgten durch Frankreich, Norwegen, Schweden, Spanien und Deutschland, vgl. *Herbert Auernhammer*, Die Europäische Datenschutz-Konvention und ihre Auswirkungen auf den grenzüberschreitenden Datenverkehr, DuD 1985, 7 (7); *Viethen*, Datenschutz als Aufgabe der EG (Fn.), 31; *Gridl*, Datenschutz in globalen Telekommunikationssystemen (Fn.), 191.

68 *Auernhammer*, DuD 1985 (Fn.), 7 (7); *Schaar*, Datenschutz im Internet (Fn.), Rz. 84. Ausführlich zu der Konvention etwa *Gridl,* Datenschutz in globalen Kommunikationssystemen (Fn.), 190 ff.; *Ferdinand Henke,* Die Datenschutzkonvention des Europarates, 1986, *passim*; *Simitis,* in: BDSG-Kommentar (Fn.), Einleitung, Rz. 137 ff.; *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr (Fn.), 463 ff.; s. auch *Kübler,* Die Säulen der EU (Fn.), 37 ff.

69 Dazu *Alfred Verdross/Bruno Simma*, Universelles Völkerrecht, 3. Aufl., 1984, § 713.

70 Vgl. *Gridl*, Datenschutz in globalen Telekommunikationssystemen (Fn.), 191.

71 Stand: 1.4.2005.

72 Der Stand der Ratifizierungen ist im Internet unter www.conventions.coe.int/ abrufbar.

73 Der Text kann unter http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/ im Internet abgerufen werden.

74 Ebenfalls unter www.conventions.coe.int/ im Internet abrufbar.

75 Vgl. in diesem Zusammenhang auch die Überlegungen bei *Jean-Philippe Walter,* La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données, in: Astrid Epiney/Marianne Freiermuth (Hrsg.), Datenschutz in der Schweiz und in Europa, 1999, 83 (112 ff.), die in eine ähnliche Richtung wie die folgenden Ausführungen gehen; s. auch die ausführliche Bewertung bei *Ellger,* Datenschutz im grenzüberschreitenden Datenverkehr (Fn.), 498 ff., die ebenfalls in eine ähnliche Richtung wie die hier aufgeführten Aspekte geht.

beeinflusst[76]. Allerdings weist die Konvention im Hinblick auf die effektive Verwirklichung eines gewissen datenschutzrechtlichen Mindeststandards in den Vertragsstaaten ins Gewicht fallende Unzulänglichkeiten auf, wobei insbesondere folgende Aspekte von Bedeutung sind:

- Zunächst ist ihr Anwendungsbereich auf die automatisierte Datenverarbeitung von personenbezogenen Daten natürlicher Personen Anwendungsbereich beschränkt, so dass in Bezug auf die nicht automatisierte Datenverarbeitung sowie den Datenschutz juristischer Personen Lücken bestehen[77].
- Weiter haben die Erweitungs- und Einschränkungsmöglichkeiten des Art. 3 Abs. 2 DSK ein unterschiedliches Datenschutzniveau in den Mitgliedstaaten zur Folge. Auch die Möglichkeit der Ausweitung des Schutzes von sensiblen Daten über Art. 11 DSK führen zu unterschiedlich hohen Schutzniveaus. Dies aber läuft einer der Zielsetzungen der Konvention – eine gewisse Vereinheitlichung der Schutzniveaus in den Vertragsstaaten, auch und gerade im Hinblick auf den Datenaustausch – entgegen. Insgesamt wird dadurch auch der Kompromisscharakter der Konvention deutlich: Zwar konnte man einen völkerrechtlich verbindlichen Standard festschreiben; allerdings führte dieser in wesentlichen Punkten (Schutz juristischer Personen, Einbezug manueller Dateien, Ausnahmebestimmungen für bestimmte Dateien) gerade nicht zu einer Harmonisierung der Rechtsordnungen der Vertragsstaaten, so dass der angestrebte Minimalstandard letztlich „durchlöchert" ist und viele zentrale Fragen des Datenschutzrechts nach wie vor allein durch nationale Standards determiniert sind.
- Besonders ins Gewicht fallen aber die durchwegs offenen Formulierungen in der Konvention[78], die den Vertragsstaaten regelmäßig einen denkbar weiten Gestaltungsspielraum einräumen und damit auf der anderen Seite auch die Reichweite bzw. Tragweite inhaltlicher Vorgaben für die Ausgestaltung des Persönlichkeitsschutzes teilweise recht weitgehend relativieren[79].
- Damit in engem Zusammenhang steht das Fehlen unabhängiger Kontrolleinrichtungen bzw. von Verpflichtungen der Vertragsstaaten, solche einzurichten: Weder kennt die Konvention selbst ein unabhängiges Kontrollorgan, das etwa mögliche Vertragsverletzungen der Vertragsstaaten prüfen kann, noch sind die Vertragsstaaten zwingend gehalten, unabhängige Kontrollorgane einzurichten, die dann möglicherweise auch gerichtliche Verfahren in Gang setzen könnten (sieht man einmal von den

