Berliner
Datenschutzbeauftragter

BERLIN

Symposium

Multimedia und Datenschutz

Multimedia and Data Protection

28. August 1995

Dokumentation

Materialien zum

22 Datenschutz

Symposium

Multimedia und Datenschutz

Multimedia and Data Protection

28. August 1995

Dokumentation

Impressum

Herausgeber: Berliner Datenschutzbeauftragter
verantwortlich: Claudia Schmid
Pallasstraße 25/26, 10781 Berlin
Telefon: (0 30) + 78 76 88 44
Telefax: (0 30) 2 16 99 27
Bildschirmtext: * 92 67 90 #

Redaktion,
Layout: Volker Brozio

Satz und Druck: Verwaltungsdruckerei Berlin

1. Auflage: Dezember 1995

Vorwort

Die Informations- und Kommunikationstechnik schreitet immer weiter fort. Mit der Integration von Telefon, Computertechnologie und Fernsehen – allgemein als „Multimedia“ bezeichnet – wird eine neue Dimension der Informationsverarbeitung erschlossen.

Wie regelmäßig anläßlich der Internationalen Funkausstellung in Berlin hat der Berliner Datenschutzbeauftragte auch diesmal zu einem Workshop eingeladen, bei dem rechtliche und technische Aspekte des Datenschutzes bei den neuesten Entwicklungen der Informationstechnik von internationalen Experten erörtert werden.

Im folgenden werden die Vorträge veröffentlicht, die am 28. August 1995 beim Symposium „Multimedia und Datenschutz“ gehalten wurden. Sie verdeutlichen die weite Spannbreite der Probleme, die Multimedia aufwirft. Die Integration verschiedener Rechtsgebiete, insbesondere des Datenschutz-, Telekommunikations- und Rundfunkrechts, sowie die Internationalität der Problemstellung zeigen, daß für die nächsten Jahre ein erheblicher Handlungsbedarf besteht.

Erneut bedanke ich mich für die fruchtbare Zusammenarbeit beim Symposium 1995 bei allen Beteiligten und lade alle Leserinnen und Leser ein, mit uns am 1. September 1997 die Diskussion in Berlin fortzusetzen.

Dr. Hansjürgen Garstka

Berliner Datenschutzbeauftragter

Inhalt

Eröffnungsansprache zum Symposium „Multimedia und Datenschutz“ beim Internationalen Mediendialog 28. August 1995 in Berlin

Hansjürgen Garstka
Berliner Datenschutzbeauftragter

Sehr geehrte Damen und Herren,

ich begrüße Sie sehr herzlich bei unserem Symposium zu Fragen des Datenschutzes, das seit vielen Jahren parallel zur Internationalen Funkausstellung stattfindet. Besonders begrüße ich wieder die Mitglieder des Internationalen Arbeitskreises Telekommunikation und Medien, der im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten gegründet worden ist und alle zwei Jahre die Gelegenheit nutzt, sich auf unserer Berliner Ausstellung über die neuesten Entwicklungen auf seinem Arbeitsgebiet zu informieren.

Unser diesjähriges Symposium befaßt sich mit Datenschutzproblemen bei Multimedia, dem großen Thema dieser Funkausstellung. Dieses Thema ist für die Arbeit in unserem Arbeitskreis in gewisser Weise denkwürdig: Die ersten Probleme, mit denen man sich befaßte, betrafen die Risiken, die möglicherweise mit den ersten Versuchen einer Integration der herkömmlichen elektronischen Medien entstehen würden: der Integration von Telefon und Fernsehen, später auch dem PC bei Videotext-Diensten, die in Deutschland unter dem Namen „Bildschirmtext“ angeboten wurden (und nicht unbedingt eine immer glückliche Entwicklung nahmen), oder ersten Experimenten mit einem Rückkanal beim Fernsehen, dessen Verkabelung die technische Voraussetzung für eine stürmische Entwicklung zunächst der Programmvielfalt, nunmehr der Einführung interaktiver Angebote wurde (wenn man sich deren Entwicklung auch viel schneller vorgestellt hatte).

Nicht ahnen können hatte man damals anfang der 80er Jahre, in welchem Maße die Entwicklung der Computertechnologie sowie der Telekommunikationsnetzwerke zu einer kaum vorstellbaren Ausdehnung der individuellen Erreichbarkeit auf Grund der PC-Technologie, der Variabilität der einbeziehbaren Informationsarten auf Grund der Digitaltechnik, der Ubiquität auf der Grundlage des zunächst im Wissenschafts- und Forschungsbereichs aufgebauten Computerverbundes, der den Namen des ihm zugrundeliegenden Kommunikationsprotokolls „Internet“ trägt, führen sollte.

Das Ergebnis dieser Entwicklung ist eine Situation, die sich grob wie folgt charakterisieren läßt:

- Verschiedenen Formen der Darstellung von Information sind nicht mehr verschiedene Informationstechniken gewidmet: Datenverarbeitung, Telekommunikation und Rundfunk sind keine kategorisch voneinander getrennten, technisch und rechtlich inkommensurablen Größen mehr, sie fließen ineinander und stellen sich dem Nutzer nur noch als verschiedene Funktionen einer einheitlichen Informationssphäre dar, die mit einheitlichen Mitteln empfangbar, aber auch manipulierbar sind.
- Medien, die traditionellerweise nur monodirektional ausgerichtet sind, ermöglichen dem Nutzer künftig, in das Geschehen einzugreifen, sei es durch Teilnahme an der Kommunikation (black boards, news groups), sei es durch Beeinflussung des kommunikativen (Programmauswahl) oder nichtkommunikativen (Fernwirkdienste) Geschehens. Dies betrifft nicht nur die Einführung der Interaktivität in die klas-

sischen Medien Rundfunk und Fernsehen, sondern auch die Mobilisierung bislang ebenfalls einseitig ausgerichteter Lebensbereiche, etwa beim Lernen, beim Spielen oder in der Politik – Teledemokratie ist eine Vokabel, die früher belächelt, heute ernsthaft diskutiert wird.

- Durch die weltweite Vernetzung werden Informationen in jeder Darstellungsform, in jeder beliebigen Menge und ohne Zeitverzug von überall her verfügbar, soweit sie nur dem globalen Netz zur Verfügung gestellt werden. Technische und rechtliche Schranken relativieren sich, ja werden bedeutungslos: Ein einziger Nutzer von Internet genügt, um den Paßwortschutz eines sensitiven Verfahrens global außer Kraft zu setzen, ein einziger Datenlieferant genügt, um ein urheberrechtlich geschütztes Werk jedermann entgeltlos verfügbar zu machen.
- Noch gravierender könnten künftig die Risiken sein, die die Verknüpfung von Hochleistungscomputern mit den Datenbeständen mit sich bringt: Insbesondere die großen Bildverarbeitungskapazitäten ermöglichen in zunehmendem Maße die unerkannte Manipulation der Informationen. Zunehmend wird sich Echtes von Gefälschtem nicht mehr unterscheiden lassen: Tatsächliche und virtuelle Welten verschmelzen.

Die Konsequenzen für die Verarbeitung personenbezogener Daten und damit für die Gewährleistung des Datenschutzes, oder wie wir es aufgrund der Rechtsprechung des Bundesverfassungsgerichts in Deutschland bezeichnen, der informationellen Selbstbestimmung, sind gravierend.

Die vordergründige Ursache hierfür ist der Umstand, daß Voraussetzung für die neuen Formen der Kommunikation, die Dienste und Dienstleistungen die Verarbeitung von Daten in einem zuvor nicht erforderlichen Umfang ist; diese Daten, die zunehmend nicht mehr endgerätebezogen sind (und damit zwar personenbezogen, aber eben nur mittelbar), sondern unmittelbar personenbezogen (die Einführung einer individuellen, weltweit gleichen Identifikationsnummer steht nicht nur beim mobilen Telefon, sondern auch bei leitungsgebundenen Diensten bevor) werden sowohl für den Aufbau der Verbindung (die, denken wir an Telespiele wie Fernschach, gegebenenfalls intermettierend über große Zeiträume aufrechterhalten werden muß) als auch für die Abrechnung der entstandenen Entgelte benötigt – auch in Bereichen, deren Nutzung, wie bei Rundfunk und Fernsehen, bisher anonym erfolgen konnte.

Im Ergebnis entstehen gigantische Datensammlungen, die dem berechtigten, aber auch dem unberechtigten Nutzer erlauben, die Kommunikations-, aber auch Konsum- und sonstigen Verhaltensgewohnheiten der Teilnehmer zu beobachten und entsprechende Persönlichkeitsprofile zu gewinnen. Dies gilt auch für diejenigen Netzteilnehmer, die am eigentlichen Kommunikationsgeschehen nicht beteiligt sind, sondern nur durch ihre Dienstleistungen die Kommunikation ermöglichen – etwa die Vielzahl der Betreiber von Netzknotenrechnern im Internet, die jeden durchlaufenden Telekommunikationsverkehr verfolgen oder zumindest verfolgen können.

Auch die Risiken, die mit der Übermittlung der Inhalte selbst verbunden sind, erhöhen sich erheblich: Die Einbeziehung von Bild und Ton in die Kommunikationsmöglichkeiten intensiviert die Eingriffsmöglichkeiten in die Privatsphäre erheblich. Kurze verbale (und damit auch steuerbare) Darstellungen werden ersetzt durch das Originalbild, den Originalton. Versteckte Zusatzinformationen, derer sich die Teilnehmer nicht bewußt sind, werden mitübermittelt, wahrgenommen und gespeichert (denken wir auf die Aufzeichnungen über Videokonferenzen, die nicht nur dem Psychologen, sondern jedem Teilnehmer vieles über die Befindlichkeiten der Partner mitteilen können).

Die zunehmende Nutzung der multimedialen Dienste wird den Zugang zu anonymen Kommunikationsformen erschweren; schon jetzt ist absehbar, daß die Nutzung von Diensten, bei denen Persönlichekitsprofile entstehen, auch finanziell honoriert, anonyme Kommunikation belastet wird. Es wird erhebliche Anstrengungen kosten, dem entgegenzusteuern.

Diese nur skizzierten Aspekte machen in verschiedener Hisicht nicht nur eine Änderung der bestehenden rechtlichen Rahmenbedingungen, sondern meines Erachtens auch die Entwicklung neuer Paradigmen in der Datenschutzdiskussion erforderlich.

Vier Punkte, die mir besonders wichtig erscheinen, möchte ich herausgreifen:

- Die meisten Datenschutzgesetze, die es in den verschiedenen Staaten bisher gibt, konzentrieren sich auf die herkömmliche Datenverbreitung: die klassische EDV, mitunter ergänzt um restriktive Regeln bei der manuellen Verarbeitung von Daten in Dateien (die neue EU-Richtlinie macht hiervon keine Ausnahme). Es müssen Regelungsformen gefunden werden, die auch die Bild- und Tondaten erfassen, ja, die offen sind für künftige Entwicklungen etwa in der Sensorenforschung. Die herkömmliche Klassifizierung der Datensensibilität nach Lebensbereichen (Adreßdaten, Personaldaten, medizinische Daten) muß ergänzt werden zumindest um Aspekte der Informationstiefe und der Informationsverfügbarkeit.
- Sektorell bestehende Privilegierungen oder aber auch Erschwernisse müssen darauf hin geprüft werden, ob sie noch Sinn haben oder zumindest modifiziert werden müssen; zum ersten Aspekt gehört die Reichweite des sogenannten Medienprivilegs, das die journalistischen Daten von datenschutzrechtlichen Verpflichtungen nahezu freistellt; zum zweiten gehört die Frage, ob das im deutschen (nicht z. B. im schweizerischen) Recht verankerte Verbotsprinzip in dieser generellen, ohnehin nur theoretisch effektiven Form weiterbestehen kann. Auf dem Gebiet der Telekommunikation sehr kennzeichnend ist in dieser Hinsicht die aktuelle Diskussion in den USA, ob die unterschiedliche Behandlung von Telefon und Kabelfernsehen auch in datenschutzrechtlicher Sicht sinnvoll ist.
- Die Sicherung der Vertraulichkeit der übermittelten Informationen, vor allem aber der Schutz vor Manipulation wird die Entwicklung geeigneter Authentifikations-, Verschlüsselungs- und Verifikationsinstrumente zu einer vordringlichen technischen Aufgaben werden lassen.
- Schließlich: Die neuen Techniken erfordern eine Modifikation der Kontrollmechanismen. Sie sind in Deutschland im privaten Bereich bekanntermaßen unterentwikkelt; die EU-Richtlinie wird hier Verbesserungen etwa im Bereich der Vollzugsmaßnahmen bringen – dies wird aber eine grundsätzliche Diskussion nicht überflüssig machen. Ganz wesentlich wird hier sein, wie der internationale Aspekt von Multimedia auf die Kontrollinstrumente abgebildet werden kann.

Meine Damen und Herren,

mit dieser Skizze wollte ich einen kleinen Einblick geben in die Vielfalt der Probleme, mit denen uns unser heutiger Tag konfrontieren wird.

Ich erhoffe für uns alle einen guten Ertrag für die Meisterung der bevorstehenden Probleme bei Multimedia und Datenschutz.

Multimedia as a new challenge and opportunity in privacy: The examples of sound and image processing

Joel R. Reidenberg
Fordham University School of Law – New York

Multimedia presents the Information Society with a variety of novel challenges and opportunities for privacy. Multimedia combines image, audio, text, data, transmission and transaction capabilities to enable the creation of products and services as varied as home shopping and PC videoconferencing. These possibilities alter the dimensions of privacy.

Prior to digitalization, recordings were relatively static media. Diversions, manipulations and modifications were possible only with special equipment and transmissions usually entailed discrete point-to-point transfers. Society generally expected sound and image to be authentic. In these contexts, voice and photographic processing implicated specific, limited privacy interests. Privacy typically meant the prevention of intrusive photographers, the restriction of the unauthorized uses of one's name or likenesses, and the preclusion of unwanted listeners.[1] Before the turn of the Twentieth Century, Warren and Brandeis wrote of the threat to privacy from intrusive new technology, the camera.[2] Well before that, in biblical times, civilization developed a strong tradition controlling images: the Ten Commandments went as far as prohibiting any attempt to make a certain graven image. More recently, in this century, communications technology spawned anti-wiretapping laws.[3]

Digitalization and the combination of transaction capabilities remove constraints on sound and image processing. Manipulations and modifications of sound, image, text and data become routine and desirable in the construction of a networked Information Society. Digitalization destablizes society's expectations for sound and image; digitalization both expands the privacy interests of individuals and consolidates diverse areas of the law. The treatment of digital images and audio implicates the control of personal information and not just the problems of intrusive recordings or unauthorized disseminations. Image and sound now fall under a broader rubric of fair information practice. Principles of fair information practice set conditions for the collection, use, storage and dissemination of personal information.[4] Digitalization further overlays the treatment of personal information with intellectual property protections that historically allocated rights to control images and sound. Already, this expansion of interests has been raised in public discus-

1 See, e.g., Restatement (Second) of Torts, § 652 (1977); William Prosser, The Right of Privacy, 48 Calif. L. Rev. 383 (1960).

2 Samuel Warren & Louis Brandeis, The Right of Privacy, 4 Harv. L. Rev. 193, 196 (1890) (the press was „overstepping in every direction the obvious bounds of propriety and of decency.")

3 See, e.g., 18 U.S.C. §§ 2510–2520 (1988 & Supp. 1993).

4 See, e.g., U.S. Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (June 6, 1995) (available on Internet World Wide Web at http:://iitf.doc.gov); U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society (1977); O.E.C.D. Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. No. C (80) 58 [hereinafter „OECD Guidelines"]; Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Euro. T.S. No. 108 (Jan. 28, 1981)[hereinafter „European Convention"]; Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (July 24, 1995) [hereinafter „European Directive"].

sions in the United Kingdom concerning image processing for college applications[5] and by regulatory authorities in France.[6]

In essence, multimedia and the Information Society are now pushing and redefining the boundary that society accepts for the observation and disclosure of an individuals thoughts and activities.[7] The multimedia "data stream" presents a critical challenge to privacy through the impact of digitalization and the structure of multimedia systems. At the same time, the multimedia data stream offers opportunities for fresh thinking about privacy boundaries and for the establishment of new consolidated norms to respond to the challenges.

I Understanding the Multimedia data stream

The development of multimedia relies on the digital conversion of sound and image and the efficient structuring of their delivery systems. Multimedia requires that sound and image be encoded to numeric representations and decoded back to aural and visual form. The characteristics create new electronic data streams of personal information with unintended consequences for privacy. These data streams encounter established principles for the fair treatment of personal information that did not expect the "processability" of sound or image. At the same time, the new data streams confront enshrined rules and norms for image and voice (intellectual property and privacy) that did not anticipate the information processing aspects of today's multimedia.

Beyond the digital conversion, networks for processing and delivering multimedia push for efficient architectures that can consolidate or distribute functions and data across a wide range of sites. For example, video-on-demand services may involve one site to store the content, another site to route content to users, and a third site to process payment aspects.[8] Alternatively, all features and functions may be centralized on one processor and one local storage medium like a CD-ROM. At any point, the architecture may also be changed. This dynamic structure leaves the dimensions of privacy in a state of flux.

A. The Digital Conversion

Digitalization is one of the keys to both the challenges and opportunities in multimedia privacy. Digitalization itself moves image and audio into the realm of complex information processing. Any personal computer can manage and modify a data stream. Digital information has significant "plasticity".[9] Digitalization also means that multimedia users become producers of components of the data stream; interactivity leaves critical traces that themselves become part of the data stream. Digitalization turns sound and image into dynamic information rather than static aural and visual representations.

The digital conversion is significant in terms of each multimedia component. For images, numeric processing allows the matching, manipulation and creation of visual information. For example, with just a few key strokes, a faxed image of a letter can be reconstituted in different computerized form by the recipient. A signature may be electronically

5 British colleges are considering accepting UCAS applications as images, but recognize that the data protection rules mean different treatment for the applications and confidential reports. This was discussed on the Internet listserve, „data-protectionδmailbase.ac.uk," during June, 1995.

6 See C.N.I.L., 14ieme Rapport, at 65–70 (1994).

7 Robert C. Post, The Social Foundations of Privacy: Community and Self in the Common Law Tort, 77 Calif. L. Rev. 957 (1989) (arguing that privacy torts form a consensual boundary in society).

8 See, e.g., C.N.I.L., Délibréation no. 94–058 du 21 juin 1994 et Délibréation no. 94–059 du 21 juin 1994, reprinted in C.N.I.L., 15ieme Rapport, 64–65 (1995) (describing some of the pay per view arrangements in France).

9 Pamela Samuelson & Robert J. Glushko, Intellectual Property Rights for Digital Library and Hypertext Publishing Systems, 6 Harv. J. Law & Tech. 237, 240 (1995) (the authors denote "plasticity" as the ease with which digital works can be manipulated and modified.)

"cut out" and saved for future use and portions of the text may similarly be cut out and saved. These elements can then easily be re-assembled with additional text or images. The personal information in the image becomes automatically processable.[10] Optical character recognition software enables the conversion of images and faxes to searchable text.[11] Hypertext software and object packaging[12] can transform images into computer searchable data. This type of software allows users to define searchable, hierarchical levels. With these features, images can be packaged as objects and linked to key words in a hierarchical level. Essentially, these features create indexed images that can be accessed, rearranged and used electronically.[13] Direct image recognition and editing software also exist.[14] For example, image processing now enables law enforcement to match eye retinas or finger prints to suspects.[15] In essence, digitalization transforms images into personal information. As such, digitalization implicates the standards for the treatment of personal information.

Similarly, for sound, digitalization creates "processability." Analog sound waves when translated into numeric representations acquire malleability and transaction processing capabilities. For example, in the United States, telephone directory services use voice recognition to provide telephone numbers to callers.[16] The local telephone company in New York, NYNEX, offers customers voice dialing.[17] With voice dialing, a caller says the name of the person to be called and voice recognition functions process the oral statement, associate the voice with the caller, check the caller's personal directory and place the call. Telemarketing order departments are also using voice recognition and digital processing to manage customer orders.[18] Compaq even brought voice processing to the desktop with digital voice messaging features built into their personal computers.[19] At the core, digitalization allows electronic sorting, organizing and categorizing of sound.

