Berliner
Datenschutzbeauftragter

BERLIN

Datenschutz bei Telekommunikation und Medien

1993/ 94

Materialien zum

21

Datenschutz bei Telekommunikation und Medien

1993/ 94

Impressum:

Herausgeber:

Berliner Datenschutzbeauftragter
Verantwortlich: Claudia Schmid
Pallasstraße 25–26, 10781 Berlin
Telefon: (0 30) 7 83 88 44
Telefax: (0 30) 2 16 99 27
Bildschirmtext: * 92 67 90 #
Redaktion: Volker Brozio
Druck: Verwaltungsdruckerei Berlin
gedruckt auf Umwelt-Recycling-Papier
1. Auflage
April 1995

Inhalt

Einleitung

Der Berliner Datenschutzbeauftragte hat dem Datenschutz bei Telekommunikation und Neuen Medien bereits vom Beginn seiner Tätigkeit an besondere Aufmerksamkeit gewidmet. Er koordiniert die Meinungsbildung der Datenschutzbeauftragten in diesem immer wichtiger werdenden Bereich auf nationaler, europäischer und internationaler Ebene und hat den Vorsitz in den Arbeitskreisen der entsprechenden Konferenzen der Datenschutzbeauftragten.

Die Entwicklung zur globalen Informationsgesellschaft hat sich in den letzten Jahren beschleunigt und stellt neue Herausforderungen an den Datenschutz gerade im Telekommunikationsbereich. Dabei sind zunehmend europäische und internationale Lösungen erforderlich, weil die Verarbeitung z. B. von Verbindungsdaten nicht an nationalen Grenzen Halt macht.

Die neueren Arbeitsergebnisse sind in unseren Jahresberichten 1993 und 1994 in eigenen Kapiteln dargestellt worden, die wir in dieser Broschüre – ergänzt um die Beschlüsse und Stellungnahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Europäischen Datenschutzkonferenz – gesondert vorlegen.

Dr. Hansjürgen Garstka

Berliner Datenschutzbeauftragter

A. Auszug aus dem Jahresbericht 1993 des Berliner Datenschutzbeauftragten

1. Geschäftsbereich: Telekommunikation und Medien

Bei der Behandlung von Datenschutzfragen bei Telekommunikation und Medien, die auch im vergangenen Jahr wieder einen Schwerpunkt unserer Tätigkeit bildeten, erweist sich, daß datenschutzgerechte Lösungen heute nicht mehr regional oder national, sondern nur auf europäischer und internationaler Ebene erreicht werden können. Umgekehrt werden europäische Initiativen zur Liberalisierung und Harmonisierung der bestehenden Netze in naher Zukunft starke Auswirkungen im nationalen Bereich haben. Im Auftrag der entsprechenden Koordinierungsgremien haben wir uns deshalb auch im Berichtszeitraum intensiv um eine Abstimmung zwischen den Datenschutzbeauftragten auf der Ebene der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und auf europäische und internationaler Ebene bemüht. Nur durch eine solche Abstimmung besteht eine gewisse Gewähr dafür, daß Gefahren für die Persönlichkeitsphäre frühzeitig erkannt und Konzepte entwickelt werden, um ihnen zu begegnen.

1.1 Berlin

Telekommunikation in öffentlichen Krankenhäusern

In einer Rehabilitationswohngemeinschaft für Jugendliche, die unter einer psychischen Erkrankung leiden, riefen Betreuer nach Telefonaten ihrer Schützlinge deren Gesprächspartner erneut an, um sich nach deren Identität und den Gesprächsinhalten zu erkundigen.

Was den Mißbrauch der Zielnummernspeicherung aus der Telefondatenerfassung einer digitalen Nebenstellenanlage vermuten ließ, war in Wirklichkeit ein Beispiel für die datenschutzrechtliche Relevanz der **Wahlwiederholfunktion** bei noch analogen Nebenstellenanlagen. Dabei wird die zuletzt gewählte Telefonnummer gespeichert. Nach dem Drücken der Wahlwiederholtaste wird diese automatisch angewählt. Genau diese Funktion wurde im beschriebenen Fall zu Kontrollanrufen genutzt.

Eine Umfrage bei den öffentlichen Krankenhäusern zur Technik der Telefonnebenstellenanlagen und dabei insbesondere zur Praxis der **Gebührenabrechnung für Patiententelefone** hat ergeben, daß auch in den Krankenhäusern eine schnelle Ablösung der alten analogen Nebenstellen durch moderne ISDN-fähige digitale Nebenstellenanlagen erfolgt. Mit dieser Umstellung wird die Chance genutzt, die beim Einsatz solcher Anlagen anfallenden Gesprächsdaten für eine detaillierte Abrechnung mit den Patienten zu verwenden.

Während bei den alten Anlagen meist Gesprächseinheitenzähler verwendet werden, die zwar die Gebühreneinheiten patientenbezogen zählen, aber Rückschlüsse auf die Gesprächspartner nicht ermöglichen, wird mit der Umstellung auf digitale Nebenstellenanlagen einer Reihe von Krankenhäusern – aber keineswegs allen – angestrebt, die Zielnummer der Patientengespräche zu erfassen, um einen detaillierten und von den Patienten besser überprüfbaren Einzelgebührennachweis liefern zu können.

In rechtlicher Hinsicht stellt die Situation im Vergleich zur Problematik des Einzelgebührennachweises der TELEKOM an ihre Kunden und zur Gesprächsdatenerfassung zur Abrechnung privater Gespräche von Dienstanschlüssen einen Sonderfall dar, denn die dafür geltenden Vorschriften[1] sind nicht unmittelbar auf die von Krankenhäusern an Patienten vermieteten Anschlüsse anwendbar. Krankenhäuser erbringen mit ihren Nebenstellenanlagen keine „Telekommunikationsdienstleistungen für andere“ im Sinne des Fernmeldeanlagengesetzes. Anwendbar ist zunächst nur das Landeskrankenhausgesetz in Verbindung mit dem Krankenhausaufnahmevertrag sowie (subsidiär) § 28 BDSG.

Allerdings sind die öffentlichen Krankenhäuser nach § 5 Abs. 4 der Rahmendienstvereinbarung zu digitalen Nebenstellenanlagen[2] daran gehindert, für die Gespräche ihres **Personals** Gebührendaten mit vollständiger Zielnummer in der Nebenstellenanlage zu speichern, da dafür eine gesonderte gesetzliche Regelung fehlt. Da nicht anzunehmen ist, daß in den Krankenhäusern verschiedene Nebenstellenanlagen für Patienten und Personal betrieben werden, muß dies indirekt auch den Patienten zugutekommen.

Abgesehen davon sollte zumindest der Rechtsgedanke der §§ 6 TDSV/UDSV auch im Verhältnis Krankenhaus-Patient entsprechend herangezogen werden, da die Patienten dem Krankenhaus gegenüber nicht schlechter gestellt werden sollten als die TELEKOM-Kunden gegenüber dem öffentlichen Netzbetreiber (ebenso die Kunden im privaten D 2-Netz). Das würde bedeuten, daß den Patienten zumindest ein Wahlrecht eingeräumt werden muß, ob sie eine verkürzte oder gar keine Speicherung der Zielrufnummer wünschen. Dieses Wahlrecht sollte sich aber nicht – wie in öffentlichen Fernsprechnetzen – auf den Einzelentgeltnachweis mit vollständiger Zielnummer erstrecken.

Allerdings erklärten verschiedene Krankenhäuser, daß bei ihrer digitalen Nebenstellenanlage die Verkürzung der Zielnummer technisch nicht möglich und aus Gründen der Abrechnungstransparenz auch nicht gewünscht sei.

Trotz aller Hinweise auf die leichte Abhörbarkeit analoger **schnurloser Telefone** besteht ein Trend, solche Telefone für die Sprachkommunikation des ärztlichen und pflegerischen Personals in Krankenkäusern einzusetzen, um die schnelle Erreichbarkeit dieser Mitarbeiter auch am Krankenbett sicherzustellen und gegebenenfalls auch Gespräche über den Zustand von Patienten unabhängig von der Verfügbarkeit stationärer Telefone führen zu können.

Wir haben in mehreren Fällen zu entsprechenden Anfragen klargestellt, daß der Nutzung solcher Telefongeräte für Gespräche mit patientenbezogenem Inhalt die ärztliche Schweigepflicht entgegen steht und empfohlen, dafür – allerdings teurere – digitale Geräte zu beschaffen, die nicht so leicht abhörbar sind.

Abhörsicherheit des Funksprechverkehrs der Behörden und Organisationen mit Sicherheitsaufgaben

Der Sprechfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) war bekanntlich seit jeher abhörbar, wenn an Empfangsgeräten geringe technische Veränderungen vorgenommen wurden. Dies war strafbar, das Entdeckungsrisiko war jedoch

[1] Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Teledienstunternehmen – Datenschutzverordnung – UDSV) vom 18. Dezember 1991, BGBl I, S. 2337; Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TELEKOM – Datenschutzverordnung – TDSV) vom 24. Juni 1991, BGBl. I S. 1390

[2] Rundschreiben über Rahmendienstvereinbarung zu digitalen Telefonnebenstellenanlagen v. 15. August 1991 (Dienstblatt I S. 305)

gering. Wirksame Maßnahmen gegen das Mithören des Sprechfunkverkehrs durch Unbefugte, insbesondere durch Straftäter, sind aus Kostengründen unterblieben. Nach der Freigabe der Frequenzbereichsgrenzen Mitte 1992 ist der Funkverkehr inzwischen mit handelsüblichen Radioempfängern mithörbar.

Aus diesem Grund wurden Überlegungen angestellt, wie in Zukunft dieser Funkverkehr vor dem Abhören durch Unbefugte geschützt werden sollte. Die Technische Kommission der Konferenz der Innenminister des Bundes und der Länder wollte die Empfehlung beschließen, nach einem in Niedersachsen erprobten Modell die vorhandenen Analogfunkgeräte mit einer Inverterschaltung (Sprachverschleierungstechnik) nachzurüsten. Diese Maßnahme ist jedoch nicht geeignet, die gewünschte Vertraulichkeit des Sprechfunkverkehrs zu erreichen, da jedermann sich legal und für einen geringen Preis geeignete Funkempfänger mit Inverter beschaffen könnte, mit denen auch das Mithören invertierter Funkgespräche möglich ist.

Es war daher zu befürchten, daß mit der unzureichenden Entscheidung der Weg verbaut wird, wirksame Methoden einzuführen. Der Innenministerkonferenz wurde daher empfohlen, die Entscheidung zu überdenken und stattdessen den Anstoß zu geben, sukzessiv den digitalen und damit leicht verschlüsselbaren Sprechfunk einzuführen, der ohnehin auf Sicht Stand der Technik und damit jedenfalls in einem Teil der Länder datenschutzrechtlich verpflichtend (vgl. z. B. § 5 Abs. 1 S. 2 BlnDSG) sein wird.

Auch aufgrund der Bedenken der Konferenz der Datenschutzbeauftragten[3] hat die Technische Kommission der Innenministerkonferenz letztlich von der Einführung der Invertertechnik Abstand genommen. Vielmehr sollen weitere technologisch und wirtschaftlich in Frage kommende Sprachverschleierungssysteme auf ihre Einsatztauglichkeit als Übergangslösungen bis zur Einführung des digitalen Funksprechverkehrs geprüft werden.

Es ist zu hoffen, daß die im Rahmen des Schengener Abkommens gefaßte Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und damit die Verschlüsselung des Funkverkehrs vorsieht, zur Beschleunigung der Einführung solcher Systeme beiträgt.

1.2 Deutschland und Europa

Zunehmende Konflikte zwischen dem Persönlichkeitsrecht des Einzelnen und der Medienfreiheit

Im Berichtszeitraum ist in der Öffentlichkeit verstärkt darüber diskutiert worden, ob die Persönlichkeitsrechte einzelner Bürger gegenüber der Berichterstattung durch die Medien ausreichend geschützt sind. Anlaß dafür waren beispielsweise

- Berichte vor allem privater Fernsehveranstalter über Unfallopfer oder Rettungseinsätze der Feuerwehr, an denen sich auch Feuerwehrbeamte oder Mitarbeiter von Rettungsdiensten beteiligten (sogenannte „Reality-TV“),
- der Fernsehbericht einer öffentlich-rechtlichen Rundfunkanstalt über Mißstände in einer Einrichtung für psychisch Kranke, bei dem die Berichterstattung keinerlei Rücksicht auf die Intimsphäre der Kranken nahm,
- die „öffentlichkeitswirksame“ Durchführung von Razzien und Maßnahmen gegen mutmaßliche Schwarzarbeiter unter Hinzuziehung von Pressevertretern, wobei die kontrollierten Personen teilweise frontal fotografiert und in den Zeitungen abgebildet wurden,

[3] vgl. Anlage 2.6

— die Weitergabe personenbezogener Daten durch öffentliche Stellen, z. B. durch Polizei und Staatsanwaltschaft, aus Ermittlungsverfahren an die Medien.

Das Grundrecht auf freie Berichterstattung durch Presse und Rundfunk hat nach unserer Verfassungsordnung einen hohen Stellenwert. Dennoch genießt dieses Grundrecht keinen generellen Vorrang vor der Menschenwürde und dem Persönlichkeitsrecht des Einzelnen, über den berichtet wird.

So unterschiedlich die genannten Fälle im einzelnen zu beurteilen sein mögen, verdeutlichen sie dennoch eine Reihe von gemeinsamen Problemen, deren Lösung gegenwärtig der Arbeitskreis Telekommunikation und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Vorsitz des Berliner Datenschutzbeauftragten erörtert.

Das sogenannte „Medienprivileg" der Datenschutzgesetze, das Rundfunk und Presse bei ihrer journalistisch-redaktionellen Tätigkeit von den materiell-rechtlichen Vorschriften des Datenschutzrechts und von der Kontrolle unabhängiger Datenschutzbeauftragter frei stellt, ist kein Freibrief für unbeschränkte Eingriffe in die Privatsphäre des Bürgers. Die Mißachtung der Menschenwürde durch die Zurschaustellung von Unfallopfern oder Menschen in Not kann nicht unter Berufung auf die Medienfreiheit gerechtfertigt werden. Dies widerspricht auch den im Rundfunkstaatsvertrag und in den Landesmediengesetzen niedergelegten Programmgrundsätzen. Vielmehr müssen die Grundrechte der Medienfreiheit und des Persönlichkeitsrechts – zu dem letztgenannten gehört auch das Recht am eigenen Bild – miteinander zum Ausgleich gebracht werden.

Daher ist der Appell der Innenministerkonferenz vom Mai 1993 an die Medien, „sich ihrer mit der Presse- und Rundfunkfreiheit verbundenen Verantwortung bewußt zu sein und von einer die Menschenwürde verletzenden Berichterstattung Abstand zu nehmen", uneingeschränkt zu begrüßen. Zwar würde der Gesetzgeber bei inhaltlichen Beschränkungen der Berichterstattungsfreiheit schnell in Konflikt mit der grundgesetzlich geschützen Medienfreiheit kommen. Andererseits muß weiter kritisch beobachtet werden, ob die bestehenden Verfahren zum Schutz des Persönlichkeitsrechts des einzelnen Bürgers (z. B. Anrufung des Deutschen Presserats und Klage vor den Zivilgerichten auf Schmerzensgeld) das Problem angemessen lösen. Zweifel bleiben angebracht.

In jedem Fall sind die Dienstbehörden in Bund und Länder verpflichtet sicherzustellen, daß sich öffentliche Bedienstete an Fernsehsendungen des sog. „Reality-TV" nicht beteiligen. Darauf haben wir den Polizeipräsidenten und die Feuerwehr hingewiesen.

Bei schweren Straftaten hat die Öffentlichkeit zwar in der Regel ein berechtigtes Informationsinteresse hinsichtlich des mutmaßlichen Täters; andererseits muß nicht jeder einer geringfügigen Straftat Verdächtigte es hinnehmen, in Presse oder Fernsehen abgebildet zu werden. Dies gilt beispielsweise bei der „öffentlichkeitswirksamen" Durchführung von Razzien und anderen polizeilichen Maßnahmen, bei denen zwar häufig die Gesichter der am Einsatz beteiligten Beamten, nicht aber die der kontrollierten Personen (z. B. mutmaßliche Schwarzarbeiter oder Hütchenspieler) auf den Pressefotos unkenntlich gemacht werden.

Erst recht ist es nicht hinnehmbar, wenn die Opfer von Straftaten, die sich dagegen nicht wehren können, zum Gegenstand einer Bildberichterstattung gemacht werden, die ausschließlich der Befriedigung von Sensationslust und der Steigerung der Zeitungsauflage dient. Die Veröffentlichung eines Fotos des abgetrennten Kopfes eines Mordopfers oder eines aus dem Fenster geworfenen Säuglings in der Boulevardpresse verletzt massiv das über den Tod hinaus zu achtende Persönlichkeitsrecht der Opfer und beeinträchtigt zudem die schutzwürdigen Belange der Angehörigen.

