Datenschutz in Europa

Walter Rudolf*

I.

Wenn vor 30 Jahren hier im Europa-Institut über Datenschutz berichtet worden wäre, hätte dem Vortrag noch etwas Exotisches angehaftet; denn Begriffe wie Datenverarbeitung, Datenbank und Datenschutz waren damals noch ziemlich neu. Es gab erst ein einziges Gesetz auf der Welt, das einen umfassenden Datenschutz des Einzelnen gegenüber dem Staat und seinen Einrichtungen vorsah, nämlich das hessische Gesetz von 1970.

Inzwischen ist Datenschutz nicht nur in Deutschland, sondern in den meisten Staaten Europas nicht nur gesetzlich fest verankert, sondern wird auch überwiegend erfolgreich praktiziert. Gleichwohl ist das Verhältnis vieler Menschen zum Datenschutz durchaus ambivalent. Man denke an den Rechtsanwalt, der sich über den Datenschutz ärgert, weil sich eine Behörde weigert, ihm Auskünfte über seinen Prozessgegner zu erteilen, sich eine Stunde später heftig erregt, weil sein Finanzamt das ihn betreffende Steuergeheimnis – vielleicht sogar zu Recht – nicht gewahrt hat.

Wenn auch der Begriff Datenschutz erst mit der elektronischen Datenverarbeitung aufkam, ist der dahinter stehende Gedanke des Schutzes personenbezogener Daten, d.h. von Einzelangaben über persönliche oder sachliche Verhältnisse von Personen, sehr viel älter. Seit der Mensch als Individuum, als eigenständige Persönlichkeit anerkannt wird, gibt es Datenschutz in Teilsektoren, auch wenn der Begriff noch unbekannt war.

Am Anfang der Entwicklung standen Geheimhaltungspflichten bestimmter Berufsgruppen, deren Angehörige die Angaben über Menschen, deren Betreuung ihnen oblag, vertraulich behandeln mussten. Das Arztgeheimnis, das die Patientendaten schützt, ist etwa 2800 Jahre alt. Es wurde zuerst in Indien niederge-

* Universitätsprofessor Dr. Walter Rudolf, Landesbeauftragter für den Datenschutz des Landes Rheinland-Pfalz, Mainz. Der Beitrag geht zurück auf einen Vortrag, den der Verfasser am 21. Januar 2003 im Europa-Institut der Universität des Saarlandes, Sektion Rechtswissenschaft gehalten hat. Der Vortragsstil wurde beibehalten.

schrieben und fand dann im 6. Jahrhundert vor Christus im Eid des Hippokrates in Griechenland seine noch heute gültige Formulierung. Für das Arztgeheimnis gab es zwei Gründe, einen das Individuum betreffenden und einen, der im Interesse der Allgemeinheit lag: Die Patienten sollten keine sozialen Nachteile durch das Bekanntwerden von Krankheiten erleiden und die Schweigepflicht des Arztes war Voraussetzung dafür, dass im Interesse einer funktionierenden Gesundheitsvorsorge dem Ärztestand Vertrauen entgegengebracht wurde.

Dem Arztgeheimnis folgten weitere Berufsgeheimnisse: das Beichtgeheimnis, das den Beichtvater zur Geheimhaltung des in der Beichte Gehörten zwang, das Amtsgeheimnis, das den Beamten zur Verschwiegenheit verpflichtete, das Steuergeheimnis, das Bankgeheimnis – um nur einige der zahlreichen Verschwiegenheitspflichten zu nennen. Alle diese Berufsgeheimnisse dienten wie das Arztgeheimnis dem Schutze des Individuums; sie dienten aber ebenso dem Interesse der Allgemeinheit. Die nahezu einhellige Warnung der Sachverständigen vor der Aufhebung des Bankgeheimnisses in der gegenwärtigen Steuerrechtsdiskussion bestätigt die Bedeutung dieser Verschwiegenheitspflichten für das Allgemeininteresse, in diesem Falle für die wirtschaftliche Entwicklung durch Verhinderung von Kapitalabfluss in das Ausland und damit für ein höheres Steueraufkommen.

Verletzt der Staat den Datenschutz, ist das Vertrauen in ihn erschüttert mit der Folge, dass er künftig keine oder unrichtige Angaben erhält und damit letztlich Schaden erleidet. Dasselbe gilt für die Verletzung des Schutzes persönlicher Daten im gesellschaftlichen und privaten Bereich, insbesondere im Wirtschaftsverkehr.

Was es ursprünglich nicht gab, war ein allgemeines Recht des Individuums, über die Erhebung und weitere Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen, d.h. ein Recht auf einen unverletzlichen Intimbereich, auf ungestörte Privatheit. Die Ersten, die ein solches Recht auf Privatheit schon 1890 gefordert und als *Key Right* bezeichnet haben, waren die amerikanischen Juristen *Louis Brandeis* und *Samuel Warren*. Die USA, die nicht nur in der Computertechnik, sondern auch in der juristischen Diskussion um den Schutz der Privatheit eine Vorreiterrolle spielten, haben freilich erst 84 Jahre später, im Jahre 1974, den *Privacy Act* erlassen.

Soweit das Verhältnis des Staates zum Einzelnen betroffen ist, ist Datenschutz Menschenrechtsschutz. Schutzgut ist die Privatsphäre des Individuums, also letztlich das allgemeine Persönlichkeitsrecht. Das bedeutet, dass nur Menschen – und zwar lebende Menschen –, nicht aber juristische Personen geschützt sind, weil nur Menschen eine Privatsphäre haben. Gesellschaften, Stiftungen oder sonstige Körperschaften sind freilich nicht ungeschützt, denn neben dem grundrechtlichen Datenschutz bestehen andere öffentliche oder private Geheimhaltungspflichten, z.B. Staatsgeheimnisse, Betriebsgeheimnisse oder das Beratungsgeheimnis der Richter. Die staatlichen Organe und Bediensteten können sich selbst nicht auf Datenschutz berufen, da sie als solche nicht Grundrechtsträger sind.