The digital conversion allows multimedia applications to combine the processability of each component (sound, image, data and text.) Electronic publishing, for example, offers complex processing capabilities inexpensively.[20] Hypertext software allows electronic sorting and organizing of sound, video and image all together.[21] High speed digital telephone lines (ISDN service) make videoconferencing on personal computers possible with

10 These activities can be accomplished readily using an IBM compatible personal computer and Windows software (e.g. WinFax Lite and Word Perfect 5.2). The entire operation takes just a few minutes.

11 Many commercial scanning devices come pre-packaged with "Optical Character Recognition" software. Hewlett Packard, for example, sells its scanners with Calera WordSCan. See, e.g., J&R Computer World, Pre-Summer Catalog, at 87 (1995).

12 Object packaging refers to the preparation of a digital image that is to be accessed by clicking on an icon at a specific point in a database file. See, e.g., Microsoft Corp, Microsoft Windows & MS-DOS 6.2 User's Guide, at 120 (1993).

13 See Folio Corp., Folio Views Personal Electronic Publishing Software User Guide Version 3.0 for Windows, at 47, 186, 292–299, 324–335 (1993).

14 See J&R Computer World, Pre-Summer Catalog, at 90 (1995) (Cannon sells its scanning devices packaged with OFOTO 2.0 image editing software.) The popular Microsoft Paintbrush program for Windows also allows image "editing" or manipulation.

15 See Ben Grove, In a blink cops find ways to ID suspects, Chicago Trib., July 14, 1995, at 1 (describing retina imaging technologies); Indentix, Inc., SEC Filing Form 10K (June 30, 1994), available on LEXIS On-Line Service, COMPNY libary, COMPNY file (describing fingerprint imaging technology).

16 See Michael T. Kaufman, Sorry, Ma'am, No Listing for 'enry 'iggins, NY Times, June 26, 1995, at D1, D4.

17 Id.

18 Richard Szathmary, Telemarketing Computer Communicates; New Technology, designed to replace operators, gets the gist of conversations, DM News, June 5, 1995, at 10.

19 The Compaq Presario line of personal computers comes equipped with a "complete phone center" that includes call switching to voice mailboxes and caller id capture features.

20 Programs are commercially available for several hundred U.S. dollars.

21 See Folio Views Corp., Folio Views Electronic Publishing Software User's Guide Version 3.0 for Windows (1993).

real time simultaneous visual, aural, textual and data communications;[22] live video and audio inputs convert to a digital data stream.[23] These services link information to individuals as do teleshopping and other on-line multimedia services. Both the act of using multimedia and the content of multimedia generate personalized processing of information.

Beyond the processability of the content of multimedia (the sound and image), users create a wealth of new information for the data stream. The customization of multimedia for users provides an increasingly precise profile of the behavior of individuals. Transaction capabilities built into multimedia products generate personal information. Imagine, for example, a film-on-demand service sponsored by advertisers who provide teleshopping opportunities during each film. The user's film preferences as well as advertising preferences can now be monitored and analyzed with details as precise as the viewer's sound volume choice for particular segments of specific commercials. Even self-contained multimedia products generate similar transaction information. Hypertext program features include the creation of an audit trail.[24] Multimedia makes knowledge of individual behavior easier to obtain; patterns and details of interactive uses flourish in the multimedia environment.

B. Dynamic System Structure

The architecture of technological systems for multimedia comprises a second key novelty that impacts on privacy interests. Multimedia may be fixed locally, such as the case with a CD-ROM, or may be designed for interactive use across distances, such as the various on-line services. System architecture takes on a complex character that implicates the responsibility for the handling of personal information. Depending on the architecture, different participants control the multimedia data stream. For example, content may be intrinsically bundled with software that only allows read access to sound and image. Or, the same sound and image may be distributed through a web site on the Internet that allows users to download the data for future applications. Technological responsibility for the treatment of personal information, thus, varies widely according to the structure of the multimedia data stream.

The architecture possibilities are also significant because distributed creation or delivery means that elements from various jurisdictions may be combined to form one multimedia production.[25] Multimedia products may be created and distributed across many computing and transmission sites at one or more locations. For example, in the area of "telemedicine", ultrasound images are transmitted from nine geographically diverse clinics in Maryland, Virginia and the District of Columbia to centrally located specialists.[26] In Georgia, North Carolina, Texas, West Virginia and twelve other U.S. states, interactive

22 Intel ProShare is one of many emerging commercial PC videoconference products; CU-SeeMe is one of the first university products that experiments with videoconferencing over the Internet. The concept is not complicated. The user mounts a small camera and microphone on a PC. With an add-on circuit board, the PC converts the camera image and microphone sound for digital transmission and displays the other party on screen. At the same time the parties communicate on screen, the PC allows the parties to share the same document or database file.

23 A "codec" converts live video and audio inputs into digital information. The device relies on emerging international standards to establish common, recognized protocols for the processing of multimedia data streams.

24 Folio Views 3.1, for example, has a "backtrack" feature that reconstructs previous use of other program features. The program also automatically tracks the databases that a user accessed during the current session.

25 See M. Ethan Katsh, Law in a Digital World 65–91 (1995) (discussing the mislabeling of information databases as "libraries.")

26 Douglas D. Bradham, Sheron Morgan & Margaret E. Dailey, The Information Superhighway and Telemedicine: Applications, Status and Issues, 30 Wake Forest L. Rev. 145, 153 (1995).

systems allow doctors to examine patients hundreds of miles away and consult with specialists at distant locations.[27] These features have the consequence of raising privacy interests in multiple places simultaneously.

Like the "plasticity" of multimedia content, the system structure itself is also malleable. Digital multimedia combines mechanisms for product creation with those of delivery. Functional capabilities of hardware and software along with transmission and storage facilities each contribute to the development of multimedia products and services and each contribute to the delivery of those products and services to users. Many alternative technological paths are available to produce and distribute the same multimedia product. If one architecture has obstacles, such as undesirable rules, another may be developed to by-pass the trouble spot. Market pressures will also drive flexible system development. Multimedia markets will push for new ways to mine and recycle data streams. These pressures embed incentives for alternative system architectures.

II. The challenge of sound and image digitalization

The multimedia data stream forces sound and image processing to confront issues of personal information and fair information practices. Sound and image relate intrinsically to identifiable individuals. With multimedia, all information in the data stream becomes "personal information" linked to specific individuals. Information processing for sound and image, thus, directly implicates fair information practice principles. The data can be collected, scanned, searched, linked, and disseminated electronically. Digital sound and image processing with intelligent communications networks nevertheless challenge the distinctiveness of standards for the fair treatment of personal information. Multimedia merges legal regimes for the protection of individuals' interests. In addition, multimedia challenges the locus of control of information flows: the data stream diffuses processing and substantially widens the access afforded to digital sound and image.

A. Merging Distinct Legal Regimes

Sound and image processing pose a challenge to the distinct nature of the legal regimes developed to secure individuals' interests in society. Assuring the fair treatment of personal information in the multimedia data streams blends different forms of privacy protection. Digitalization of sound and image radically expands the applicability of principles for fair information practice, while at the same time merges intellectual property protections with the objectives of fair information practice principles.

Twentieth Century privacy law draws its origin in the "right to be let alone."[28] This basic concept grew in the United States to enshrine interests against intrusions upon one's seclusion, the appropriation without authority of one's name or likeness for commercial purposes, the publication of private facts about a person, and the publication of facts that portray an individual in a false light.[29] During the last twenty years, distinct standards for fair information practices developed to assure the protection of individual interests in response to the transformation of record keeping from paper trails to electronic files. Fair information practice principles in the United States and data protection laws in other countries sought to establish standards for the collection, use, storage and dissemination of personal information subject to electronic processing.[30]

27 Id., at 154–59.

28 Warren & Brandeis, supra note 1.

29 Restatement (Second) of Torts, § 652; See also Raymond Wacks, Personal Information: Privacy and the Law (1989); William Prosser, The Right of Privacy, 48 Calif. L. Rev. 383 (1960).

30 See supra note 4; Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L. J. 195 (1992).

Before digitalization, the protection of rights to solitude and publicity offered individuals a specific mechanism to control image and voice recordings and transmissions, while fair information practice doctrines designed unique treatment for electronic personal information. Multimedia and the digital conversion links these two strands of privacy protection. The concept of electronic files and discrete processing activity no longer exists. Data streams and networks replace the data file. Multimedia automatically implicates the classic rights to prevent unauthorized publication of one's name, likeness and even voice.[31] These 'rights to publicity' traditionally protected against the commercial appropriation of individuals' interests in their identity. Digital imaging and sound sampling cross these rights with fair information practice principles. For example, one of the major U.S. banks now issues a credit card with the cardholder's digital photograph imprinted on the card.[32] Although U.S. rules for the treatment of personal information do not prohibit the card issuer from disclosing the details of a cardholder's transactions, the right of publicity would nevertheless restrict the issuer from using the digital photograph.[33] Similar crossovers exist in other legal systems.[34]

The solitude strand of privacy protection faces challenging scrutiny. The tort of intrusion upon seclusion traditionally applied to the manner in which sound and images were collected. The protection guards against hidden surveillance. To benefit from the seclusion right, some violation of private space must occur. Similarly, the protection against the dissemination of private facts historically assured individuals of control of sensitive or highly embarrassing information that was not publicly known. In informational privacy terms, solitude is only offended if multimedia derives from non-publicly accessible sources. By contrast, fair information practice principles maintain that personal information may not be collected surreptitiously, even if the information does originate in publicly available places. Under data protection standards individuals have rights of notice and consent to data collection.[35]

In according individuals control over sound and image data, solitude objectives overlap with the control granted to individuals by fair information practice principles. However, the threshold of interdiction is significantly lower for solitude than for fair information practice. Solitude would not, for example, protect against the use of digital recordings made while an individual was in a public square, but fair information practice rules might. Multimedia effectively eliminates the different thresholds. The overlap between solitude and fair information practice principles allows restrictions on the use of multimedia based on the lowest common denominator. In this environment, either solitude gains strength as a protection applicable even for public activities or fair information practices loses strength as a protection for all gatherings of personal information.

Another particular challenging aspect of the multimedia data stream is the allocation of responsibility for the accuracy of digital sound and image. System architecture may result in receipt by multiple participants of personal information. The server, processing nodes, user and data subject each may technologically gain access and store elements of the

31 The right of publicity protects a celebrity's interest in the prevention of unauthorized endorsements. The right has been extended to protection for voice. See Cal. Civ. Code, § 3344; Midler v. Ford Motor Co., 849 F. 2d 460 (9th Cir., 1988), cert. denied 112 S. Ct. 1513, 1514 (1992) (Ford violated Bette Midler's rights when it used her voice in a commercial). But see Tin Pan Apple, Inc. v. Miller Brewing, 737 F. Supp. 826 (1990) (strict interpretation of New York privacy statute does not extend protection to voice).

32 Citibank encourages its Visa cardholders to provide a photograph for use in digital form on the card.

33 See, e.g., Restatement (Second) of Torts, § 652C; N.Y. Civ. Rights Law, §§ 50–51 (McKinney 1990).

34 See Gilles Nejman, Les applications multimedias interactives: une analyse juridique pluridisciplinaire, 1994/4 Rev. de droit de l'informatique et des telecomms, at 12–13 (similar questions raised in France.)

35 See Joel R. Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 Iowa L. Rev. 497 (1995).

multimedia data stream. The "plasticity" of content and dynamic system architectures hides the actual control of personal information. Sorting out the site of particular multimedia activities and the treatment of personal information is not likely to be easy. For the application of basic fair information practice rights of access and correction, these features pose an important obstacle to individuals. Similarly, assuring data minimization and deletion of stale personal information becomes uncertain with robust and diverse multimedia data streams. Ironically, at the same time as responsibility becomes diffused, the transmission or delivery mechanisms for multimedia increase opportunities for unintended access to the data stream. For example, data traffic on the Internet is accessible to anyone connected to this global network. Thus, security precautions, including encryption, surround issues of accessibility and accuracy of data.

Specific attributes of digital sound and image processing also raise hybrid challenges. An act of "multimedia consumption" produces a wealth of personal information in the form of network transaction data and patterns. "Netsurfing," for example, becomes attractive to find patterns or other identifiable information. On the Internet's world wide web, the names of users who accessed on-line pictorial catalogs are for sale.[36] One company, eWatch, already monitors thousands of discussion groups on the Internet for clients who are interested in learning whether others are saying negative things about them.[37] The same functions will become available to scan and search images and sound for particular characteristics.

Sound and image processing also pose a challenge to the principle of fair information practice that seeks distinct protection for sensitive data. Every sound and image falls within the category of "sensitive data." Images of individuals reveal racial characteristics and medical conditions such as skin or eye problems. Sound processing reveals nationality or ethnic origin through the classification and recognition of accents. For example, voice dialing must distinguish accents for the transaction features to work. Yet, to treat all sound and image as "sensitive data" diminishes the meaning of the term and the level of protection. The data stream from telemedicine, for example, is at once as intrusive, obtuse and anonymous as any information can be. Telemedicine may contain the most sensitive health information such as a magnified image of a person's sexually transmitted disease virus, yet be incomprehensible to the untrained eye of anyone in the data stream other than a specialist physician. Similarly, the image may not be identified to any particular patient at sites along the data path. In effect, the multimedia data stream introduces ambiguity for special protections for "sensitive" information.

Beyond the hybrid challenges to principles of fair information practice, the treatment of digital information mixes with the treatment of intellectual property. While data privacy may have a foundation in property and intellectual property theories,[38] multimedia works directly evoke the protection of intellectual property laws.[39] Copyright historically accorded rights to control the exploitation of expression. These principles apply to the storage, dissemination, and use of image and audiovisual works. The dissemination of information becomes complex with distributed computing systems and the application

36 See Larry Jaffee, Web Firm Offers to Sell Requesters' Names: Catalogers can buy them from software firm, The Marketeers, DM News, Aug. 14, 1995, at 8.

37 See Larry Jaffee, Is Big Brother Netsurfing for Business Clients?, DM News, June 5, 1995, at 1.

38 See Yves Poullet, Data Protection between Property and Liberties in Amongst Friends in Computers and Law (H.W.K. Kaspersen and A. Oskamp, eds., 1990) (rejecting property basis for data protection in favor of foundation relying on liberty.)

39 See C.N.I.L., 14ieme Rapport, 65–70 (1994)

of conventional copyright rules to multimedia becomes uncertain.[40] "Digital libraries" place newstrains on the use of information and traditional works of audiovisual entertainment.[41] Despite the special problems applying intellectual property rights to multimedia works distributed through digital networks,[42] evolving standards for intellectual property will continue to mediate aspects of the control of images and sound. This overlaps with the objectives of fair information practices and further erodes the distinctiveness of the two legal and policy regimes.

The emphasis in intellectual property law on rights to control the commercialization of works of authorship parallels the concern in data protection for the finality of data use. Protection for the ownership of sound and image data under intellectual property may operate to impose limits on multiple uses of the data stream. For example, Microsoft's arrangement with content providers for its new global network, MSN, establishes rules of control of personal information generated through the system.[43] The rules set up by Microsoft protect the privacy of network users by banning content providers' use of network client data, but they also assure to Microsoft the proprietary value of the users' information. Although the results of protection for fair information practice and intellectual property may overlap, they cannot be co-extensive. Copyright protects individuals as such only as an incident to the allocation of valuable economic rights, and fair information practice principles impinge on the copyright allocation of those economic rights. In essence, digitalization challenges the boundary between intellectual property and fair information practices.

Even beyond the general body of privacy law and intellectual property law, multimedia merges the treatment of personal information with previously unrelated areas of law. For example, the telecommunications doctrine that provides immunity to carriers for liability based on the content of communications is now under scrutiny.[44] Whether or not new liability standards are imposed on networks for the content of the data stream, the scrutiny will have an effect on the processing of sound and image. Liability threats will push networks to force content providers (i.e. the producers of multimedia) to examine the treatment of personal information. This does not, however, suggest any specific outcome. Similarly, labor laws condition employer monitoring activities and regulate image and sound surveillance of employees.

The expansion of the scope of treatment of personal information and the merger of legal regimes poses a further challenge to efficient network architecture. Uncertainty and confusion over legal standards will affect the development of multimedia infrastructures. The technological systems for multimedia networks will be structured around the legal challenges. Participants in the data stream will try to by-pass rules and standards they find undesirable. This can present either an opportunity or a hindrance to business activity.

40 See Pamela Samuelson, Legally Speaking: The NII Intellectual Property Report, Communications of the ACM (Dec. 1994); Katsh, supra note 25, at 215–227.

41 See, e.g., Pamela Samuelson, Copyright and Digital Libraries, Communications of the ACM, Apr. 1995, 15; Pamela Samuelson & Robert J. Glushko, Intellectual Property Rights for Digital Library and Hypertext Publishing Systems, 6 Harv. J. Law & Tech. 237 (1993).

42 Id.; see also U.S. Congress Office of Technology Assessment, Information Security and Privacy in Network Environments, 106–108 (1994); U.S. Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure (Sept. 1995) (available on Internet World Wide Web at http::/iitf.doc.gov).

43 See Denise Caruso, New Microsoft Network will offer a wealth of Privacy, N.Y. Times, July 24, 1995, at D4.

44 See Stratton Oakmont, Inc. v. Prodigy Services, 1995 N.Y. Misc. Lexis 229; Cubby v. CompuServe, 776 F. Supp. 135 (S.D.N.Y. 1991). There are also controversial debates in the U.S. Congress regarding liability for the electronic distribution of pornography and within the Administration concerning liability for electronic dissemination of copyrighted works.

B. Shifting Control of Information

Multimedia technology also effects a significant shift in technical control of personal information. Any computer can manipulate the multimedia data stream. Every access point to multimedia services can simultaneously generate a data stream. The architecture of multimedia systems increases in geometric fashion the number of processors of personal information and the availability of access to the data stream.

Multimedia empowers government, businesses and citizens with new scanning capabilities and applications. This technical empowerment of all segments of society diminishes the relative strength of individual participation in the circulation of personal information. For example, video surveillance once was the province primarily of the state and has now become ubiquitous.[45] The pressures to increase digital surveillance shift greater control of data streams away from individuals and toward institutions.[46] Paradoxically, wider access to the data stream and personal computers defy any central control of data streams. Instead, digital sound and image processing may be controlled simultaneous by various participants. Intelligent transportation systems ("ITS") provide a good example of this combination. Various forms of ITS surveillance rely on image and sound processing capabilities.[47] At Newark airport in New Jersey, the license plate of every vehicle exiting the parking lot is scanned and matched against a list of suspect plates. Matching drivers is similarly available. These features may be controlled by law enforcement or by an administrative agency.[48] Yet, at the same time, private sector companies may control parts of the data stream or have access to key elements such as the cars passing through Newark airport.[49] One private organization, ITS America, for example, wants to develop national standards for the data stream.[50]

The multimedia data stream also shifts significant stakes in the regulatory control of the data stream. This shift occurs across subject areas and territorial jurisdictions. The digitalization of sound and image confers substantially greater power on data protection regulatory authorities. Fair information practice takes on an overarching role in the flows of data. The shifting regulatory stakes are not a positive sum transfer. Mediators of intellectual property rights lose a degree of control to data protection authorities. The more robust role for data protection may also come at the expense of other regulatory authority. For example, those responsible for labor laws and employee monitoring will be marginalized in comparison to data protection. A key reason for this shift will be the body of expertise that data protection authorities already have in the supervision of fair treatment for personal information.

Because the multimedia data stream is global, national regulatory control also loses efficacy. The identical data stream (or elements of it) will encounter both national and foreign regulation. Consequently, foreign standards emanating from the various privacy,

45 The installation of surveillance cameras now permeates urban banks, supermarkets, and workplaces. See also, C.N.I.L. Délibération no. 93–001 du 12 jan. 1993 reprinted in C.N.I.L., 14ieme Rapport, 66–70 (1994) (discussion of concerns over increase in surveillance programs).

46 See Simon Davies, Welcome Home Big Brother, Wired, May 1995, at 58 (discussion of pressures to increase video surveillance in Kings Lynn, United Kingdom.)

47 See, e.g., Sheri Alpert, Privacy and Intelligent Highways: Finding the Right of Way, 11 Santa Clara Computer & High Tech. L. J. 97, 101 (1995).