Auch die gezielte Weitergabe personenbezogener Daten durch öffentliche Stellen – z. B. Polizei und Staatsanwaltschaft – aus laufenden Ermittlungsverfahren, an denen die Öffentlichkeit ein legitimes Informationsinteresse hat, ist bisher nicht hinreichend normenklar geregelt. Weder der allgemeine Informationsanspruch der Presse nach dem Landespressegesetz noch die bundeseinheitlichen Richtlinien für das Straf- und Bußgeldverfahren enthalten verfassungskonforme Regelungen, die die Weitergabe personenbezogener Daten an die Medien rechtfertigen. Bisher müssen Polizei und Staatsanwaltschaft selbst bei einem berechtigten Informationsinteresse der Öffentlichkeit bei einer Abwägung im Einzelfall auf die Verfassung zurückgreifen, was nicht immer hinreichend geschieht und in der Praxis Probleme bereitet.

Es ist deshalb notwendig, daß der Bundesgesetzgeber durch entsprechende Festlegungen im Rahmen der ohnehin längst überfälligen Novellierung der Strafprozeßordnung und der Landesgesetzgeber durch Präzisierungen des Landespressegesetzes für einen sachgerechten Ausgleich zwischen den schutzwürdigen Belangen der betroffenen Bürger und dem Informationsinteresse der Allgemeinheit sorgen.

Die Länder haben durch den Abschluß des Staatsvertrages über die Körperschaft des öffentlichen Rechts „Deutschlandradio" und eines entsprechenden Hörfunk-Überleitungsstaatsvertrages mit der Bundesrepublik Deutschland[4] eine neue Rundfunkanstalt gegründet, die zwei Hörfunkprogramme veranstaltet. In ihnen sind die Programme von RIAS 1 und DS-Kultur aufgegangen. Das Deutschlandradio hat seinen Sitz in Berlin und Köln. Der „Deutschlandradio"-Staatsvertrag enthält auch Datenschutzvorschriften, die allerdings erheblich hinter dem Standard zurückbleiben, den das Berliner Datenschutzgesetz für den Sender Freies Berlin vorsieht. Während beim Sender Freies Berlin die Verarbeitung personenbezogener Daten im Verwaltungsbereich, also insbesondere der Daten von Gebührenzahlern und Mitarbeitern, durch den Berliner Datenschutzbeauftragen kontrolliert werden, gibt es beim Deutschlandradio keine vergleichbare unabhängige Datenschutzkontrolle. Vielmehr werden die Datenschutzvorschriften des „Deutschlandradio"-Staatsvertrages ausschließlich durch den internen Rundfunkdatenschutzbeauftragten überwacht. Bei den Verhandlungen über diesen Staatsvertrag sind wir nicht beteiligt worden, so daß es uns nicht möglich war, auf eine Verbesserung des Datenschutzes bei der neuen Rundfunkanstalt hinzuwirken.

GEZ: schneller als der Möbelwagen?

Der Sender Freies Berlin (SFB) betreibt gemeinsam mit den übrigen öffentlich-rechtlichen Rundfunkanstalten die Gebühreneinzugszentrale (GEZ) in Köln. Diese Einrichtung verarbeitet aufgrund des Rundfunkstaatsvertrages zentral die Daten der Rundfunkteilnehmer im Auftrag der jeweiligen Landesrundfunkanstalt, also auch des Sender Freies Berlin. Können Mitteilungen oder Zahlungsaufforderungen der GEZ von der Post nicht zugestellt werden, so holt der SFB gegenwärtig eine Melderegisterauskunft beim Landeseinwohneramt über den betroffenen Bürger ein, um ihm das Schreiben zustellen zu können. Dies geschieht in der Praxis mittels Magnetbändern, mit denen die Daten postalisch nicht erreichbarer Bürger aus dem Bestand der Rundfunkanstalt mit dem Adressenbestand der Meldebehörde verglichen werden. Dabei handelt es sich um gebündelte Einzelauskünfte aus dem Melderegister, die nach § 25 Meldegesetz zulässig sind. Dieses Verfahren ist nicht zu beanstanden und hat sich auch nach Auffassung der Senatsverwaltung für Inneres bewährt.

[4] vgl. das Berliner Zustimmungsgesetz vom 25. Oktober 1993, GVBl. 1993, S. 473 ff.

Demgegenüber fordert der SFB gemeinsam mit den anderen Rundfunkanstalten, in Zukunft sollten die Meldebehörden verpflichtet werden, von sich aus regelmäßig bei einer Reihe von Änderungen des Meldedatenbestandes – bei jedem Umzug und jedem Sterbefall – die GEZ hierüber unaufgefordert zu informieren. In Hessen und Nordrhein-Westfalen ist dies bereits geltendes Recht. Hintergrund für diese Forderung der Rundfunkanstalten ist der härter werdende Konkurrenzkampf mit den privaten, nicht gebührenfinanzierten Rundfunkveranstaltern, der die öffentlich-rechtlichen Rundfunkanstalten neben Einsparungen im eigenen Bereich dazu zwingt, den Gebühreneinzug effektiver zu gestalten. Nach Angaben der Rundfunkanstalten ist der Adressenbestand der GEZ deshalb vielfach veraltet, weil die Rundfunkteilnehmer der GEZ Anschriftenänderungen entweder überhaupt nicht oder verspätet mitteilen. Durch die regelmäßige Übermittlung von Meldedatenänderungen hoffen die Rundfunkanstalten, ihr Gebührenaufkommen entscheidend zu erhöhen, indem der von ihnen vermutete erhebliche Anteil der „Schwarzseher“ ermittelt werden könnte.

Die Konferenz der Ministerpräsidenten der Länder hat die Forderung der Rundfunkanstalten aufgegriffen und die Innenministerkonferenz um einen Vorschlag zur bundeseinheitlichen Änderung des Melderechts gebeten. Der Entwurf der Innenministerkonferenz, der bei Stimmenthaltung Berlins beschlossen wurde, sieht eine Änderung des Melderechtsrahmengesetzes vor, wonach künftig alle Meldebehörden im Fall der Anmeldung, der Abmeldung oder des Todes eines volljährigen Einwohners dessen Namen, Geburtstag, gegenwärtige und frühere Anschriften, Tag des Ein- bzw. des Auszuges, Familienstand und im Todesfall den Sterbetag den Rundfunkanstalten übermitteln sollen.

Bei einer Verwirklichung dieses Vorschlags würde ein entscheidender Schritt in Richtung auf ein Bundesmelderegister aller volljährigen Einwohner der Bundesrepublik getan, das bei den Beratungen des Melderechtsrahmengesetzes im Bundestag ausdrücklich aus Gründen des Datenschutzes abgelehnt worden ist. Zwar sieht der Rundfunkstaatsvertrag vor, daß die Rundfunkanstalten jeweils nur auf die Daten der zu ihrem Sendebereich gehörenden Hörer und Zuschauer zugreifen dürfen, im Fall des Umzugs in die Bereiche anderer Sender darf aber auch auf deren Datenbestände zugegriffen werden. Außerdem ist abzusehen, daß schon die Existenz des dann entstehenden bundesweiten Meldedatenbestandes bei der GEZ zu großen Begehrlichkeiten bei einer Vielzahl von öffentlichen und privaten Stellen führen würde.

Entscheidend ist aber, daß bei dem vorgeschlagenen Verfahren in großem Umfang Meldedaten an die Rundfunkanstalten übermittelt würden, die diese zum Einzug von Rundfunkgebühren nicht benötigen. Viele Bürger teilen von sich aus der GEZ mit, daß sie ein Rundfunkgerät zum Empfang bereithalten oder daß sie umgezogen sind. Durch die vorgeschlagene regelmäßige Meldedatenübermittlung an die Rundfunkanstalten würde in unverhältnismäßiger Weise in das informationelle Selbstbestimmungsrecht dieser Bürger eingegriffen. Ein solcher Eingriff läßt sich weder mit den finanziellen Problemen der öffentlich-rechtlichen Rundfunkanstalten noch mit deren verfassungsrechtlicher Bestandsgarantie rechtfertigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb die vorgeschlagene regelmäßige Übermittlung von Meldedaten an die öffentlich-rechtlichen Rundfunkanstalten abgelehnt[5]. Selbst wenn der Entwurf der Innenministerkonferenz Eingang in das Melderechtsrahmengesetz finden sollte, sind wir mit der Senatsverwaltung für Inneres[6] der Auffassung, daß eine entsprechende Änderung des Berliner Meldegesetzes nicht in Betracht kommt, solange datenschutzrechtliche Alternativen nicht einmal geprüft worden sind.

Dringend erforderlich ist dagegen die bereits Anfang 1992 von uns **angemahnte Ergänzung der Verordnung über die Feststellung der Befreiung von der Rundfunkgebührenpflicht**[7] um die erforderlichen Befugnisse zur Datenverarbeitung. Insbesondere die Übermittlung der Daten von Personen, die von der Rundfunkgebührenpflicht durch die Sozialämter befreit worden sind, an den SFB erfolgt gegenwärtig immer noch ohne die erforderliche Rechtsgrundlage.

Die zweite Stufe der Postreform – Privatisierung der TELEKOM zu Lasten der Kunden?

Die vollständige Privatisierung der Deutschen Bundespost TELEKOM, die in eine AG umgewandelt werden soll, ist politisch beschlossene Sache. Die Beratungen über die dazu erforderliche Grundgesetzänderung und ergänzende gesetzliche Regelungen haben Anfang 1994 begonnen.

Schon im Juni 1993 hat die TELEKOM allerdings ein Tochterunternehmen, die DeTeMobil-GmbH, gegründet und ihr den Betrieb sämtlicher Mobilfunkeinrichtungen (C- und D 1-Netze, Eurosignal, CITY-Ruf, Bündelfunk) übertragen.

Die mit jeder Privatisierung öffentlicher Aufgabenerfüllung verbundenen datenschutzrechtliche Probleme sind bereits an anderer Stelle[8] behandelt worden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat gerade im Zusammenhang mit der zweiten Stufe der Postreform betont, daß die Privatisierung der TELEKOM nicht zu einer Schlechterstellung der Bürger durch eine Absenkung des materiell-rechtlichen Datenschutzstandards führen darf. Dies gilt insbesondere bei dem wichtigsten von der TELEKOM angebotenen Dienst, dem Sprachtelefondienst. Außerdem muß der Gesetzgeber sicherstellen, daß für eine zukünftige TELEKOM-AG und ihre Tochterunternehmen eine einheitliche Datenschutzkontrolle gewährleistet wird, bei der auch eine Kontrolle von Amts wegen möglich ist. Die Aufsichtsbehörden für den privaten Bereich können dagegen nach dem geltenden Bundesdatenschutzgesetz nur einschreiten, wenn ihnen hinreichende Anhaltspunkte für eine Verletzung datenschutzrechtlicher Bestimmungen vorliegen. Die meisten Aufsichtsbehörden werden deshalb erst auf Beschwerden von Bürgern hin tätig. Dies ist jedoch gerade im Bereich der Telekommunikation nicht ausreichend, zumal der Bürger die Datenverarbeitung in digitalen Telekommunikationsnetzen kaum durchschauen kann und deshalb nur selten Anlaß für eine Beschwerde sehen wird[9].

Die durch den **Fangschaltungsbeschluß** des Bundesverfassungsgerichts[10] notwendig gewordene Neuregelung des Telekommunikationsrechts steht noch immer aus und soll jetzt im Zusammenhang mit der zweiten Stufe der Postreform erfolgen. Dabei wird es darauf ankommen, eine verfassungskonforme Rechtsgrundlage für die Verarbeitung der zwangsläufig anfallenden Verbindungsdaten in öffentlichen und privaten Telekommunikationsnetzen zu schaffen. Zugleich muß der verfassungsrechtlich bedenkliche Zustand beendet werden, daß gegenwärtig Auskünfte über Verbindungsdaten an die Strafverfolgungsbehörden auch bei Bagatelldelikten zulässig sind.

---

5 Anlage 2

6 vgl. die Antwort des Senats auf die Kleine Anfrage Nr. 4619 LPD v. 15. Dezember 1993

7 vgl. Jahresbericht 1991, 2.3

8 vgl. 3.2

9 vgl. Anlage 2.4

10 dazu vgl. Jahresbericht 1992, 5.2

Zum 1. Januar 1994 ist eine Vorschrift der TELEKOM-Datenschutzverordnung (TDSV) in Kraft getreten, die dem Telefonkunden das Recht gibt, fallweise – also bei jedem Telefongespräch – darüber zu entscheiden, ob er die bei ISDN-fähigen Telefonapparaten mögliche **Anzeige seiner Rufnummer** beim Angerufenen unterdrücken will oder nicht. Dies könnte technisch durch Knopfdruck oder durch Wahl einer bestimmten Nummer vor der eigentlichen Rufnummer geschehen. Bisher ist jedoch nicht erkennbar, daß die TELEKOM oder andere Hersteller von Telefonapparaten entsprechende Geräte anbieten. Damit droht ein wichtiges Wahlrecht der TDSV leerzulaufen, weil der Telefonkunde, der einen ISDN-Hauptanschluß hat, bisher darauf verwiesen wird, sich ein für alle Mal für oder gegen die Rufnummernanzeige zu entscheiden. Die Anzeige der Rufnummern von analogen Anschlüssen, von denen aus beim Inhaber eines ISDN-fähigen Telefons angerufen wird, ist zwar technisch möglich, wird aber nach Angaben der TELEKOM bisher nicht durchgeführt. Nach dem Wortlaut der TDSV müßte auch in diesem Fall eine individuelle Unterdrückungsmöglichkeit (z. B. durch Wahl einer bestimmten Ziffer) geschaffen werden, bevor Rufnummern von analogen Anschlüssen angezeigt werden dürfen.

Auf der Ebene der **Europäischen Union** tritt die Entwicklung des Telekommunikationsdatenschutzrechts noch immer auf der Stelle. Die Europäische Kommission hat im Berichtszeitraum keine geänderte Fassung ihres Vorschlags für eine **ISDN-Richtlinie** beschlossen, so daß der Abstand zwischen diesem für den europäischen Telekommunikationsmarkt so wichtigen Vorhaben und der **allgemeinen Datenschutzrichtlinie,** mit der er ursprünglich gemeinsam in Kraft gesetzt werden sollte, immer größer wird. Gleichzeitig sind andere Initiativen der Europäischen Kommission im Telekommunikationssektor schon sehr viel weiter gediehen, etwa der Entwurf für eine Richtlinie über den **offenen Netzzugang im Sprachtelefondienst**[11], die zum Teil Regelungen enthält, die erheblich hinter dem Vorschlag für eine ISDN-Datenschutzrichtlinie zurückbleiben. Die endgültige Beschlußfassung im Rat bleibt allerdings abzuwarten.

Besonderes Gewicht mißt die Kommission auch dem Aufbau der im Europäischen Unionsvertrag von Maastricht genannten **transeuropäischen Netze** bei. Insbesondere das ISDN wird zu einem der ersten transeuropäischen Netze ausgebaut werden[12]. Auch der grenzüberschreitende Datenaustausch zwischen Verwaltungen wird von der Kommission gefördert[13].

Der Ministerrat der Europäischen Gemeinschaften (Europäische Rat) hat am 22. Juli 1993[14] beschlossen, daß die Monopole im öffentlichen Sprachtelefondienst europaweit bis zum 1. Januar 1998 beseitigt werden müssen. Dies soll im Zuge der zweiten Stufe der Postreform auch in der Bundesrepublik umgesetzt werden. Damit wird es in naher Zukunft in der Europäischen Union zu einem Wettbewerb zwischen zahlreichen Diensteanbietern kommen, so daß sich das oben beschriebene Problem der Gewährleistung eines einheitlichen hohen Datenschutzstandards auch auf europäischer Ebene stellen wird. Schon deshalb ist es dringend erforderlich, **daß die von der Kommission vorgeschlagene Datenschutzrichtlinie für das ISDN** zügig verabschiedet wird. Darauf hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hingewiesen[15].