Die ersten Datenschutzgesetze entstanden im Zuge der rasanten Entwicklung der Informationstechnik. Sie dienten dem Schutze des Einzelnen vor dem Staat. Auf das hessische Datenschutzgesetz folgte als zweites das schwedische 1973 und als drittes das von Rheinland-Pfalz 1974. Ihm folgten die übrigen Länder, wobei alle diese Landesgesetze nur den Schutz personenbezogener Daten gegenüber der öffentlichen Hand betrafen. Um den öffentlichen Datenschutz ging es auch im Verfahren vor dem Bundesverfassungsgericht über das Volkszählungsgesetz. Mit dem Volkszählungsurteil vom 15. Dezember 1983 war das Recht auf informationelle Selbstbestimmung geboren, ein Grundrecht, dass das Bundesverfassungsgericht auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz gestützt hat. Dieses Grundrecht wurde erstmals in Deutschland 1978 in eine Verfassung eingestellt nämlich in die von Nordrhein-Westfalen: „Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Eingriffe sind nur im überwiegenden Interesse der Allgemeinheit und aufgrund eines Gesetzes zulässig." Dem nordrhein-westfälischen Beispiel folgten 1983 das Saarland, 1990 Berlin, 1992 Sachsen, Sachsen-Anhalt und Brandenburg, 1993 Mecklenburg-Vorpommern und Thüringen, 1997 Bremen und 2001 Rheinland-Pfalz. Datenschutz im nicht-öffentlichen Bereich, also zwischen Privatrechtssubjekten, regelte das Bundesdatenschutzgesetz von 1977. Der Versuch, den Datenschutz als eigene Norm in das Grundgesetz anlässlich der durch die deutsche Einheit initiierten Grundgesetzreform einzustellen, scheiterte; die erforderliche Zweidrittelmehrheit war nicht zu erreichen.

Neben den Datenschutzgesetzen des Bundes und der Länder existieren zum Teil voluminöse bereichsspezifische datenschutzrechtliche Normen, welche die Materie des Datenschutzrechts in Deutschland unübersichtlich machen. Während ursprünglich die bereichsspezifische Regelung des Datenschutzes favorisiert wurde, versucht man nun gegenzusteuern, ohne dass eine Trendwende wirklich erkennbar ist.

Das bedeutet nicht, dass übereinstimmende Grundsätze des deutschen Datenschutzrechts fehlen. In der Begründung zum Volkszählungsurteil hatte das Bundesverfassungsgericht die für den Datenschutz entscheidenden Kriterien genannt. Oberster Grundsatz ist, dass jede Person grundsätzlich selbst über die Preisgabe und Verwendung ihrer Daten bestimmen kann. Dies gilt für die Datenerhebung, -speicherung, -übermittlung und -nutzung. Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn eine Rechtsvorschrift die Erhebung, Nutzung oder Weitergabe der Daten ausdrücklich erlaubt oder der Betreffende hierzu seine Einwilligung erteilt hat. Personenbezogene Daten sind grundsätzlich bei den Betroffenen selbst zu erheben. Ohne deren Mitwirkung dürfen solche Daten nur bei Vorliegen bestimmter Voraussetzungen erhoben werden. Dies gilt auch für die Erhebung personenbezogener Daten bei Dritten. Die Einwilligung zur Datenverarbeitung muss zulässig und sie muss freiwillig sein. Der Einwilligende muss auf den Zweck der Verarbeitung im Einzelnen hingewiesen werden. Ohne Einwilligung ist Datenverarbeitung nur zulässig im Rahmen der Zweckbestimmung eines

Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der Daten verarbeitenden Stelle oder eines Dritten erforderlich ist. Für Speicherung und Nutzung von Daten gilt der Grundsatz der Zweckbindung. Die weitere Verarbeitung erhobener Daten ist nur zulässig, wenn dies für Zwecke erfolgt, für die die Daten erhoben worden sind. Übermittlung von Daten ist zulässig, wenn dies bei einer öffentlichen Stelle zur Aufgabenerfüllung erforderlich oder eine Zweckänderung ausdrücklich erlaubt ist. Nicht-öffentliche Stellen müssen ein rechtliches Interesse glaubhaft machen oder es muss ein öffentliches Interesse bestehen. Auch darf kein Grund zur Annahme bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Im privaten Bereich der Bürger untereinander findet der Datenschutz dort seine Grenze, wo die rechtlichen Interessen nach Abwägung mit den Interessen des Datenschutzes Vorrang haben. Daten dürfen nur so lange gespeichert werden, wie dies erforderlich ist. Die Betroffenen sind über die erstmalige Datenspeicherung grundsätzlich zu benachrichtigen, sie haben Auskunftsrechte, das Recht zur Berichtigung, zur Löschung und zur Sperrung von Daten und ein Recht auf Schadensersatz.

Dass dieses Grundrecht nicht schrankenlos gewährleistet ist, versteht sich von selbst. Es darf eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern. Dabei hat der Gesetzgeber den Grundsatz der Verhältnismäßigkeit zu beachten, der wie überall im öffentlichen Recht auch im Datenschutzrecht eine erhebliche Rolle spielt. Wie bei jedem Grundrecht gilt auch hier das Prinzip des geringst möglichen Eingriffs. Ist aber eine Information zur Erfüllung einer Aufgabe für eine Behörde unerlässlich und kann diese Aufgabe ohne Kenntnis der Information nicht erfüllt werden oder nicht rechtzeitig oder nur mit unverhältnismäßigem Aufwand oder nur mit sonstigen unverhältnismäßigen Nachteilen, dann darf die Information auch an die Behörde weitergegeben werden.

Die nach wie vor verbreitete Auffassung, Datenschutz behindere die Verwaltungstätigkeit, ist insofern richtig, als die Verwaltung das Grundrecht auf informationelle Selbstbestimmung – wie jedes andere Grundrecht auch – zu respektieren hat. Dies ist im Rechtsstaat unerlässlich. Auch die Verwaltungsgerichtsbarkeit behindert insofern die Verwaltung. Das aber ist gewollt. Ein weit verbreitetes Märchen ist, dass der Datenschutz die Polizei bei der Verbrechensbekämpfung behindere. Bei genauerem Hinsehen ist die Zahl der Fälle, bei denen dies geschehen ist, ganz minimal. Die Polizei hat das Recht jedes Einzelnen auf Schutz vor Kriminalität gegen das Recht auf Privatheit abzuwägen, wobei der Datenschutz nicht selten zurückzutreten hat. Man denke an die Rasterfahndung im Gefolge des 11. September 2001.