48 The New York and New Jersey Port Authority have responsibility for Newark airport.

49 See, e.g., Dorothy Glancy, Privacy and Intelligent Transportation Technology, 11 Santa Clara Computer & High Tech. L. J. 151, 170 (1995).

50 See Glancy, supra note 49, at 183,

intellectual property and fair information practice doctrines will impact on national standards for the treatment of sound and image processing. No single set of regulations nor any single territory will be able to dictate a complete set of standards for multimedia and privacy.

These shifts in technical and regulatory control of personal information are unlikely to be smooth. The specific implications of the technical power shift will be hard to recognize ex ante. Privacy consequences of a particular technological change will emerge ex poste after movements in the data stream. In contrast, the regulatory shifts face interbureaucratic struggles for power as multimedia data streams develop. Jurisdiction over the data stream goes to the heart of future power in an Information Society. Throughout these shifts, a social consensus on sound and image processing will be elusive because the issues are complex and span a diverse international community.

III. The Opportunity for Converging Protections

Despite all the challenges, multimedia offers an unusual opportunity to enhance individual interests through the convergence of privacy protections. The merging of fair information practices with other concepts of protection for information can create new "privacy" for individuals based on the combined application of standards from different areas. By assembling a package of protections, the fair treatment of personal information may acquire an important conceptual strengthening and may gain significant technological enhancements.

A. Conceptual Strengthening

Although multimedia erodes the distinctiveness of standards for the treatment of personal information, the expansion of fair information practice coverage and the merger of legal disciplines does not weaken the underlying goal of protecting the interests of individuals. Rather, the convergence of privacy protections provides a subtle, but important conceptual strength to fair information practice principles. By overlapping intellectual property rights with fair information practice principles, multimedia introduces major political and intellectual allies to the cause of fair treatment of personal information.

The legacy of intellectual property rights for image and sound offers an intuitive basis for protection of digital multimedia. Individuals readily perceive the abuse from an unauthorized use of their photograph or voice. Because economic value is allocated to intellectual property rights, the stakeholders recognize an immediate need to protect ownership in the multimedia data stream. These stakeholders including content providers and infrastructure developers are well organized and have strong incentives to promote legal protections for image and sound processing.

In contrast, fair information practice principles have a more subtle, sophisticated basis for the protection of individuals. Fair information practice standards enshrine human rights and democracy values in society.[51] The ground rules for the treatment of personal information address intangible social issues like citizen rights and free flows of information.

51 See, e.g., Symposium: Data Protection Law and the European Union's Directive – The Challenge for the United States, 80 Iowa L. Rev. 431 (1995); Joel R. Reidenberg, Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms, 6 Harvard J. Law & Tech. 287 (1993).

These concepts are more difficult to grasp than the economic interests in intellectual property. As a result, the stakeholders are diffused across society with many divergent interests and not readily organized.

By crossing the lines of privacy protections, multimedia crystallizes the problems for individuals and mobilizes the organized stakeholders from the intellectual property arena in a way that can benefit individual interests in fair information practice. Multimedia augments the conceptual appeal of standards for the treatment of personal information. Multimedia makes the treatment of information an immediate and significant issue for individuals; the convergence with intellectual property results in an intuitive grasp of the need to protect individuals in the multimedia data stream. Individuals perceive how integrity is directly implicated by the appropriation of any elements of one's image or voice. Yet, for the typical forms of personal information gathering, integrity only becomes an issue when a sufficient amount of personal information is aggregated. For the average citizen, the details are often hard to obtain and therefore difficult to perceive as problematic.[52] Now, the traditionally strong protections of intellectual property and tort re-enforce the protections for personal information. Simultaneously, multimedia raises an immediate and significant need for intellectual property owners to assure fair protection of information. This promotes efforts to create legal protections for the treatment of sound and image.

Ultimately, the merging of legal doctrines offers novel possibilities for devising new protections. Elements of previously diverse legal doctrines, such as rights of publicity and copyright, may now be assembled to provide a single coherent legal structure to the processing of sound and image. The coherence results from the aggregate effects that protect individual interests.

B. Technical Mechanisms

The multimedia data stream also invites opportunities to develop technical mechanisms for the protection of individuals. Technical measures for self-help have a long, sometimes tortured, history.[53] Technical choices can embed privacy interests in the multimedia data stream.[54] For example, the choice of delivering content via a CD ROM rather than a client server network has a major impact on finality of personal information and access to transaction patterns. With the CD ROM, the recipient can control the usage data and may not be limited in the manipulation of the images and sound stored on the disk. In the network environment, the server, rather than the recipient, has greater control over both. In any event, a range of technological options from encryption to digital signature standards responds to disclosure and authentication concerns of digital works.[55]

The business community often looks to security protections to assure its ownership interests in intellectual property "assets."[56] The implementation of security provides valuable control over the treatment of digital images and sound. Although this control seeks to protect business ownership, it can offer possibilities for fair information practices that

52 See Joel R. Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 Iowa L. Rev. 497 (1995).

53 As Pamela Samuelson notes, Umberto Eco's famous novel, The Name of the Rose, points to a peculiar form of self-help to control readership of illuminated manuscripts from the middle ages. Pamela Samuelson, Copyright and Digital Libraries, Communications of the ACM, at 16 (1995).

54 See Joel R. Reidenberg, Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms, 6 Harvard J. Law & Tech. 287 (1993).

55 See, e.g., U.S. Congress Office of Technology Assessment, Information Security and Privacy in Network Environments (1994).

56 See U.S. Congress, Office of Technology Assessment, Issue Update on Information Security and Privacy in Network Environments, 71–72 (1995)

protect individuals' interests. Security can assure accuracy and integrity of personal information. At the same time, security can be used to accomplish limitations on the use and circulation of personal information on a network. These features are each critical for multimedia in a dynamic network environment and show that business and individual interests may be contiguous.

Technical standards, like those established by the International Standards Organization or the American National Standards Institute, for equipment, transmission and processing interoperability may also provide options for the treatment of personal information. As standard formats develop to facilitate the electronic exchange of information,[57] coding for the treatment of personal information becomes a logical corollary. Standards organizations can, for example, develop protocols to include permission codes along with transmissions of multimedia works. Already, electronic royalty clearing systems are emerging to allow calculations of copyright fees based on network usage.[58] These systems electronically tag digital works to identify owners and execute royalty payments. For the multimedia data stream, similar electronic tags can be created to preserve the participation and interests of individuals in sound and image. As an example, protocols may be developed to lock data after use or to assure only specific uses of image and sound.

Finally, technical standards may be used as a means to regulate the appropriate treatment of personal information. For example, the Canadian Standards Association has prepared a code for data privacy and is contemplating a proposal for audit certifications.[59] In today's financial marketplace, no major corporation would ever fathom doing business without regular financial audits. In tomorrow's Information Society, no multimedia enterprise will contemplate participation without information audits and fair treatment of personal information.

IV. Conclusion

Multimedia presents significant challenges to privacy. Digitalization expands the scope of activities that involve the computerized treatment of information about individuals. In blurring boundaries, multimedia merges intellectual property, traditional privacy, and established fair information practice norms together. Sorting out the appropriate treatment for the multimedia data stream calls for new models and tools.

The complexity and overlapping nature of privacy protections in the context of the multimedia data stream provides opportunities for customized rules for the treatment of personal information. Society has an interest in standardizing privacy features in network architecture. Technological options and developments should be regarded as valuable components of a system of standards for fair information practice in the multimedia arena. The elements of varied regimes for legal protection including intellectual property rights should be assembled to frame the treatment of sound and image as personal information.

As a high priority, the multimedia data stream requires institutionalized vigilance. Society has an enormous stake in the manner in which multimedia products and services develop and the outcome of varied protections. Both the planning and implementation stages of multimedia products and services must consider the fair treatment of individuals. Yet, the challenges and opportunities of multimedia for all participants in society cannot be understood in an ad hoc fashion. Review of the treatment of sound and image as well as strategic analysis must be systemic in the Information Society. Satisfactory solutions will only come from careful, multifaceted and interdisciplinary thinking.

57 See Henry H. Perritt, Jr., Format and Content Standards for the Electronic Exchange of Legal Information, 33 Jurimetrics 265 (1993).
58 U.S. Congress Office of Technology Assessment, Information Security and Privacy in Network Environments, at 108–110 (1994).
59 See Colin Bennett, Implementing Privacy Codes of Conduct: A Report to the Canadian Standards Association (April, 1995).

Der Freiburger Kommunikationsassistent – Sicherheit in multimedialen Kommunikationsnetzen durch nutzerbezogene Dezentralisation –

Günter Müller, Frank Stoll
Universität Freiburg, Institut für Informatik und Gesellschaft, Abteilung Telematik

Abstract

In der Informationsgesellschaft von morgen werden verstärkt persönliche, multimediale Kommunikationsdienste mittels Mobilkommunikationssystemen nachgefragt werden. Dies erfordert zunehmend die Speicherung personenbezogener Daten in Teilnehmerprofilen und deren Übertragung über die Mobilfunknetze. Daher wird die Nutzung von Mobilkommunikationssystemen möglicherweise große Auswirkungen auf hochsensible Bereiche wie die Kommunikation von Teilnehmern, deren Bewegungen sowie deren Verhalten haben und das Recht auf informationelle Selbstbestimmung der Teilnehmer gefährden.

In diesem Papier wird gezeigt, daß eine nutzerbezogene Dezentralisation von Daten und bestimmten Netzfunktionen ermöglicht, einen höheren Grad an Persönlichkeitsschutz und informationeller Selbstbestimmung für die Mobilfunkteilnehmer zu erreichen als er derzeit realisiert ist. Hierzu wird eine alternative GSM-Netzinfrastruktur mit dem Freiburger Kommunikationsassistenten (FKA) als wesentlicher Komponente eingeführt. Der FKA ist einem Teilnehmer zugeordnet und steht unter dessen Kontrolle. Er bildet die organisatorische und funktionelle Schnittstelle zwischen dem Teilnehmer und dem Mobilkommunikationssystem. Der FKA speichert insbesondere personenbezogene und vermittlungstechnische Daten, die somit ausschließlich vom Mobilfunkteilnehmer kontrolliert werden. Allein der Mobilfunkteilnehmer entscheidet, inwieweit seine Daten gegenüber dem Mobilfunknetz offengelegt werden. Ein derartiger, dezentraler Gestaltungsansatz läßt sich auch allgemein auf multimediale Kommunikationsinfrastrukturen übertragen.

1 Einleitung

Ausgelöst durch die fortschreitende Deregulierung und Liberalisierung kristallisieren sich zwei maßgebliche Entwicklungslinien innerhalb des Telekommunikationsbereichs heraus: Multimedia und Mobilkommunikation.

Bei Multimedia handelt es sich um die gleichzeitige Übertragung von Sprache, Bildern, Texten und Daten über dieselbe Kommunikationsnetzinfrastruktur. In der Vision von der Informationsgesellschaft von morgen werden diese multimedialen Netzinfrastrukturen als „Nationale Informationsinfrastrukturen“ oder „Datenautobahnen“ bezeichnet. Vorläufer der Datenautobahnen ist das besonders in den USA – mittlerweile auch in Europa – in einem erheblichen Maße genutzte Internet. In den USA soll das Internet durch ein großflächiges Angebot an neuartigen Diensten, beispielsweise Tele-Shopping und öffentliche Bibliotheksdienste, weiterentwickelt werden. Unter dem Begriff „informationelle Grundversorgung“ wird ein kostenloser Zugriff für Bürger auf Informationen, die für das öffentliche Leben wichtig sind, diskutiert. Ferner werden Feldversuche auf der Basis breitbandiger Kommunikationsnetzinfrastrukturen zur Übertragung von interaktivem Fernsehen, beispielsweise in Orlando, Florida, durchgeführt (Wilson 1995).

In Europa wird für die Bereitstellung multimedialer Dienste wegen den daraus resultierenden hohen Anforderungen an Übertragungskapazitäten die Schaffung einer breitbandigen Kommunikationsnetzinfrastruktur diskutiert. Die wesentlichen Bausteine sollen dabei das diensteintegrierende digitale Netz ISDN (Integrated Services Digital Network), Breitbandkommunikationsnetze auf der Basis von ATM (Asynchronous Transfer Mode) als Vermittlungstechnik, die Mobil- und Satellitenkommunikation sowie bestehende Kabel-TV-Netze darstellen (Bangemann 1994; Armbrüster 1995 a). In der Informationsgesellschaft von morgen sollen alle Privathaushalte an multimediale Kommunikationsnetzinfrastrukturen angeschlossen sein, um vielfältigste multimediale Dienste nutzen zu können. Diese Dienste lassen unterschiedliche Industriesektoren wie die Unterhaltungs-, die Telekommunikations-, die Computer- und Informationsindustrie sowie den Handel verschmelzen. Die Brandbreite der sich abzeichnenden multimedialen Dienste reicht von Videokonferenzdiensten, der Bildkommunikation, Datenbankdiensten, elektronischer Post, Video-on-Demand, interaktivem Fernsehen, elektronischer Stimmabgabe bis hin zu Tele-Banking und Tele-Shopping. Viele dieser Dienste werden derzeit in Feldversuchen auch im Hinblick auf die zu nutzende Vermittlungs- und Teilnehmeranschlußtechnik erprobt (Gabel 1995 a; Armbrüster 1995 b; Hechler 1995). Bild 1 zeigt exemplarisch den Informationsraum bei Multimedia.

Bild 1. Der Informationsraum bei Multimedia.

Noch rasanter als die derzeitigen Multimedia-Visionen hat sich seit Anfang der 90er Jahre die Mobilkommunikation entwickelt. Die zweite Systemgeneration in Form digitaler zellularer Mobilfunknetze auf der Basis des europäischen Standards GSM (Global System for Mobile Communications) (ETSI 1993; Mouly/Pautet 1992) hat eine stetig wachsende Nachfrage nach Mobilkommunikationsdiensten hervorgerufen. Mit verbesserten Mobilfunktechnologien sowie einem weiteren, deutlichen Preisverfall bei Mobilfunkendgeräten und angebotenen Diensten wird sich die Mobilkommunikation zu einem Massenmarkt entwickeln. Für die Europäische Union werden 40 Millionen Mobilfunkteilnehmer im Jahr 2000 und 80 Millionen bis zum Jahr 2010 prognostiziert (EU_145 1994). In einem Massenmarkt werden vermehrt persönliche Kommunikationsdienste nachgefragt werden. Persönlich bedeutet hierbei (Dupuis 1995): zu jeder Zeit, an jedem Ort und abhängig von einer selbstgewählten Rolle als Kommunikationspartner ist ein Teilnehmer in der Lage, mittels eines kleinen, leichten Taschentelefons Gespräche zu empfangen, zu initiieren sowie angebotene Kommunikationsdienste zu nutzen.

Mobilkommunikationsnetze auf der Basis des GSM-Standards als auch auf dessen Weiterentwicklung, dem DCS (Digital Cellular System) 1800 Standard, in Form von Personal Communications Networks (PCNs) (Lobensommer 1994) werden den Anforderungen eines Massenmarktes und persönlicher, multimedialer Kommunikationsdienste nur zum Teil gerecht. Sie erlauben nur geringe Teilnehmer- und Übertragungskapazitäten und können unterschiedlichste Funkräume nur kostenineffizient abdecken (Callendar 1994; Norp/Roovers 1994). Weltweit wird daher an Mobilkommunikationssystemen der nächsten – dritten – Generation geforscht, deren Konzepte auf denen der zweiten Generation wie GSM aufbauen sollen (Dupuis 1995). Projekte umfassen das europäische Universal Mobile Telecommunications System (UMTS) (Rapeli 1995) und das von der ITU (International Telecommunication Union) initiierte Future Public Land Mobile Telecommunication System (FPLMTS) (Callendar 1994). Bild 2 skizziert die Entwicklungsstufen von Mobilkommunikationssystemen.

Bild 2: Entwicklungsstufen von Mobilkommunikationssystemen; in Anlehnung an (Schwarz DaSilva/Fernandes 1995).

Multimedia- und Mobilkommunikationsdienste werden auf längere Sicht hin konvergieren. Hierfür gibt es mehrere Gründe:

- Ab der dritten Generation werden Mobilfunknetze die gleichen Dienste in der gleichen Qualität wie bei breitbandigen Festnetzen verfügbar machen. Daher können auch multimediale Dienste zukünftig in Mobilfunknetzen genutzt werden (Cheung et al. 1994; Fernandes 1995; Chia 1992).
- Zukünftig wird der größte Teil des Telekommunikationsverkehrs über mobile Endgeräte abgewickelt werden (Rapeli 1995).
- Prognosen schätzen den Marktdurchdringungsgrad individueller Mobilkommunikation langfristig auf etwa 80 % der Gesamtbevölkerung in Europa, wohingegen Festnetzanschlüsse durchschnittlich nur etwa 50 % erreichen werden (EU_145 1994).

Darüber hinaus erfordern multimediale Dienste als auch allgemein persönliche Mobilkommunikationsdienste aufgrund ihres individuellen Zuschnitts in einem verstärkten Maß die Übertragung personenbezogener Daten über die Kommunikationsnetze. Daher ist mit einem Anwachsen personenbezogener Verbindungs- und Inhaltsdaten (Nutzdaten), die in Mobilkommunikations- und Multimedianetzen gespeichert und zunehmend zwischen Teilnehmern, Diensteanbietern und Mobilfunknetzbetreibern ausgetauscht werden müssen, zu rechnen (Jabbari et al. 1995). Bei UMTS ist sogar geplant, teilnehmerbezogene Informationen in Benutzerprofilen, sogenannten UMTS User Profiles, netzseitig zu speichern (Eleftheriadis/Theologou 1994). In diesen Benutzerprofilen ist verzeichnet, in welchen Gebieten und unter welchen Bedingungen ein bestimmter Dienst für einen Teilnehmer verfügbar ist. Darüberhinaus werden teilnehmerspezifische Authentifizierungs- und Abrechnungsdaten gespeichert.

Die wachsende Anhäufung personenbezogener Daten bei der Nutzung multimediafähiger Mobilkommunikationssysteme wird daher möglicherweise große Auswirkungen auf hochsensible Bereiche, wie beispielsweise die Kommunikation von Teilnehmern, deren Bewegungen und deren Verhalten, haben. Damit ist der Persönlichkeitsschutz sowie das Recht auf informationelle Selbstbestimmung[1] der Teilnehmer potentiell gefährdet. Dies trifft insbesondere deshalb zu, da bereits der GSM-Standard in bezug auf die Behandlung personenbezogener Daten und das realisierte Sicherheitsniveau erhebliche Defizite aufweist (Stoll 1995; Cooke/Brewster 1992; Rueppel/Massey 1992).

Der Bangemann-Bericht „Europa und die globale Informationsgesellschaft“ nennt als einen der wesentlichen Punkte den Schutz der Privatsphäre und stellt fest (Bangemann 1994): „Die Anforderungen an den Datenschutz werden in dem Maße zunehmen, wie das Potential der neuen Technologien (auch grenzüberschreitend), detaillierte Informationen über Privatpersonen aus Daten, Sprache und Bildquellen zu gewinnen und zu manipulieren, genutzt wird.“ Die schnelle Verabschiedung entsprechender Richtlinienvorschläge zum Datenschutz wird angemahnt, da nur durch die Existenz eines rechtlichen, unionsweiten Konzepts und damit eines glaubhaften Schutzes der Privatsphäre die Teilnehmerakzeptanz und das Vertrauen in die der Informationsgesellschaft zugrundeliegenden Technologien gestärkt werden kann.