Einer Lösung auf europäischer Ebene bedürfen auch die Datenschutzprobleme im Zusammenhang mit der Mobilkommunikation. So müssen die Daten der Mobilfunkteilnehmer auf der Funkstrecke wirksam verschlüsselt werden. Eine bloße Digitalisierung

11 KOM (92) 247 endg. – SYN 437; geänderter Vorschlag KOM (93) 182 endg. – SYN 437

12 KOM (93) 347 endg.

13 KOM (93) 69 endg.

14 Amtsblatt der EG Nr. C 213 vom 6. August 1993

15 Anlage 2.5

der Signale reicht nicht aus, denn durch sie wird das Abhören nur erschwert, nicht aber zuverlässig ausgeschlossen. Den Benutzern sollte eine kostenlose Ende-Zu-Ende-Verschlüsselung angeboten werden. Vor allem aber müssen gerade bei der Mobilkommunikation, wo Informationen über den jeweiligen Standort des Teilnehmers auch dann verarbeitet werden, wenn sein Gerät nur empfangsbereit ist, wirksame Vorkehrungen gegen die Entstehung von Bewegungsbildern getroffen werden. Dazu müssen laufende und künftige Normierungsprozesse entsprechend beeinflußt werden. Wenn schon der Anfall solcher Standortdaten nicht von vornherein technisch ausgeschlossen werden kann, muß durch die Gesetzgebung der Union oder der Mitgliedstaaten eine strenge Zweckbindung dieser Daten an die technische Vermittlung der Telekommunikationsverbindung gewährleistet werden. Jede darüber hinausgehende Nutzung sollte ausdrücklich untersagt werden.

Gerade im Bereich der Telekommunikation ist es entscheidend, daß die Europäische Union nicht unter Hinweis auf den Grundsatz der Subsidiarität davon absieht, die angesprochenen Fragen möglichst einheitlich zu regeln. Die Mobilkommunikation wird gerade im grenzüberschreitenden Verkehr große Bedeutung erlangen, wie das Beispiel der Erhebung von Straßenbenutzungsgebühren zeigt[16]. Einheitliche hohe Datenschutzanforderungen sind deshalb eine Grundvoraussetzung für die Akzeptanz dieser Technik, der die Europäische Kommission mit Recht so große Bedeutung beimißt.

2. Entschließung der 46. Konferenz am 26./27. Oktober 1993 zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)

(gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens)

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung insbesondere aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

16 vgl. oben 4.11

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

3. Entschließung der 46. Konferenz am 26./27. Oktober 1993 zum Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste

Im Zuge der sog. Postreform II soll die Deutsche Bundespost Telekom – nach der dafür notwendigen Änderung des Grundgesetzes – in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. August 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der „Telekom AG“ auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Diensteanbieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die – wie der Telefondienst – der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

4. Entschließung der 46. Konferenz am 26./27. Oktober 1993 zur Gewährleistung des Datenschutzes bei der Mobilkommunikation

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits jetzt in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunikationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind – wie z. B. in den digitalen D-Netzen –, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzliche Sicherheitsvorkehrungen trifft, also z. B. die übertragenen Daten anwendungsseitig verschlüsselt.

Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen – den sogenannten Service-Providern, die lediglich Dienste vermarkten –, personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten an der EG-Richtlinie über Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

5. Bericht der Arbeitsgruppe Telekommunikation und Medien an die 15. Internationale Konferenz der Datenschutzbeauftragten in Manchester (27. bis 30. September 1993)

Die Arbeitsgruppe hat im laufenden Jahr zwei Treffen abgehalten.

1.

Seit 1991 nimmt der Direktor des Instituts für Systemanalyse der Russischen Akademie der Wissenschaften, der für die Automatisierung der russischen Verwaltung zuständig ist, als Gast an den Treffen der Arbeitsgruppe teil. Während dieser Treffen hat er immer wieder auf die Wichtigkeit der Schaffung von Datenschutzregelungen insbesondere bei der Einführung neuer Telekommunikationsstrukturen hingewiesen.

Auf seine Initiative hin hat das Regierungskomitee für Informatisierung der Russischen Föderation die Arbeitsgruppe eingeladen, ihr Frühjahrstreffen vom 17. bis 19. Mai 1993 in Moskau abzuhalten.

Um die Arbeitsgruppe über die gegenwärtige Situation im Bereich der Automatisierung und Telekommunikation zu informieren, haben dort Experten von verschiedenen russischen Regierungsstellen und akademischen Institutionen Vorträge über die gegenwärtige Situation in ihren jeweiligen Bereichen gehalten. Die Berichte umfaßten

- —den Fortschritt in der Russischen Föderation bei der Entwicklung von gesetzlichen Grundlagen für die Benutzung von Informationstechnologien;
- —den Gesetzentwurf der Russischen Föderation über Information, Automatisierung und Informationssicherheit;
- —die Entwicklung von Satellitenkommunikations- und Mobilkommunikationssystemen. (Diese Systeme spielen in Rußland eine besondere Rolle, da die existierenden Festnetze in sehr schlechtem Zustand sind.)

Mitglieder der Arbeitsgruppe berichteten über

- —Maßnahmen zur Datensicherheit in der Telekommunikation;
- —Regelungen zur Datensicherheit in Westeuropa;
- —Nachrichtenstandards, Sicherheit und rechtliche Aspekte des elektronischen Datenaustausches (Electronic Data Interchange – EDI);
- —neuere Entwicklungen bei der Anwendung von Prinzipien der Datensicherheit auf Mobilkommunikationssysteme.

Die Diskussion mit den russischen Experten zeigte, daß das Bewußtsein für Datenschutzprobleme im Zusammenhang mit der schnellen Ausbreitung von Telekommunikationsnetzen und -diensten, die gegenwärtig in Rußland stattfindet, bisher wenig entwickelt ist.

Es ist daher dringend notwendig, die existierenden Initiativen im Bereich der Datenschutzgesetzgebung und die Anwendung von Datensicherungsmaßnahmen bei den sich ausbreitenden Telekommunikationsnetzen zu unterstützen. Vor diesem Hintergrund erklärte sich die Arbeitsgruppe bereit, Möglichkeiten zu prüfen, wie der Informationsaustausch über Datenschutzregelungen im Bereich der Telekommunikation mit dem Russischen Komitee für Informatisierung verbessert werden könnte.

Auf Wunsch der Vertreter des Russischen Komitees für Informatisierung und des Instituts für Systemanalyse der Russischen Akademie der Wissenschaften bot die Arbeitsgruppe fachliche Unterstützung bei aufkommenden Problemen in diesem Bereich an.

2.

Traditionsgemäß wurde die zweite Sitzung der Arbeitsgruppe in Berlin während der Internationalen Funkausstellung 1993 abgehalten (30. August 1993).

2.1

Die Privatisierung, Liberalisierung und Deregulierung von Telekommunikationsnetzen und -diensten findet in den meisten in der Arbeitsgruppe repräsentierten Ländern statt, wobei Geschwindigkeit und Ausmaß dieser Bemühungen differieren.

Aufgrund eines von uns erarbeiteten Fragebogens erhielten wir schriftliche Länderberichte aus Österreich, Belgien, Finnland, Frankreich, den Niederlanden, Norwegen, Portugal und Großbritannien. Die Vertreter Ungarns, Luxemburgs, Rußlands und Schwedens berichteten mündlich während des Treffens über die Situation in ihren Ländern. In den meisten westlichen Ländern, über die berichtet wurde, ist das allgemeine Datenschutzrecht sowohl auf den öffentlichen als auch auf den privaten Sektor anwendbar. Trotzdem haben bisher nur wenige Länder bereichsspezifische Regelungen erlassen, die die Speicherung und den Schutz von Verkehrsdaten, die in modernen Kommunikatonsnetzen erzeugt werden, regeln.

Die Mitglieder der Arbeitsgruppe waren sich einig, daß Bürger, die Telekommunikationsnetze oder -dienste benutzen, unabhängig davon, ob die Netze oder Dienste von einer öffentlichen oder einer privaten Telekommunikationsorganisation betrieben werden, dasselbe Datenschutzniveau genießen sollen. Die Arbeitsgruppe sieht jedoch die Gefahr, daß die Privatisierung, Liberalisierung und Deregulierung dieser Märkte tatsächlich zu einer Absenkung des Datenschutzstandards führen könnte.

Es ist daher dringend notwendig, auf den Erlaß spezifischer gesetzlicher Regelungen zu dringen, die im Zusammenhang mit dem Wettbewerb zwischen Netzbetreibern und Dienstanbietern einen gleichmäßig hohen Standard des Datenschutzes für die Benutzer regeln. Darüber hinaus sollten für private und öffentliche Netzbetreiber und Dienstanbieter die gleichen Regelungen gelten.

2.2

Die Anwendung moderner Telekommunikationseinrichtungen zur Überwachung des Straßenverkehrs wird gegenwärtig in verschiedenen Ländern diskutiert. Die Überwachung des Verkehrs dient so unterschiedlichen Zwecken wie dem Flottenmanagement, der Wiederauffindung gestohlener Fahrzeuge sowie der Erhebung von Straßenbenutzungsgebühren. Diese Pläne lassen ernsthafte Bedenken bezüglich der damit verbundenen Datenschutzrisiken aufkommen.

Die Mitglieder der Arbeitsgruppe für Telekommunikation und Medien waren sich darüber einig, daß solche Pläne nur dann umgesetzt werden sollten, wenn gleichzeitig wirksame Maßnahmen gegen diese Risiken getroffen werden. Insbesondere sollte die Erstellung von Bewegungsbildern einzelner Verkehrsteilnehmer ausdrücklich verboten werden.

Die Arbeitsgruppe wird die weitere Entwicklung auf diesem Gebiet gründlich untersuchen und sich dabei insbesondere um die Findung alternativer Technologien kümmern, die besser im Einklang mit den Prinzipien des Datenschutzes stehen.

2.3

Darüber hinaus wurden erörtert

- Datenschutz im Bezug auf grenzüberschreitende Telekommunikation mit Mobiltelefonen („International Roaming“);
- die Ausbreitung nationaler und internationaler Teilnehmerverzeichnisse in Forschungs- und sonstigen Telekommunikationsnetzen („X.500 directories“);
- Mobilkommunikation in Luftfahrt und Verkehr.

Die Arbeitsgruppe wird diese Probleme auf ihren nächsten Sitzungen näher untersuchen.

B. Auszug aus dem Jahresbericht 1994 des Berliner Datenschutzbeauftragten

1. Geschäftsbereich: Telekommunikation und Medien

1.1 Telekommunikation in Deutschland und Europa

Postreform II – Gesetz zur Neuordnung des Postwesens und der Telekommunikation

Der Bundestag hat im September 1994 das Gesetz zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz – PTNeuOG[17]) beschlossen, das neben den Weichenstellungen für die Umwandlung der Deutschen Bundespost in drei Aktiengesellschaften auch zahlreiche Änderungen des materiellen Datenschutzrechts im Bereich der Telekommunikation enthält. Das Gesetz ist am 1. Januar 1995 in Kraft getreten. Zu den aus Datenschutzsicht wichtigsten Änderungen zählen insbesondere folgende:

Nach Art. 13 § 1 Nr. 3 PTNeuOG tritt das Postverfassungsgesetz zum 1. Januar 1995 außer Kraft. Damit entfällt insbesondere die Verordnungsermächtigung aus § 30 Abs. 2 Postverfassungsgesetz, **aufgrund deren die TELEKOM-Datenschutzverordnung (TDSV) und die Teledienstunternehmen – Datenschutzverordnung (UDSV),** die gegenwärtig den Datenschutz in diesem Bereich regeln, erlassen worden sind. Gleichzeitig ermächtigt das Gesetz über die Regulierung der Telekommunikation des Postwesens (PTRegG, Art. 7 PTNeuOG) in § 10 die Bundesregierung, eine entsprechende Rechtsverordnung zum Schutz personenbezogener Daten der am Fernmeldeverkehr oder am Postverkehr Beteiligten zu erlassen, welche die Erhebung, Verarbeitung und Nutzung dieser Daten regelt. Eine solche Rechtsverordnung, die der Zustimmung des Regulierungsrates und damit auch der Bundesländer bedarf, steht noch aus.

Für die Übergangszeit gelten die Regelungen von TDSV und UDSV mit den im Fangschaltungsbeschluß des Bundesverfassungsgerichts[18] getroffenen Einschränkungen fort.

Der Gesetzgeber hat in § 10 PTRegG gleichzeitig versucht, die Konsequenzen aus dem Fangschaltungsbeschluß zu ziehen und Vorgaben für den Inhalt der zu erlassenen Rechtsverordnung im Gesetz formuliert.

Es ist leider nicht gelungen, im Rahmen der Postreform II eine wesentliche Verbesserung des Datenschutzes in der Telekommunikation zu erreichen. Teilweise bewirkt das Postneuordnungsgesetz sogar eine Verschlechterung der Positionen der Betroffenen.

So ist die dringend notwendige Erstreckung des Post- und Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG auf die Rechtsnachfolger der Deutschen Bundespost nicht erfolgt. Das Post- und Fernmeldegeheimnis schützt den Bürger bisher ausschließlich vor Eingriffen des Staates und der Deutschen Bundespost. Die Geltung des Fernmeldegeheimnisses ist lediglich einfachgesetzlich (durch § 10 Fernmeldeanlagengesetz – FAG –) auf private Betreiber einer für den öffentlichen Verkehr bestimmten Fernmeldeanlage erstreckt worden. Durch die vollständige Privatisierung der bisher in Behördenform geführten Unternehmen der Deutschen Bundespost fällt ein Hauptadressat des ausschließlich staatsge-

[17] BGBl. I, 2325 ff.

[18] BVerfGE 85, 386; dazu vgl. Jahresbericht 1992, 1.1

richteten Grundrechts aus Art. 10 Abs. 1 GG weg. Die gesetzliche Erstreckung des Fernmeldegeheimnisses auf alle Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, wird außerdem befristet, denn das gesamte Fernmeldeanlagengesetz tritt mit Ablauf des 31. Dezember 1997 außer Kraft (§ 23 PTRegG). Wie der Grundrechtsschutz des Bürgers nach dem Wegfall des Monopols der Deutschen Telekom AG gesichert wird, ist gegenwärtig völlig offen.

Bereits in früheren Jahresberichten hatten wir darauf hingewiesen, daß § 12 FAG, der eine Auskunftserteilung über Verbindungsdaten für jedes beliebige Strafverfahren zuläßt, dringend änderungsbedürftig ist[19]. Auch diese Änderung ist im Rahmen der Postreform II unterblieben.

Das Postneuordnungsgesetz stellt auch nicht die einheitliche Kontrolle der Einhaltung von Datenschutzbestimmungen bei allen Nachfolgeunternehmen der Deutschen Bundespost sicher. Artikel 12 Abs. 16 PTNeuOG beschränkt die Kontrollkompetenz des Bundesbeauftragten für den Datenschutz vielmehr auf die „aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen . . .“. Dies hat bereits jetzt zur Folge, daß nicht durch Gesetz entstandene Tochterunternehmen der Deutschen Bundespost TELEKOM, wie z. B. die DeTeMobil und die DeTeMedien zum 1. Januar 1995 nicht mehr in die Kontrollkompetenz des Bundesbeauftragten für den Datenschutz (BfD), sondern in die der lokal zuständigen Aufsichtsbehörde fallen. Darüber hinaus fällt die Kontrollbefugnis des BfD mit dem Wegfall der Monopole ebenfalls der jeweiligen Aufsichtsbehörden zu, wenn im Zuge der jetzt bevorstehenden **Postreform III** keine anderen Entscheidungen getroffen werden. Damit bleibt eine wesentliche Forderung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder unberücksichtigt, die die Sicherstellung einer bundesweit einheitlichen Kontrolle gefordert hatten[20]. Im Rahmen der Beratungen im Bundestagsausschuß für Post und Telekommunikation bestand jedoch Einigkeit darüber, „. . . daß für die Zeit, wenn DBP TELEKOM und DBP Postdienst über keine Monopole mehr verfügen und daher § 2 Abs. 1 BDSG für die Zuständigkeit des Bundesbeauftragten für den Datenschutz bei den Unternehmen seine Wirkung verlieren wird, in Absprache mit den Bundesländern eine zentrale Kontrollstelle für den Datenschutz bestimmt werden soll.“[21]

Auch die von uns bereits mehrfach kritisierte Regelung zur **Anzeige der Rufnummer des Anrufers bei telefonischen Beratungsstellen** sowie der Aufnahme der Rufnummern dieser Stellen in **Einzelentgeltnachweise**[22] ist eher noch zu Lasten des Bürgers verändert worden. Die im Gesetz bezüglich der telefonischen Beratungsstellen getroffenen Festlegungen sind jedenfalls nach wie vor unzureichend. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat demgegenüber in ihrer Entschließung[23] das „Holländische Modell“ favorisiert, bei dem jeder Kunde selbst darüber entscheiden kann, ob seine Rufnummer in Einzelentgeltnachweise von Anrufern aufgenommen wird oder nicht.

Bisherige Dauer der Speicherung von Verbindungsdaten bei der TELEKOM rechtswidrig?