---

76 *Herbert Burkert,* in: Alexander Rossnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 2.3, B, II, 4, Rz. 35.

77 Zu diesem Aspekt auch etwa *Walter,* in:, Datenschutz in der Schweiz und in Europa (Fn.), 83 (113).

78 Hierzu auch etwa *Henke*, Datenschutzkonvention (Fn.), 57 f., der auch darauf hinweist, dass diese Offenheit zu Lasten der Rechtssicherheit geht.

79 Immerhin sei auch darauf hingewiesen, dass die Flexibilität des Textes auf der anderen Seite eine Anpassung an technologische Neuerungen erlaubt. Zudem ist die „Hemmschwelle" für eine Ratifizierung durch einen Staat nicht so hoch, was auch im Interesse des Europarates liegt und gleichzeitig dem internationalen Datenschutz zu Gute kommt. Vgl. hierzu *Walter,* in:, Datenschutz in der Schweiz und in Europa (Fn.), 83 (105).

Ergänzungen durch das erwähnte Zusatzprotokoll ab). Damit können – im Gegensatz etwa zur EMRK oder zum europäischen Gemeinschaftsrecht – die unscharfen Begriffe in der Konvention und die Reichweite der vertraglichen Pflichten auch nicht auf diesem Wege präzisiert werden, sondern es bleibt den Vertragsstaaten überlassen, innerhalb des von der Konvention gesteckten sehr weiten Rahmens die ihnen obliegenden Pflichten zu präzisieren. Dies birgt einerseits die Gefahr unterschiedlicher Schutzniveaus in den Vertragsstaaten, andererseits diejenige eines unzureichenden Schutzniveaus im Hinblick auf den Schutz der Rechte Einzelner mit sich.

Insgesamt mag man daher der Konvention ihre Verdienste, den Datenschutz auch ausgehend von einem gewissen Anspruch auf Universalität auf internationalem Niveau vorangetrieben zu haben, nicht abzusprechen, und ihre Bedeutung ist insofern bemerkenswert und sollte nicht unterschätzt werden. Dieser Befund darf aber nicht darüber hinwegtäuschen, dass die Konvention nur einen ersten Schritt darstellen kann und noch zahlreiche Schwächen aufweist, wobei die Offenheit ihrer Verpflichtungen und die fehlende Kontrolle sicherlich von besonderer Bedeutung sind. Daher sollte die Konvention eher als Ausgangspunkt für weitere und ggf. auch spezifische datenschutzrechtliche Instrumente angesehen werden.

- Schließlich hat die EG verschiedene datenschutzrelevante Rechtsakte erlassen, wobei die RL 95/46 und die RL 2002/58 von besonderer Bedeutung sind. Deren Bedeutung ist kaum zu unterschätzen, beschränkt sich aber auf die EU-Mitgliedstaaten.