Zur Kontrolle der Einhaltung des Datenschutzes hatte das Bundesverfassungsgericht bereits im Volkszählungsurteil ausgeführt, dass „wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten

unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung" ist. Diese Ausführungen des Bundesverfassungsgerichts beziehen sich ausschließlich auf den öffentlichen Bereich. Demgemäß ist die Unabhängigkeit der Datenschutzbeauftragten des Bundes und der Länder gesetzlich verbürgt, in Nordrhein-Westfalen seit 1977 sogar in der Landesverfassung verankert. Auch die Länder Brandenburg, Mecklenburg-Vorpommern, Niedersachsen und Sachsen-Anhalt haben eine Regelung über die Unabhängigkeit der Datenschutzbeauftragten jeweils in ihre Verfassung aufgenommen. Die Rechtsstellung der 17 Datenschutzbeauftragten des Bundes und der Länder und ihre Verankerung im staatlichen Organisationsgefüge ist zwar unterschiedlich geregelt, doch bestehen hinsichtlich der Unabhängigkeit keine Zweifel. Ein Nebeneffekt der Datenschutzkontrolle ist übrigens die Entlastung der Verwaltungsgerichtsbarkeit.

Von Kontrollrechten der Datenschutzbeauftragten ausgenommen sind die Parlamente, die Gerichte und Rechnungshöfe, soweit sie nicht Verwaltungsaufgaben wahrnehmen. Die öffentlich-rechtlichen Rundfunkanstalten besitzen ein „Medienprivileg", womit gemeint ist, dass sie den allgemeinen Datenschutzvorschriften nur unterliegen, soweit nicht aus der Rundfunkfreiheit des Art. 5 Abs. 1 Satz 2 Grundgesetz folgende bereichsspezifische Ausnahmen geboten sind. Eine externe Datenschutzkontrolle findet bei den Rundfunkanstalten nicht oder jedenfalls in einigen Ländern nur hinsichtlich ihrer Verwaltungstätigkeit statt. Sie haben statt dessen interne Datenschutzbeauftragte, die den Aufsichtsgremien der Rundfunkanstalten Tätigkeitsberichte zu erstatten haben, die nur dem Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten in Bayern, im Saarland und in Rheinland-Pfalz (ZDF) zu übermitteln sind. Auch die öffentlich-rechtlichen Religionsgemeinschaften unterliegen nicht dem Datenschutzgesetz und damit auch nicht der Kontrolle durch die Datenschutzbeauftragten der Länder, sondern haben eigene Regelungen mit eigenen Kontrollstellen.

Anders als im öffentlichen Bereich des Datenschutzes, sind im privaten Bereich für den Datenschutz Aufsichtsbehörden zuständig, die im Gegensatz zu den Datenschutzbeauftragten im öffentlichen Bereich, die nur Kontroll- und Beanstandungsrechte besitzen, auch exekutive Befugnisse haben. Diese Aufsichtsbehörden sind in den meisten Bundesländern entweder bei einem Ministerium oder den Mittelbehörden der allgemeinen inneren Verwaltung eingerichtet. In Berlin, Brandenburg, Bremen, Hamburg, Niedersachsen und Nordrhein-Westfalen sind die Datenschutzbeauftragten für den öffentlichen Bereich zugleich Aufsichtsbehörden, wobei sie insoweit allerdings der Rechtsaufsicht entweder der Regierung oder eines Ministeriums unterliegen. In Schleswig-Holstein liegt sowohl der öffentliche als auch der nicht-öffentliche Datenschutz in der Hand einer Anstalt des öffentlichen Rechts mit dem Landesbeauftragten für Datenschutz an der Spitze.

Das Saarland hat die Übertragung des privaten Datenschutzes auf den Landesbeauftragten wieder rückgängig gemacht. Auf die Trennung der Kontrolle im öffentlichen und im nicht-öffentlichen Datenschutz komme ich noch im Zusammenhang mit der Europäischen Datenschutzrichtlinie zurück.

II.

International ist der Schutz der Privatsphäre erstmals in der Allgemeinen Erklärung der Menschenrechte vom 10. Dezember 1948 erwähnt. Artikel 12 dieser Erklärung der Generalversammlung der Vereinten Nationen, die ohne Gegenstimmen bei Stimmenthaltung der kommunistischen Staaten, Saudi-Arabiens und Südafrikas angenommen wurde, besagt, dass niemand willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel ausgesetzt werden darf. Diese Allgemeine Menschenrechtserklärung von 1948 ist zwar nach der UN-Charta nur eine unverbindliche Empfehlung, sie wird aber inzwischen von sehr vielen Juristen als Gewohnheitsvölkerrecht, ja sogar als zwingendes Recht betrachtet, was m.E. nicht für alle dort genannten Menschenrechte nachzuweisen ist. Es gibt aber inzwischen den Internationalen Pakt für bürgerliche und politische Rechte vom 19. Dezember 1966, dessen Art. 17 fast wortgleich mit Art. 12 der Allgemeinen Menschenrechtserklärung ist. Dieser Internationale Pakt ist völkerrechtlich verbindlich für die Staaten die ihn ratifiziert haben, und das sind inzwischen mehr als drei Viertel aller souveräner Staaten, die es gibt. Was dem internationalen Pakt fehlt, sind gerichtlich durchsetzbare Sanktionsmöglichkeiten im Falle von Menschenrechtsverletzungen.