Das Oberverwaltungsgericht Bremen hat[24] die TELEKOM verpflichtet, Rufnummern von angerufenen Teilnehmern aus dem digitalen Telekommunikationsnetz ISDN nur höchstens vier Tage in voller Länge zu speichern. Danach müssen die letzten drei Ziffern des

19 vgl. Jahresbericht 1992, 5.2 sowie Jahresbericht 1991, 2.3

20 Jahresbericht 1993, Anlage 2.4

21 vgl. den Anschlußbericht BT-Drs. 12/8060, S. 200, Anm. zu § 10

22 vgl. Jahresbericht 1991, 2.3

23 vgl. Anlage 2.5

24 Az. OVG 1 BA 30/92 v. 14. Juli 1994

angerufenen Anschlusses gelöscht werden. Die Kläger hatten die sofortige Löschung der Telefondaten aus dem digitalen Telefonnetz ISDN gefordert und angeführt, für eine weitergehende Speicherung und den damit verbundenen Eingriff in das Fernmeldegeheimnis bestehe gegenwärtig keine gesetzliche Grundlage. Nach Auffassung des Gerichts ist zur Aufrechterhaltung des Telefonverkehrs eine kurzfristige Speicherung jedoch weiterhin zulässig.

Die TELEKOM hat gegen das Urteil Revision eingelegt. Sollte diese Entscheidung vor dem Bundesverwaltungsgericht Bestand haben, so wäre die entsprechende Regelung der TDSV, die eine Speicherung der Zielnummern von bis zu 80 Tagen vorsieht und ohnehin ersetzt werden muß, rechtswidrig.

Daten der Telefonauskunft auf CD-ROM

Bereits mehrfach haben wir in vergangenen Jahresberichten über das Angebot von Teilnehmerverzeichnissen der TELEKOM auf elektronisch lesbaren Datenträgern berichtet[25]. Dabei hatten wir kritisiert, daß der Benutzer der Eintragung seiner Daten in das Telefonbuch (§ 10 Abs. 3 TDSV) nicht so differenziert widersprechen kann, daß lediglich eine Eintragung auf elektronischen Datenträgern ausgeschlossen wird[26]. Die Einführung eines solchen differenzierten Widerspruchsrechts ist umso dringlicher, als die DeTeMedien (ehem. Deutsche Postreklame GmbH) künftig neben der bereits bestehenden Möglichkeit, eine zu einem Namen gehörige Telefonnummer aufzufinden, weitere Suchmöglichkeiten plant, wie z. B. die „invertierte Suche“, bei der der Name des Benutzers zu einer eingegebenen Telefonnummer aufgefunden wird. Damit werden die bereits bisher bestehenden erheblichen Auswertungsmöglichkeiten elektronischer Telefonbücher nochmals erweitert. Die TELEKOM hat es auch in den neuen Telefonbüchern 1994/95 unterlassen, die Kunden über die Folgen einer Weitergabe ihrer Daten auf elektronischen Datenträgern umfassend aufzuklären.

Telekommunikation in Europa

Im Rahmen der **Europäischen Union** sind im Berichtszeitraum zahlreiche Initiativen im Bereich der Telekommunikations- und Medienpolitik ergriffen worden. Verbindliche Regelungen zum Schutz der Daten von Telekommunikationskunden und Mediennutzern stehen allerdings nach wie vor aus. Die Konferenz der Europäischen Datenschutzbeauftragten hat bei ihrer Sitzung in Madrid[27] darauf hingewiesen, daß die zahlreichen Initiativen der Europäischen Kommission zur schnellen Einführung neuer Telekommunikationsdienste und transeuropäischer Telekommunikationsnetze den Datenschutz bisher nur unzureichend berücksichtigen und sehr viel weiter gediehen sind, als die Beratungen über die allgemeine Datenschutzrichtlinie und die ISDN-Richtlinie. Insofern besteht ein erheblicher **Harmonisierungsbedarf** zwischen Maßnahmen zur Öffnung der Märkte und der europäischen Datenschutzgesetzgebung. Die Datenschutzbeauftragten sehen die konkrete Gefahr, daß die beiden Datenschutzrichtlinien, wenn sie verabschiedet werden, möglicherweise bereits von den zahlreichen umgesetzten Maßnahmen zur Einführung neuer Dienste und Netze überholt sein könnten. Sie haben deshalb die Europäische Union aufgefordert, schon jetzt spezielle Datenschutzvorschriften in diejenigen Rechtsakte aufzunehmen, die im Telekommunikationsbereich vor Verabschiedung der Datenschutzrichtlinien beschlossen werden.

25 vgl. z. B. Jahresbericht 1991, 2.3

26 vgl. Jahresbericht 1992, 5.2

27 vgl. Anlage 3.1

Fast vier Jahre nachdem die Europäische Kommission einen ersten Vorschlag für eine **ISDN-Richtlinie** gemacht hatte, hat die Kommission im Juni 1994 einen geänderten Vorschlag für diese Richtlinie vorgelegt[28], nachdem zeitweise die Gefahr bestanden hatte, daß die Kommission ihr ursprüngliches Vorhaben völlig aufgeben würde. Die Änderungen werden von der Kommission in erster Linie mit dem Hinweis auf das vom Europäischen Rat in Edinburgh als Maßstab für die Unionsgesetzgebung festgelegte Subsidiaritätsprinzip und mit einer Beschränkung des Richtlinieninhalts auf telekommunikationsspezifische Fragen begründet, während allgemeine datenschutzrechtliche Fragen von der bereits weiter fortgeschrittenen Datenschutzrichtlinie beantwortet werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung[29] die Bundesregierung aufgefordert, noch unter der deutschen Ratspräsidentsschaft diesen geänderten Vorschlag vordringlich zu behandeln, damit er möglichst bald vom Rat und vom Europäischen Parlament beschlossen werden kann. Dies ist deshalb nicht gelungen, weil sich die Beratungen über die allgemeine Datenschutzrichtlinie im Rat bis Ende 1994 hingezogen haben. Auch inhaltlich haben sowohl die deutschen als auch die europäischen Datenschutzbeauftragten[30] Verbesserungsvorschläge zum geänderten Richtlinienentwurf der Kommission gemacht.

Die „Gruppe von Persönlichkeiten zur Informationsgesellschaft“ hat unter dem Vorsitz von Kommissionsmitglied Bangemann in ihren Empfehlungen für den Europäischen Rat **„Europa und die globale Informationsgesellschaft“**[31] zwar die rasche Verabschiedung des Richtlinienvorschlags der Kommission über allgemeine Prinzipien des Datenschutzes durch die Mitgliedstaaten als erforderlich bezeichnet, weil ohne die rechtliche Sicherheit eines unionsweiten Konzepts für den Datenschutz der Vertrauensmangel auf seiten des Verbrauchers einer raschen Entwicklung der Informationsgesellschaft im Wege stehe. Bedauerlicherweise wird der Vorschlag für eine ISDN-Richtlinie aber nicht erwähnt. **Demgegenüber hat die Kommission in ihrem Dokument „Europas Weg in die Informationsgesellschaft – ein Aktionsplan“**[32] deutlich gemacht, daß im einzelnen durch unionsweite Regelungen festzulegen ist, wie die allgemeinen Datenschutzgrundsätze auf spezifische Situationen anzuwenden sind, die sich aus der Einführung neuer Technologien ergeben. Gerade diesem Zweck dient der Entwurf für eine erste bereichsspezifische Richtlinie über den Datenschutz im ISDN.

Die Europäische Kommission hat ein Grünbuch über ein gemeinsames Konzept für Mobilkommunikation und Personal Communications in der Europäischen Union[33] vorgelegt, das eine europäische Gesetzgebung vorbereiten soll. In diesem Grünbuch wird erstmals umfassend beschrieben, in welche Richtung sich die Telekommunikation in Europa und auch weltweit in den nächsten Jahren bewegen wird: Es wird in absehbarer Zeit keine Unterschiede mehr zwischen dem herkömmlichen Festnetz und den Mobilfunknetzen geben, jeder Teilnehmer kann in beiden Netzen erreicht werden und seinerseits anrufen, wenn er eine entsprechende Chipkarte in ein beliebiges (stationäres oder mobiles) Telefon steckt. Damit wird die Mobilität und Erreichbarkeit erhöht. Die Telekommunikation gleicht sich immer mehr der persönlichen, unmittelbaren Kommunikation an, auch wenn die Unterschiede noch auf absehbare Zeit überwiegen werden.

28 KOM (94) 128 endg. – COD 288

29 vgl. Anlage 2.13

30 vgl. Anlage 3.4

31 sog. Bangemann-Bericht vom 26. Mai 1994, erstellt für die Tagung des Europäischen Rats am 24./25. Juni 1994 auf Korfu

32 KOM (94) 347 endg.; BR-Drs. 792/94

33 KOM (94) 145 endg.

Gleichzeitig entstehen qualitativ neue Gefahren für die Privatsphäre. Im „persönlichen Kommunikationsnetz“ der Zukunft werden nämlich nicht mehr Telefone, sondern Personen direkt angewählt, unabhängig davon, ob sie zuhause sind oder mit einem Mobilfunkgerät unterwegs sind. Damit erhält die Telefonnummer den Charakter eines Personenkennzeichens. Das Recht jedes Nutzers, unbeobachtet zu kommunizieren, könnte entscheidend verkürzt werden. Das vor kurzem gegründete Europäische Amt für Numerierung in Kopenhagen hat zwar gegenwärtig nur die Aufgabe, nationale und europäische Numerierungspläne für die Telekom-Gesellschaften zu koordinieren und neu zu konzipieren. Sobald diese oder eine andere **Institution aber beginnt, sich mit der Numerierung von Menschen** zu befassen, ist dies keine Frage der Verteilung knapper Ressourcen mehr, sondern in erster Linie eine Frage der grundrechtlich geschützten Privatsphäre. Dies haben die europäischen Datenschutzbeauftragten in ihrer von uns initiierten Stellungnahme zum Grünbuch der Kommission[34] deutlich gemacht. Auch in einem zukünftigen universellen Telekommunikationsnetz muß zumindest die Möglichkeit für den einzelnen Teilnehmer erhalten bleiben, mit anderen zu kommunizieren, ohne sich selbst identifizieren zu müssen.

Die Europäische Kommission hat unsere Stellungnahme aufgegriffen und in ihrer Mitteilung an das Europäische Parlament und den Rat[35] betont, daß das Konzept der Anrufe von Person zu Person, der einheitlichen Nummernvergabe an Individuen und der personalisierten Karten unter dem Aspekt des Schutzes der Privatsphäre untersucht werden muß. Die Kommission hat erklärt, sie werde noch vor dem 1. Januar 1996 einen Bericht darüber vorbereiten, ob weitere Maßnahmen bezüglich eines Schutzes personenbezogener Daten notwendig sind.

Für den Telekommunikationssektor und insbesondere für das immer weiter verbreitete **Teleshopping** von Bedeutung ist der geänderte **Vorschlag der Kommission für eine Richtlinie des Rates über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz**[36]**.** Dieser Vorschlag ist – im Gegensatz zur ISDN-Richtlinie – bereits Gegenstand der Beratung im Rat. Wir haben im Rahmen der Europäischen Datenschutzkonferenz gemeinsam mit der französischen Datenschutzkommission und dem britischen Datenschutzbeauftragten eine Stellungnahme zu diesem Entwurf aus datenschutzrechtlicher Sicht formuliert, die dem Rat zugeleitet wurde. Auch wenn der Schwerpunkt dieser Richtlinie beim Verbraucherschutz liegt, so hat es doch zugleich Auswirkungen auf den Schutz der Privatsphäre, ob etwa das Telefon oder die elektronische Post zum Abschluß von Kaufverträgen im Fernabsatz ohne vorherige Zustimmung des Käufers benutzt werden darf. Der Richtlinienvorschlag enthält auch eine Regelung über kartengestützte Zahlungsverfahren im Fernabsatz.

In diesem Zusammenhang ist auch das von der Kommission im **April 1994 vorgelegte Grünbuch zu strategischen Optionen für die Stärkung der Programmindustrie im Rahmen der audiovisuellen Politik der Europäischen Union** zu erwähnen. Zwar nennt das Grünbuch die Wahrung des Datenschutzes und der Privatsphäre als ein Ziel der europäischen Strategie; dennoch spielen Datenschutzaspekte bei der Entwicklung neuer audiovisueller Dienste bisher offenbar nur eine untergeordnete Rolle.

Zu diesen neuen Diensten zählen vor allem Pay-per-View, Video-on-Demand und Shopping-Channels, mit denen Angebote immer stärker individualisiert werden. In dem

34 vgl. Anlage 3.2

35 KOM (94) 492 endg. v. 23. November 1994

36 KOM (93) 396 endg. SYN 411

Maße, wie der herkömmliche Rundfunk vom Massenmedium zum individuellen Bestell- und Konsummedium wird, bei dem über einen Rückkanal Daten der Nutzer an den Anbieter übermittelt werden, entstehen neue Gefährdungen für die Privatsphäre. Die Anbieter solcher Dienste haben ein starkes wirtschaftliches Interesse daran, Informationen über das Konsum- und Nutzungsverhalten der Kunden zu erhalten und individuelle Nutzungsprofile zu erstellen.

Demgegenüber haben wir die Kommission darauf hingewiesen, daß bereits bei der Konzeption audiovisueller interaktiver Dienste die Verarbeitung personenbezogener Daten auf ein möglichst geringes Maß reduziert werden muß **(Grundsatz der Datensparsamkeit).** Eine Speicherung von (zwingend erforderlichen) Daten sollte soweit wie möglich dezentral und unter der Kontrolle des Benutzers erfolgen. Gebühren sollten von Guthabenkarten (prepaid cards) abgebucht werden können. Die Datenverarbeitung muß für den Benutzer transparent sein. Schließlich sind diejenigen Daten, die Systembetreiber und Diensteanbieter erhalten müssen, einer strikten Zweckbindung zu unterwerfen.

Die verschiedenen **Richtlinien über den offenen** Netzzugang, die bereits seit mehreren Jahren in Kraft sind, sollen im Laufe des Jahres 1995 aktualisiert werden. Zu diesem Zweck erstellt die Europäische Kommission einen Bericht, für den wir eine Stellungnahme der Europäischen Datenschutzkonferenz koordiniert haben[37]. Die Datenschutzbeauftragten dringen in diesem Zusammenhang darauf, daß dem Datenschutz ein höherer Stellenwert beigemessen wird als dies in der ursprünglichen Rahmenrichtlinie über den offenen Netzzugang der Fall war. Nachdem der Entwurf **einer Richtlinie über den offenen Netzzugang im Sprachtelefondienst** zunächst am Widerstand des Europäischen Parlaments gescheitert ist, besteht außerdem die Möglichkeit, diese Richtlinie von vornherein datenschutzgerechter zu gestalten, als es der ursprüngliche Kommissionsvorschlag vorsah. Dieser Richtlinienvorschlag muß auch besser als bisher mit dem Vorschlag für eine ISDN-Richtlinie abgestimmt werden.

Das Programm des offenen Netzzugangs, das von der Kommission bereits verfolgt wurde, bevor spezielle Datenschutzrichtlinien vorgeschlagen wurden, sieht die **Schaffung eines allgemeinen Basistelekommunikationsdienstes** in allen Mitgliedstaaten vor, der jedem Unionsbürger den Zugang zu bestimmten unionsweiten Dienstemerkmalen ermöglichen soll. Der Entwurf für eine Ratsentschließung über diesen Basisdienst[38] erwähnt das Problem des Persönlichkeitsschutzes mit keinem Wort und nimmt noch nicht einmal Bezug auf die grundlegenden Anforderungen der Rahmenrichtlinie über den offenen Netzzugang, zu denen – wenn auch in schwacher Form – der Datenschutz zählt. Die europäischen Datenschutzbeauftragten haben es in ihrer Stellungnahme als entscheidend bezeichnet, daß Datenschutzmaßnahmen Teil jedes allgemeinen Basisdienstes werden, der in der Europäischen Union angeboten wird.

Die Liberalisierung auf dem europäischen Telekommunikationsmarkt wird in naher Zukunft weitergehen, nachdem zunächst im Bereich des Mobilfunks das Netzmonopol abgeschafft wurde. Als nächstes wird das Monopol für den Sprachtelefondienst auch im Festnetz zum Ende des Jahres 1997 fallen und spätestens zu diesem Zeitpunkt wird es in der Europäischen Union auch kein Netzmonopol der Telekommunikationsorganisationen mehr geben. Dann werden auch andere Unternehmen, die über „alternative Netze" verfügen (z. B. Energieversorgungsunternehmen), Telekommunikationsnetze betreiben; der Unterschied zwischen Diensteanbietern und Netzbetreibern wird weitgehend bedeutungslos werden. Die damit verbundenen Auswirkungen für den Persönlichkeitsschutz der Bürger sind noch nicht im einzelnen absehbar. Es wird entscheidend darauf ankommen, daß der einzelne Unionsbürger sowohl im Verhältnis zu den Netzbetreibern als auch zu den Diensteanbietern nicht schlechter gestellt ist, als er gegenwärtig im Verhältnis zu den herkömmlichen Telekommunikationsorganisationen steht.