Deutlich wird durch diesen Überblick, dass auf internationaler Ebene – sieht man von der Konvention des Europarates von 1981 ab, die aber die skizzierten Unzulänglichkeiten aufweist – eigentlich kein völkerrechtlich verbindliches Instrument besteht, das die Staaten direkt und unmittelbar verpflichtet, beim Datenschutz gewisse Mindeststandards zu befolgen. Vor diesem Hintergrund wäre es – auch und gerade angesichts der sich intensivierenden Zusammenarbeit der Staaten im Zuge der Terrorismusbekämpfung und der internationalen Kriminalität[80], aber auch im Zuge der Globalisierung, die es neben allgemein vermehrten Datentransfers etwa auch mit sich bringt, dass Firmen ihre Datenverwaltung oft in Drittländer auslagern, was zumindest immer dann Probleme verursacht, wenn diese keine oder unzureichende Datenschutzstandards kennen, sowie angesichts zumindest potentieller extraterritorialer Wirkungen (unzureichender) Datenschutzstandards[81] – sehr sinnvoll, sich im Rahmen der Vereinten Nationen auf ein solches Instrument zu verständigen. Die Richtlinien der Generalversammlung aus dem Jahr 1990 könnten und sollten hier einen Ausgangspunkt darstellen. Eine solche Rechtsentwicklung erscheint gerade angesichts der in diesem Beitrag

---

80 S. in diesem Zusammenhang auch die Bemerkungen bei *Herbert Burkert*, Globalization – Strategies for Data Protection, 8 f. (zitiert nach Manuskript), der darauf hinweist, dass es schwer nachvollziehbar sei, dass die Cybercrime-Convention nicht in verbindlicher Weise die Einhaltung datenschutzrechtlicher Standards verlangt.

81 Wie etwa das Beispiel der USA zeigt, hierzu mit konkreten Beispielen NZZ am Sonntag vom 3.7.2005, 31; *Georges de la Loyère,* Flux transfrontières et mondialisation: comment protéger la vie privée dans un monde global.

angesprochenen Herausforderungen – zunehmende internationale Zusammenarbeit im Hinblick auf die Bekämpfung von Terrorismus und internationaler Kriminalität sowie technologische Entwicklung, die bekanntlich an Grenzen nicht halt macht – unentbehrlich: Nur internationale Standards können vor diesem Hintergrund tatsächlich sicherstellen, dass sowohl die Rechte der Betroffenen beachtet als auch der Datenschutz als öffentliches Interesse ausreichend verfolgt werden kann.

Die Herausforderung ist hier aber nicht zu unterschätzen: Sie besteht insbesondere darin, eine allgemein annehmbare Definition des Ausmaßes des Persönlichkeitsschutzes sowie des Datenschutzes als Teil des öffentlichen Interesses zu formulieren und hieraus gewisse allgemeine und grundlegende Anforderungen im Hinblick auf den Datenschutz zu formulieren. Trotz der damit zu erwartenden Schwierigkeiten dürfte es sich aber lohnen, die Herausforderung anzunehmen; auch erscheint ein Erfolg eines solchen Vorhabens durchaus möglich, wie nicht nur die bislang erzielten Fortschritte auf dem Gebiet des Datenschutzes auf internationaler Ebene, sondern auch die Einigung auf universelle Standards in anderen Bereichen – so insbesondere den Menschenrechten – zeigen (womit selbstverständlich die durchaus fortbestehenden Auslegungsprobleme nicht negiert werden sollten). Jedenfalls sollte ein neues internationales Instrument auf dem Gebiet des Datenschutzes sicherstellen, dass ein unabhängiger Kontrollmechanismus – wenn möglich unter Einbezug von Individual- und Verbandsbeschwerden – geschaffen wird und dass die zentralen Rechte der Individuen als *self-executing*-Normen ausgestalten werden, jedenfalls soweit sie sich gegen hoheitliche Eingriffe richten.

> Im Hinblick auf den Inhalt einer solchen internationalen Konvention wäre es im Übrigen sicherlich sinnvoll, nicht nur die traditionellen Datenschutzgrundsätze zu verankern, sondern sich auch den Zusammenhang von Datenschutz und Informationszugangsrechten zu berücksichtigen[82].

Neben einem solchen internationalen Rechtsinstrument ist es nach der hier vertretenen Auffassung unentbehrlich, dass sich internationale und supranationale Organisationen im Zuge der vermehrten Zusammenarbeit im Bereich der internationalen Sicherheit und der vermehrten Möglichkeiten des Datenaustausches zwischen den Staaten im Gleichschritt zu dieser Entwicklung auf eine Internationalisierung bzw. Supranationalisierung auch der Datenschutzstandards einigen; dies gilt insbesondere für die Europäische Union.