In Europa gibt es eine durchsetzbare internationale Kontrolle bei Verletzungen von Menschenrechten aufgrund der Europäischen Menschenrechtskonvention vom 4. November 1950 durch den Europäischen Menschenrechtsgerichtshof in Straßburg. Die Privatsphäre wird durch Art. 8 der Konvention geschützt, dem übrigens Art. 11 der amerikanischen Menschenrechtskonvention etwa entspricht. Der Europäische Menschenrechtsgerichtshof und die nicht mehr bestehende Europäische Kommission für Menschenrechte haben inzwischen auch etliche Entscheidungen zum Schutz der Privatsphäre insbesondere auch in Sachen Datenschutz gefällt.

Einen datenschutzrechtlichen Mindeststandard, der für alle Mitgliedstaaten verbindlich ist, legte das im Europarat entstandene Übereinkommen zum Schutze der Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 fest. Durch ein Zusatzprotokoll vom 23. Mai 2001 ist dieser Mindeststandard verbessert worden: Das Zusatzprotokoll sieht völlig unabhängige Kontrollbehörden in jedem Mitgliedstaat vor und bestimmt, dass personenbezogene Daten in das Ausland nur weitergegeben werden dürfen, wenn im Empfangsstaat der Datenschutz gewährleistet ist.

Das Ministerkomitee des Europarats hat bereits seit 1983 eine ganze Reihe von Empfehlungen zum Datenschutz beschlossen, etwa für automatisierte medizinische Datenbanken, zu Sozialdaten, zur polizeilichen Datenverarbeitung, zum Arbeitsrecht, zum Telekommunikationsdatenschutz oder zum Zugang zu Archiven. Obwohl diese Empfehlungen nicht bindend sind, hat man teilweise mit dem Trick gearbeitet, dass Vorbehalte gegen die rechtlich unverbindlichen Empfehlungen zulässig seien, wie es nur bei völkerrechtlichen Verträgen möglich ist. Wurden keine Vorbehalte gemacht, ging man davon aus, dass die Empfehlung in den Mitgliedstaaten befolgt wird. Diese Empfehlungen haben dann auch in der Tat in den Mitgliedstaaten des Europarats die Gesetzgebung zum Datenschutz stark beeinflusst.

III.

Auch die Europäische Gemeinschaft hatte sich dem Thema Datenschutz zugewendet. Zunächst hatte die Kommission unverbindliche Empfehlungen zum Datenschutz ausgesprochen. Am 24. Oktober 1995 wurde dann nach langen Vorarbeiten vom Europäischen Parlament und dem Rat die als Europäische Datenschutzrichtlinie bekannte Richtlinie 95/46 EG erlassen, die bis zum 25. Oktober 1998 in nationales Recht umgesetzt werden sollte. Deutschland gehörte zu den Staaten, die den Termin erheblich überschritten hatten, so dass sogar ein Vertragsverletzungsverfahren gegen Deutschland in Gang gesetzt wurde. Erst durch die Gesetzesnovelle vom 18. Mai 2001 hat der Bund das Bundesdatenschutzgesetz entsprechend den Brüsseler Vorgaben geändert. Das Land Rheinland-Pfalz hat sogar erst durch Gesetz vom 8. Mai 2002 sein Landesdatenschutzgesetz gemäß der Europäischen Datenschutzrichtlinie novelliert. Die landesrechtlichen Regelungen betrafen allerdings nur weniger wichtige Punkte.

Durch die Richtlinie 95/46 EG wird die datenschutzrechtliche Terminologie in den Staaten der Europäischen Gemeinschaft vereinheitlicht. Die Richtlinie betrifft alle Verarbeitung personenbezogener Daten, nicht nur die elektronische und enthält Regeln über Grundsätze in Bezug auf die Zulässigkeit, über besondere Kategorien der Datenverarbeitung, über Informations-, Auskunfts- und Widerspruchsrechte, über Vertraulichkeit und Sicherheit des Datenschutzes, über Meldepflichten sowie über Rechtsbehelfe, Haftung und Sanktionen, und die Übermittlung von Daten an Drittländer sowie über Verhaltensregeln. Der Datenschutz in Europa wird damit auf ein Niveau gebracht, das dem in Deutschland allemal entspricht.

Zu einem Streitpunkt entwickelte sich die in Art. 28 der Datenschutzrichtlinie geregelte Datenschutzkontrolle; denn die Datenschutzrichtlinie macht keinen Unterschied zwischen öffentlichem und nicht-öffentlichem Datenschutz. Die Mitgliedstaaten haben eine oder mehrere öffentliche Stellen zur Überwachung der

Anwendung und Umsetzung der Vorschriften aufgrund der Richtlinie einzurichten. Diese Stellen „nehmen die ihnen zugewiesenen Arbeiten in völliger Unabhängigkeit wahr". Jede Kontrollstelle soll über Untersuchungs- und wirksame Einwirkungsbefugnisse und ein Klagerecht oder eine Anzeigebefugnis bei Datenschutzverstößen verfügen. Hinsichtlich des Datenschutzes im öffentlichen Bereich bestanden in Deutschland Bedenken hinsichtlich der Regelungsbefugnis der Europäischen Gemeinschaft zur Datenschutzkontrolle. Abgesehen davon entspricht das deutsche System der Datenschutzkontrollen im öffentlichen Bereich den Vorgaben der Richtlinie.

Schwierigkeiten entstehen im nicht-öffentlichen Bereich. Problematisch war – und ist es noch –, was unter völliger Unabhängigkeit der Datenschutzkontrollstellen zu verstehen ist. Ist mit völliger Unabhängigkeit gemeint, dass die Kontrollstellen nur unabhängig von den zu Kontrollierenden sein müssen, wären die deutschen Regelungen über die Datenschutzaufsicht im privaten Bereich richtlinienkonform. Ist damit aber bezweckt, die Datenschutzaufsichtsbehörden auch unabhängig von jeglicher staatlicher Aufsicht auszugestalten, erheben sich verfassungsrechtliche Bedenken. Unabhängigkeit besteht nach deutschem Verfassungsrecht nur für Richter, Rechnungshöfe und die Bundesbank und nur in fünf Ländern für die Datenschutzbeauftragten. Ansonsten sind die Datenschutzbeauftragten nur hinsichtlich des öffentlichen Bereichs unabhängig, da sie insoweit keine exekutiven Befugnisse besitzen und nicht besitzen dürfen; denn alle Behörden in Deutschland, die über Exekutivbefugnisse verfügen, unterliegen zumindest der Rechtsaufsicht parlamentarisch kontrollierbarer Organe. Der Rechtsaufsicht unterliegen auch die Gemeinden und sonstigen Selbstverwaltungskörperschaften, ja sogar die völlig staatsunabhängigen Rundfunkanstalten.