[37] vgl. Anlage 3.3

[38] KOM (93) 543 endg. v. 15. November 1993

1.2 Telekommunikation in der Berliner Verwaltung

Vielfach besteht Unklarheit in der Verwaltung darüber, ob – und wenn ja, welche – Daten in **Telefonnebenstellenanlagen** gespeichert werden dürfen.

Nach der Rahmendienstvereinbarung über den Einsatz und den Betrieb von digitalen Nebenstellenanlagen vom 15. August 1991[39] ist die Speicherung von Verbindungsdaten, wie beispielsweise die Rufnummer der Anrufenden und angerufenden Teilnehmer, nach Beendigung der Verbindung unzulässig (§ 5 Abs. 2 BlnDSG).

Darüber hinaus ist der Einsatz digitaler Telefonanlagen nur gestattet, wenn zwischen dem örtlich zuständigen Personalrat und der Behördenleitung eine besondere Dienstvereinbarung über die eingesetzten Leistungsmerkmale getroffen worden ist (§ 4 Rahmendienstvereinbarung). Wir haben gegenüber den öffentlichen Stellen des Landes Berlin auf diesen Umstand hingewiesen. Daraufhin sind in mehreren Dienststellen Dienstvereinbarungen zwischen örtlichen Personalräten und Behördenleitungen zum Einsatz der dortigen digitalen Telefonnebenstellenanlagen nachträglich getroffen worden.

> Sowohl bei analogen als auch bei digitalen Nebenstellen steht vielfach die Funktion „Lauthören/Freisprechen" zur Verfügung. Dabei kann mit aufgelegtem Telefonhörer über ein Mikrofon gesprochen werden, die Stimme des Gesprächspartners wird über einen Lautsprecher übertragen. Mehrfach haben uns Behördenmitarbeiter um Stellungnahme gebeten, unter welchen Voraussetzungen die Nutzung dieser Funktion möglich ist.

Die Nutzung der **Funktion „Freisprechen/Lauthören"** ist nur mit Einwilligung aller am Gespräch beteiligten Personen zulässig. Die Einwilligung muß vor Aktivierung der Funktion eingeholt werden. Die heimliche Nutzung kann strafrechtliche Konsequenzen nach sich ziehen, da das heimliche Mithören des Telekommunikationsverkehrs unter Strafe gestellt ist (§ 201 Abs. 1 StGB). Auch die Rahmendienstvereinbarung über den Einsatz und den Betrieb von digitalen Telefonnebenstellenanlagen enthält eine entsprechende Regelung (§ 5 Abs. 5 Satz 3 BlnDSG).

> Im Unterausschuß Kommunikations- und Informationstechnik des Hauptausschusses wurde der Senat aufgefordert, ein Konzept zur **Abrechnung privater Telefongespräche** vorzulegen. Gleichzeitig war die Verwaltungsvorschrift, die das Verfahren bisher regelt, außer Kraft getreten. Dies haben wir zum Anlaß genommen, das bisherigen Verfahren der Abrechnung zu überprüfen, insbesondere in welchem Umfang bisher Daten über die Gespräche aufgezeichnet werden.

Kernstück des Verfahrens ist bisher ein **Sammelformular,** das vierteljährlich in den Verwaltungen zirkuliert, und in das die Mitarbeiter die Anzahl der privat geführten Telefoneinheiten eintragen. Hierdurch wird zumindest die Häufigkeit privater Telefongespräche einzelner Mitarbeiter dienststellenweit bekannt. Wir haben daher empfohlen, für die

[39] Dienstblatt des Senats von Berlin I, 305 ff.; vgl. auch Jahresbericht 1991, 2.3

Erfassung der Gebühren für jeden Mitarbeiter ein gesondertes Formular zu verwenden, so daß die Kenntnisnahme seiner personenbezogenen Daten durch nicht mit dem Abrechnungsverfahren befaßte Dritte ausgeschlossen wird.

Vielfach werden in den Dienststellen bei dienstlichen (und – obwohl grundsätzlich nicht zulässig – auch bei privaten) Ferngesprächen die **Zielnummern der angerufenen Personen** in Fernsprechbüchern oder -listen der Vermittlungsstellen der einzelnen Dienststellen gespeichert. Für diese Speicherung existiert bisher keine Rechtsgrundlage. Wir haben angeregt, auf die Speicherung der Zielnummer bei privaten Telefongesprächen künftig ganz zu verzichten und die Zielnummer bei dienstlichen Ferngesprächen nur noch unter Verkürzung um die letzten drei Ziffern zu speichern. Durch die Verwendung von Büchern bei der Speicherung der Daten wird eine **zeitnahe Löschung** der Daten nach dem Wegfall der Erforderlichkeit erheblich erschwert. Daher haben wir gegenüber den betroffenen Stellen die Verwendung von Einzelbelegen angeregt.

Auf dem Hintergrund der Beschlußfassung des Unterausschusses KIT plant die Verwaltung, eine **automatisierte Erfassung der Gebühren für Privatgespräche von Dienstapparaten** einzuführen. Der Bericht der Senatsverwaltung für Inneres sieht dazu folgendes Verfahren vor:

Bei dienstlichen Ortsgesprächen werden für jede Kostenstelle die Anzahl der Gebühreneinheiten und die daraus resultierenden Gesprächskosten ohne Personenbezug aufsummiert. Zur Erfassung dienstlicher Ferngespräche wird den zur Führung solcher Gespräche berechtigten Personen eine **Identifikationsnummer** zugeordnet. Über die Eingabe dieser Nummer wird die Freischaltung für dienstliche Ferngespräche erteilt und zugleich der entstehende Gebührendatensatz (Identifikationsnummer, Name, Datum/Uhrzeit, Gesprächseinheiten, Kosten) gespeichert. Für die Abrechnung privater Orts- und Ferngespräche wird allen Mitarbeitern eine weitere persönliche Identifikationsnummer zugeordnet. Nach Eingabe dieser Nummer werden die Gebührendaten registriert und bilden die Grundlage für die Erstattung der Kosten für die Gespräche. Auch hier soll die Identifikationsnummer als Teil des Datensatzes abgelegt werden.

Die Speicherung der Nummer des Angerufenen (Zielnummer) soll nach den Plänen der Innenverwaltung grundsätzlich unterbleiben. Um zu überprüfen, ob Mitarbeiter privat geführte Gespräche auch ordnungsgemäß angeben, soll die zuständige Dienststelle im **Verdachtsfall** für die Dauer von längstens drei Monaten die Speicherung der Verbindungsdaten der Dienstgespräche bestimmter Beschäftigter mit den ungekürzten Rufnummern der angerufenen Anschlüsse anordnen können. Die zuständige Personalvertretung soll vorher, der Betroffene nachher über die Maßnahme informiert werden.

Allerdings bedarf die Verarbeitung personenbezogener Daten des Anrufers einer **bereichsspezifischen Rechtsgrundlage,** in der Art und Umfang der Datenspeicherung und -nutzung sowie deren Dauer, Verwendungszweck und der Kreis der Zugriffsberechtigten festgelegt werden. Wir haben hierzu einen entsprechenden Vorschlag zur Änderung des Informationsverarbeitungsgesetzes unterbreitet[40].

Problematisch ist die Nutzung einer Identifikationsnummer in der geplanten Form: Jedes Verfahren, mit dem die von einzelnen Teilnehmern verursachten Gebühren ermittelt werden sollen, setzt eine verläßliche Identifizierung und Authentifizierung des jeweiligen Mitarbeiters voraus (vgl. § 5 Abs. 3 Nr. 4 BlnDSG). Das zu diesem Zweck vorgeschlagene Verfahren, bei dem der Benutzer eine Identifikationsnummer am Telefon eingibt, die dann im Gebührendatensatz abgelegt wird, erfüllt diese Anforderungen nicht, da

[40] vgl. Anlage 4

nicht ausgeschlossen werden kann, daß andere Mitarbeiter Kenntnis von der Identifikationsnummer des Bediensteten erhalten und auf dessen Kosten telefonieren. Die persönliche Identifikationsnummer darf daher nur dem Beschäftigten bekannt sein und muß – wenn sie anderen Mitarbeitern bekannt geworden ist – für den Administrator der Telefonanlage (besser für den Beschäftigten selbst an einem Endgerät) änderbar sein. Von einer Speicherung in den Gebührendatensätzen sollte abgesehen werden. Besonders problematisch ist ferner die geplante ungekürzte Speicherung der Zielnummer. Hier bestehen erhebliche Bedenken, ob die Verhältnismäßigkeit im Hinblick auf das informationelle Selbstbestimmungsrecht des Angerufenen noch gewahrt ist.

Telefondienstleistungen der Berliner Sparkasse

Telekommunikationsunternehmen und Geldinstitute bieten zunehmend Dienstleistungen an, die eine Abrechung von Telefongebühren über besondere sog. **„Calling Cards“** oder bereits vorhandene **Kreditkarten** ermöglichen. Das Funktionsprinzip ist in beiden Fällen dasselbe:

Der Benutzer wählt die gebührenfreie Nummer eines Telekommunikationsanbieters. Er identifiziert sich durch Eingabe der Kartennummer (beispielsweise der Kreditkartennummer) sowie einer zusätzlichen, meist vierstelligen Geheimzahl. Danach kann die gewünschte Telefonnummer gewählt werden. Die Abrechnung der Gespräche erfolgt im Falle der Kreditkartennutzung über das Kreditkartenkonto, ansonsten werden die Kosten durch das Telekommunikationsunternehmen direkt dem Anrufer in Rechnung gestellt.

Die Berliner Sparkasse, ein Geschäftsbereich der Landesbank Berlin, bietet im Zusammenhang mit einer von ihr vertriebenen Kreditkarte eine derartige Dienstleistung an. Mehrere Petenten hatten uns darauf hingewiesen, daß die vierstellige Geheimzahl standardmäßig mit den ersten vier Ziffern des Geburtsdatums des Benutzers belegt sei und darüber hinaus der Service automatisch für alle Inhaber dieser Kreditkarten freigeschaltet werde, ohne daß diese gesondert informiert würden.

Diese Sicherungsmaßnahme war nicht ausreichend, da sowohl die Kreditkartennummer als auch Geburtstag und -monat nicht nur den Benutzern, sondern einem nicht näher bestimmbaren Kreis weiterer Personen bekannt sein kann und eine mißbräuchliche Nutzung des Angebots damit nicht wirksam ausgeschlossen ist. Damit sind die Anforderungen des Berliner Datenschutzgesetzes an technische und organisatorische Maßnahmen zur wirksamen Speicher- und Benutzerkontrolle (§ 5 Abs. 3 Nr. 3, 4 BlnDSG) nicht erfüllt.

Das Verfahren wurde insofern geändert, als eine automatische Freischaltung unterbleibt und das Paßwort durch den Kunden künftig frei gewählt werden kann.

Zunehmend bieten auch Berliner Kreditinstitute sog. **„Phone-Banking“-Dienste** an, bei dem Bankkunden verschiedenste Bankgeschäfte – wie z. B. Abfragen des Kontostandes und Überweisungen – über Telefon abwickeln können.

> Ein Petent wandte sich an uns, der bei der Berliner Sparkasse eine telefonische Beratung zu Phone-Banking in Anspruch genommen hatte. Im Laufe des Gesprächs teilte ihm der Berater der Sparkasse mit, daß aus Sicherheitsgründen alle Transaktionen, die von Bankkunden telefonisch abgewickelt werden, bei der Sparkasse aufgezeichnet würden. Dies gelte auch für das gerade geführte Informationsgespräch.

Die **Aufzeichnung von Beratungsgesprächen** im Rahmen des Phone-Banking war zu beanstanden, da es hier an der für die Aufzeichnung personenbezogener Daten erforderlichen Rechtsgrundlage mangelt. Die Speicherung kann insbesondere nicht auf § 28 BDSG

gestützt werden, da die Erforderlichkeit der Speicherung bei Beratungsgesprächen regelmäßig nicht gegeben ist. Unabhängig davon, ob sich die von der Landesbank gegenwärtig verwendete Klausel im allgemeinen Vertrag zur Errichtung eines Girokontos oder in einem speziellen Vertrag für das Phone-Banking befindet, rechtfertigt diese Klausel nicht das lückenlose Mitschneiden von Anrufen solcher Kunden oder potentieller Kunden, die sich in allgemeiner Form über die Modalitäten des Phone-Banking informieren wollen. Darüber hinaus wird durch die heimliche Aufzeichnung der Telefongespräche das Recht der Betroffenen auf Vertraulichkeit der Kommunikation (dessen Verletzung nach § 201 Strafgesetzbuch strafbar sein kann) verletzt. Schließlich fordert das BDSG, daß personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise zu erheben sind (§ 28 Abs. 1 Satz 2 BDSG). Dies ist bei der heimlichen Aufzeichnung von Telefongesprächen ebenfalls nicht der Fall. Eine Einwilligung der Betroffenen liegt bei der Aufzeichnung von Beratungsgesprächen regelmäßig nicht vor.

Wir haben gegenüber der Berliner Sparkasse angeregt, das Verfahren insoweit zu ändern, als der Kunde zusätzlich zu den Vertragsunterlagen eine gesonderte Einwilligungserklärung erhält, mit der er ausführlich über Umfang und Dauer der Speicherung personenbezogener Daten beim Phone-Banking informiert wird. Ein vom Kunden unterschriebenes Doppel sollte an die Berliner Sparkasse zurückgesandt und dort zu den Kundenunterlagen genommen werden. Dies betrifft jedoch nur die Aufzeichnung einzelner Transaktionen bei telefonischen Bankgeschäften. Die Aufzeichnung von Beratungsgesprächen bleibt unzulässig. Wir haben daher die Berliner Sparkasse aufgefordert, die Speicherung von Beratungsgesprächen einzustellen und bereits aufgezeichnete Beratungsgespräche zu löschen.

1.3 Datenschutz und Medien

Die Medienfreiheit rechtfertigt nicht die Mißachtung der Menschenwürde durch die Zurschaustellung von Unfallopfern oder Menschen in Not in Rundfunksendungen, die ein tatsächliches Geschehen wiedergeben **(Reality TV)**[41]. Es ist deshalb zu begrüßen, daß durch den **Ersten Rundfunkänderungsstaatsvertrag** mit Wirkung vom 1. August 1994[42] ein ausdrückliches Ausstrahlungsverbot für solche Sendungen in den Rundfunkstaatsvertrag aufgenommen worden ist, die Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, in einer die Menschenwürde verletzenden Weise darstellen und ein tatsächliches Geschehen wiedergeben, ohne daß ein überwiegendes berechtigtes Interesse gerade an dieser Form der Berichterstattung vorliegt. Das Ausstrahlungsverbot gilt auch dann, wenn die Betroffenen eingewilligt haben (§ 3 Abs. 1 Nr. 5 Rundfunkstaatsvertrag). Es bleibt abzuwarten, welche Auswirkungen diese Regelung haben wird. Es gibt Anzeichen dafür, daß Reality TV-Sendungen vor allem deshalb zunehmend aus dem Programm genommen werden, weil die Einschaltquoten nachgelassen haben.

Die in Köln ansässige **Gebühreneinzugszentrale (GEZ)** zieht seit 1976 im Auftrag der Landesrundfunkanstalten der ARD, also auch des Senders Freies Berlin (SFB), bundesweit Rundfunk- und Fernsehgebühren auf der Grundlage des Rundfunkgebührenstaatsvertrags ein.

Auf den Zentralrechnern der GEZ werden ungefähr 33 Millionen Teilnehmerkonten geführt, an die ca. 800 Endgeräte der Zentral-EDV der GEZ sowie weitere ca. 350 Endgeräte bei den Gebührenabteilungen der einzelnen Landesrundfunkanstalten angeschlossen sind. Neben Teilnehmerstammdaten (wie Name, Vorname, Adresse etc.) werden hier auch Daten über die Zahlungsmodalitäten wie die Bankverbindung des Teilnehmers sowie Angaben zu von der GEZ in Rechnung gestellten Beträgen und eingegangenen Zahlungen des Teilnehmers gespeichert.

Im Jahr 1991 wurden bei der GEZ ca. 155,7 Millionen Geschäftsvorfälle (An-, Ab- und Ummeldungen, eingehende Zahlungen, Mahnverfahren etc.) durchgeführt. Um die Verwaltung der hierbei anfallenden Belegmengen zu erleichtern, werden eingehende Belege und Schreiben der Teilnehmer unmittelbar nach deren Eingang bei der GEZ mikroverfilmt. Die Mikrofilme werden in einem automatisierten Datenträgerarchiv aufbewahrt, aus dem einzelne Belege automatisiert wieder lesbar gemacht werden können.