Im Februar 1995 wurde bereits ein gemeinsamer Standpunkt zur Rahmenrichtlinie zum Schutz personenbezogener Daten vom Rat der Europäischen Union festgeschrieben (DuD 1995 a). Diese allgemeine Datenschutzrichtlinie wurde Ende Juli 1995 mit geringen Änderungen durch das Europäische Parlament vom Rat der Europäischen Union angenommen (DuD 1995 b). Damit existiert ein Mindestmaß für den Schutz der Privatsphäre

1 BVerfGE 65, 1 ff.

in der EU. Auch wird der Transfer personenbezogener Daten in Staaten außerhalb der EU, deren Datenschutz nicht dem EU-Datenschutzstandard genügt, erheblich erschwert. Hier wird allerdings die zunehmende globale Vernetzung eine effiziente Kontrolle verhindern. Spezielle auf die Telekommunikation bezogene Regelungen sind nicht in der Richtlinie enthalten – dafür hat die Europäische Kommission bereits eine sektorielle Richtlinie zum Datenschutz bei ISDN und Mobilkommunikationsnetzen vorgelegt (EU_128 1994). Aber angesichts weiter bestehender Defizite, beispielsweise fehlt in der Richtlinie ein explizites Verbot, personenbezogene Daten zur Erstellung elektronischer Profile zu nutzen, ist ein rechtlicher Regelungsbedarf weiterhin notwendig (DuD 1994). Darüber hinaus muß die Richtlinie an die von der EU-Kommission angestrebte vollständige Liberalisierung der Telekommunikationsinfrastrukturen angepaßt werden, da sie noch von besonderen Rechten für den Betrieb von Telekommunikationssystemen in den EU-Mitgliedsstaaten ausgeht.

Es ist überhaupt sehr fraglich, ob rechtliche Rahmenbedingungen neben dem Datenschutz auch für die Informationssicherheit, den Urheberschutz und das Wettbewerbsrecht, die angesichts fortschreitender Technologien und globaler Kommunikationsinfrastrukturen nicht vollständig überprüfbar sind, den Anforderungen der Informationsgesellschaft von morgen genügen können. Multimediale Technologien und Anwendungen entwickeln sich derart schnell, daß der Benutzer in bezug auf seine Datenschutzrechte noch nicht berücksichtigt wird. Außerdem verlaufen gegenwärtig viele technologische Entwicklungen derart, daß zuerst eine betriebsfähige Systemversion zur (vorläufigen) Standardisierung kommt. Erst danach wird über notwendige Sicherheitsanforderungen und die damit verbundenen Probleme, beispielsweise Integration und Komplexität, nachgedacht. Die Entwicklung der für Multimedia wohl grundlegenden Übertragungstechnik ATM ist dafür ein Beispiel (Rendleman/Sweeny 1995). Ferner ist auch im Zuge der EU-Datenschutzrichtlinien erkennbar, daß deren Verabschiedung teilweise sehr lange braucht, manchmal erheblich länger als die Standardisierung von technischen Systemen.

In diesem Papier wird daher ein technischer Gestaltungsansatz (Müller/Stoll 1995) vorgestellt, der durch eine teilnehmerbezogene Dezentralisierung von Daten und bestimmten Funktionen ermöglicht, einen höheren Grad an Persönlichkeitsschutz und informationeller Selbstbestimmung für die Teilnehmer in Mobilfunknetzen zu erreichen. Dazu wird eine alternative GSM-Mobilfunknetzinfrastruktur eingeführt, deren wesentliche Komponente der Freiburger Kommunikationsassistent (FKA) ist. In Form eines persönlichen digitalen Assistenten ist der FKA einem Mobilfunkteilnehmer zugeordnet und steht unter dessen Kontrolle. Der FKA bildet die organisatorische und funktionelle Schnittstelle zwischen dem Teilnehmer und dem Mobilkommunikationsnetz. Das hier vorgestellte Konzept läßt sich auch allgemein auf multimediale Kommunikationsnetzinfrastrukturen übertragen. Es kann daher Denkanstöße und Ideen liefern, wie sich der Persönlichkeitsschutz und das Recht auf informationelle Selbstbestimmung technisch in Multimedia-Systeme integrieren läßt.

2 Der Freiburger Kommunikationsassistent

Die Idee, die herkömmliche GSM-Netzinfrastruktur zu verändern, wird durch drei Annahmen motiviert (Stoll 1995):

- Die zunehmende Komplexität und das Anwachsen der Datenvolumen in Mobilfunknetzen wird Netzbetreiber und Diensteanbietern zwingen, datensparsame Netzstrukturen zu nutzen. Dies führt zu einer höheren Dezentralisierung von Daten und Netzfunktionen (Grillo et al. 1993; Norp/Roovers 1994); insbesondere müssen Teilnehmer ihre personenbezogenen Daten verwalten.

- Eine mögliche Gefährdung des Persönlichkeitsschutzes und des Rechts auf informationelle Selbstbestimmung kommunizierender Teilnehmer ist nicht auszuschließen, da GSM-Mobilfunknetze auf einem zentralistischen Funktionskonzept beruhen. Vordergründig vertrauenswürdige aber für den Teilnehmer fremde Netzdatenbanken – Heimatregister (HLR, Home Location Register), Besucherregister (VLR, Visitor Location Register) und Authentifizierungszentrum (AC, Authentication Centre) speichern beispielsweise Teilnehmer- und Ortskenndaten zur Mobilitätsunterstützung umherwandernder Teilnehmer sowie Parameter zur Teilnehmerauthentifizierung, die gleichsam mit den Teilnehmern über ungeschützte Kommunikationsverbindungen durch das Mobilfunknetz wandern (Molva et al. 1994). Hinzu kommt, daß in den Vermittlungsstellen (Mobile Switching Centres, MSCs) während eines multimedialen Kommunikationsvorgangs eine Vielzahl an Nutz- und Verbindungsdaten (GSM TS 12.05)[2] zu Abrechnungszwecken gesammelt, gespeichert und zu Dienst- und Anrufdatensätzen zusammengestellt wird. Damit ist potentiell die Möglichkeit gegeben, Bewegungs- und Kommunikationsprofile aufzustellen (Bathe-Peters 1993). Die Teilnehmer müssen sich darauf verlassen, daß bestimmte persönliche Daten durch den Netzbetreiber ausgewählt und entsprechend seinem Anforderungsniveau geheimgehalten werden. Dies führt dazu, daß die Privatsphäre des Teilnehmers gegenüber dem Netzbetreiber nicht ausreichend geschützt ist (Rueppel/Massey 1992).

- Das gegenwärtig realisierte Sicherheitsniveau in GSM (GSM TS 02.09, GSM TS 03.20) erweist sich als ein Resultat des Abwägens zwischen einerseits der Bereitstellung angemessener Sicherheitsmaßnahmen, der damit verbundenen Kosten und Systemkomplexität, und andererseits der angenommenen geringen Auswirkungen auf die Gesellschaft bei einer weitverbreiteten Nutzung von GSM – sofern derartige Sicherheitsmaßnahmen teilweise fehlen (Mouly/Pautet 1992). Letzteres resultierte sicherlich von dem geringeren gesellschaftlichen Bewußtsein der Notwendigkeit eines garantierten Persönlichkeitsschutzes, als GSM Mitte der 80er Jahre spezifiziert wurde. Insgesamt fehlen geeignete Sicherheitsmaßnahmen (Cooke/Brewster 1992; Molva et al. 1994). Heutige Forderungen nach mehrseitiger Sicherheit (Rannenberg 1994) können ebenso nicht erfüllt werden.

Dezentralen, in bezug auf personenbezogene Daten sparsamen Netzkonzepten, verbesserten Sicherheitsstrategien und einem gewachsenen Bedürfnis an Persönlichkeitsschutz kann in einem Ansatz Rechnung getragen werden, bei dem der Teilnehmer personen- und sicherheitsbezogene Daten dezentral unter seiner Kontrolle verantwortet. Ansatzpunkte des hier beschriebenen technischen Gestaltungskonzepts sind dabei die GSM-Netzdatenbanken (Stoll 1994).

In einer alternativen GSM-Netzinfrastruktur werden die Netzdatenbanken durch einen teilnehmerbezogenen, persönlichen digitalen Assistenten, den Freiburger Kommunikationsassistenten (FKA), ersetzt (Bild 3). Der FKA-Ansatz zielt darauf ab,

- die Menge an personenbezogenen Daten im Mobilfunknetz durch eine nutzerbezogene Dezentralisierung zu reduzieren sowie

- den Persönlichkeitsschutz und das Recht auf informationelle Selbstbestimmung von Mobilfunkteilehmern zu gewährleisten.

2 GSM TS xx.yy: GSM Technical Specification <Serie>. <laufende Nummer> (ETSI 1993; Mouly/Pautet 1992).

Bild 3: a) Herkömmliche GSM-Netzinfrastruktur.
b) Alternative GSM-Infrastruktur mit nur einer Netzdatenbank und FKA (für Teilnehmer T).

Der FKA übernimmt im wesentlichen die auf den jeweiligen Teilnehmer bezogenen Datenspeicherungsaufgaben der Netzdatenbanken. GSM-Netzfunktionen, beispielsweise die Teilnehmerauthentifizierung, gehen in diesem Fall auf die Vermittlungsstellen über. Aus Gründen der Netzleistungsfähigkeit muß daher eine einzige Netzdatenbank erhalten bleiben. Sie übernimmt spezielle Netzfunktionen und entlastet so das MSC. Diese einzige an einem MSC angeschlossene Netzdatenbank weist allerdings eine erheblich veränderte Datenbasis auf – personenbezogene Daten sind darin nicht mehr enthalten.

Verschiedene Arbeiten haben sich bereits mit dem teilnehmerüberprüfbaren Schutz von Nutz- und Verkehrsdaten in Form sogenannter Funk-Mixe (Pfitzmann 1993), einer Kombination aus Ende-zu-Ende-Verschlüsselung, Verbindungsverschlüsselung, ortsfesten umcodierenden Mixen und der Verteilung gefilterter Verbindungswünsche, und der Dezentralisierung von Aufenthalts- und Erreichbarkeitsinformation in Mobilfunknetzen (Hetschold 1993) beschäftigt. Bei beiden Arbeiten wurde weitgehend die derzeitige GSM-Netzinfrastruktur beibehalten. Die Arbeiten zeigten, daß es möglich ist, Aufenthaltsinformationen eines Teilnehmers lokal zu speichern, indem ein ortsfestes Terminal, vorzugsweise am Wohnort des Teilnehmers, eingeführt wird, und dabei gleichzeitig die GSM-Funktionalität aufrechtzuerhalten. Offene Fragen betreffen die Bereitstellung der Aufenthaltsinformation des Teilnehmers für das Mobilfunknetz und Authentifizierungsverfahren. Diese Probleme werden im FKA-Ansatz besonders berücksichtigt.

Alle diese Ansätze sind aufgrund der notwendigen dienst- und teilnehmerbezogenen dezentralen Sicherheitsmaßnahmen kostspieliger und komplexer im Gegensatz zum gegenwärtigen zentralistischen GSM-Schema – erreichen aber, daß Teilnehmer Mobilfunknetzen mehr Vertrauen schenken.

Der FKA ist als ein persönlicher digitaler Assistent – vergleichbar mit Newton von Apple oder dem Magic Link Personal Intelligent Communicator (Gabel 1995 b) – konzipiert. Er ist einem Teilnehmer als Ergänzung seiner GSM-Freischaltung zugeordnet. Aus Teilnehmersicht ist der FKA vertrauenswürdig und kann nicht durch Dritte manipuliert werden, was durch kryptographische Verfahren, sichere Hard- und Software sowie Plausibilitätskontrollen erreicht wird. Da der FKA Aufgaben übernimmt, die zuvor den Netzdatenbanken HLR, VLR und AC zugeordnet waren, muß er in die GSM zugrundeliegende Struktur eines Intelligenten Netzes eingebunden werden. Um Nutz-, Verkehrs- und Signalisierungsdaten austauschen zu können, muß der FKA des ITU-T Zeichengabesystem Nummer 7, den Anwendungsteil für Mobilfunk MAP (Mobile Application Part) (GSM TS 09.02) und den Kurznachrichtendienst SMS (Short Message Service) (GSM TS 03.40) unterstützen.

Der gegenwärtige Ansatz sieht vor, daß der FKA am Wohnort des Teilnehmers lokalisiert ist und dort an das öffentliche Telefonnetz (Public Switched Telephone Network, PSTN) angeschlossen ist. Es ist ebenso vorstellbar, daß mehrere FKAs aus ökonomischen Gründen an einem Ort konzentriert werden oder daß ein FKA von mehreren Teilnehmern gleichzeitig genutzt wird, beispielsweise innerhalb von Familien („Familien-FKA“). Mit der Einführung von Universal Personal Telecommunications (UPT) Diensten (Lauer 1994), die Teilnehmern im Festnetz eine diskrete, räumlich begrenzte Mobilität ermöglichen, könnte der FKA beweglich sein und damit an beliebigen Orten lokalisiert werden. Die Wahl einer festen Heimatstation erlaubt, die in Festnetzen existierende traditionelle Ortsbezogenheit des Telefonierens wieder einzuführen, wobei aber gleichzeitig modernes personenbezogenes Telefonieren sowie die Mobilitätsunterstützung der Teilnehmer aufrechterhalten bleiben.

Weiterhin wird auch eine weitgehende Trennung persönlicher Teilnehmerdaten von denjenigen Daten erreicht, die das Kommunikationsnetz für einen normalen Betrieb benötigt. Somit wird verhindert, daß Dritte detaillierte Datenspuren eines Teilnehmers aufzeichnen können. Lediglich der FKA ist Dritten gegenüber explizit bekannt, wobei die Zuordnung FKA zu Teilnehmer für Dritte nicht nachvollziebar sein darf.

Ein ähnliches Trennungsprinzip in Form eines Gebührensplittings findet bereits im herkömmlichen GSM bei der Entgeltabrechnung im Falle eines im Mobilfunknetz endenden Rufes (Mobile Terminated Call, MTC) statt (Mouly/Pautet 1992). Der rufende Teilnehmer zahlt jeweils das Entgelt für die Verbindung zum Heimatbereich des gerufenen (mobilen) Teilnehmers. Der gerufene Teilnehmer seinerseits zahlt nur dann ebenfalls ein Entgelt, sofern er sich außerhalb seines Heimatbereichs befindet. Damit läßt sich zum einen erreichen, daß der rufende Teilnehmer die Gebühren für seinen Anruf unabhängig vom wirklichen Aufenthaltsort des gerufenen Teilnehmers stets im voraus abschätzen kann, zum anderen soll verhindert werden, daß der Anrufer weiß, daß sich der Angerufene außerhalb seines Heimatbereichs aufhält, wenn er den Ruf entgegennimmt. Damit läßt sich der Aufenthaltsort des gerufenen Teilnehmers vor dem Anrufer verbergen.

Der FKA speichert personenbezogene Daten und Verbindungsdaten, die seinem Teilnehmer zugesordnet sind (GSM TS 03.08, GSM TS 12.05) (ETSI 1993). Darunter befinden sich beispielsweise: der öffentliche Teilnehmerschlüssel; eine Diensteselektionsliste für das Erreichbarkeitsmanagement, zu dessen Zweck eingehende Dienste entsprechend

dem Teilnehmerwunsch gefiltert und gegebenenfalls blockiert werden; eine Diensteausführungsliste, die anzeigt, welche Dienste die mobile Station des Teilnehmers ausführen kann. Weiterhin speichert der FKA Daten, die seine eigene Funktionalität unterstützen, beispielsweise seinen privaten Schlüssel. Zukünftig, sofern der FKA bei Systemen der dritten Mobilfunknetzgeneration eingesetzt wird, verwaltet er auch das Benuterprofil seines Teilnehmers. Der FKA sieht für die Entgeltabrechnung einer Dienstenutzung die Funktionalität einer elektronischen Geldbörse vor. Ferner generiert er Schlüsselpaare, private und öffentliche Schlüssel, auf Basis eines RSA-Schemas (Rivest 1978) für seine eigenen und die Zwecke des ihm zugeordneten Teilnehmers. Die Schlüssel werden bei der Datenverschlüsselung und beim asymmetrischen Authentifizierungsverfahren benützt. Die öffentlichen Schlüssel werden bei einer vertrauenswürdigen Schlüsselverwaltung (VSV) registriert – wie später noch weiter ausgeführt wird.

Daten, die ein Teilnehmer für die Diensteabwicklung über das Mobilfunknetz benötigt, werden auf dem Teilnehmeridentifikationsmodul SIM (Subscriber Identity Module) (GSM TS 11.11) gespeichert. Dies sind insbesondere der private Teilnehmerschlüssel, Quittungen für die Entgeltabrechnung sowie Verfahren für die Generierung sitzungsspezifischer Datenschlüssel und Identitäten, die eine anonyme oder pseudonyme Dienstenutzung zulassen. Die oben erwähnte Generierung von Schlüsselpaaren könnte alternativ auch auf dem SIM durchgeführt werden. Dann müßte der private FKA-Schlüssel noch in den sicheren Speicherbereich des FKA übertragen werden.

Der FKA bildet die organisatorische und funktionelle Schnittstelle zwischen dem Teilnehmer, dem er zugeordnet ist, und dem Mobilfunknetz. Vom Teilnehmer initiierte Dienste werden alle zunächst über den FKA geleitet. Sofern eine Dienstesignalisierung für einen Teilnehmer im Mobilfunknetz vorliegt, wendet sich das Netz an den zugeordneten, aus der Rufnummer ersichtlichen FKA. Dieser übermittelt dem Mobilfunknetz den Aufenthaltsort des betreffenden Teilnehmers – sofern der Teilnehmer derzeit diesen Dienst annehmen möchte. Der Gütegrad der Aufenthaltsinformation wurde zuvor durch den Teilnehmer bestimmt und an den FKA übertragen. Damit liegt es an einem Teilnehmer, inwieweit er seine Daten gegenüber dem Mobilfunknetz offenlegen möchte. Somit läßt sich ein gradueller Schutz der Aufenthaltsinformation des Teilnehmers und seiner Bewegungen abhängig vom situativen Kontext erreichen. Selbst wenn der Teilnehmer letztendlich eine Dienstesignalierung durch das Mobilfunknetz nicht akzeptiert, ist er immer noch in der Lage, seinen Aufenthaltsort bis zu dem von ihm spezifizierten Grad geheimzuhalten. Unterschiedliche Dienstesignalisierungen im mobilen Endgerät können dabei den Teilnehmer auf die Dringlichkeit eines Dienstes hinweisen. Ein Teilnehmer nimmt grundsätzlich nur Dienstesignalisierungen an, die zuvor von dem ihm zugeordneten FKA überprüft wurden, ansonsten wäre es aus Netzsicht möglich, mit fingierten Dienstesignalisierungen den momentanen Aufenthaltsort eines Teilnehmers herauszubekommen. Daten für die Entgeltabrechnung laufen grundsätzlich beim FKA auf, Inhaltsdaten werden bis zum Teilnehmer durchgestellt. Die Vertraulichkeit der Kommunikation ließe sich beispielsweise durch eine geeignete Ende-zu-Ende-Verschlüsselungsvereinbarung zwischen rufendem Teilnehmer und dem FKA des gerufenen Teilnehmers erreichen. Bei Annahme des Kommunikationswunsches durch den gerufenen Teilnehmer wird die Verschlüsselungsvereinbarung weiter zum mobilen Teilnehmer durchgereicht oder ein neuer Schlüssel wird vereinbart.

Es ist in diesem Zusammenhang auch wichtig anzumerken, daß die mobilen Endgeräte von Teilnehmern grundsätzlich lokalisierbar sind, wenn sie senden. Der Einsatz von Spreizbandverfahren in Verbindung mit einer Definition vertrauenswürdiger Kommunikationsbereiche (Thees/Federrath 1995), in denen jede Übertragung durch einen Spreizcode geschützt wird, erscheint geeignet, die Lokalisierung von sendenden Teilnehmern durch Dritte zu verhindern. Ein derartiges Verfahren ließe sich auch in den FKA-Ansatz integrieren.

Die Funktion des FKA und weitere Daten, die hierzu gespeichert werden müssen, sollen kurz in folgenden drei Bereichen erläutert werden: Authentifizierung und Datenverschlüsselung, Ortsregistrierung sowie im Mobilfunknetz endende Kommunikationsdienste.