Bei der Anpassung des Bundesdatenschutzgesetzes an die Richtlinie 95/46 EG hat der Gesetzgeber die bestehende Aufsichtsregelung nicht in Richtung auf „völlige Unabhängigkeit" festgelegt. § 38 Abs. 6 BDSG bestimmt lediglich, dass die Landesregierungen oder die von ihnen ermächtigten Stellen die für den Datenschutz zuständigen Aufsichtsbehörden bestimmen. Daraus folgt, dass die Aufsichtsbehörden Teil der Exekutive sind und in die Verwaltungshierarchie eingeordnet werden können. Von Seiten der Europäischen Gemeinschaft wurde nicht widersprochen; denn nach Erlass der Novelle 2001 wurde das Vertragsverletzungsverfahren gegen die Bundesrepublik eingestellt. Meines Erachtens ist eine völlige Unabhängigkeit im Sinne der Richtlinie auch dann gewahrt, wenn die Aufsichtsbehörden (nur) der Rechtsaufsicht unterliegen.

Im Vertrag von Amsterdam ausdrücklich vorgeschrieben ist die Beachtung des Datenschutzes für Europol. Der einschlägige Art. 30 bringt Regelungen über das gemeinsame Vorgehen im Bereich der polizeilichen Zusammenarbeit, darunter über Europol, die intendieren, die Kompetenzen von Europol nach dem Europol-Abkommen zu erweitern. Bei Einschaltung von Europol sind die entsprechenden

Vorschriften über den Schutz personenbezogener Daten zu beachten. Es gibt also jetzt eine spezielle Regelung des Datenschutzes auch für die Zusammenarbeit in Bereich von Justiz und Inneres. Ein Blick auf das Inhaltsverzeichnis des Europol-Übereinkommens von 1995 zeigt, dass die Mehrzahl der Bestimmungen die Datenverarbeitung und den Datenschutz betreffen. Der die Erhebung, Verarbeitung und Nutzung personenbezogener Daten regelnde Art. 10 ist im Amtsblatt der Gemeinschaft fast vier Spalten lang.

Kernstück der Arbeit von Europol sind die automatisierten Informationssammlungen, also Dateien. Da ist zunächst das Informationssystem zum schnellen Nachweis über die bei den Mitgliedstaaten und bei Europol vorhandenen Informationen, das die unmittelbar von den Mitgliedstaaten eingegebenen Daten sowie diejenigen von Europol, die aus andern Quellen oder aus dessen Analysetätigkeit stammen, enthält. Im Rahmen seiner Aufgabenstellung kann Europol auch die für spezielle Analysezwecke erforderlichen Dateien speichern, ändern und nutzen. Hier geht es um einen gegenüber der Informationsdatei erweiterten Kreis von Betroffenen, nämlich um Personen, die bei Ermittlungen in den betreffenden Straftaten oder bei künftigen Strafverfolgungen in Betracht kommen, also potentielle Opfer, Kontakt- und Begleitpersonen, Personen, die Informationen über die betreffende Straftat liefern können. Da in diesen Dateien Daten gespeichert werden können, die über die Speicherung nach deutschem Recht hinausgehen, wurde dieser Regelung erhebliche Aufmerksamkeit seitens des Datenschutzes gewidmet. Datenschutzrechtliche Bedenken richteten sich gegen die Analysedateien. Es ist nun dafür Sorge getragen, dass die Datensätze je nach Betroffenheit der einzelnen Personen unterschiedlich sind: Sie sind bei Verdächtigen umfangreicher als beispielsweise bei potentiellen Opfern, Kontakt- oder Begleitpersonen sowie bei Personen, die Informationen über die betreffende Straftat liefern können. Analysedateien werden auch nicht auf Dauer, sondern fallweise auf Initiative von Mitgliedstaaten bei Vorliegen verschiedener Voraussetzungen eingerichtet. Die Dateien werden gegenüber anderen Dateien, auch gegenüber anderen Analysedateien, abgeschottet. Weitere Speicherung von Daten nach Abschluss der Analyse bedarf jeweils einer neuen Projektvereinbarung. Die Verwendung der Daten muss in jeder einzelnen Einrichtungsanordnung für eine Analysedatei als „unbedingt erforderlich" gesondert spezifiziert werden. Sie darf nur auf ausdrücklichen Antrag von zwei oder mehr an der Analyse beteiligten Mitgliedstaaten erfolgen. Außerdem bedürfen die einzelnen Einrichtungsanordnungen der Zustimmung des Europol-Verwaltungsrats mit Zweidrittelmehrheit, welcher seinerseits alle diesbezüglichen Bemerkungen der gemeinsamen Kontrollinstanz berücksichtigt. Diese Kontrollinstanz setzt sich aus je zwei Vertretern aller Mitgliedstaaten zusammen. Nach dem deutschen Europol-Gesetz werden die deutschen Vertreter vom Bundesministerium des Innern ernannt, einer auf Vorschlag des Bundesbeauftragten für den Datenschutz, der andere auf Vorschlag des Bundesrats. Schließlich liefern die Mitgliedstaaten die Daten nach ihrem eigenen Recht an.

Die vor allem von den Datenschutzbeauftragten angesprochene Gefahr, dass die geplante Analysetätigkeit als selbständiger Verarbeitungszweck für eine Vielzahl von Dateien gesehen wird, der neben die klassischen polizeilichen Aufgabengebiete der Gefahrenabwehr und Strafverfolgung tritt, ist damit jedenfalls deutlich verringert. Die Geeignetheit dieser neuen kriminalistischen Arbeitsmethode kann sich erst in der Praxis erweisen. Auch dann wird sich erst beurteilen lassen, ob die damit verbundenen Eingriffe in Bürgerrechte verhältnismäßig sind. Aus der Sicht des Datenschutzes bleibt insoweit mindestens zu fordern, dass in der Praxis die Ziele der einzelnen Analyseprojekte in den Projektvereinbarungen und in den entsprechenden Vorgaben in den Einrichtungsanordnungen möglichst eindeutig festgelegt werden.