Der Landesbeauftragte für den Datenschutz Bremen, der Hessische Datenschutzbeauftragte und wir haben eine **gemeinsame Prüfung der Gebühreneinzugszentrale** vor Ort durchgeführt. Die Datenschutzgesetze dieser drei Bundesländer enthalten Kontrollbefugnisse der Landesbeauftragten für den Datenschutz gegenüber ihren jeweiligen Rundfunkanstalten, soweit diese administrativ-wirtschaftlich tätig werden. Damit konnte die Einhaltung der datenschutzrechtlichen Bestimmungen bei der GEZ erstmals durch unabhängige, externe Datenschutzinstitutionen kontrolliert werden.

Im Bereich der Datensicherheit hat die – stichprobenhafte – Untersuchung gezeigt, daß die GEZ die notwendigen Voraussetzungen für eine ordnungsgemäße Datenverarbeitung geschaffen hat. Die getroffenen technischen und organisatorischen Maßnahmen und Regelungen entsprechen den gesetzlichen Vorgaben. Die Dokumentation der Datenträger- und Belegvernichtung konnte auf Anregung der Datenschutzbeauftragten weiter verbessert werden.

Wir hoffen, auch die noch offen gebliebenen Fragen im Zusammenhang mit Aufbewahrungsfristen für Teilnehmerdaten sowie Einzelfragen des Umfangs der Datenspeicherung im Laufe des nächsten Berichtsjahres befriedigend klären zu können.

> Zwei Petenten wandten sich an uns, denen die GEZ Aufforderungen geschickt hatte, ihre Rundfunk- und Fernsehgeräte bis zu einer bestimmten Frist anzumelden, obwohl sie ihre Geräte bereits jahrelang ordnungsgemäß angemeldet hatten. Die Petenten fragten nach der Herkunft der Daten.

Die GEZ hatte im Laufe des Jahres 1993 bei der DeTeMedien GmbH **(ehemals Deutsche Postreklame GmbH) die Daten von über 49 000 Berliner Fernsprechteilnehmern angemietet.** Diese Daten wurden mit dem bei der GEZ vorhandenen Datenbestand Berliner Rundfunkteilnehmer abgeglichen; alle Personen, die nicht bereits im Datenbestand der GEZ vorhanden waren, erhielten ein Schreiben mit der Aufforderung, etwa vorhandene Rundfunk- und Fernsehgeräte umgehend anzumelden. Durch Bearbeitungsfehler der GEZ bzw. der bis 1975 für die Beitreibung von Rundfunkgebühren zuständigen Deutschen Bundespost wurden die beiden Petenten nicht als bereits zahlende Rundfunkteilnehmer erkannt und erhielten ebenfalls derartige Schreiben.

Die „Satzung der Rundfunkanstalt Sender Freies Berlin über das Verfahren zur Leistung von Rundfunkgebühren“[43] enthält in § 8 eine Ermächtigung des SFB, „ . . . andere Rundfunkanstalten oder andere Stellen bei der Erhebung, der Einziehung oder bei Inkassomaßnahmen von Rundfunkgebühren einschließlich Säumniszuschlägen und Kosten . . . einzuschalten.“ Zwar kann dem SFB nicht verwehrt werden, sich wie jedes andere Unternehmen auch des unter bestimmten Voraussetzungen gesetzlich erlaubten Adreßhandels

41 vgl. dazu Jahresbericht 1993, 5.2

42 GVBl. 1994, 221

43 vom 25. November 1993 (ABl. Nr. 2 v. 14. Janaur 1994, S. 88)

zur Verbesserung des Rundfunkgebührenaufkommens zu bedienen. Die Regelung in § 8 der Satzung entspricht jedoch nicht dem verfassungsrechtlichen Grundsatz der Normenklarheit, da der Bürger aus der dort getroffenen Formulierung nicht mit hinreichender Klarheit entnehmen kann, daß die Beiziehung anderer Stellen sich auch auf die Einschaltung kommerzieller Adressenhändler wie der DeTeMedien GmbH bezieht. Der SFB hat auf unsere Anregung hin eine entsprechende Klarstellung in der Satzung in Aussicht gestellt.

Anläßlich einer weiteren Eingabe stellte sich heraus, daß der SFB bereits seit den 80er Jahren regelmäßig ein **privates Inkassobüro** in Mainz einschaltet, wenn die Beitreibung von Rundfunkgebühren im gesetzlich vorgeschriebenen Verwaltungszwangsverfahren ergebnislos bleibt. Die dazu erforderliche Datenübermittlung an das Inkassobüro bedarf nach § 13 des Berliner Datenschutzgesetzes einer bereichsspezifischen Rechtsgrundlage. Eine solche Rechtsgrundlage bestand jedenfalls bis zum Inkrafttreten der Satzung der Rundfunkanstalt Sender Freies Berlin über das Verfahren zur Leistung von Rundfunkgebühren am 1. Januar 1994 nicht. Wir haben daher das Verfahren für den vorhergehenden Zeitraum gegenüber dem SFB beanstandet.

2. Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation

(Postneuordnungsgesetz – PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs. 12/6717)

I.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.

Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten inbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer – auch nach dem Wegfall der Monopole – einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kriterien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

3. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 48. Sitzung

Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994

(KOM [94] 128 endg. – COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß

die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen. Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.

2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei „berechtigten Interessen“ der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.

3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte – wie im ursprünglichen Richtlinienentwurf vorgesehen – untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte – wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah – auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z. B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z. B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedstaaten, diese Anregungen zu unterstützen.

4. Gemeinsame Erklärung der Konferenz der Europäischen Datenschutzbehörden zu dem Verhältnis zwischen den Datenschutzrichtlinien des Europäischen Parlamentes und des Rates und Maßnahmen zur Entwicklung neuer Telekommunikationsnetze und -dienste

Konferenz in Madrid am 25./26. Mai 1994

Seit der Veröffentlichung des Grünbuchs über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte (KOM [87] 290, 30. Juni 1987) hat die Europäische Kommission zahlreiche Vorschläge für Richtlinien und andere Maßnahmen zur schnellen Einführung neuer Telekommunikationsdienste und zum Aufbau transeuropäischer Telekommunikationsnetze gemacht. Einige dieser Vorschläge sind bereits angenommen worden oder werden bald angenommen.

Während keine dieser vorgeschlagenen oder beschlossenen Maßnahmen selbst ein hinreichendes Niveau zum Schutz personenbezogener Daten und der Privatsphäre von Unionsbürgern vorsieht, werden die wichtigen Vorschläge für eine Richtlinie betreffend den Schutz personenbezogener Daten und der Privatsphäre im Zusammenhang digitaler Telekommunikationsnetze (ISDN-Richtlinie SYN 288) und für eine Rahmenrichtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Rahmenrichtlinie SYN 287) nur zögerlich beraten.

Die Europäischen Datenschutzbeauftragten sehen die konkrete Gefahr, daß beide Datenschutzrichtlinien schon obsolet sein könnten, wenn sie schließlich in Kraft gesetzt werden, weil zahlreiche spezielle Maßnahmen der Union zur Einführung neuer Telekommunikationsdienste und -netze dann bereits umgesetzt sein werden. Die Datenschutzbeauftragten halten eine Synchronisierung und Harmonisierung zwischen den Datenschutzrichtlinien und Richtlinien sowie anderen Maßnahmen zur Entwicklung von neuen Telekommunikationsdiensten und -netzen für dringend erforderlich.

Es gibt zahlreiche Vorschläge und Dokumente auf europäischer Ebene im Bereich Telekommunikation, die in bisher unbekanntem Ausmaß zu einer Verarbeitung personenbezogener Daten führen werden, die aber Probleme des Persönlichkeitsschutzes und des Datenschutzes nicht einmal erwähnen. Ein aktuelles Beispiel ist die vorgeschlagene Verordnung des Rates über Gemeinschaftszuschüsse für transeuropäische Netze (KOM [94] 62 endg.).

Die Europäischen Datenschutzbeauftragten fordern deshalb die Organe der Europäischen Union auf, spezielle Datenschutzvorschriften in diejenigen Rechtsakte in diesem Bereich aufzunehmen, deren Verabschiedung vor der Annahme der Rahmenrichtlinie und der Richtlinie zum Datenschutz im ISDN für notwendig gehalten wird.

5. Stellungnahme der Europäischen Datenschutzbeauftragten zum Grünbuch über ein gemeinsames Konzept für Mobilkommunikation und Personal Communications in der Europäischen Union

(von der Kommission vorgelegt)
KOM (94) 145 endg.

Es ist zu begrüßen, daß die Kommission in diesem Grünbuch die Bedeutung eines effektiven Schutzes der Privatsphäre und personenbezogener Daten in der Telekommunikation sehr viel stärker betont, als sie es in zwei vorangegangenen Grünbüchern (KOM [87] 290, 30. Juni 1987; KOM [90] 490, 20. November 1990) getan hat. Die Europäischen

Datenschutzbeauftragten unterstützen ausdrücklich die Feststellung der Kommission, daß ohne einen wirksamen Schutz der Privatsphäre die öffentliche Akzeptanz unionsweiter Netze und Dienste nicht sichergestellt werden kann. Das Grünbuch zur Mobilkommunikation enthält die klare Botschaft für Netzbetreiber, Diensteanbieter, Hersteller und Standardisierungsgremien, daß Datenschutz ein Problem von hoher Priorität ist.

I.

Ein wirksamer Schutz der Privatsphäre ist umso wichtiger, als dieses Grünbuch eine qualitative Veränderung in der Entwicklung der Telekommunikationsnetze und -dienste einleitet: In einem zukünftigen Personal Communications System werden einzelne Menschen anstelle von Endgeräten adressiert. Gleichzeitig verschwimmt die Trennungslinie zwischen Fest- und Mobilnetzen. Dieser Wechsel zur Adressierung von Personen anstelle von Endgeräten wirft grundlegend neue Fragen des Persönlichkeitsschutzes auf. In einem zukünftigen nahtlosen Telekommunikationsnetz kann das Recht jedes Nutzers, unbeobachtet zu kommunizieren, entscheidend verkürzt werden. Personen, die eine persönliche Nummer benutzen, sollten über die Wirkung einer derartigen Nummer als Personenkennzeichen aufgeklärt werden.

Die Numerierung von Endgeräten ist schon gegenwärtig nicht nur ein Problem der Verteilung knapper Ressourcen und der Begrenzung von Kosten der Programmanpassung (vgl. Grünbuch IV. 2 VI Numerierung), sondern sie wirft auch datenschutzrechtliche Fragen auf. Dies wird eine der wesentlichen Aufgaben des entstehenden Europäischen Amtes für Numerierung (ENO) sein, das in Kopenhagen eingerichtet werden soll. Mit der Einführung von Personal Communications wird man jedoch Menschen, und nicht nur Endgeräte, numerieren müssen. Die Numerierung von Menschen ist keine Frage der Verteilung knapper Ressourcen, sondern in erster Linie eine Frage des Grundrechtsschutzes und insbesondere des Schutzes der Privatsphäre.

Aus der Sicht des Persönlichkeitsschutzes ist es deshalb entscheidend, daß bei der Entwicklung neuer weltweiter Telekommunikationsnormen wie z. B. für das Universelle Mobile Telekommunikationssystem (UMTS) zumindest die alternative Option erhalten bleibt, ohne Zwang zur Identifizierung kommunizieren zu können. Diese alternative Option kann nicht den Marktkräften überlassen bleiben, sondern muß vom europäischen Gesetzgeber gesichert werden. Sie sollte ohne zusätzliche Kosten für den Benutzer angeboten werden.

II.

Was die Frage freiwilliger Verhaltenskodizes für Diensteanbieter (vgl. Grünbuch, IV. 2 II Bereitstellung von Diensten, Randziffer 4) betrifft, ist darauf hinzuweisen, daß in einigen Mitgliedstaaten spezielle nationale Rechtsvorschriften (nicht nur freiwillige Verhaltenskodizes) zum Datenschutz gelten, die unter anderem auf Diensteanbieter Anwendung finden. Falls das Gemeinschaftsrecht – wie es das Grünbuch vorschlägt – unterscheiden sollte zwischen zwingenden grundlegenden Anforderungen für Netzbetreiber auf der einen Seite und freiwilligen Verhaltenskodizes für Diensteanbieter auf der anderen Seite, könnte nationales Recht, das Diensteanbieter verpflichtet, möglicherweise gegen Gemeinschaftsrecht verstoßen. Bei dem Konsultationstreffen am 16./17. Juni 1994 in Brüssel wurde von Seiten der Generaldirektion XIII betont, daß dies nicht der Fall sei, und daß das Grünbuch sich lediglich zu zusätzlichen Anforderungen für Diensteanbieter äußere. Die bestehenden rechtlichen Anforderungen sollten unverändert fortgelten, aber zusätzliche Anforderungen sollten nur in freiwillige Verhaltenskodizes aufgenommen werden. Dies sollte zumindest in der zukünftigen Gemeinschaftsgesetzgebung klargestellt werden.

Die zugrundeliegende Unterscheidung des Grünbuchs zwischen Netzbetreibern, die rechtlichen Verpflichtungen und Lizenzvereinbarungen unterliegen sollen, und Diensteanbietern, die lediglich an freiwillige Verhaltenskodizes gebunden sein sollen, überzeugt allerdings nicht völlig. Es mag durchaus sein, daß Netzbetreiber größere Datenbestände verarbeiten, aber Diensteanbieter verarbeiten ebenfalls personenbezogene Daten, insbesondere wenn sie Dienste wie Abrechnung, Mailboxen etc. anbieten. Es erscheint deshalb erforderlich, daß das Gemeinschaftsrecht entweder die gleichen rechtlichen Verpflichtungen für Diensteanbieter und Netzbetreiber vorsieht, soweit es die grundlegende Anforderung „Datenschutz“ betrifft, oder zumindest einzelstaatliche Gesetzgebung dieses Inhalts zuläßt. Die Tatsache, daß Netzbetreiber quantitativ mehr personenbezogene Daten verarbeiten als Diensteanbieter, rechtfertigt keine Privilegien für Diensteanbieter. Dies erscheint als Deregulierung vom falschen Ende her, die nicht gerechtfertigt ist durch die Grundsätze der Verhältnismäßigkeit und der Subsidiarität.

III.

Mit der bevorstehenden Überarbeitung der Ratsrichtlinie zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provison – ONP-90/387/EWG) und der übrigen ONP-Richtlinien sollte die restriktive Bestimmung zum Datenschutz als einer grundlegenden Anforderung, „wo dies angebracht ist“ (Artikel 3 Abs. 2 ONP-Rahmenrichtlinie), geändert werden. Der Datenschutz, wie er im entstehenden Gemeinschaftsrecht (z. B. in der vorgeschlagenen Rahmenrichtlinie zum Datenschutz und in der ISDN-Richtlinie) vorgesehen ist, ist nicht nur eine grundlegende Anforderung, „wo dies angebracht ist“, sondern unter allen Umständen, die das Gemeinschaftsrecht (ebenso wie einzelstaatliches Recht in Übereinstimmung mit dem Gemeinschaftsrecht) vorsieht. Die ONP-Rahmenrichtlinie enthält keine vergleichbaren Einschränkungen anderer grundlegender Anforderungen wie etwa der Sicherheit des Netzbetriebes oder der Aufrechterhaltung der Netzintegrität. Der Datenschutz hat keine geringere Bedeutung und sollte nicht hinten angestellt werden dürfen, wenn Netzbetreiber oder Diensteanbieter dies für angemessen halten.

IV.

Die Frage der gegenseitigen Anerkennung von Lizenzen erhebt sich in Bezug auf Netzbetreiber und Diensteanbieter, wie man dem geänderten Vorschlag für eine Richtlinie über die gegenseitige Anerkennung von Lizenzen und anderen nationalen Genehmigungen für Telekommunikationsdienste (KOM [94] 41 endg.) entnehmen kann. Weder die gegenseitige Anerkennung von Lizenzen noch – in Zukunft – ein europäisches Lizenzierungssystem sollte zu einer Absenkung der bestehenden Standards für den Datenschutz und den Schutz der Privatsphäre führen, wie sie durch nationale Gesetzgebung und Lizenzbedingungen festgelegt sind. Das muß auch gelten, wenn die vorgeschlagenen Datenschutzrichtlinien in Kraft treten; die Umsetzung des darin vorgesehenen Datenschutzstandards sollte weder durch die gegenseitige Anerkennung von Lizenzen, noch durch ein europäisches Lizenzierungssystem beeinträchtigt werden.

V.

Satellitenkommunikation unter Einsatz von niedrigfliegenden Satelliten (Low earth orbit-satellites/LEOs) wird eine immer wichtigere Rolle im System der weltweiten Personal Communications spielen (vgl. Grünbuch, IV. 2 VII Randziffer 7).