2.1 Authentifizierung und Datenverschlüsselung

Hier wird vorausgesetzt, daß eine Infrastruktur zur Verwaltung öffentlicher Schlüssel verfügbar ist. Deren Existenz kann mit dem Aufkommen globaler Datenautobahnen und einem damit einhergehenden Anwachsen des telekooperativen, elektronischen Handels mittels multimedialer Dienste motiviert werden (Chokhani 1994). Um die Integrität öffentlicher Schlüssel sowie die Zuordnungsintegrität von Schlüssel zu Teilnehmer sicherzustellen, werden vertrauenswürdige Schlüsselverwaltungen (VSVs) benötigt, die öffentliche Benutzerschlüssel registrieren, verteilen und Zertifikate für die registrierten Schlüssel auf Anfrage ausgeben. Letzteres erfordert auch, daß es mehrere VSVs geben muß, um einem Benutzer zu ermöglichen, eine oder mehrere ihm vertrauenswürdig erscheinende VSVs auszuwählen. Mit der Einführung einer VSV-Infrastruktur erscheint es sinnvoll, asymmetrische Authentifizierungsverfahren bei Mobilkommunikationssystemen einzusetzen. Dezentralisierte VSVs wie auch die verteilte Registrierung öffentlicher (Teilnehmer-)Schlüssel unterstützen die Anwendung asymmetrischer Authentifizierungsverfahren in Mobilfunknetzen, insbesondere wenn sich Teilnehmer außerhalb ihres Heimatbereichs aufhalten.

Das FKA-Konzept nutzt ein asymmetrisches Authentifizierungsverfahren, um zu verhindern, daß teilnehmerbezogene, private Schlüssel in Komponenten des Mobilfunknetzes gespeichert werden müssen. Der Authentifizierung des FKA und des ihm zugeordneten Teilnehmers gegenüber dem Mobilfunknetz liegt die Nutzung eines RSA-Verfahrens zugrunde. Die hierzu notwendigen Schlüsselpaare werden vom FKA generiert. Der private Schlüssel des Teilnehmers ($priK_{MS}$)[3] muß dabei in einer sicheren Art und Weise auf das SIM des zugehörigen Teilnehmers übertragen werden. Die öffentlichen Schlüssel von FKA (puK_{FKA}) und Teilnehmer (puK_{MS}) müssen bei einer oder mehreren VSVs registriert werden. Alternativ wäre es möglich, Schlüsselpaare auf dem SIM zu generieren, und, sofern das SIM sich im FKA befindet, den privaten FKA-Schlüssel von dort in einen gesicherten FKA-Speicherbereich zu übertragen.

Sobald ein Dienstwunsch für einen Teilnehmer vorliegt, erhält der zugeordnete FKA eine Dienstesignalisierung. Da die Entgeltabrechnung vom FKA übernommen werden soll, authentifiziert sich der FKA mittels eines Challenge-Response-Verfahrens gegenüber dem Mobilfunknetz (Bild 4).

Dies wird genauso durchgeführt wie im gegenwärtigen GSM (GSM TS 03.20) (ETSI 1993), das heißt für eine vom Netz übertragene Zufallszahl *z* wird eine Signatur *Sig z* durch die Mobilstation berechnet. Das Mobilfunknetz kann gegebenenfalls das Zertifikat einer VSV für den öffentlichen FKA-Schlüssel verlangen. Der FKA berechnet einen spezifischen Datenschlüssel k_d für die aufzubauende Kommunikationsverbindung und wählt eine eigene temporäre Identität (Temporary Stationary Subscriber Identity, TSSI) aus. Die Signatur wird im Klartext, der Datenschlüssel, der öffentliche Teilnehmerschlüssel

3 puK_X/$priK_X$: öffentlicher/privater Schlüssel von X.

und die temporäre Identität werden mit dem öffentlichen Netzschlüssel verschlüsselt an das Mobilfunknetz übertragen.[4] Um einen häufigen Gebrauch öffentlicher Schlüssel zu vermeiden, werden anschließend alle Kommunikationsvorgänge zwischen FKA und Mobilfunknetz, so die Bereitstellung des Teilnehmeraufenthaltsorts, Entgeltabrechnungsdaten und temporäre FKA-Identitäten, mit dem sitzungsspezifischen Datenschlüssel verschlüsselt. Der dazu verwendete Verschlüsselungsalgorithmus wird zwischen Netz und FKA verhandelt. In einer entsprechenden Weise findet dieses Authentifizierungsverfahren auch zwischen dem Mobilfunknetz und der Mobilstation des Teilnehmers statt.

Bild 4: Asymmetrische Authentifizierung und Datenverschlüsselung (Synopse der Aktionen zwischen Mobilfunknetz und FKA).

Der Vorteil der asymmetrischen Authentifizierung ist, daß keine teilnehmerbezogenen Schlüssel und andere im voraus berechneten Authentifizierungsparameter im Mobilfunknetz gespeichert werden müssen. Dies vereinfacht gleichfalls die Generierung der sicherheitsrelevanten teilnehmerbezogenen Schlüssel, da diese anschließend nicht gleichzeitig an unterschiedlichen Stellen vorgehalten werden müssen – wie gegenwärtig bei GSM der persönliche Teilnehmerschlüssel k_i auf dem SIM und im AC. Das RSA-Verfahren ist jedoch aufwendiger und komplexer. Zu untersuchen ist noch, inwieweit die

4 $puK_X/priK_X(N)$ bedeutet: die Nachricht N wird mit dem öffentlichen/privaten Schlüssel von X verschlüsselt.

vorgegebenen Berechnungszeiten für eine RSA-Entschlüsselung eingehalten werden können, was letztendlich von den verwendeten Schlüssellängen und damit vom garantierten Sicherheitsmaß abhängt. Hier fällt auch der Schlüsseldynamik eine wesentliche Bedeutung zu. Wegen der Zeitbedingungen muß eine Kommunikationsverbindung unter Vorbehalt aufgebaut und sofort abgebrochen werden, sobald sich die Authentifizierung Beteiligter als falsch herausstellt.

2.2 Aufenthaltsregistrierung

Damit nicht mehr vollständige Bewegungsprofile von Teilnehmern erstellt werden können, speichert der FKA die Aufenthaltsinformation des ihm zugeordneten Teilnehmers. Dies wirft die Frage auf, wie der Teilnehmer seinen eigenen Aufenthaltsort bestimmt. Er muß die globale Funkzellenkennung (cell global identity, CGI) in Erfahrung bringen, die sich aus der Aufenthaltsgebietskennung (location area identity, LAI) und der Zellenkennung (cell identity, CI) zusammensetzt.

Diese Daten – in Bild 5 mit LOC-Info (Location Information) bezeichnet – werden gegenwärtig über einen Verteilkanal, den Broadcast Control Channel (BCCH), zum Zweck der Funkzellenauswahl übertragen und vom mobilen Endgerät des Teilnehmers passiv empfangen. Der Teilnehmer kann damit eine Nachricht (Short Message, SM) zusammenstellen, die seinen Aufenthaltsort (Location, LOC) enthält. Die Güte dieser Ortsinformation hängt jedoch davon ab, inwieweit ein Teilnehmner seinen exakten Aufenthaltsort für spätere Dienstesignalisierungen offenbaren möchte. Die Ortsinformation kann dabei auf der Basis des Funkabdeckungsgebiets einer einzelnen Zelle, einer Basisstation oder eines MSC in Abhängigkeit eines Zeitraums, des Ortes oder der jeweiligen Teilnehmerrolle bestimmt werden. Damit läßt sich ein gradueller, situativer Schutz des Aufenthaltsortes und der Bewegung des Teilnehmers erreichen. Selbst wenn der FKA dem Mobilfunknetz den Aufenthaltsort seines Teilnehmers mitgeteilt hat und dieser Teilnehmer letztendlich den signalisierten Dienst nicht entgegennehmen möchte, bleibt der exakte Aufenthaltsort des Teilnehmers dem Mobilfunknetz gegenüber verborgen – vorausgesetzt der Unschärfegrad der Ortsinformation war groß genug.

Die Aufenthaltsinformation des Teilnehmers wird mittels eines paketvermittelnden Dienstes an den FKA übertragen (Bild 5). Hierbei entstehen nur streckenweise Kommunikationsverbindungen. Durch ein Abhören bestimmter Übertragungsstrecken kann nicht auf die Zuordnung Teilnehmer zu FKA geschlossen werden. Der für GSM spezifizierte Kurznachrichtendienst SMS (short message service) (GSM TS 03.40) erscheint hier als ein geeigneter Übertragungsdienst (Hetschold 1993). Es können maximal 160 Zeichen in einer einzelnen Kurznachricht nach dem store-and-forward Prinzip übertragen werden. Der FKA muß hierzu die Funktionalität eines SMS Service Centers erhalten, um in der Lage zu sein, Kurznachrichten speichern, weiterleiten, entsprechende Fehlerreports verarbeiten und gegebenenfalls die Mobilstation auf fehlerhafte Übertragungen hinweisen zu können.

Sofern ein Teilnehmer seine Aufenthaltsinformation im FKA aktualisieren möchte, sendet er eine Kurznachricht an den FKA, die den in einer bestimmten Unschärfe spezifizierten Aufenthaltsort enthält. Der Nachrichteninhalt wird dabei mit dem öffentlichen Schlüssel des FKA (puK_{FKA}) verschlüsselt und enthält eine Teilnehmersignatur. Die Mobilstation muß nicht authentifiziert werden. Das Mobilfunknetz wickelt die Entgeltabrechnung über den FKA ab, sofern nicht eine pauschale Tarifierung wie gegenwärtig in GSM vorgesehen gewählt wird. Der FKA muß sich authentifizieren, bevor er die Nachricht vom Netz zugestellt bekommt. Er kann anhand der Teilnehmersignatur

($priK_{MS}[id_{MS}, id_{FKA}, LOC]$), die die Teilnehmer- und FKA-Identität[5] sowie den Aufenthaltsort enthält, überprüfen, ob sein Teilnehmer die Kurznachricht gesendet hat. Optional kann ein Zertifikat ($priK_{VSV}[id_{MS}, puK_{MS}]$) für den öffentlichen Teilnehmerschlüssel mitübertragen werden. Dadurch wird ausgeschlossen, daß der FKA für fremde, vorsätzlich an ihn gesendete Nachrichten ein Entgelt entrichten muß.

Bild 5: Ortsregistrierung (schematisch): Feststellung des Aufenthaltsortes und Übertragung der Information an den FKA.

Es gilt hier noch zu untersuchen, ob der Durchsatz an Kurznachrichten mit der Häufigkeit an Aufenthaltsregistrierungen durch die Teilnehmer in Einklang zu bringen ist, da Kurznachrichten relativ lange Laufzeiten haben können. Durch diesen Ansatz wird auch ein enormer Bedarf an Signalisierungskapazitäten sowohl in der Mobilstation wie auch im Mobilfunknetz generiert. Dies muß durch eine geeignete technische Systemgestaltung bewältigt werden. Offen ist auch noch die Behandlung von Fehlerreports und entsprechender Recovery-Prozeduren. Weiterhin sollte die Möglichkeit, Kurznachrichten sendende Teilnehmer lokalisieren zu können, verhindert werden.

Wegen der genannten Gründe erscheint es aber sinnvoll, zukünftig einen allgemeinen mobilen Datendienst anstelle des GSM-Kurznachrichtendienstes für die Übertragung von Teilnehmerortsinformationen in Betracht zu ziehen.

2.3 Ankommende Dienste im Mobilfunknetz

Sobald eine Dienstesignalisierung für einen Teilnehmer im Mobilfunknetz vorliegt, wird der zugeordnete FKA informiert (Bild 6). Der FKA prüft, ob sein Teilnehmer zu diesem Zeitpunkt, für diesen Dienst überhaupt erreichbar ist, und authentifiziert sich gegenüber dem Netz für eine spätere Nutzungsentgeltabrechnung, wenn der Teilnehmer den Dienst annimmt. Sofern der Teilnehmer erreichbar ist, überträgt der FKA die Aufenthaltsinformation (LOC_{MS}) sowie eine spezielle Nachricht zum Mobilfunknetz. Sie enthält die mit

5 Die Identitäten müssen nicht die richtigen Identitäten sein. Sie können anonym oder pseudonym sein.

Bild 6: Verbindungsherstellung (schematisch): LOC_{MS} enthält die Aufenthaltsinformation in der vom Teilnehmer spezifizierten Güte.

dem öffentlichen Teilnehmerschlüssel (puK_{MS}) verschlüsselte eigene Signatur, optional ein VSV-Zertifikat und eine spezielle Dienstesignalisierung (ServInd). Das Mobilfunknetz verteilt die Nachricht anschließend im spezifizierten Aufenthaltsgebiet.[6] Der betreffende Teilnehmer kann die Diensteanzeige mit seinem privaten Schlüssel entschlüsseln. Er erkennt, daß die Dienstesignalisierung von seinem FKA bearbeitet wurde, und kann selbst entscheiden, ob er den Dienst übernehmen möchte. Sofern er dies möchte, schaltet das Mobilfunknetz einen Nutzdatenkanal, auf dem nur die Inhaltsdaten übertragen werden, mittels der korrekten Wegeinformation vom FKA zum Teilnehmer durch.[7] Die Daten zur Entgeltabrechnung laufem beim FKA auf. Sinnvoll erscheint bei dieser Trennung, daß dem FKA durch das Netz eine Sitzungsidentifikationsnummer mitgeteilt wird, die dann auch an die mobile Teilnehmerstation weitergereicht wird. Nach der Beendigung des Dienstes kann damit ein Datensatz von der Mobilstation für den FKA zusammengestellt werden, der den Startzeitpunkt und das Ende des von der mobilen Station genutzten Dienstes enthält. Damit lassen sich Nutzungsentgeltabrechnungen, die der FKA für seinen Teilnehmer gegenüber dem Mobilfunknetz zu leisten hat, verifizieren.

6 Die Verteilung von Dienstesignalisierungen durch das Mobilfunknetz kann auch mit der Verteilung von Aufenthaltsinformationen (siehe Kapitel 2.2) für die mobilen Teilnehmer gekoppelt werden und umgekehrt. Die Reservierung eines festen Broadcast-Kanals erscheint hierfür am sinnvollsten zu sein.

7 Die Kommunikationsverbindung zwischen FKA und Teilnehmer läßt sich dann durch den Einsatz eines Spreizbandverfahrens schützen, um selbst bei einer bestehenden Verbindung noch den Aufenthaltsort des Teilnehmers zu schützen.

Problematisch ist hier der Datenüberhang im Mobilfunknetz, der durch die Verteilung der Diensteanzeigen in zum Teil großräumigen Gebieten und vor allem für viele Teilnehmer generiert wird. Außerdem wird die Belastung des mobilen Endgeräts größer, da sie ständig den für die Diensteanzeigen bestimmten Verteilkanal abhören, eingehende Datensignale überprüfen und Quittierungen für Entgelte übertragen muß.

3 Zusammenfassung

Der FKA-Ansatz vermittelt die Idee, wie durch eine nutzerbezogene Dezentralisierung personenbezogener Daten in Mobilkommunikationsnetzen ein verbesserter Persönlichkeitsschutz und das Recht auf informationelle Selbstbestimmung technisch realisiert werden können. Teilnehmerbezogene Daten werden unter der Kontrolle des Teilnehmers außerhalb des Mobilfunknetzes angesiedelt. Dieser allein kann damit entscheiden, inwieweit er seine Daten gegenüber dem Mobilfunknetz offenlegt. Damit ist ein abgestufter, situationsabhängiger Persönlichkeitsschutz realisierbar. Der Ansatz läßt sich relativ problemlos in bestehende Mobilfunknetz-Infrastrukturen integrieren, da er im wesentlichen Datenspeicherfunktionen der GSM-Netzdatenbanken an anderer Stelle allokiert, dabei aber lediglich fortgeschrittene Vermittlungs- und Verteilfunktionen benötigt. Gerade diese werden aber durch die Entwicklung mobiler Breitbandkommunikationssysteme (Fernandes 1995) zukünftig verfügbar sein. Damit wäre eine schrittweise Umgestaltung herkömmlicher GSM-Infrastrukturen in Richtung eines FKA-basierten Ansatzes möglich.

Darüber hinaus lassen sich Kriterien mehrseitiger Sicherheit wie anonyme und pseudonyme Kommunikation in diesem Ansatz realisieren. Das Kommunikationsnetz kann lediglich detaillierte Daten über den FKA sammeln, nicht jedoch über den zugehörigen Teilnehmer – sofern man natürlich die Möglichkeit zur Peilung, der ein sendender Teilnehmer unterliegt, vermindern kann. Die Trennung der teilnehmerbezogenen Datensphäre von derjenigen des Netzbetreibers bzw. Diensteanbieters ist wegweisend für die Gestaltung multimedialer Kommunikationsnetzinfrastrukturen, die derzeit noch stark zentral organisiert sind, und wird zunehmend wichtiger bei der Nutzung multimedialer Dienste.

Wichtige Bausteine, die zur Sicherheit in multimedialen Kommunikationsnetzen beitragen, sind: eine nutzerbezogene Datendezentralisation durch persönliche digitale Kommunikationsassistenten, die Einführung dezentraler Entgeltabrechnungsverfahren, insbesondere mittels elektronischen Geldes, asymmetrische Authentifizierungsverfahren und damit einhergehend der Aufbau von Infrastrukturen für die Verwaltung öffentlicher Schlüssel sowie die Nutzung von Ende-zu-Ende-Verschlüsselung.

Literatur

Armbrüster, H. (1995 a): Video- und Multimedia-Kommunikation über öffentliche Netze (Teil 1). ntz Nachrichtentechnische Zeitschrift, Bd. 48 (1995) Heft 4, S. 10–17

Armbrüster, H. (1995 b): Video- und Multimedia-Kommunikation über öffentliche Netze (Teil 2). ntz Nachrichtentechnische Zeitschrift, Bd. 48 (1995) Heft 5, S. 16–23

Bangemann, M. (1994): Europa und die globale Informationsgesellschaft. ntz Nachrichtentechnische Zeitschrift, Bd. 47 (1994) Heft 11, S. 806–813, und Heft 12, S. 884–890; Bd. 48 (1995) Heft 1, S. 38–41; englische Version via WWW: http://www.ispo.cec.be/infosoc/backg/bangemann.html

Bathe-Peters, B. (1993): Datenschutzprobleme und Lösungsansätze im Mobilfunk. In: Vorträge der ITG-Fachtagung Mobile Kommunikation vom 27. bis 29. September 1993 in Neu-Ulm, ITG-Fachbericht 124, Berlin, Offenbach: vde-verlag, 1993, S. 377–386

Callendar, M. H. (1994): Future Public Land Mobile Telecommunication Systems. IEEE Personal Communications, Vol. 1, No. 4, Fourth Quarter 1994, pp. 18–22

Cheung, J. C. S. et al. (1994): Network Planning for Third-Generation Mobile Radio Systems. IEEE Communications Magazine, Vol. 32, No. 11, November 1994, pp. 54–59

Chia, S. (1992): The Universal Mobile Telecommunication System. IEEE Communications Magazine, Vol. 30, No. 12, December 1992, pp. 54–62

Chokhani, S. (1994): Toward a National Public Key Infrastructure. IEEE Communications Magazine, Vol. 32, No. 9, September 1994, pp. 70–74

Cooke, J. C./Brewster, R. L. (1992): Cryptographic Security Techniques for Digital Mobile Telephones. IEE 2nd. International Conference on Private Switching Systems and Networks, London, UK, June 23–25, 1992, pp. 123–130

Dupuis, Ph. (1995): A European view on the Transition Path Toward Advanced Mobile Systems. IEEE Personal Communications, Vol. 2, No. 1, February 1995, pp. 60–63

DuD (1995 a): Datenschutzrichtlinie der EU. Gemeinsamer Standpunkt des Rates der Europäischen Union vom 20. 2. 1995 im Hinblick auf den Erlaß der Richtlinie zum Schutz natürlicher Personen bei der Verabeitung Personenbezogener Daten und zum freien Datenverkehr. Datenschutz und Datensicherheit (DuD) 4/95, April 1995, S. 215–223

DuD (1995 b): Datenschutzrichtlinie der EU – endgültig! Datenschutz und Datensicherheit (DuD) 8/95, August 1995, S. 483

DuD (1994): Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer 48. Sitzung (26./27. September 1994). Datenschutz und Datensicherheit (DuD) 12/94, Dezember 1994, S. 697–698

Eleftheriadis, G. P./Theologou, M. E. (1994): User Profile Identification in Future Mobile Telecommunications Systems. IEEE Network, Vol. 8, No. 5, September/October 1994, pp. 33–39

ETSI (1993): ETSI-GSM Technical Specifications Phase 1, Release List 1/1992 and Phase 2 Release List, ETSI Publication Office, Sophia Antipolis, Update July 1993

EU_128 (1994): Modified Proposal for a Directive of the European Parliament and the Council concerning the Protection of Personal Data and Privacy in the Context of Digital Telecommunications Networks, in particular the Integrated Services Digital Network (ISDN) and Digital Mobile Networks. Commission of the European Communities, Provisional Text COM (94) 128 final, April 1994