Datenschutzrechtlich völlig unzureichend ist dagegen noch das im Aufbau begriffene Eurojust, eine institutionalisierte Zusammenarbeit der Staatsanwaltschaften der Staaten der Europäischen Union zur Verbrechensbekämpfung. Zu dieser in Den Haag eingerichteten internationalen Koordinierungsstelle sind aus jedem Mitgliedstaat zwei Staatsanwälte abgeordnet worden, bei denen Informationen aus den jeweiligen Heimatstaaten nach Bedarf ausgetauscht werden. Es fehlt jedoch bisher eine die Datenübermittlung tragende Rechtsgrundlage. Nach deutschem Recht dürfen schon Daten aus Ermittlungsverfahren bei deutschen Staatsanwaltschaften an den abgeordneten Bundesanwalt nicht übermittelt werden, da dieser nicht mehr staatsanwaltschaftliche Tätigkeit ausübt, sondern als abgeordneter Beamter nur der Beschleunigung des Informationsaustausches dienender Vermittler ist. Hier ist zumindest eine vorläufige datenschutzrechtliche Regelung überfällig.

Unabhängig von der Europäischen Gemeinschaft ist das Schengener Übereinkommen zwischen einigen Staaten der Union über den Abbau der Kontrolle an den gemeinsamen Grenzen von 1985 entstanden, dass durch das Schengener Durchführungsübereinkommen von 1990 ergänzt wurde. Diese Abkommen wurde hinsichtlich der operativen Bestimmungen erst im März 1995 in Kraft gesetzt. Nach dem Vertrag von Amsterdam war das gesamte Schengener System in den EU-Vertrag zu überführen. Damit nehmen alle Mitgliedstaaten der EU an den bisher nur für eine Gruppe der Mitglieder gültigen Regelungen teil und auch die vertraglich festgesetzten Verfahren werden unter Nutzung der Organe und Institutionen der Europäischen Gemeinschaft angewendet. Außerdem ist für wesentliche Materien der Schengener Abkommen eine richterliche Kontrolle durch den Europäischen Gerichtshof sowie eine parlamentarische Kontrolle durch das Europäische Parlament gewährleistet.

Der Datenschutz innerhalb der Europäischen Gemeinschaft hinsichtlich ihrer Organe und Einrichtungen ist erst recht spät eingeführt worden. Seit dem Amsterdamer Vertrag gibt es im EG-Vertrag den Art. 286 über Datenschutz, der bestimmt, dass ab 1. Januar 1999 die Rechtsakte der Gemeinschaft über den Schutz natürlicher Personen bei der Datenverarbeitung auf die Organe und Einrichtungen der

Gemeinschaft Anwendung finden. Vor 1999 sollte der Rat mit dem Parlament die Errichtung einer unabhängigen Kontrollinstanz beschließen. Diese existiert freilich bis heute nicht. Erst die Verordnung 45/2001 EG des Europäischen Parlaments und des Rates zum Schutze natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr vom Dezember 2000 brachte eine abschließende Regelung. Im systematischen Aufbau folgt diese Verordnung nur zum Teil der an die Mitgliedstaaten gerichteten Datenschutzrichtlinie. Die Regelung ist zum Teil detaillierter. Behandelt wird auch der Datenschutz und der Schutz der Privatsphäre interner Telekommunikationsnetze. Während die Datenschutzrichtlinie nur einen Artikel über die Datenschutzkontrolle enthält, sind es bei der Verordnung acht Artikel.

Anders als in den meisten Mitgliedstaaten ist die Datenschutzkontrolle in der EG monokratisch geregelt. Es wird ein Europäischer Datenschutzbeauftragter als unabhängige Kontrollbehörde eingerichtet, der sicherzustellen hat, dass die Grundrechte und Grundfreiheiten natürlicher Personen von den Organen und Einrichtungen der Gemeinschaft geachtet werden. Er wird vom Europäischen Parlament und dem Rat ernannt. Seine Befugnisse sind in Art. 47 enumeriert: Er kann betroffene Personen beraten, Vorschläge zur Beseitigung von Missständen und zur Verbesserung des Datenschutzes der Betroffenen machen, die Verantwortlichen ermahnen oder verwarnen, gegebenenfalls die Errichtung, Sperrung, Löschung oder Vernichtung von Daten anordnen, die Verarbeitung vorübergehend oder endgültig verbieten, dass betreffende Organ und darüber hinaus das Europäische Parlament, den Rat und die Kommission mit der Angelegenheit befassen, den Europäischen Gerichtshof anrufen und dort anhängigen Verfahren beitreten. Der Europäische Datenschutzbeauftragte hat umfassende Informations- und Zugangsrechte. Er ist jährlich an das Europäische Parlament, den Rat und die Kommission berichtspflichtig.

Schließlich ist noch auf die vom Europäischen Rat am 7. Dezember 2000 in Nizza feierlich proklamierte Charta der Grundrechte der Europäischen Union hinzuweisen. Bei den in Kapitel II enthaltenen Freiheiten wird nach dem Recht auf Freiheit und Sicherheit und dem Recht auf Achtung des Privat- und Familienlebens in Art. 8 der Schutz personenbezogener Daten postuliert. Danach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Personen oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht. Die bisher unverbindliche Charta garantiert damit nicht nur ein Recht auf Datenschutz, sondern gewährleistet auch die Einrichtung von unabhängigen Kontrollstellen.

IV.

Wie steht es um den Datenschutz in den großen und den Nachbarstaaten der Europäischen Gemeinschaft?