Einerseits kann die Satellitenkommunikation das Risiko der Aufzeichnung präziser Bewegungsprofile begrenzen, soweit ein satellitengestütztes Netz nicht auf kleinen Zellen

wie die terrestrischen Mobilfunknetze beruht. Der angerufene Teilnehmer empfängt Signale innerhalb der verhältnismäßig großen Ausleuchtzone des Satelliten und kann deshalb nicht in derselben Weise lokalisiert werden, wie er in terrestrischen Zellularsystemen lokalisiert werden könnte. Auf der anderen Seite birgt die Satellitenkommunikation eine größere Gefahr für die Vertraulichkeit, weil Daten von leistungsstarken Erdfunkstationen zum Raumsegment (uplink) übermittelt werden und dann zurückübermittelt werden zu anderen Erdfunkstationen (downlink). Effektive Verschlüsselungstechniken müssen deshalb schon innerhalb der Erdfunkstation angewandt werden, bevor Daten zum Raumsegment übertragen werden, um das Abhören der Verbindung in der Nähe der Erdfunkstation zu verhindern.

VI.

Diese Stellungnahme kann nicht auf alle Details des Grünbuchs eingehen. Die Europäischen Datenschutzbeauftragten bitten jedoch die Kommission darum, möglichst frühzeitig Gelegenheit zu weiteren Stellungnahmen zu Vorschlägen für eine Gemeinschaftsgesetzgebung oder Normentwicklung zu erhalten, die sich aus diesem Grünbuch und dem anschließenden Konsultationsprozeß ergeben kann.

6. Stellungnahme der Europäischen Konferenz der Datenschutzbeauftragten zum Analysebericht der Europäischen Kommission (DG XIII) entsprechend der ONP-Rahmenrichtlinie – (Richtlinie des Rates 90/387/WG) –

– Übersetzung aus dem Englischen –

Allgemeine Anmerkungen

Der Rat der Europäischen Gemeinschaften hat die Harmonisierung der Bedingungen für offenen und effizienten Zugang zu Telekommunikationsnetzen und -diensten (Open Network Provision – ONP) vorrangig behandelt.

Die Europäischen Datenschutzbeauftragten sind der Ansicht, daß Datenschutz eine bedeutendere Rolle spielen sollte, als dies jetzt der Fall ist. In seiner ONP-Richtlinie zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (90/387/EWG vom 28. Juni 1990) hat der Rat bestimmt, daß die ONP-Bedingungen „. . . den Zugang zu öffentlichen Telekommunikationsnetzen oder öffentlichen Telekommunikationsdiensten nicht beschränken (dürfen), es sei denn aus Gründen, die auf grundlegenden Anforderungen beruhen und die in Übereinstimmung mit dem Gemeinschaftsrecht stehen. Diese **grundlegenden Anforderungen sind . . . Datenschutz, wo dies angebracht ist“.**

Die Europäischen Datenschutzbeauftragten sind der Ansicht, daß diese eingeschränkte Vorstellung über den Schutz personenbezogener Daten revidiert werden sollte. Der Schutz personenbezogener Daten, wie er durch das zukünftige Gemeinschaftsrecht (wie die vorgeschlagene Rahmenrichtlinie über den Schutz personenbezogener Daten und die ISDN-Richtlinie über den Datenschutz) sichergestellt wird, ist nicht nur eine grundlegende Anforderung, „wo dies angebracht ist“, sondern unter allen im Gemeinschaftsrecht beschriebenen Umständen (sowie dem nationalen Recht in Übereinstimmung mit dem Gemeinschaftsrecht). Die ONP-Rahmenrichtlinie enthält keine solchen Einschränkungen für andere grundlegende Anforderungen wie die Sicherheit des Netzbetriebs und die Aufrechterhaltung der Netzintegrität. Der Schutz personenbezogener Daten ist nicht von geringerer Bedeutung, und es sollte nicht erlaubt sein, ihn zu beeinträchtigen, wenn Netzbetreiber und Diensteanbieter dies für angemessen halten.

Der Analysebericht schlägt vor, die Anwendung der ONP-Prinzipien auf verschiedene andere Telekommunikationsdienste zu erweitern, insbesondere intelligente Netzfunktionen, Netzmanagement, den Nahverkehrsbereich und die Breitbandkommunikation. Die Europäischen Datenschutzbeauftragten sind der Ansicht, daß spezifische Datenschutzregelungen in jede der zukünftigen ONP-Richtlinien aufgenommen werden sollten. Es ist von großer Bedeutung, die Schaffung neuer Telekommunikationsdienste und -infrastrukturen ohne hinreichende Datenschutzmaßnahmen zu verhindern. Die gegenwärtigen Fassungen der Vorschläge für die ISDN-Richtlinie und die allgemeine Datenschutzrichtlinie decken nur einige der spezifischen Probleme von Telekommunikationsdiensten ab. Besonders der geänderte Vorschlag für die ISDN-Richtlinie ist in seinem Anwendungsbereich im Vergleich mit dem ursprünglichen Vorschlag erheblich eingeschränkt worden. Die Europäischen Datenschutzbeauftragten beabsichtigen, kurzfristig eine Erklärung zu dem geänderten Vorschlag für eine ISDN-Richtlinie abzugeben.

Grundsätzlich sollte die Verarbeitung personenbezogener Daten zur Erbringung von Telekommunikationsdiensten auf ein Minimum reduziert werden. Dies gilt besonders für Verbindungsdaten. Die verbleibenden notwendigen Daten sollten im Prinzip nicht an Dritte weitergegeben werden (Zweckbindungsgrundsatz).

Anwendung von ONP-Prinzipien auf intelligente Netzfunktionen

Der Bericht stellt fest, daß die Kommission sicherstellen wird, daß die relevanten Regelungen der vorgeschlagenen Richtlinie für den Sprachtelefondienst vollständig in diesem Bereich angewendet werden (S. 9). Dies sollte die Datenschutzregelungen der Richtlinie einschließen (weitere Anmerkungen zu dieser Richtlinie siehe unten).

Anwendung der ONP-Prinzipien auf das Netzmanagement

Die NERA-Studie empfiehlt, daß die Kommission die Wettbewerbsgleichheit zwischen Telekommunikationsorganisationen und unabhängigen Mehrwertdienstanbietern sicherstellen sollte (S. A 1 – 5, Empfehlung 1). Die Europäische Union sollte in diesem Zusammenhang ebenfalls sicherstellen, daß das Prinzip des Fernmeldegeheimnisses – wie in der nationalen Gesetzgebung der Mitgliedstaaten für Telekommunikationsorganisationen niedergelegt – auch in vollem Umfang auf Mehrwertdienstanbieter anwendbar ist.

Die Studie empfiehlt auch die Einführung von einzeln aufgeschlüsselten Rabatten auf den Rechnungen (Tabelle: Open Network Provision Supply Conditions proposed by the study, S. A 1 – 6). Die Europäischen Datenschutzbeauftragten sind der Auffassung, daß die Informationen über einzelne Rabatte auf den Rechnungen nicht mehr personenbezogene Daten enthalten sollten, als die Rechnung selbst, z. B. sollten keine Nummern von Angerufenen aufgenommen werden, wenn der Teilnehmer sich nicht für einen Einzelentgeltnachweis entschieden hat. Der extensiven Datenverarbeitung, die dem gesamten Prozeß der Rechnungsstellung zugrunde liegt, sollte unabhängig von der Option, die der Teilnehmer gewählt hat, mehr Aufmerksamkeit gewidmet werden.

Zugang zum Breitbandnetz

Betreffend die Anwendung von ONP-Prinzipien auf Breitbandkommunikation, besonders Video- und Multimedia-Applikationen, sind die Europäischen Datenschutzbeauf-

tragten der Auffassung, daß hierdurch völlig neue Fragen aufgeworfen werden. Da die Grenze zwischen Telekommunikation und Rundfunk zunehmend verwischt wird, wird es immer wichtiger werden, die Teilnehmer effektiv gegen die Schaffung elektronischer Profile über ihr Verhalten zu schützen.

Anwendung der ONP-Prinzipien auf den Sprachtelefondienst

Der Vorschlag für eine Richtlinie des Rates zur Einführung des offenen Netzzugangs (ONP) beim Sprachtelefondienst ist in diesem Juni vom Europäischen Parlament zurückgewiesen worden. Daher nehmen die Europäischen Datenschutzbeauftragten die Gelegenheit wahr, zu den Datenschutzregelungen des zurückgewiesenen Vorschlags Stellung zu nehmen, um zur Verbesserung der Datenschutzregelung in späteren Vorschlägen beizutragen.

Der geänderte Vorschlag der ONP-Sprachtelefondienstrichtlinie (KOM [93] 182 endg. – SYN 437) enthielt Regelungen zum Einzelentgeltnachweis (Artikel 14), Teilnehmerverzeichnissen (Artikel 15) und die Begründungen, die auf grundlegende Anforderungen in Einklang mit dem Gemeinschaftsrecht gestützt werden (Artikel 21 Ziffer 5).

Der geänderte Vorschlag enthielt nur generelle Verweise auf die relevante Gesetzgebung über den Schutz personenbezogener Daten (Artikel 14, 15, 21 Ziffer 5 d). In dieser Hinsicht war der Vorschlag unvollständig und bedurfte der Ergänzung durch substantielle Regelungen über den Datenschutz beim Sprachtelefondienst.

Es muß jedoch zur Kenntnis genommen werden, daß der Vorschlag der Kommission ausdrücklich feststellt, daß „Nutzungseinschränkungen, die aus grundlegenden Anforderungen abgeleitet werden, . . . mit ordnungspolitischen Mitteln und nicht durch technische Einschränkungen durchzusetzen (sind)". Dieser Vorschlag könnte – wenigstens in der englischen Version – so ausgelegt werden, daß keinerlei technische Einschränkungen zur Sicherstellung des Datenschutzes verhängt werden könnten. Dies würde im Widerspruch zu der Ansicht verschiedener Europäischer Datenschutzbeauftragter stehen, daß effektive Maßnahmen zum Schutz personenbezogener Daten nicht allein auf gesetzliche Regelungen gestützt werden können, sondern auch durch technische Standards unterstützt werden müssen. Daher bedarf wenigstens der englische Text der Klarstellung („. . . **nicht nur** durch technische Einschränkungen . . .").

Darüber hinaus wurde im geänderten Vorschlag der Kommission für eine Sprachtelefondienstrichtlinie die Regelung über Einzelentgeltnachweise derart geändert, daß alle Teilnehmer, die dem nicht widersprochen haben, automatisch Einzelentgeltnachweise erhalten würden (Artikel 14). Der Verweis auf die relevante Datenschutzgesetzgebung blieb unverändert. Die Europäischen Datenschutzbauftragten haben es begrüßt, daß der gemeinsame Standpunkt vom 30. Juni 1993 den ursprünglichen Vorschlag in dieser Hinsicht wiederhergestellt hat, so daß Einzelentgeltnachweise nur auf Verlangen erhältlich sind. Diese Regelung sollte in dem neuen Vorschlag, der durch die Kommission vorbereitet werden wird, erhalten bleiben. Der extensiven Datenverarbeitung, die dem gesamten Verfahren der Rechnungserstellung zugrunde liegt, sollte wiederum mehr Aufmerksamkeit gegeben werden, unabhängig davon, welche Option der Teilnehmer gewählt hat.

Der Rat hat ebenfalls die Regelung aus Artikel 15 b gestrichen, nach dem die Benutzer berechtigt sind, sich „ohne zusätzliche Kosten" in öffentliche Telefonverzeichnisse eintragen oder nicht eintragen zu lassen. Dies würde es für die Benutzer schwieriger machen, sich nicht in öffentliche Telefonverzeichnisse eintragen zu lassen, ein Recht, das die meisten Europäischen Datenschutzbeauftragten bisher für wesentlich gehalten haben.

Vorschlag für eine Entscheidung des Rates über Grundsätze für den universellen Dienst im Bereich der Telekommunikation (KOM [93] 543 endg. v. 15. November 1993)

Das Konzept des offenen Netzzugangs sorgt auch für die Schaffung eines universellen Basisdienstes in allen Mitgliedstaaten. Dieser universelle Dienst soll bestimmte gemeinschaftsweite Basismerkmale enthalten, die für jeden Bürger der Gemeinschaft erhältlich sein sollen. Zusätzlich zu diesen Basismerkmalen können Zusatzmerkmale von konkurrierenden Diensteanbietern angeboten werden. In seinem Vorschlag für eine Entscheidung des Rates über Grundsätze für den universellen Dienst im Bereich der Telekommunikation (KOM [93] 543 endg.) hat die Kommission diese Struktur näher ausgeführt, ohne das Problem der Datensicherheit und des Datenschutzes für die Teilnehmer in diesem Bereich überhaupt zu erwähnen. Es gibt nicht einmal einen Verweis auf die grundlegenden Anforderungen aus Artikel 3 Ziffer 2 der allgemeinen ONP-Richtlinie, die den Datenschutz enthalten.

Die Europäischen Datenschutzbeauftragten halten es für wesentlich, daß Maßnahmen zum Datenschutz Bestandteil jedes universellen Basistelekommunikationsdienstes werden, der in der Europäischen Union angeboten wird.

7. Gemeinsame Erklärung der Europäischen Datenschutzbeauftragten zum geänderten Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen vom 13. Juni 1994 KOM [94] 128 endg. – COD 288

A. Allgemeine Anmerkungen

Die Datenschutzbeauftragten in der Europäischen Union haben in ihrer gemeinsamen Erklärung, die am 25./26. Mai 1994 in Madrid angenommen wurde, betont, daß eine Notwendigkeit für die Schaffung spezifischer Datenschutzregelungen im Bereich der Telekommunikation besteht, in dem gegenwärtig zahlreiche Dienste und transeuropäische Netze eingeführt werden. Der geänderte Vorschlag für eine ISDN-Richtlinie ist ein bedeutender Schritt in diese Richtung. Wie in Madrid dargelegt wurde, müssen andere Gesetzgebungsvorhaben in diesem Bereich mit der ISDN-Richtlinie harmonisiert werden.

B. Einzelne Anmerkungen

1. Artikel 2 – Begriffsbestimmungen

Der Begriff „Telekommunikationsdienste" sollte definiert werden. Dieser Begriff wird in Artikel 3 benutzt, um den Anwendungsbereich der Richtlinie festzulegen. Während der Begriff „öffentlicher Telekommunikationsdienst" in Artikel 2 Nr. 6 definiert ist, wird in Artikel 3 Nr. 2 der Begriff „andere Telekommunikationsdienste, die über das öffentliche Telekommunikationsnetz angeboten werden", benutzt. Beide Regelungen sollten klargestellt werden, indem in Artikel 2 eine Definition für „Telekommunikationsdienste" aufgenommen wird.

Artikel 2 Nr. 1 und 6 des geänderten Vorschlags beziehen sich auf Telekommunikationsorganisationen und öffentliche Telekommunikationsdienste in nicht liberalisierten Märk-

ten. Unter Berücksichtigung der Tatsache, daß in manchen Mitgliedstaaten die Liberalisierung von Diensten und Netzen unter Umständen schon vor 1998 stattfinden wird, schlagen die europäischen Datenschutzbeauftragten eine flexiblere Formulierung für diese Regelung vor. Wenn die Worte „oder die Europäische Union/ Europäische Gemeinschaft“ nach den Worten „Mitgliedstaat“ und „Mitgliedstaaten“ eingefügt würden, wäre die Richtlinie in zukünftig liberalisierten Märkten mit unionsweiten Lizensierungsverfahren anwendbar.

Die Ausnahme von Rundfunk und Fernsehen in Artikel 2 Nr. 2 verstehen die Datenschutzbeauftragten in der Europäischen Union so, daß nur Rundfunk im klassischen Sinne aus dem Anwendungsbereich des Richtlinienvorschlags ausgenommen werden soll. Im Gegensatz dazu sollten interaktive Dienste, die über ein öffentliches Telekommunikationsnetz erbracht und Telefondienste, die von Kabelfernsehunternehmen angeboten werden, von der Richtlinie erfaßt werden. Sollte es diesbezüglich irgendwelche Zweifel geben, so sollte der Text entsprechend geändert werden.

Es wird allgemein notwendig sein, auf der europäischen Ebene Maßnahmen zu ergreifen, um personenbezogene Daten von Radio- und Fernsehkonsumenten zu schützen, sobald es möglich wird, sie – z. B. im Falle von „Video on demand“ – zu identifizieren und elektronische Profile ihres Verhaltens zu erstellen. Die Datenschutzbeauftragten in der Europäischen Union akzeptieren zwar, daß Rundfunk und Fernsehen im klassischen Sinne von diesem Richtlinienvorschlag nicht erfaßt werden, werden aber trotzdem die weitere Entwicklung in diesem Bereich genau beobachten, um Empfehlungen für eventuell notwendige spezifische Maßnahmen durch das Europäische Parlament und den Rat zu geben.