EU_145 (1994): Grünbuch über ein gemeinsames Konzept für Mobilkommunikation und Personal Communications in der Europäischen Union. Kommission der Europäischen Gemeinschaften, KOM (94) 145 endg., April 1994

Fernandes, L. (1995): Developing a System Concept and Technologies for Mobile Broadband Communications. IEEE Personal Communications, Vol. 2, No. 1, February 1995, pp. 54–60

Gabel, Jürgen (1995 a): Sieben Versuche mit interaktiven Videodiensten. ntz Nachrichtentechnische Zeitschrift, Bd. 48 (1995) Heft 4, S. 43–45

Gabel, Jürgen (1995 b): Telekom-Dienst PersonaLink in den USA gestartet. ntz Nachrichtentechnische Zeitschrift, Bd. 48 (1995) Heft 3, S. 26–29

Grillo, D. et al. (1993): Towards third generation mobile systems: a European possible transition path. Computer Networks and ISDN Systems, Vol. 25, No. 8, March 1993, pp. 947-961

Hechler, M. (1995): Digital-Video – Dienste, Technologien und Architekturen. ntz Nachrichtentechnische Zeitschrift, Bd. 48 (1995), Heft 3, S. 18–25

Hetschold, Th. (1993): Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformationen im Gewahrsam des Endbenutzers unter Einhaltung der GSM-Funktionalität eines Funknetzes. GMD Studien Nr. 222, Sankt Augustin 1993

Jabbari, B. et al. (1995): Network Issues for Wireless Communications. IEEE Communications Magazine, Vol. 33, No. 1, January 1995, pp. 88–98

Lauer, G. S. (1994): IN Architectures for Implementing Universal Personal Telecommunications. IEEE Network, Vol. 8, No. 2, March/April 1994, pp. 6–16

Lobensommer, H. (1994): PCN/DCS 1800 – europäisches Mobilfunksystem für alle. ntz Nachrichtentechnische Zeitschrift, Bd. 47 (1994) Heft 8, S. 550–557

Molva, R. et al. (1994). Authentication of Mobile Users. IEEE Network, Vol. 8, No. 2, March/April 1994, pp. 26–34

Mouly, M./Pautet, M.-B. (1992): The GSM System for Mobile Communications. Published by the authors, ISBN 2-9507190-0-7, Palaiseau, France, 1992

Müller, G./Stoll, F. (1995): The Freiburg Communications Assistant Enabling Decentralization and Privacy in Mobile Communications Systems. In: Speaker's Papers, 7th World Telecommunication Forum, Technology Summit, ITU Telecom 95, Geneva, 3–11 October 1995, International Telecommunication Union, October 1995, pp. 245–249

Norp, T./Roovers, A. J. M. (1994): UMTS Integrated with B-ISDN. IEEE Communications Magazine, Vol. 32, No. 11, November 1994, pp. 60–65

Pfitzmann, A. (1993): Technischer Datenschutz in öffentlichen Funknetzen. Datenschutz und Datensicherheit (DuD) 8/93, August 1993, S. 451–463

Rannenberg, K. (1994): Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for Multilateral Security. In: Sizer, R./Yngström, L./Kaspersen, H./Fischer-Hübner, S. (eds.): Security and Control of Information Technology in Society, Proceedings of the IFIP TC9/WG 9.6 Working Conference, August 12–17, 1993, St. Petersburg, Russia, Amsterdam: North-Holland, 1994, pp. 113–128

Rapeli, J. (1995): UMTS: Target, System Concept, and Standardization in a Global Framework. IEEE Personal Communications, Vol. 2, No. 1, February 1995, pp. 20–28

Rendleman, J./Sweeny, T. (1995): Forum turns to ATM security before technology takes off. Communications Week International, 7 Auust 1995, pp. 38–39

Rivest, R. L. et al. (1978): A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21, No. 2, February 1978, pp. 120–126

Rueppel, R. A./Massey, J. L. (1992): Feind hört mit. In: ascom Mobile Telekommunikation, Sonderdruck der Technischen Rundschau anläßlich des 4. Berner Technologie-Forums der Stiftung Hasler-Werke und Ascom-Konzernforschung, Bern: Hallwag AG, 1992, S. 16–19

Schwarz DaSilva, J./Fernandes, B. E. (1995): The European Research Program for Advanced Mobile Systems. IEEE Personal Communications, Vol. 2, No. 1, February 1995, pp. 14–19

Stoll, F. (1995): The Need for Decentralization and Privacy in Mobile Communications Networks. Computers & Security, Vol. 14, No. ??, 1995 (to be published); first presented at 10th IFIP SEC'94 Conference, Curaçao, Netherlands Antilles, May 23–37, 1994

Stoll, F. (1994): Sicherheit in Mobilfunknetzen. Datenschutz-Berater, Heft Nr. 9, September 1994, S. 11–15

Thees, J./Federrath, H. (1995): Methoden zum Schutz von Verkehrsdaten in Funknetzen. In: Brüggemann H. H./Gerhardt-Häckl, W. (Hrsg.): Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS'95, Rostock, April 1995, Braunschweig/Wiesbaden; Vieweg, S. 181–192

Wilson, R. (1995): Reading Interactive TV's future. OEM Magazine, Juni 1995, pp. 34–42/81

Multimedia – Herausforderung für den medienrechtlichen Persönlichkeitsschutz*

Prof. Dr. Carl-Eugen Eberle

Die Technik als Schrittmacher der Medien: Immer wieder waren es technische Entwicklungen, die das Erscheinungsbild der Medien, aber auch die Fortentwicklung des Medienrechts prägten. Dies wird auch für eine neue, durch den Begriff *„Multimedia“* gekennzeichnete Epoche der elektronischen Medien gelten. Das Zusammenwachsen von Datenverarbeitung, Telekommunikation und Fernsehen stellt für das Medienrecht und insbesondere für die Ausgestaltung des Persönlichkeitsschutzes in den Medien eine Herausforderung dar. Deshalb lohnt es sich, den unter dem Begriff Multimedia zusammengefaßten medialen Dienstleistungen und Präsentationsformen nachzugehen (1), die Wurzeln und Grundzüge des Persönlichkeitsschutzes in den Medien in Erinnerung zu rufen (2) und auf dieser Basis einigen ausgewählte Fragen des Persönlichkeitsschutzes bei neuen rundfunkähnlichen Telediensten anzugehen (3).

1. Erscheinungsformen von Multimedia

Das Zukunftsszenario der elektronischen Medien wird geprägt durch die Digitalisierung und die mit ihr verbundenen Folgen[1]. Fernsehbilder werden künftig nicht mehr analog, sondern in der Form digitaler Signale übertragen. Die dabei angewandte Technik der Datenkompression spart Übertragungskapazität mit der Folge, daß innerhalb weniger Jahre Platz für die Satelliten- und Kabelübertragungen von bis zu 400 zusätzlichen Fernsehprogrammen und anderen Telediensten verfügbar sein wird (Information Highway).

Vermehrte und preisgünstigere Übertragungsmöglichkeiten begünstigen neue, entgeltliche Medienangebote[2] wie Pay per Channel, Pay per View, Near Video on Demand und Video on Demand. Neben diesen Fernsehprogrammdiensten werden wohl fernsehmäßige Datendienste (DataBroadcasting) stark zunehmen. Sie werden in der Form von Programmübersichten (TV Guide), Zusatzinformationen zu Sendungen, spezieller Datendienste sowie interaktiver Dienste angeboten werden.

Dieses Multimedia-Szenario gründet sich nicht zuletzt auf die Vorstellung, daß die bislang eher getrennten Welten des Rundfunks und der Datenverarbeitung bzw. der Telekommunikation zusammenwachsen und dem Benutzer ein mediales Gesamtangebot über ein einheitliches Empfangsgerät liefern, den oft apostrophierten elektronischen Kiosk. Dabei wird jedoch der unterschiedliche praktische und habituelle Kontext von Fernsehempfang einerseits und PC-Datenverarbeitung andererseits außer acht gelassen.

* Um Fußnoten erweiterter Beitrag zum Symposium „Multimedia und Datenschutz“ am 28. 08. 1995 in Berlin.

1 Vgl. zum ganzen Das ZDF vor den Herausforderungen des digitalen Fernsehens (ZDF-Schriftenreihe Heft 48), Mainz 1994, Hoffmann-Riem/Vesting (Hrsg.), Perspektiven der Informationsgesellschaft, Baden-Baden 1995.

2 Zur Beschreibung neuer Teledienstleistungen und deren Finanzierungsmöglichkeiten vgl. Prognos AG, Digitales Fernsehen – Marktchancen und ordnungspolitischer Regelungsbedarf, München 1995 sowie Das ZDF vor den Herausforderungen des digitalen Fernsehens (Fn. 1), 17 f., 25 f. Zur medienrechtlichen Einordnung der Dienste vgl. Eberle, ZUM 1994, 530.

Dieser läßt sich mit dem Gegensatzpaar Couch-Viewing versus Desk-Viewing auf einen griffigen Nenner bringen.

Der Fernsehzuschauer sitzt auf der Couch (deshalb Couch-Viewing), mehrere Meter vom Empfangsgerät entfernt. Den Fernsehempfang steuert er über eine Fernbedienung. Diese ist sehr einfach zu handhaben und kann deshalb von jedermann leicht und ohne weitere Einübung benutzt werden, dafür ist sie aber auch relativ funktionsarm und taugt nicht für komplexere Steuerungsaufgaben. Schließlich hat das Fernsehen auch eine – wenn auch gegenüber früher möglicherweise schwindende – soziale Dimension, soweit der Zuschauer, wie häufig, das Programm nicht allein, sondern im familiären Kreis oder mit Freunden verfolgt.

Der PC-Nutzer dagegen sitzt in der Regel allein unmittelbar vor dem zum Greifen nahen Bildschirm am Schreibtisch (deshalb Desk-Viewing). Die Informationsauswahl steuert er über eine multifunktionale Tastatur. Ihre Handhabung ist – wie der Umgang mit dem PC insgesamt – nicht einfach, sondern setzt professionelles Einüben voraus.

Veranschaulicht man sich diese höchst unterschiedlichen Nutzerwelten, dann fällt es schwer, sich die prognostizierte Verschmelzung von Fernsehgerät und PC vorzustellen. Stattdessen erscheint ein Szenario realistischer, bei dem der Zuschauer ein um Spartenkanäle angereichertes Fernsehangebot erlebt, das durch zusätzliche Informationen zum Programm nach Art des Videotextes und durch spezielle Datenangebote (DataBroadcasting) komplettiert wird. Dieses insgesamt der Fernsehfunktion zuzurechnende mediale Gesamtangebot wird dabei unter einer gemeinsamen Benutzeroberfläche nach Art eines elektronischen Programmführers (TV Guide) angeordnet und über eine vielleicht funktionsmäßig dem Dienstspektrum angepaßte, dem PC-Keyboard aber noch nicht vergleichbare, weil einfacher zu bedienende Fernbedienung zugänglich gemacht.

Aus der Sicht des Zuschauerverhaltens spricht demnach viel dafür, daß der Freizeitkonsum elektronischer Medien nach Art des Couch-Viewing vor dem Fernsehgerät stattfindet. Den geschilderten Präsentationserfordernissen kommt darüber hinaus die digitale Programmverbreitung entgegen. Sie erlaubt es, dem Zuschauer das mediale Gesamtangebot so zu präsentieren, daß er die Übersicht behält, nach den für ihn maßgeblichen Bedarfskriterien die Angebotsvielfalt ordnen und den gewünschten einzelnen Programmbeitrag auswählen kann.

Die Technik hierzu besteht darin, eine Vielzahl von Einzelprogrammen und dazugehörigen Teledienstleistungen zu Programmbouquets zu bündeln und unter einem einheitlichen elektronischen Programmführer (TV Guide) anzubieten. Das bedeutet, daß die großen Veranstaltergruppen künftig vermehrt Spartenkanäle anbieten werden. Sie ergänzen die Vollprogramme durch themen- und zielgruppenbezogene Programmangebote, die teils entgeltlich, teils unentgeltlich verbreitet werden. Hinzu treten videotextähnliche Informationsdienste, die Hintergrundinformationen zu den Sendungen liefern, die aber auch für Telespiele oder für Bestellvorgänge genützt werden können.

Vor dieses mediale Gesamtangebot wird der elektronische Programmführer wie eine Art Inhaltsverzeichnis gelegt. Er informiert – je nach Wunsch – über die zeitliche Abfolge von Sendungen, ordnet diese zugleich aber auch ihrem Inhalt nach bestimmten Sparten, wie z. B. Information, Sport, Spielfilm, Dokumentation, Kinder oder Ratgeber zu und erleichtert es somit, Sendungen nach inhaltlichen Kriterien auszuwählen. Über den elektronischen Programmführer wird es zukünftig wohl auch in einfacher Weise möglich sein, Videorecorder vorzuprogrammieren und Bestellungen abzuwickeln.

Für die medienrechtliche Beurteilung kommt es darauf an, ob die genannten Multimedia-Dienstleistungen unter den Begriff des Rundfunks gefaßt werden können[3]. Dies gilt wohl unstreitig für Pay TV und Pay per View-Dienste, erfüllen sie jedoch aufgrund ihrer Zugänglichkeit für jedermann und ihre Organisation als Verteildienst die für die klassische Definition des Rundfunks relevanten Merkmale der *„gleichzeitigen Veranstaltung für die Allgemeinheit"*[4]. Gleiches muß aber auch für die oben angeführten On Demand-Dienste gelten, insbesondere für Video on Demand[5]. Hierbei handelt es sich zwar um den individuellen Abruf bestimmter Einzelsendungen, die aber in das tatsächliche Erscheinungsbild des Fernsehens in seiner neuen Funktionsvielfalt eingefügt sind. Schließlich sind On Demand-Dienstleistungen ebenfalls für die Allgemeinheit bestimmt. Der Unterschied zum herkömmlichen Programm besteht lediglich darin, daß diese Sendungen erstens permanent zur Verfügung stehen und zweitens nicht am empfangsbereiten Fernsehgeräte, sondern in der Datenverarbeitungsanlage des Anbieters ständig verfügbar gehalten werden. Aus der Sicht des Teilnehmers unterscheidet sich dieses Angebot jedoch nicht von dem übrigen, im Verteilwege angebotenen Sendematerial. Daß die Übertragung erst auf seinen Abruf hin initiiert wird, stellt sich für ihn nicht als eine medienspezifisch relevante Besonderheit dar. Auch die Komplementärfunktion dieser Dienste, die das übrige Fernsehangebot ergänzen und komplettieren, legt es sodann nahe, diese zum Rundfunk zu zählen. Dies gilt um so mehr, als der Rundfunkbegriff dynamisch angelegt ist und auch schon bisher technische Weiterungen wie etwa Videotext, die sich als funktionell äquivalent erwiesen haben, in sich aufgenommen hat. Diese Ansicht kann sich – jedenfalls für den Bereich des Video on Demand – auch auf das Bundesverfassungsgericht berufen, das den Unterschied zwischen dem herkömmlichen Rundfunkempfang und dem Empfang *„auf Abruf"* einerseits sowie *„auf Zugriff"* andererseits als für den Rundfunkbegriff nicht relevant angesehen hat und deshalb die Rundfunkfreiheit nach Art. 5 Abs. 1 Satz 2 GG für alle diese Dienste gleichermaßen einschlägig hält[6]. Das schließt dienstespezifische Regelungen (wie z. B. im baden-württembergischen Landesmediengesetz) nicht aus, die jedoch – und darauf hat das Bundesverfassungsgericht vielfach hingewiesen – die aus der Sicht des Rundfunks gebotenen Gestaltungskriterien nicht hintanstellen können. Auch hiernach ergibt sich jedenfalls ein Ausgreifen des Rundfunks und der ihn prägenden rechtlichen Gesichtspunkte in die genannten neuen rundfunkähnlichen Kommunikationsformen.

2. Persönlichkeitsschutz in den Medien

Kontrolle und Kritik, aber auch die Informationsfunktion der Massenmedien können in Widerstreit mit den schutzwürdigen Belangen des im Einzelfall betroffenen Bürgers oder Unternehmens treten. Deswegen ist unumstritten, daß der Schutz Betroffener gegenüber einer Berichterstattung in den Massenmedien besonderer gesetzlicher Regelung bedarf. So stellt das Medienrecht für den Persönlichkeitsrechtsschutz gegenüber Presse und Rundfunk spezielle Instrumente bereit[7]. Insbesondere der Anspruch auf Gegendarstellung wird, obwohl jedenfalls nicht nur zu diesem Zweck eingerichtet, oftmals auch in den Fällen erfolgter oder vermeintlicher Persönlichkeitsverletzung erhoben. Darüber hinaus

3 Vgl. zuletzt Gersdorf, Der verfassungsrechtliche Rundfunkbegriff im Lichte der Digitalisierung der Telekommunikation, Berlin 1995.
4 Vgl. z. B. § 2 Abs. 1 RfStV sowie Eberle, ZUM 1994, 530, 531 m. w. N.
5 Vgl. Eberle, ZUM 1995, 249, 254.
6 BVerfGE 74, 297, 350 ff.
7 Vgl. dazu ausführlich Wenzel, Das Recht der Wort- und Bildberichterstattung, 4. Aufl. Köln 1994 sowie – speziell zum Gegendarstellungsrecht – Seitz/Schmidt/Schoener, Der Gegendarstellungsanspruch in Presse, Film und Fernsehen, 2. Aufl. München 1990. Das Gegendarstellungsrecht dient zwar nicht in erster Linie dem Persönlichkeitsschutz, kann jedoch auch mit dieser Zielrichtung eingesetzt werden.

kann der Betroffene gegenüber einer Verletzung seines Persönlichkeitsrechts bürgerlichrechtliche Widerrufs- und Unterlassungsansprüche bis hin zu Schmerzensgeldforderungen geltend machen. Er kann dies mit Ansprüchen auf die Vernichtung von Filmmaterial und auf die Veröffentlichung des Unterlassungsurteils verbinden.

Kann so der Persönlichkeitsschutz gegenüber Rundfunk und Fernsehen auf ein tradiertes und bewährtes Rechtsinstrumentarium zurückgreifen, so hat der Gesetzgeber auf die Gefahren der elektronischen Datenverarbeitung erst seit den siebziger Jahren mit der Schaffung allgemeiner und bereichsspezifischer Datenschutzgesetze reagiert. Obwohl Datenschutz ebenfalls dem Persönlichkeitsschutz dient, löst er das Spannungsverhältnis zwischen dem Betroffenen und der seine Daten verarbeitenden Stelle auf andere Weise als der medienrechtliche Persönlichkeitsrechtsschutz. Das Datenschutzrecht konkretisiert das vom Bundesverfassungsgericht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 abgeleitete informationelle Selbstbestimmungsrecht[8] für den Bereich der administrativen und geschäftsmäßigen, kurz der bürokratischen Datenverarbeitung. Regelungsziel des Datenschutzrechts ist der Schutz des informationellen Selbstbestimmungsrechts durch Verbote, deren Einhaltung mittels Auskunftsansprüchen überwacht und deren Mißachtung mit Berichtigungs-, Sperrungs- und Löschungsansprüchen verfolgt und zuletzt als Ordnungswidrigkeit bzw. Straftat geahndet werden kann. Der datenschutzrechtliche Ansatz schlägt sich im Konflikt zwischen Informationsverarbeitungsinteressen und dem Schutz des Persönlichkeitsrechts zunächst auf die Seite des Persönlichkeitsrechts. Jede Verarbeitung personenbezogener Daten wird nach dem Prinzip „in dubio pro securitate" zunächst als eine Gefährdung des Persönlichkeitsrechts des Betroffenen angesehen. Das für die Datenschutzgesetzgebung charakteristische Instrument des Verbots mit Erlaubnisvorbehalt[9] auferlegt jedem, der gesetzlich geschützte Daten verarbeiten möchte, einen Begründungs- und Rechtfertigungszwang: Die Verarbeitung gesetzlich geschützter personenbezogener Informationen ist verboten, es sei denn, der Verarbeiter kann einen gesetzlichen Ausnahmetatbestand oder die Einwilligung des Betroffenen nachweisen.