Frankreich hat 1978 ein Datenschutzgesetz erlassen, das im Juli 1999 der Europäischen Datenschutzrichtlinie angepasst wurde. Für die Einhaltung der Bestimmungen des Gesetzes sorgt die *Commission Nationale de l'Information et des Libertés* als unabhängige Verwaltungsbehörde, deren Mitglieder bei der Erfüllung ihrer Aufgaben keinerlei Weisungen irgendeiner Stelle unterliegen. Sie setzt sich aus 17 auf fünf Jahre oder die Dauer ihres Mandats ernannten nebenamtlichen Mitgliedern zusammen nämlich je zwei von der Nationalversammlung bzw. dem Senat gewählte Abgeordnete und Senatoren, je zwei vom Wirtschafts- und Sozialrat, vom Conseil d'Etat vom Kassationshof und vom Rechnungshof gewählte Mitglieder dieser Organe, zwei auf Vorschlag des Präsidenten der Nationalversammlung bzw. des Senats durch die Regierung ernannte Personen und drei aufgrund ihres Ansehens und ihrer Sachkenntnis von der Regierung unmittelbar ernannte Persönlichkeiten. Der Vorsitzende und die beiden Stellvertreter werden aus der Mitte der Kommission auf fünf Jahre gewählt. Ein vom Ministerpräsidenten ernannter Regierungsbeauftragter nimmt an den Sitzungen der Kommission teil. Für Ermittlungs- und Überprüfungsaufgaben kann die Kommission bei den Präsidenten der Appelationsgerichtshöfe und der Verwaltungsgerichte die Abordnung durch Sachverständige unterstützte Richter verlangen.

In Italien ist der Datenschutz erst 1996, dann aber schon entsprechend der Europäischen Richtlinie umfassend geregelt worden. Der Schutz persönlicher Daten obliegt einer Kontrollinstanz, die ihr Amt vollkommen selbständig ausübt und in ihrem Urteil und ihren Bewertungen völlig unabhängig ist. Sie besteht aus nur vier Personen, zwei vom Abgeordnetenhaus und zwei vom Senat auf vier Jahre gewählt. Es müssen Fachleute auf dem Gebiet des Rechts und der Informatik sein, die hauptamtlich tätig sind.

Auch das spanische Datenschutzgesetz vom Dezember 1999 trägt der Europäischen Datenschutzrichtlinie Rechnung. Es unterscheidet zwischen Daten öffentlicher und nicht öffentlicher Stellen. Datenschutzbehörde ist eine öffentlichrechtliche Körperschaft. Der Direktor als Leiter der Behörde übt sein Amt in völliger Unabhängigkeit und Objektivität aus und unterliegt dabei keinerlei Weisungen. Er wird auf vier Jahre aus dem Kreis der Mitglieder des beratenden Beirats vom König ernannt. Der Beirat unterstützt den Direktor. Je eines seiner Mitglieder wird von der Abgeordnetenkammer, vom Senat, von der Zentralverwaltung, von der Kommunalverwaltung, von der Königlichen Akademie der Geschichte, von den Universitäten, von den Nutzern und Verbrauchern der Datenverarbeitung des nicht öffentlichen Bereichs und je einer von jeder Autonomen Region vorgeschlagen, die auf ihrem Gebiet eine Datenschutzbehörde eingerichtet hat.

Großbritannien hatte 1984 ein Datenschutzgesetz erlassen, das 1998 an die Europäische Datenschutzrichtlinie angepasst wurde. Die Kontrolle des Datenschutzes obliegt einem von der Königin ernannten *Data Protection Commissioner* und seiner Behörde sowie einem *Data Protection Tribunal*, dessen Vorsitzender und ein Teil der Mitglieder vom *Lord Chancellor*, die übrigen Mitglieder vom *Secretary of State* jeweils aus dem Kreis der Anwaltschaft ernannt werden. Auffallend ist der umfangreiche Katalog von Ausnahmen vom Datenschutz. Das britische Gesetz trägt Besonderheiten in Schottland, Wales und Nordirland Rechnung. Guernsey, Jersey und die Isle of Man haben eigene Datenschutzgesetze und eigene Kontrollbehörden.

Von unseren Nachbarstaaten hat Österreich 1978 ein Datenschutzgesetz erlassen, das dem Grundrecht Verfassungsrang verlieh. Es wurde durch das am 1. Januar 2000 in Kraft getretene Datenschutzgesetz 2000 ersetzt, das die Europäische Datenschutzrichtlinie umgesetzt hat. Auch die Ausübung der Kontrollbefugnisse gegenüber den obersten Organen, die Weisungsfreiheit und das Recht zum Erlass einer Geschäftsordnung der Datenschutzkommission haben verfassungsrechtlichen Rang. Diese Kontrollkommission besteht aus sechs (bis auf das geschäftsführende Mitglied) nebenamtlich tätigen Mitgliedern, die auf Vorschlag der Bundesregierung vom Bundespräsidenten für fünf Jahre bestellt werden. Die Mitglieder müssen rechtskundig sein, eines – der Vorsitzende – muss dem Richterstand angehören. Auf Vorschläge des Präsidenten des obersten Gerichtshofs, der Länder, der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer ist Bedacht zu nehmen. Ein Mitglied ist aus dem Kreise der rechtskundigen Bundesbeamten vorzuschlagen. Neben der Datenschutzkommission besteht ein Datenschutzrat beim Bundeskanzleramt, der die Bundesregierung und die Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes berät. Seine Mitglieder kommen aus dem Kreis der politischen Parteien, der Kammern, der Länder und der beiden kommunalen Spitzenverbände.