V. Schluss

Insgesamt – und hierfür ist gerade diese Tagung ein wichtiges Zeichen – dürften damit die größten Herausforderungen für den Datenschutz in den nächsten Jahren durch drei Aspekte zusammengefasst werden können:

---

[82] Vgl. hierzu etwa die Überlegungen bei *Herbert Burkert*, Globalization – Strategies for Data Protection, 14 f. (zitiert nach Manuskript).

- Zum einen wird es darum gehen, die Hintergründe des Datenschutzes (wieder) in Erinnerung zu rufen, der ja gerade keinen Selbstzweck darstellt, sondern dem Schutz der Privatsphäre der Betroffenen dient und im Übrigen unentbehrlicher Bestandteil jedes demokratischen Rechtsstaats ist. Insofern gilt es insbesondere, den Ausgleich zwischen Freiheit und Sicherheit immer wieder neu herzustellen, wobei die Erkenntnis, dass eine Aufgabe der Freiheit wegen der Sicherheit letztlich auch die Freiheit in Frage stellte, von zentraler Bedeutung ist. In einem Rechtsstaat kann und wird es nie eine absolute Sicherheit geben, ganz abgesehen davon, dass viele Maßnahmen nur scheinbar zu einer verbesserten Bekämpfung der Kriminalität führen dürften.

  Nur am Rande sei hier nochmals auf die nach wie vor überragende Rolle und Bedeutung des Grundsatzes der Verhältnismäßigkeit hingewiesen: Dieser Grundsatz ist – abgesehen von der allgemeinen Erwägung, dass nicht übermäßig in grundrechtlich geschützte Rechte eingegriffen werden darf – auch insofern von Bedeutung, als es immer wieder zu Missbräuchen einmal vorhandener Daten kommen kann und gerade Bestimmungen über den Verwendungszweck von Daten im Falle des Bestehens einer entsprechenden politischen und gesellschaftlichen „Stimmungslage" leicht (legal oder auch illegal) übergangen bzw. modifiziert werden können[83]. Im Übrigen ist er auch insofern von besonderer Bedeutung, als sich bei manchen der in Aussicht gestellten oder bereits verwirklichten Maßnahmen (insbesondere im Bereich der Terrorismus- und Kriminalitätsbekämpfung) der Verdacht aufdrängt, es gehe weniger um eine wirksame Bekämpfung bestimmter Bedrohungen, denn um eine Demonstration der jeweiligen Hoheitsträger, dass „etwas" getan wird und der Staat oder die supranationaler Organisation auf diesem Gebiet nicht untätig bleibt. Symbolische Politik in diesem Bereich ist aber unter datenschutzrechtlichen Gesichtspunkten nicht nur nicht opportun, sondern häufig auch rechtswidrig[84].
- Zum anderen ist die Verankerung datenschutzrechtlicher Grundprinzipien in einer universellen völkerrechtlich verbindlichen Konvention voranzutreiben; die einzelstaatlichen Instrumente laufen notwendigerweise teilweise ins Leere, und ein effektiver Datenschutz kann durch rein nationale oder auch supranationale Lösungsansätze nicht mehr verwirklicht werden. Letztlich geht es darum, wie auch auf der Konferenz formuliert wurde, einen *Global Privacy Standard*[85] zu umschreiben.
- Schließlich ist ganz allgemein daran zu erinnern, dass jede Liberalisierung des Datenaustauschs – aus welchen Gründen sie auch immer erfolgt – immer mit einer entsprechenden Harmonisierung des Datenschutzstandards auf der jeweiligen Ebene einhergehen sollte, können doch ansonsten die jeweiligen Schutzstandards unterlaufen

---

83 Vgl. die Beispiele bei *Claudia Mund,* Biobanken – Datenquellen ohne Grenzen?.

84 S. in diesem Zusammenhang auch die Bemerkungen bei *Klaus-R. Kalk,* Sind Datenschutz und der Kampf gegen den Terrorismus miteinander vereinbar?; *Ann Cavoukian,* The New Breed of Practical Privacy: an Evolution.

85 Vgl. *Ann Cavoukian,* The New Breed of Practical Privacy: an Evolution, 8 (zitiert nach Manuskript).

werden, wie das Beispiel internationaler oder supranationaler Fahndungs-, Beweisaustausch oder Informationssysteme, die auf dem Prinzip gegenseitiger Anerkennung beruhen, zeigt.