Mit dem Aufkommen der Datenschutzgesetzgebung stellte sich auch die Frage, ob die Instrumentarien der Datenschutzgesetze auch auf die Datenverarbeitung bei Presse und Rundfunk Anwendung finden sollten. Dabei wurde rasch erkannt, daß ein präventives Verbot mit Erlaubnisvorbehalt für die Informationsverarbeitung zu medialen Zwecken nicht in Betracht kommen kann[10]. Die Begründung hierfür liegt einmal im verfassungsrechtlichen Zensurverbot, mit dem sich eine präventive (externe) Inhaltskontrolle der journalistischen Arbeit nicht vertragen würde. Darüber hinaus wird der mediale Persönlichkeitsschutz auch und vor allem durch die dargestellten bereichsspezifischen medienrechtlichen Instrumente gewährleistet. Hinzu kommen neben einer tradierten journalistischen Ethik insbesondere vielfältige organisatorische Sicherungen, die über berufsständische Organisationsformen (Presserat) bis hin zu den pluralistischen Aufsichtsgremien im öffentlich-rechtlichen Rundfunk reichen[11].

8 Vgl. zum informationellen Selbstbestimmungsrecht grundlegend BVerfGE 65, 1, 41 ff. (Volkszählungsurteil); Schlink, Der Staat 1986, 233 ff.; Rosenbaum, JURA 1988, 278 ff. jeweils m. w. N. Das BVerfG verwendet seit dem Quellensteuerurteil auch den Terminus „Grundrecht auf Datenschutz" (BVerfGE 84, 239, 280).
9 Vgl. dazu auch Dörr, AfP 1993, 709; Bergmann/Möhrle/Herb, Handkommentar Datenschutzrecht, Stand: 16. Ergänzungslieferung März 1995, § 4 BDSG Rdnr. 8
10 Vgl. hierzu Eberle, Computer und Recht 1992, 757, 759.
11 Vgl. dazu insbesondere Eberle, Selbstkontrolle und Persönlichkeitsschutz in elektronischen Medien in: Mestmäcker (Hrsg.), Selbstkontrolle und Persönlichkeitsschutz in den Medien, Gütersloh 1990, 50., 54 ff.

Anders als im Datenschutzrecht bedarf es beim Konflikt zwischen journalistischer Tätigkeit und Persönlichkeitsrecht keiner vorgängigen Rechtfertigung der Recherche durch den Journalisten[12]. Diese für das Medienrecht typische Präponderanz der Kommunikationsgrundrechte trägt der besonderen Bedeutung und Gewichtigkeit dieser Grundrechte gegenüber dem Persönlichkeitsrecht Rechnung: Die massenmediale Meinungsäußerung und -verbreitung ist nicht nur Ausdruck individualrechtlicher Grundrechtsbetätigung, sondern verkörpert zugleich die für die individuelle und gesellschaftliche Meinungsbildung essentielle Aufgabenerfüllung von Presse und Rundfunk als Institutionen in deren dienender Funktion gegenüber der Informationsfreiheit aller Bürger[13].

Es handelt sich also beim Interessenkonflikt zwischen Medien und Persönlichkeitsrecht nicht, wie beim Datenschutzrecht, um einen bipolaren Konflikt, sondern um ein Geflecht miteinander verwobener und verschränkter medialer Grundrechtspositionen einerseits und dem persönlichkeitsrechtlichen Individualrechtsschutz andererseits. Diese Konstellation stellt an die Abwägung der konfligierenden Interessen besonders hohe Anforderungen. Sie widerstreitet einer generalisierenden gesetzlichen Regelung und verlangt nach fallspezifischen Lösungsmustern, wie sie die Rechtsprechung im Laufe der Zeit entwickelt hat.

In Erkenntnis all dessen hat die Gesetzgebung die Besonderheiten des Persönlichkeitsschutzes gegenüber Presse und Rundfunk zunächst respektiert und bei diesen Unternehmen zwischen der Datenverarbeitung zu journalistischen Zwecken und der übrigen Datenverarbeitung, etwa zu betrieblichen und sonst geschäftsmäßigen Zwecken, unterschieden. Während für letztere die allgemeine Datenschutzgesetzgebung zur Anwendung kommt, wurde die Datenverarbeitung zu eigenen journalistischen Zwecken von der Anwendung der Datenschutzgesetzgebung weitgehend ausgenommen, in dem für sie nurmehr die Verpflichtung auf das Datengeheimnis und auf Datensicherungsmaßnahmen gelten soll (Medienprivileg)[14]. Mit dem Medienprivileg wurde den bereichsspezifischen Besonderheiten des Persönlichkeitsschutzes Rechnung getragen. Dies zeigt die folgende Gegenüberstellung: Im Datenschutzrecht geht es um die Integrität der Selbstdarstellung des Betroffenen. Deshalb besteht ein Rechtfertigungszwang für die Sammlung, Verarbeitung und Weitergabe der auf die Person bezogenen Daten, eine Bindung der Daten an den jeweiligen Verarbeitungskontext (Zweckbindungsgebot) sowie ein auf den Betroffenenschutz ausgerichtetes Durchsetzungsinstrumentarium von Auskunfts- und Folgeansprüchen. Der medienrechtliche Persönlichkeitsrechtsschutz dagegen berücksichtigt in viel stärkerem Maße die auf Verarbeitung und Verbreitung von Informationen angelegten Interessen von Presse und Rundfunk. Rechtfertigungszwang und Zweckbindungsgebot sind der journalistischen Recherche fremd und würden sie unzumutbar beeinträchtigen. Datenschutz darf nicht dazu führen, daß die journalistische Verarbeitung personenbezogener Daten gewissermaßen die rechtfertigungsbedürftige Ausnahme und die informationelle Abschottung die Regel darstellt. In der Arbeit von Presse und Rundfunk kommt vielmehr die Gemeinschaftsbezogenheit des Individuums zum Ausdruck: Die informationelle Selbstbestimmung findet ihre Grenzen in einer Art informationellen Sozialbindung des einzelnen, deren Reichweite durch das legitime Unterrichtungsinteresse der Allgemeinheit bestimmt wird.

12 Ebenso Dörr, AfP 1993, 710.
13 Vgl. BVerfGE 20, 162, 174 f. (zur Pressefreiheit); BVerfGE 57, 295, 320; 74, 297, 323 (zur Rundfunkfreiheit).
14 Vgl. § 1 Abs. 3 BDSG (1977) sowie den bei der Novellierung des BDSG an dessen Stelle getretenen § 41 BDSG (1990).

Diese Sonderstellung der Medien gegenüber dem allgemeinen Datenschutzrecht ist inzwischen auch europarechtlich anerkannt. So sieht Art. 9 der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr in der vom Europäischen Parlament modifizierten Fassung[15] folgende Regelung vor:

> „Die Mitgliedsstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von diesem Kapitel sowie von den Kapiteln IV und VI nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Meinungsäußerungsfreiheit geltenden Vorschriften in Einklang zu bringen."

Bei dieser Vorschrift fällt auf, daß sie die Datenverarbeitung durch Medienunternehmen immer dann privilegiert, wenn sie „allein zu journalistischen Zwecken" erfolgt. Nicht erforderlich ist dagegen, daß die personenbezogenen Daten, wie dies die deutsche Regelung[16] vorschreibt, „ausschließlich zu *eigenen* journalistisch-redaktionellen Zwecken verarbeitet oder genutzt werden". Die europarechtliche Regelung gewährt das Medienprivileg also auch dann, wenn z. B. ein Medienarchiv nicht nur von Journalisten im eigenen Haus, sondern auch von außenstehenden dritten Medienunternehmen genutzt wird, vorausgesetzt, es handelt sich um die Verwendung der Daten für journalistisch-redaktionelle Zwecke. Dies erscheint sachgerecht, da der Grund für die Privilegierung der journalistischen Datenverarbeitung die Nutzung zu journalistischen Zwecken ist und es nicht darauf ankommen kann, ob die Journalisten nun Angestellte des Medienunternehmens sind oder nicht. Die legislatorische Beschränkung auf die eigene journalistische Verarbeitung orientiert sich allzu stark am Typus der pressemäßigen Datenverarbeitung, bei der z. B. Journalisten eines Zeitungsverlages auf das Pressearchiv ebendieses Verlages zugreifen. Es verkennt die Praxis der Fernsehberichterstattung, bei der die Fernsehunternehmen sich häufig freier Mitarbeiter oder außenstehender, freier Produktionsteams bedienen. Daß alle diese Journalisten, deren Sendungen dann unter der medienrechtlichen Verantwortung des jeweiligen Sendeunternehmens ausgestrahlt werden, sich nach der geltenden Rechtslage[17] nicht des Medienarchivs dieses Hauses bedienen dürfen, ohne daß das Medienprivileg verlorengeht, erscheint nicht einleuchtend. Aber auch in den Fällen, in denen mehrere Sendeunternehmen zur Erzielung von Synergieeffekten auf das bei einem dieser Unternehmen betriebene Medienarchiv zugreifen, fehlt ein sachlicher Differenzierungsgrund dafür, diese Form der Datenverarbeitung zu journalistischen Zwecken vom Medienprivileg auszunehmen.[18] Deshalb greift die Beschränkung auf *eigene* journalistische Zwecke in unverhältnismäßiger Weise in die Presse- und Rundfunkfreiheit ein. Die im Zuge der Umsetzung der EU-Datenschutzrichtlinie gegebenenfalls notwendige Anpassung des deutschen Datenschutzrechts sollte deshalb zu einer entsprechenden Korrektur des Bundesdatenschutzgesetzes sowie der entsprechenden landesrechtlichen Vorschriften benutzt werden.

15 Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. 07. 1995.
16 § 41 Abs. 1 Satz 1 BDSG.
17 Zwar mag eine rundfunkfreundliche Auslegung des Medienprivilegs – Nutzung zu *eigenen* journalistischen Zwecken auch bei Einsatz freier Mitarbeiter – dieses Ergebnis vermeiden helfen. Doch führt die unten vorgeschlagene Novellierung des Medienprivilegs zu größerer Rechtsklarheit.
18 Kritisch insoweit auch Bergmann/Möhrle/Herb, Handkommentar Datenschutzrecht (Fn. 9), § 41 Rdnr. 41.

Als verfehlt anzusehen sind auch neuere medienrechtliche Regelungen, die im Fall von Gegendarstellungen und von Persönlichkeitsrechtsverletzungen Auskunfts–[19], Speicherungs- und Berichtigungsansprüche[20] im Hinblick auf das Sendematerial sowie die der Berichterstattung zugrundeliegenden personenbezogenen Daten gewähren.[21] Der datenschutzrechtliche Auskunfts- und Berichtigungsanspruch eröffnet dem von ihm Begünstigten die Möglichkeit, sich gegebenenfalls schon frühzeitig über Gegenstand und Material einer journalistischen Recherche Kenntnis zu verschaffen und sich gegen die Berichterstattung mit dem medienrechtlichen Unterlassungsanspruch zur Wehr zu setzen.[22] Zwar kann die datenschutzrechtliche Auskunft aus Gründen des Informantenschutzes verweigert werden, doch läßt dies die Tatsache unberührt, das mit dem Auskunftsanspruch unter der Fahne des Datenschutzes Terrain erobert wird, daß zum grundrechtlich geschützten Kernbereich journalistischer Betätigung zählt.

Der datenschutzrechtliche Berichtigungsanspruch steht, soweit er sich im Rundfunk auf gesendetes Material bezieht, im Widerspruch zu der gesetzlichen Aufzeichnungspflicht, der die Sendungen zu Beweiszwecken unterliegen und die naturgemäß auf die unveränderte Aufzeichnung der Sendungen gerichtet ist. Der isoliert auf die Daten des Betroffenen gerichtete Berichtigungsanspruch verkennt zudem, daß diese nicht – bürokratische Verarbeitungsweise entsprechend – vorgangsbezogen gespeichert sind, sondern im Kontext einer Sendung stehen, deren Sinngehalt insgesamt von der Berichtigung betroffen sein kann. Schließlich bestehen technische und praktische Schwierigkeiten, eine Datenberichtigung innerhalb einer archivierten Sendung vorzunehmen: Die sendetechnische Aufzeichnung läßt sich nicht ohne weiteres nachträglich in einer Weise verändern, die der Berichtigung von Dateien entspricht.[23]

Auch die Pflicht, Gegendarstellungen zu den gespeicherten Daten zu nehmen, macht nur Sinn, wenn man unter diesen nicht die Sendung als solche, sondern die dazugehörigen journalistischen Unterlagen versteht. Am archivierten Sendeband selbst könnte allenfalls ein Hinweis auf eine Gegendarstellung angebracht werden.[24] Problematisch ist aber vor allem die Aufwertung der Gegendarstellung, die durch den Speicherungszusammenhang gewissermaßen in den gleichen Rang wie die Sendung selbst gehoben wird. Dabei besteht insofern zwischen beiden ein erheblicher Unterschied, als die journalistischen Daten nach Maßgabe der journalistischen Standesregeln und nach den für den Rundfunk geltenden gesetzlichen und hausinternen Programmgrundsätzen verarbeitet worden sind, während für die Gegendarstellung dergleichen Gestaltungsregeln nicht gelten, ja nicht einmal ihr Wahrheitsgehalt gewährleistet ist.

19 Vgl. § 63 Abs. 3 HPRG; § 56 Abs. 2 HambMedienG; § 74 Abs. 7 LRG Saarl.; vgl. auch § 50 Abs. 3 WDR-G und § 17 Abs. 3 ZDF-StV. Vgl. weiter § 31 Abs. 3 LDSG BW; § 28 Abs. 3 ThürDSG sowie § 41 Abs. 3 BDSG im Hinblick auf die Bundesrundfunkanstalten; vgl. dazu Bergmann/Möhrle/Herb, Handkommentar Datenschutzrecht (Fn. 9), § 41 Rdnr. 63 ff.

20 Vgl. § 50 Abs. 2, 3 WDR-G sowie § 17 Abs. 3 S. 3 ZDF-StV; § 56 Abs. 3 HambMedienG; § 74 Abs. 6 LRG Saarl.; § 31 Abs. 3 Satz 3 LDSG BW; § 28 Abs. 3 Satz 3 ThürDSG sowie § 41 Abs. 3 S. 3 BDSG.

21 Ähnlich kritisch wie hier zum Auskunftsanspruch auch Dörr, AfP 1993, 710.

22 A. A. Schrader, AfP 1994, 114, 115, der insoweit aber – mindestens implizit – jedenfalls für § 17 Abs. 3 S. 3 ZDF-StV eine solche Gefährdungslage aufgrund einer möglichen Fehlinterpretation dieser Vorschrift eingesteht. Ihr soll durch eine modifizierte Fassung der Parallelvorschrift § 56 Abs. 2 HambMedienG vorgebeugt werden.

23 Die von Schrader, AfP 1994, 115 vorgeschlagene Lösung, wonach die falschen Daten unverändert bleiben und lediglich der richtige Sachverhalt hinzugefügt werden soll, erscheint vernünftig. Nur findet sie angesichts der Differenzierung in § 17 Abs. 3 S. 3 ZDF-StV in die Vorgänge der „Berichtigung“ einerseits und der „Hinzufügung einer eigenen Darstellung“ andererseits im Wortlaut der Vorschrift nur schwerlich eine Stütze.

24 Bergmann/Möhrle/Herb (Fn. 9), § 41 Rdnr. 56.

Völlig verfehlt erscheinen schließlich Vorschläge der Datenschutzbeauftragten[25], wenn sie die Nutzung von Medienarchiven im Hinblick auf lang zurückliegende Publikationen in einer Weise beschränken wollen, die dem *„Recht auf Vergessen“* in der Form von Löschungsvorschriften für das Bundeszentralregister entspricht. Eine solchermaßen geforderte Neubestimmung des Medienprivilegs beeinträchtigt völlig die auch in der Zeitachse wirkende Informationsfunktion der Medien. Sie verabsolutiert das Schutzbedürfnis des einzelnen und verkennt nicht nur die Kommunikationsgrundrechte der Medien, sondern auch deren gesellschaftliche und demokratische Funktion in ihrer auch historischen Dimension. Beide Rechtsgüter sind letztlich in einem am Einzelfall orientierten Abwägungsprozeß zum Ausgleich zu bringen[26], der einer rigiden gesetzlichen Löschungsverpflichtung nach dem Muster des Bundeszentralregistergesetzes widerstreitet.

3. Persönlichkeitsschutz bei neuen Telediensten

Soweit es sich bei den neuen Telediensten in dem oben unter dem Stichwort „Couch-Viewing“ beschriebenen Sinne um Rundfunk bzw. rundfunkähnliche Dienste handelt, ist wiederum zwischen den verschiedenen Zwecken der Datenverarbeitung zu unterscheiden. Für die übermittelten Sendungsinhalte und die ihnen zugrundeliegende Datenverarbeitung gilt das Medienprivileg. Dies läßt sich damit rechtfertigen, daß bei diesen Diensten die publizistische Funktion im Vordergrund steht, die sie entweder selbst oder als Annex zu anderen solchermaßen geprägten Diensten erfüllen. Die Abwägung zwischen der kommunikationsrechtlich geschützten Entfaltung einerseits und dem Persönlichkeitsschutz auf der anderen Seite folgt deshalb dem gleichen Muster wie beim Rundfunk im traditionellen Sinne und bei der Presse. Das bedeutet, daß der Persönlichkeitsrechtsschutz im Rahmen der Datenverarbeitung zu journalistischen Zwecken nicht nach den Regeln des Datenschutzes, sondern auf der Grundlage des medienrechtlichen Instrumentariums (Gegendarstellung, Widerruf, Unterlassung, Schadenersatz) erfolgt. Das Medienprivileg gilt demnach, soweit es die Inhalte der Kommunikation anbelangt, nicht nur für den Rundfunk, sondern auch für rundfunkähnliche Dienste.

Bei der mit der Abwicklung der Dienste verbundenen administrativen Datenverarbeitung dagegen sind, soweit es private Rundfunkveranstalter anbelangt, Sondervorschriften für den Umgang mit Abrechnungs- und Verbindungsdaten nach § 28 Rundfunkstaatsvertrag zu beachten, die dem BTX-Staatsvertrag entlehnt sind. Sie stellen bereichsspezifisches Datenschutzrecht für entgeltliche Fernsehprogramme und On Demand-Teledienste dar und tragen den besonderen Gefahrentatbeständen dieser Verarbeitungsvorgänge Rechnung. Soweit diese Vorschriften – wie z. B. gegenüber den öffentlich-rechtlichen Rundfunkanstalten – nicht zur Anwendung kommen, verbleibt es dagegen bei der Anwendung der allgemeinen Datenschutzvorschriften. Für die Zukunft könnte überlegt werden, die bislang nur für private Rundfunkveranstalter geltenden Datenschutzvorschriften in den allgemeinen Teil des Rundfunkstaatsvertrages zu übernehmen und sie damit für alle Rundfunkveranstalter verbindlich zu machen. Doch erscheint auch die geltende Rechtslage im Hinblick auf die öffentlich-rechtlichen Rundfunkanstalten insoweit hinnehmbar, als bei ihnen angesichts der jahrzehntelangen Erfahrungen im Umgang mit den personenbezogenen Daten der Gebührenzahler ein mißbräuchlicher Umgang mit Abrechnungs- und Verbindungsdaten, der besondere gesetzliche Vorkehrungen erforderlich machen würde, nicht zu befürchten ist.

25 AfP 1995, 482.

26 BVerfGE 35, 202, 223 f.

4. Schlußbetrachtung

Datenschutzregelungen sind ebenso unverzichtbar wie tiefgreifende Rahmenbedingungen moderner Kommunikation. Damit berühren sie die Interessen all derer zentral, bei denen Kommunikation nicht nur irgendein Teil ihrer geschäftlichen Entfaltung ist, sondern deren Aufgabe gezielt auf die Massenkommunikation ausgerichtet ist. Dies gilt in besonderem Maße für den Rundfunk und seine modernen Erscheinungsformen. Er wird – vor allem als öffentlich-rechtlicher Rundfunk – nicht nur um seiner selbst willen veranstaltet, sondern ist elementarer Faktor der individuellen und öffentlichen Meinungsbildung und erfüllt so eine für die Gemeinschaft unverzichtbare öffentliche Aufgabe. Deshalb bin ich besonders dankbar, daß mir hier Gelegenheit geboten wurde, die Belange des Rundfunks darzustellen und mit denen des Datenschutzes abzuwägen.