Nach dem niederländischen Gesetz über den Schutz personenbezogener Daten vom Juli 2000 wird das Kontrollorgan auf Vorschlag des Justizministers von der Königin ernannt, der Vorsitzende auf sechs, die übrigen Mitglieder auf vier Jahre. Belgien hat ein Gesetz zur Implikation der Richtlinie 95/46 EG im Dezember 1998 erlassen. Kontrollorgan ist eine unabhängige Kommission zum Schutze der Privatheit, die beim Ministerium der Justiz eingerichtet ist und aus acht auf sechs Jahre abwechselnd vom Abgeordnetenhaus und dem Senat aus einer Vorschlagsliste des Ministerrats gewählten nebenamtlich tätigen Mitgliedern besteht – paritätisch holländisch- und französischsprachig besetzt. Der Kommission müssen angehören ein Richter als Vorsitzender, mindestens ein weiterer Jurist, ein Informatiker und je eine Person mit beruflicher Erfahrung im Umgang mit persönlichen Daten aus dem privaten bzw. dem öffentlichen Bereich. Nach dem dänischen Gesetz über die Verarbeitung personenbezogener Daten vom Mai 2000 ist Kontrollinstanz die Datenschutzkommission, die aus einem Rat und einem von einem Direktor geleiteten Sekretariat besteht. Der vom Justizminister eingesetzte

Rat besteht aus dem Vorsitzenden, der die Befähigung zum Richteramt besitzen muss und sechs weiteren nebenamtlich tätigen Mitgliedern.

V.

Als Resümee lässt sich feststellen, dass beginnend mit dem hessischen Datenschutzgesetz vom 1970 Deutschland im Datenschutz führend war. An das aufgrund des Volkszählungsurteils von 1983 erreichte hohe Datenschutzniveau kamen die anderen Staaten Europas anfangs nicht heran. Das zeigt z.B. die Bezugnahme auf die aus deutscher Sicht unzureichende Datenschutzkonvention des Europarats von 1982. Bei den Durchführungsverhandlungen über Europol stand die deutsche Delegation in Datenschutzfragen häufig allein. Sowohl die Datenschutzregeln des Schengener Durchführungsabkommens als auch die Europäische Datenschutzrichtlinie lassen inzwischen einen höheren Grad an Motivation zum Datenschutz auch bei den anderen Staaten der Europäischen Union erkennen. Die Kommission hat die Umsetzung der Datenschutzrichtlinie in nationales Recht gründlich überprüft, so dass nunmehr in allen Staaten der Europäischen Union ein Standard im Datenschutz erreicht ist, der dem deutschen kaum nachsteht. Die Datenschutzpraxis wird im Laufe der Zeit wie in Deutschland den normativen Vorgaben weitgehend entsprechen. Seit 1987 habe ich als Vertreter der Landesregierung in der Datenschutzkommission von Rheinland-Pfalz und seit 1991 als Datenschutzbeauftragter die Beobachtung gemacht, dass im öffentlichen Bereich die Behörden immer stärker für den Datenschutz sensibilisiert wurden. Dies gilt vor allem auch für die Polizei mit ihren zahlreichen Dateien.

Weniger erfreulich wird die Situation im privaten Sektor geschildert, da die Kontrolldichte dort wesentlich geringer ist. Es kommt hinzu, dass vielen Menschen der Schutz der Intimsphäre nichts gilt, wofür die in den Nachmittagssendungen des privaten Fernsehens gezeigten Szenen ebenso ein Beweis sind wie das ungenierte laute Telefonieren mit dem Handy in der Öffentlichkeit z.B. auf der Straße, in Gebäuden und in Zügen. Den privaten Bereich – wie in sieben deutschen Ländern bereits geschehen – auch dem Landesbeauftragten für den Datenschutz zu übertragen, ist kein Allheilmittel, wenn nicht gleichzeitig Personal und technische Mittel erheblich erhöht werden, was angesichts der Finanzlage der Länder derzeit illusorisch ist. Der vielberufene Synergieeffekt vor allem im technischen Bereich wird aufgewogen durch den bestehenden Synergieeffekt der räumlichen Nähe von Verwaltungs- und Aufsichtsbehörden auf der selben Stufe wenn nicht gar im selben Hause der Ministerien oder Mittelbehörden der allgemeinen inneren Verwaltung. Eine Konzentration der Aufsichtsbehörden – wie z.B. in Bayern bei der Bezirksregierung von Mittelfranken – wäre freilich sinnvoll.

Ausgenommen von der externen Kontrolle durch staatliche Instanzen ist – was vor allem den privaten Bereich betrifft – nach der Europäischen Datenschutzrichtlinie die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt. Dieses sogenannte „Medienprivileg", das kein Privileg ist, sondern nur die Unabhängigkeit von Presse und Rundfunk vom Staat respektiert, ist berechtigt. Die Datenschutzrichtlinie spricht selbst davon, dass Abweichungen und Ausnahmen vom allgemeinen Datenschutz sich als notwendig erweisen können, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsbildung geltenden Vorschriften in Einklang zu bringen. In Deutschland findet seit 2002 eine nachträgliche Kontrolle durch den Presserat statt. Es gibt inzwischen auch einige Fälle, in denen eine Verletzung des Datenschutzes gerügt wurde. Bemängelt wird allerdings zu Recht, dass nicht alle Presseunternehmen dem Presserat angehören, so dass für diese letztlich überhaupt keine eigenständige Datenschutzkontrolle stattfindet, sondern nur für die Verletzten die Möglichkeit bleibt, den (teuren) Gerichtsweg zu beschreiten.

Die eigentlichen Gefahren für den Datenschutz entstehen durch die rasante technische Entwicklung. Von der Industrie entwickelte Kommunikationseinrichtungen vernachlässigen häufig den Datenschutz. Deshalb ist die beratende Tätigkeit von Fachleuten vor allem des technischen Datenschutzes insbesondere durch die Datenschutzbeauftragten bei der Einrichtung von Informationssystemen außerordentlich wichtig. Das vom schleswig-holsteinischen Landesbeauftragten für den Datenschutz erprobte Datenschutz-Audit und die Lizenzierung datenschutzsicherer Geräte und Verfahren sollte weiter entwickelt werden. Eine Datenschutzsicherheitsplakette sollte aber auch nicht überbewertet werden, da die Einrichtung neuer Informationssysteme eine komplexe Angelegenheit ist und die Ingenieure und Informatiker vor immer neue und jeweils andere Probleme stellt. Ein lückenloser Datenschutz in Europa ist nicht erreichbar, so lange es nicht nur Kriminelle, Gangster und über Gebühr Neugierige, sondern überhaupt unvollkommene Menschen gibt.