2. Artikel 3 – Betroffene Dienste

Das Verhältnis zwischen der zukünftigen allgemeinen Datenschutzrichtlinie (KOM [92] 422 endg. – SYN 287) und dem Vorschlag für eine ISDN-Richtlinie sollte im Text der ISDN-Richtlinie klargestellt und der vorrangige Charakter der allgemeinen Richtlinie bekräftigt werden. Erwägungsgrund 9 sollte überarbeitet werden; die gegenwärtige Formulierung stimmt nicht mit den Regelungen des Artikel 3 Nr. 1 überein.

Der geänderte Vorschlag für eine ISDN-Richtlinie (Artikel 3 Nr. 2) unterscheidet zwischen Telekommunikationsorganisationen und Diensteanbietern. Während Telekommunikationsorganisationen völlig von der Richtlinie erfaßt werden, gelten für die Diensteanbieter nur die Artikel 4, 5, 6, 11, 14 und 16. Die Datenschutzbeauftragten sind der Auffassung, daß einige der übrigen Artikel ebenfalls auf Diensteanbieter angewandt werden sollten. Artikel 3 sollte geändert werden, um dies klarzustellen. Die Unterscheidung zwischen Telekommunikationsorganisationen und Diensteanbietern ist nicht gerechtfertigt. Für den Benutzer macht es keinen praktischen Unterschied, ob seine Daten von einer Telekommunikationsorganisation oder einem Anbieter von Telekommunikationsdienstleistungen verarbeitet werden (unabhängig davon, ob diese besonders vertrauenswürdig sind oder nicht). Daher sollte ihm in beiden Fällen ein gleiches Schutzniveau gewährt werden.

Artikel 3 Nr. 3 beschreibt die Situation, in der Dienste nicht durch digitale sondern durch analoge Netzwerke erbracht werden. Es ist zu begrüßen, daß die Mitgliedstaaten die Anwendung der Regelungen dieser Richtlinie auf Dienste, die in analogen Netzwerken erbracht werden, sicherstellen sollen, wo dies technisch möglich ist. Allerdings werden selbst in den Ländern, in denen die Digitalisierung der Netzwerke bereits fortgeschritten

ist, überwiegend analoge Endgeräte an digitale Vermittlungsstellen angeschlossen sein (vgl. Artikel 12 Nr. 3 des ursprünglichen Vorschlags). Da diese Situation in den meisten Mitgliedstaaten für einige Zeit bestehen bleiben wird, ist es von Bedeutung, daß die vorgeschlagene Richtlinie hier genauso anwendbar ist wie bei Dienstleistungen, die über analoge Netzwerke erbracht werden. Dies könnte erreicht werden, indem die Worte „und Geräte“ nach „Netzwerken“ in Artikel 3 Nr. 3 eingefügt werden.

Bezüglich der Voraussetzung „soweit technisch möglich“ sollte bedacht werden, daß eine Reihe von Regelungen der Richtlinie unabhängig von technischen Grenzen angewandt werden können. Dies gilt besonders für Artikel 11 bezüglich der Teilnehmerverzeichnisse. „Technische Unmöglichkeit“ sollte daher nicht als eine Rechtfertigung zur Abweichung von diesen Regelungen akzeptiert werden. Dies sollte im Text der Nr. 3 entsprechend deutlich gemacht werden.

3. Artikel 4 des ursprünglichen Vorschlags – Zweckbindungsgebot/ elektronische Profile

Artikel 4 Nr. 1 des ursprünglichen Vorschlags enthielt eine Beschränkung für die Erhebung, Speicherung und Verarbeitung personenbezogener Daten durch Telekommunikationsorganisationen auf Telekommunikationszwecke (Zweckbindungsgebot). Die Streichung dieser Regelung im geänderten Vorschlag würde dazu führen, daß nur Artikel 7 Buchstabe f des Entwurfs für eine allgemeine Datenschutzrichtlinie anwendbar wäre, der die Befugnis, personenbezogene Daten zu verarbeiten, auf alle Situationen ausdehnt, in denen die Verarbeitung „erforderlich ist zur Verwirklichung des Allgemeininteresses oder des berechtigten Interesses, das von dem Verantwortlichen der Verarbeitung oder von dem Dritten wahrgenommen wird, dem die Daten übermittelt werden, sofern nicht die Interessen des Betroffenen überwiegen“. Dies scheint für die Verarbeitung personenbezogener Daten in Telekommunikationsnetzen unzureichend und zu vage zu sein. Aufgrund der spezifischen Beschaffenheit digitaler Nachrichtenübermittlungssysteme sollte das besondere Zweckbindungsprinzip, das in Artikel 4 Nr. 1 des ursprünglichen Vorschlags enthalten war, wieder in die ISDN-Richtlinie aufgenommen werden. Das spezifische Zweckbindungsgebot wird an Bedeutung gewinnen, da die Telekommunikationsorganisationen ihre Aktivitäten in zunehmenden Maße diversifizieren. Das Zweckbindungsgebot sollte ebenso für die Verarbeitung personenbezogener Daten durch Diensteanbieter gelten.

Artikel 4 Nr. 2 des ursprünglichen Vorschlags verbot die Nutzung personenbezogener Daten, um elektronische Profile der Teilnehmer zu erstellen oder einzelne Teilnehmer nach Kategorien zu sortieren. Diese Regelung ist im geänderten Vorschlag gestrichen worden.

Die Europäischen Datenschutzbeauftragten sind der Auffassung, daß die Nutzung von Verbindungs- und anderen personenbezogenen Daten über das Telekommunikationsverhalten einzelner Teilnehmer zur Erstellung von elektronischen Profilen prinzipiell verboten werden sollte. Die entsprechende Regelung der allgemeinen Datenschutzrichtlinie (Artikel 16 Nr. 1 – automatisierte Einzelentscheidungen) bietet in dieser Hinsicht wiederum keinen ausreichenden Schutz für den Teilnehmer. Entsprechend der vom Europäischen Parlament vorgeschlagenen Änderung sollte das Erstellen derartiger elektronischer Profile durch Telekommunikationsorganisationen nur mit der informierten Einwilligung des Teilnehmers erlaubt sein. Die Erbringung von Basisdiensten darf nicht verweigert werden, wenn der Teilnehmer nicht in die Erstellung eines elektronischen Profils einwilligt (vgl. Artikel 7 §3 des ursprünglichen Vorschlags).

4. Artikel 5 des ursprünglichen Vorschlags –
Speicherung der übertragenen Inhaltsdaten nach dem Ende der Übertragung

Der Vorschlag für eine allgemeine Richtlinie beantwortet die Frage, in welchem Ausmaß die übertragenen Informationen nach dem Ende der Übertragung von Telekommunikationsorganisationen oder Diensteanbietern gespeichert werden dürfen. Daher sollte Artikel 5 Nr. 2 des ursprünglichen Vorschlags in einer modifizierten Form wieder aufgenommen werden. Die notwendige spezifische Regelung könnte wie folgt lauten:

„Die Inhalte der übertragenen Informationen dürfen nach Beendigung der Übertragung nicht von der Telekommunikationsorganisation gespeichert werden, es sei denn, dies ist aufgrund von Verpflichtungen erforderlich, die in den Mitgliedstaaten dem Gemeinschaftsrecht entsprechend gesetzlich vorgeschrieben sind."

5. Artikel 7 des ursprünglichen Vorschlags
– Vertraulichkeit/Geheimhaltung der Telekommunikation

Obwohl viele Mitgliedstaaten für die Vertraulichkeit oder Geheimhaltung der Telekommunikation in ihrer nationalen Gesetzgebung gesorgt haben (einige sogar in ihren Verfassungen) ist es notwendig, dies in die ISDN-Richtlinie aufzunehmen, um einen gemeinschaftsweiten Minimalstandard zu etablieren. Artikel 7 Nr. 1 des ursprünglichen Vorschlags sollte daher in einer geänderten Version wieder aufgenommen werden, die wie folgt lauten könnte:

„Die Mitgliedstaaten sollen sicherstellen, daß alle personenbezogenen Daten, die in Verbindung mit Telekommunikationsnetzen und -diensten verarbeitet werden, vertraulich behandelt werden müssen."

Die Vertraulichkeit sollte ausdrücklich auf Verbindungsdaten erstreckt werden, die für die Beobachtung des einzelnen Teilnehmers genauso gut genutzt werden können wie Inhaltsdaten. Andererseits könnte es mehr Ausnahmen von der Vertraulichkeit von Verkehrsdaten geben, während der Inhalt der übertragenen Informationen nur unter sehr eingeschränkten Bedingungen Dritten bekanntgegeben werden darf (vgl. Artikel 7 Nr. 2 des ursprünglichen Vorschlags).

6. Artikel 5 – Abrechnungsdaten

Die Datenschutzbeauftragten betonen nochmals, daß anonyme Zahlungsverfahren den Benutzern in der Europäischen Union als ein Basisdienst angeboten werden sollten. Der Teilnehmer sollte in die Lage versetzt werden, eine informierte Auswahlentscheidung bezüglich der Art der Abrechnung aus einer Reihe von Möglichkeiten einschließlich der Beschränkung auf die Summe der Gebühren zu treffen. Im Falle der Erstellung eines Einzelentgeltnachweises sollte die Speicherung von Daten dem in Erwägungsgrund (10) niedergelegten Prinzip entsprechen, das heißt die Speicherung sollte auf den unbedingt für die Erbringung des Dienstes notwendigen Zeitraum beschränkt werden.

Artikel 5 Nr. 1 sollte durch Hinzufügen der Worte „innerhalb der Telekommunikationsorganisation oder des Diensteanbieters" nach dem Wort „Daten" im letzten Satz klarer formuliert werden.

In Artikel 5 Nr. 2 sollte das Wort „gesetzlich" gestrichen werden. Dies ist notwendig, da der Zeitraum, innerhalb dessen die Rechnung angefochten werden kann, auch vertraglich festgelegt sein könnte. Datenschutzfreundliche Auswahlmöglichkeiten („privacy options"), wie sie gegenwärtig in den Niederlanden diskutiert werden, wo überhaupt

keine Daten für einen längeren Zeitraum als für die Erstellung der Rechnung notwendig gespeichert werden (falls der Benutzer dies wünscht), sollten auch nach der ISDN-Richtlinie erlaubt bleiben.

7. Artikel 6 – Verkehrsdaten

Artikel 6 sollte wie folgt geändert werden:

„Verkehrsdaten zum Aufbau von Verbindungen, die personenbezogene Daten enthalten, müssen gelöscht werden, sobald ihre Speicherung nicht mehr für die Abrechnung oder andere vertraglich festgelegte Dienste erforderlich ist."

Die gegenwärtige Formulierung von Artikel 6 im geänderten Vorschlag ist zu eng, weil Verkehrsdaten nicht nur in den Vermittlungsstellen der Telekommunikationsorganisationen gespeichert werden könnten. Andererseits ist die Formulierung „zur Bereitstellung des entsprechenden Dienstes" im Vergleich zu Artikel 10 Nr. 2 des ursprünglichen Vorschlags nicht hinreichend präzise.

8. Artikel 8 – Anzeige der Rufnummer des Anrufers

Artikel 8 Nr. 1 sollte neu gefaßt werden, um ausdrücklich klarzustellen, daß der anrufende Teilnehmer (oder einzelne Benutzer) in der Lage sein sollte, die Anzeige seiner Rufnummer von seinem Endgerät aus in einfacher Weise in jedem Einzelfall zu unterdrücken, ohne daß die Einschaltung der Telekommunikationsorganisation, des Diensteanbieters oder irgendeines Dritten notwendig ist.

Artikel 8 Nr. 2 bezieht sich nur auf Telekommunikationsorganisationen. Die Anwendung dieser Regelung sollte ebenfalls auf Diensteanbieter erstreckt werden.

Die Datenschutzbeauftragten in der Europäischen Union sind generell der Auffassung, daß die Speicherung der übermittelten Rufnummer durch den angerufenen Teilnehmer ohne entsprechende Information des Anrufers eine unfaire Datenverarbeitung darstellt.

In Bezug auf den letzten Satz von Artikel 8 Nr. 3 gibt es gute Gründe dafür, die Möglichkeit der Beschränkung ankommender Verbindungen auf diejenigen, bei denen die Anzeige der Rufnummer des Anrufers nicht ausgeschlossen worden ist, privaten Einzelpersonen vorzubehalten. Kein Bürger sollte gezwungen werden, sich zu identifizieren, wenn er eine öffentliche Stelle anruft. Telekommunikationsorganisationen, die bisher überhaupt keine derartigen „block-blocking-Einrichtungen" anbieten, sollten damit unter der zukünftigen europäischen Gesetzgebung fortfahren dürfen.

In Artikel 8 Nr. 5 sollten die Worte „für den Teilnehmer, der diese Möglichkeit wahrnimmt," nach „kostenfrei" eingefügt werden.

9. Artikel 11 – Teilnehmerverzeichnisse

Die Datenschutzbeauftragten in der Europäischen Union unterstützen die in Artikel 11 Satz 2 getroffene Regelung, die den Teilnehmer berechtigt, **kostenfrei** ohne Geschlechtsangabe oder überhaupt nicht ins Teilnehmerverzeichnis aufgenommen zu werden. Ein flexibleres System der Nichtaufnahme in Teilnehmerverzeichnissen, wie es in verschiedenen Mitgliedstaaten existiert, sollte erwogen werden (z. B. Nichtaufnahme in das Teilnehmerverzeichnis bei gleichzeitiger Erlaubnis für die Telekommunikationsorganisation oder den Diensteanbieter, die Telefonnummer auf Anfrage weiterzugeben). Diesen Mit-

gliedstaaten sollte wenigstens gestattet werden, ihre verschiedenen Grade der Nichtaufnahme in Verzeichnisse, die einen höheren Datenschutzstandard ausmachen, beizubehalten.

Artikel 11 sollte für alle Arten von Teilnehmerverzeichnissen (konventionelle und elektronische [X-500 etc.]) gelten. Dies sollte in der Regelung entsprechend klargestellt werden.

10. Artikel 12 – Überwachung der Kommunikation

Das Verhältnis zwischen Artikel 12 Nr. 1 und Artikel 12 Nr. 2 muß klargestellt werden. Nr. 1 scheint sich auf die Lizensierung von Abhöreinrichtungen oder anderen Einrichtungen zum Abfangen von Gesprächen auf einer gesetzlichen Basis zu beziehen. Nr. 2 scheint sich genereller auf das Abhören sowie die Weitergabe des Inhalts von Telefongesprächen zu beziehen. Beide Regelungen bedürfen der Klarstellung.

Im einzelnen sollte Nr. 2 nicht auf eine spezielle Technik („auf Band gespeichert“) beschränkt werden, die bald veraltet sein könnte. Sie sollte ebenso auf das Speichern auf Mikrochips und anderen Medien anwendbar sein.

Der Verweis in Artikel 12 Nr. 2 sollte auf den gesamten Artikel 9 ausgedehnt werden. Anderenfalls wäre die Aufzeichnung von Notrufen bei der Feuerwehr unter der europäischen Gesetzgebung illegal.

11. Artikel 13 – Unerbetene Anrufe

In Artikel 13 Nr. 2 gibt es einen Unterschied zwischen der englischen Version auf der einen Seite und der französischen und der deutschen Version auf der anderen Seite. Die beiden letzteren beschränken die Anwendbarkeit dieser Ziffer auf die Übermittlung automatischer Ansagen auf „Werbung oder Verkaufsförderung/-forschung“ entsprechend Artikel 13 Nr. 1. Diese Beschränkung fehlt im englischen Text ohne ersichtlichen Grund. Sie sollte auch in die englische Fassung aufgenommen werden. Sonst wäre es nicht möglich, automatische Telefaxnachrichten an Teilnehmer zu schicken, die darin nicht eingewilligt haben (vgl. Artikel 13 Nr. 3).

12. Artikel 16 – Rechtsmittel und Ahndung

Artikel 16 enthält nur eine Regelung bezüglich der Rechte des Einzelnen, die in der allgemeinen Datenschutzrichtlinie enthalten ist. Dies könnte zu rechtlichen Streitigkeiten darüber führen, ob andere ähnliche Regelungen der allgemeinen Richtlinie, besonders Artikel 23 über die Haftung, im Telekommunikationskontext angewandt werden kann oder nicht. Um dies zu verhindern, sollte es entweder einen allgemeineren Verweis auf die entsprechenden Artikel in der allgemeinen Richtlinie geben oder sie sollten alle in die ISDN-Richtlinie aufgenommen werden.

13. Artikel 17 – Arbeitsgruppe zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

Artikel 17 Nr. 2 bestimmt, daß die Arbeitsgruppe speziell für den Zweck dieser Richtlinie konstituiert werden wird.

Unabhängig davon, welchen Zwecken diese Regelung dienen soll, sind die europäischen Datenschutzbeauftragten der Auffassung, daß es den Mitgliedstaaten überlassen werden sollte, selbst über die Zusammensetzung der Arbeitsgruppe zu entscheiden. Artikel 17 Nr. 2 sollte daher gestrichen werden.