Der ordnungspolitische Rahmen für Europas Weg in die Informationsgesellschaft*

Marcel Haag

I. Einleitung

Der Informations- und Kommunikationssektor der fortgeschrittenen Industriegesellschaften befindet sich gegenwärtig in einem tiefgreifenden Wandel. Auch wenn das volle Ausmaß dieser Änderungen und ihrer Auswirkungen derzeit nur in Konturen erkennbar ist, steht jedoch bereits heute fest, daß der Informationszugang und die Informationsverarbeitung in wichtigen Lebensbereichen stark an Bedeutung gewinnen wird. Die Einführung neuer Informations- und Kommunikationstechniken und insbesondere die Konvergenz von Informationstechnologie, Telekommunikation und audiovisuellem Sektor stellt auch die Ordnungspolitik vor neue Aufgaben. Diese sind nicht zuletzt durch Probleme geprägt, die durch das Zusammentreffen eines bislang weitgehend unregulierten Sektors, der Informationstechnologie, mit zwei traditionell hochregulierten Sektoren, deren Regulierung überdies nach unterschiedlichen Grundsätzen erfolgt, entstehen.

Die Europäische Kommission hat den mit der Entwicklung der Informations- und Kommunikationsgesellschaft zusammenhängenden Fragen höchste Priorität eingeräumt. Bereits in ihrem Weißbuch zu „Wachstum, Wettbewerbsfähigkeit, Beschäftigung“[1] vom Dezember 1993 erklärte die Kommission die Schaffung eines „Gemeinsamen Informationsraums“ in der Europäischen Union und die Entwicklung der Informationsgesellschaft zu einem der vorrangigen Ziele ihrer Tätigkeit zur Wiederbelebung der europäischen Volkswirtschaften. Der auf der Grundlage von Überlegungen einer Gruppe hochrangiger europäischer Industrievertreter unter dem Vorsitz von Kommissar Bangemann erstellte Bericht vom 26. Mai 1994[2] bestätigte die Dringlichkeit einer europäischen Initiative zur Informationsgesellschaft und sprach eine Reihe von Empfehlungen aus.

Im Juli 1994 legte die Kommission einen Aktionsplan für „Europas Weg in die Informationsgesellschaft“ vor. Dieser enthält einen weitreichenden Katalog von Maßnahmen, mit denen die Herausforderungen der entstehenden Informationsgesellschaft in der Europäischen Union angenommen werden sollen.[3] Dabei liegt dem Aktionsplan kein geschlossener Entwurf einer neuen künftigen Gesellschaft zugrunde. Den Ausgangspunkt des Aktionsplans bildet vielmehr die Annahme, daß die sich im Informations- und Kommunikationssektor vollziehenden Entwicklungen wirtschaftliche, politische und soziale Chancen bieten, die nicht ungenutzt bleiben sollten.

Eine der zentralen Grundvoraussetzungen für die Entwicklung der Informationsgesellschaft ist die Schaffung elektronischer Superhighways, das heißt hochleistungsfähiger Kommunikationsverbindungen zur Übertragung von Daten, Sprache und Bildern. Im

* Der Beitrag stellt eine persönliche Meinungsäußerung dar und bindet nur den Verfasser.

1 Europäische Kommission, Wachstum, Wettbewerbsfähigkeit, Beschäftigung – Herausforderungen der Gegenwart und Wege ins 21. Jahrhundert, Weißbuch, KOM (93) 700 endg., 5. 12. 83 = Bull. EG, Beil. 6/93.

2 Europa und die globale Informationsgesellschaft, Empfehlungen an den Europäischen Rat, Brüssel, 26. Mai 1994 (sog. Bangemann-Bericht).

3 Europas Weg in die Informationsgesellschaft – Ein Aktionsplan, Mitteilung der Kommission an den Rat und das Europäische Parlament sowie an den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen, KOM (94) 347 endg., 19. 07. 94.

Mittelpunkt der Initiative der Kommission steht deshalb, ebenso wie bei den entsprechenden Initiativen von Industriestaaten außerhalb Europas, die ordnungspolitische Reform des Telekommunikationssektors mit dem Ziel einer umfassenden Liberalisierung, welche die privatwirtschaftliche Finanzierung der zur Entwicklung der Informationsgesellschaft benötigten leistungsfähigen Informationsinfrastrukturen ermöglicht.

II. Die Transformation des Telekommunikationssektors

Die Vorarbeiten der Kommission zu einer umfassenden Reform des ordnungspolitischen Rahmens für den Telekommunikationssektor sind mit der Vorlage des Grünbuchs über Telekommunikationsinfrastrukturen[4] und dem Bericht über die öffentliche Konsultation zu diesem Grünbuch am 3. Mai 1995[5] weitgehend abgeschlossen. Mit diesen Vorarbeiten leitet die Kommission eine neue Phase ihrer Telekommunikationspolitik ein, in der sie das bisherige Liberalisierungsprogramm auf den Bereich der Telekommunikationsinfrastrukturen ausdehnt, um den Übergang in eine europäische Informations- und Kommunikationsgesellschaft zu erleichtern und zu beschleunigen.

1. Liberalisierung der Telekommunikationsmärkte

Die Weichen sind auf Gemeinschaftsebene inzwischen eindeutig zugunsten einer vollständigen Öffnung der Telekommunikationsmärkte in der Union gestellt. Eine wichtige Vorentscheidung für die volle Liberalisierung des Sektors hat der Rat der für Telekommunikation zuständigen Minister auf der Grundlage des von der Kommission durchgeführten „Review“[6] bereits vor zwei Jahren getroffen, als er sich auf die Aufhebung des Sprachmonopols in der Union bis spätestens zum 1. Januar 1998 – vorbehaltlich zusätzlicher Übergangsfristen für Mitgliedstaaten mit weniger ausgebauten oder sehr kleinen Netzen – einigte. In der Entschließung vom 22. Juli 1993 legte sich der Rat, den Vorschlägen der Kommission folgend, auf die vollständige Öffnung aller Telekommunikationsdienste für den Wettbewerb fest.[7] Inzwischen bereiten sich Wettbewerber in praktisch allen Mitgliedstaaten – nicht zuletzt auch hier in der Bundesrepublik – auf die Liberalisierung des Telefondienstes vor.

In der Ratsentschließung vom 22. Juli 1993 wurde auch die Überprüfung des letzten noch verbleibenden reservierten Bereichs in der Telekommunikation, d. h. die Netzmonopole, auf die Tagesordnung der Union gesetzt. Die kostengünstige Bereitstellung hochleistungsfähiger Infrastrukturen bildet eine Grundvoraussetzung für die Entwicklung der Telekommunikations- und Informationsmärkte, da sie den Zugang zu den neuen Diensten und Anwendungen erst ermöglichen. In dieser Hinsicht ist die Situation nach den Feststellungen der Kommission in Europa, im Vergleich etwa mit den USA, noch unbefriedigend. In Europa bestehen nicht nur vielfach noch Engpässe bei der Bereitstellung von Hochgeschwindigkeitsmietleitungen, sondern auch Mietleitungstarife, die zum Teil um das Zehnfache über den vergleichbaren Tarifen in den USA liegen. Die Kommission

4 Grünbuch über die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze, Teil I: Grundsätze und Zeitrahmen, KOM (94) 440 endg., 25. 12. 94; Teil II: Ein gemeinsames Konzept zur Bereitstellung einer Infrastruktur für Telekommunikation in der Europäischen Union, KOM (94) 682 endg., 25. 01. 95.

5 Konsultation zum Grünbuch über die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze, Mitteilung der Kommission an den Rat und das Europäische Parlament, KOM (95) 158 endg., 03. 05. 95.

6 Mitteilung über die Prüfung der Lage im Bereich der Telekommunikationsdienste (1992), SEK (92) 1048 endg., 21. 10. 92; Mitteilung an den Rat und das Europäische Parlament über die Konsultation zur Lage im Bereich der Telekommunikationsdienste, KOM (93) 158 endg., 28. 04. 93.

7 Entschließung des Rates vom 22. Juli 1993 zur Prüfung der Lage im Bereich Telekommunikation und zu den notwendigen künftigen Entwicklungen in diesem Bereich, ABl. Nr. C 213, 06. 08. 93, S. 1.

geht davon aus, daß sich die Aufhebung der Übertragungswegemonopole in den Mitgliedstaaten auf zweifache Weise positiv auswirken wird: Zum einen wird sie private Investitionen ermöglichen, die angesichts der zum Ausbau von elektronischen Highways notwendigen Investitionsvolumen unverzichtbar sind. Zum anderen wird sie durch die Einführung von Wettbewerb zu stärker an den Kosten orientierten und damit deutlich niedrigeren Preisen für Infrastrukturen führen.[8]

Die Kommission hat deshalb im ersten Teil des Infrastruktur-Grünbuchs, der im Oktober 1994 vorgelegt wurde, die volle Öffnung der Telekommunikationsinfrastrukturen für den Wettbewerb parallel zur vollständigen Diensteliberalisierung bis zum 1. Januar 1998 vorgeschlagen.[9]

Auf seinem Treffen am 17. November vergangenen Jahres hat der Rat der Telekommunikationsminister diesem Vorschlag zugestimmt.[10] Das Zieldatum 1. Januar 1998 gilt damit sowohl für die Liberalisierung des Telefondienstes als auch für die Errichtung und den Betrieb von Telekommunikationsnetzen. Dabei finden die für einige Mitgliedstaaten beim Telefondienst gewährten Übergangsfristen auch auf die Netzliberalisierung Anwendung (Portugal, Griechenland, Spanien, Irland: 5 Jahre; Luxemburg: 2 Jahre). Nachdem Spanien angekündigt hat, von dieser Möglichkeit keinen Gebrauch machen zu wollen, dürften sich die anderen Mitgliedstaaten ebenfalls dazu entschließen, die zusätzliche Übergangsfrist nicht oder nicht vollständig in Anspruch zu nehmen, so daß im Ergebnis eine weitgehend zeitgleiche europaweite vollständige Öffnung der Telekommunikationsmärkte erreicht werden könnte.

Nachdem damit die politische Entscheidung für die Schaffung vollständig geöffneter Telekommunikationsmärkte bis 1998 getroffen ist, stellt sich für die zuständigen Gemeinschaftsinstanzen nunmehr die Frage nach der konkreten rechtlichen Ausformung dieser Entscheidung. Auf der Grundlage der Konsultation zum Infrastruktur-Grünbuch hat die Kommission in ihrer Mitteilung vom 3. Mai einen detaillierten Reformfahrplan festgelegt. Dieser sieht die Vorlage und Annahme der auf EU-Ebene erforderlichen Maßnahmen bis zum 1. Januar 1997 vor. Die zur Festsetzung des Reformprozesses auf nationaler Ebene zentralen Liberalisierungsschritte auf der Grundlage der Wettbewerbsregeln sind sogar noch vor dem 1. Januar 1996 vorgesehen. Sie werden durch flankierende Harmonisierungsmaßnahmen und eine allgemeine Reform des EG-Telekommunikationsrechts ergänzt, das insgesamt dem künftig vollständig liberalisierten Umfeld angepaßt werden muß. Vor allem mit der frühzeitigen Vorlage der Liberalisierungsmaßnahmen werden die Voraussetzungen dafür geschaffen, daß die nationale Regulierung in den Mitgliedstaaten auf der Grundlage der gemeinschaftsrechtlichen Rahmenvorgaben so rechtzeitig angepaßt werden kann, daß spätestens zum 1. Januar 1998 auch tatsächlich Wettbewerb bei den Netzen und Diensten bestehen wird.

Im Einklang mit dem in der Mitteilung der Kommission zur Konsultation über das Infrastruktur-Grünbuch festgelegten Zeitplan hat die Kommission die Entwürfe für die zur schrittweisen Einführung von Wettbewerb erforderlichen Maßnahmen bereits vorgelegt. Es handelt sich um drei Ergänzungen der sogenannten Dienste-Richtlinie, der Kommissionsrichtlinie 90/388/EWG von 28. Juni 1990, in der die europaweite Öffnung aller Tele-

8 Vgl. insbesondere das Grünbuch über die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze, Teil I, S. 22–29.

9 Grünbuch über die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze, Teil I, S. 40 f.

10 Vgl. Entschließung des Rates vom 22. Dezember 1994 über die Grundsätze und den Zeitplan für die Liberalisierung der Telekommunikationsinfrastrukturen, ABl. Nr. C 379, 31. 12. 94, S. 4.

kommunikationsdienste mit Ausnahme des Sprachtelefondienstes geregelt ist.[11] Diese Richtlinie, die im vergangenen Jahr bereits in bezug auf die Satellitenkommunikation ergänzt wurde,[12] bildete bereits bisher das Fundament der Liberalisierung des europäischen Telekommunikationssektors. Mit den drei vorgesehenen Ergänzungen im Hinblick auf Kabelfernsehnetze, auf Mobilkommunikation und schließlich auf die vollständige Liberalisierung wird die Dienste-Richtlinie auch über das Zieldatum 1. Januar 1998 hinaus ihre zentrale Rolle für die Telekommunikationspolitik in der Europäischen Union behalten.

a) Die Ergänzung der Dienste-Richtlinie in bezug auf Kabelfernsehnetze

Bereits im Dezember vergangenen Jahres hat die Kommission den Entwurf einer Richtlinie zur Ergänzung der Dienste-Richtlinie in bezug auf die Öffnung von Kabelfernsehnetzen für Telekommunikationsdienste vorgelegt.[13] Der Entwurf sieht vor, daß genehmigte Kabelfernsehnetze zum 1. Januar 1996 für die Erbringung von bereits liberalisierten Telekommunikationsdiensten geöffnet werden. Er verlangt zudem die Schaffung einer transparenten Rechnungslegung in den Fällen, in denen Kabelfernsehnetze auch für die Erbringung von Telekommunikationsdiensten genutzt werden. Schließlich ist zum 1. Januar 1998 eine Überprüfung der Fälle vorgesehen, in denen, wie in der Bundesrepublik, Fernsehkabelnetze und öffentliches Telekommunikationsnetz von ein und demselben Unternehmen betrieben werden.

Der Richtlinienentwurf trifft dagegen keine Regelungen hinsichtlich der Genehmigung von Kabelfernsehnetzen noch hinsichtlich der Regulierung von über Kabelfernsehnetze erbrachten Rundfunkdiensten. Der Entwurf beinhaltet deshalb lediglich rein telekommunikationsrechtliche Bestimmungen.

Die Richtlinie soll zum einen bestehende Engpässe bei der Bereitstellung von Telekommunikationsnetzinfrastruktur lockern und zum anderen die Errichtung multimediafähiger hybrider Netze attraktiver machen. Von der Richtlinie werden deshalb auch Anreize zu einer beschleunigten Entwicklung und Erbringung von Multimedia-Diensten erwartet.

Der Richtlinienentwurf wurde im März dieses Jahres zur öffentlichen Konsultation im Amtsblatt der EG veröffentlicht. Im Rahmen der Konsultation wurde von verschiedenen Seiten darauf hingewiesen, daß das parallele Problem der Erbringung von Kabelfernsehkapazität über Telekommunikationsnetze in dem Richtlinienentwurf nicht geregelt wird. Insbesondere das Europäische Parlament sprach sich in seiner, im übrigen positiven, Stellungnahme zu dem Entwurf dafür aus, zusammen mit der Öffnung der Kabelfernsehnetze für Telekommunikationsdienste auch die Öffnung der Telekommunikationsnetze für die Bereitstellung von Kabelfernsehkapazität zu regeln.[14]

Im Hinblick auf diese Frage ist einerseits zu berücksichtigen, daß die Schaffung hybrid nutzbarer Infrastrukturen den Übergang zur Informationsgesellschaft begünstigt, andererseits muß aber auch dem Umstand Rechnung getragen werden, daß die Öffnung der öffentlichen Telekommunikationsnetze für Kabelfernsehdienste es den traditionellen

11 Richtlinie der Kommission vom 28. Juni 1990 über den Wettbewerb auf den Märkten für Telekommunikationsdienste (90/388/EWG), ABl. Nr. L 192, 24. 07. 90, S. 10.
12 Richtlinie 94/46/EG der Kommission vom 13. Oktober 1994 zur Änderung der Richtlinien 88/301/EWG und 90/388/EWG, insbesondere betreffend die Satelliten-Kommunikation, ABl. Nr. L 268, 19. 10. 94, S. 15.
13 Entwurf einer Richtlinie der Kommission zur Änderung der Richtlinie 90/388/EWG betreffend die Aufhebung der Einschränkung bei der Nutzung von Kabelfernsehnetzen für die Erbringung von Telekommunikationsdiensten, ABl. Nr. C 76, 28. 03. 95, S. 8.
14 ABl. Nr. C 166, 03. 07. 95, S. 109.

Telekommunikationsorganisationen unter Umständen ermöglichen kann, ihre marktbeherrschende Stellung im Bereich der Telekommunikationsübertragungswege auf den Bereich der Kabelfernsehnetze auszudehnen.

Nach Abschluß der internen Meinungsbildung der Kommission über die aus der Konsultation zu ziehenden Schlußfolgerungen ist die endgültige Annahme der Richtlinie im Herbst zu erwarten.

b) Die Ergänzung der Dienste-Richtlinie in bezug auf Mobilkommunikation und persönliche Kommunikation

Am 21. Juni hat die Kommission den Entwurf einer weiteren Ergänzungsrichtlinie zur Dienste-Richtlinie im Hinblick auf Mobilkommunikation und persönliche Kommunikation vorgelegt.[15] Die Mobilkommunikation ist einer der Sektoren, von dem die stärksten innovativen Impulse für den Telekommunikationsmarkt ausgehen. Bereits in ihrem Grünbuch zur Mobilkommunikation aus dem vergangenen Jahr hat die Kommission dargelegt, daß die Entwicklung von persönlichen Kommunikationssystemen ein zentrales Element der künftigen Informationsgesellschaft sein wird.[16] Neben intelligenten Festnetzen werden digitale Funktechnologien das Rückgrat dieser neuen Kommunikationssysteme bilden.

Der Richtlinienentwurf sieht die Beseitigung von einer Reihe von Restriktionen vor, die die Entwicklung der Mobilkommunikationsmärkte zu Massenmärkten heute in Europa noch behindern. Er regelt die Aufhebung aller ausschließlichen und besonderen Rechte, welche die Mitgliedstaaten in bezug auf Mobilkommunikationssysteme gewähren. Bestehende Beschränkungen bei der Zusammenschaltung mit anderen mobilen und festen Netzen sollen aufgehoben werden. Darüber hinaus ist vorgesehen, daß die Mitgliedstaaten die Errichtung eigener Netzinfrastruktur sowie die Nutzung der Netzinfrastruktur Dritter durch die Mobilfunkbetreiber uneingeschränkt zulassen müssen.

Der Richtlinienentwurf enthält ferner Bestimmungen über die Vergabe von DCS-1800-Lizenzen und Lizenzen nach dem DECT-Standard sowie zum Zugang zu den GSM- und DCSW-1800-Erweiterungsbändern, die sich wettbewerbs- und innovationsfördernd auswirken werden.

Mit der Veröffentlichung des Entwurfs der Richtlinie im Amtsblatt der EG am 1. August 1995 wurde eine öffentliche Konsultationsperiode von zwei Monaten eingeleitet. Der von der Kommission festgelegte Zeitplan sieht vor, daß die Richtlinie noch vor Ende des Jahres endgültig angenommen wird, damit sie, wie geplant, am 1. Januar 1996 in Kraft treten kann. Die Richtlinie wird europaweit klare Rahmenbedingungen und größere unternehmerische Freiräume für die Mobilnetzbetreiber schaffen und damit dem Wachstumsmarkt Mobilkommunikation wichtige neue Impulse geben.

c) Die Ergänzung der Dienste-Richtlinie zur Einführung vollständigen Wettbewerbs

Schließlich hat die Kommission am 19. Juli, also noch vor der Sommerpause, eine weitere Ergänzung der Dienste-Richtlinie vorgelegt, mit der die Rahmenbedingungen für die vollständige Liberalisierung, das heißt der Liberalisierung der öffentlichen Sprachtelefo-

15 Entwurf einer Richtlinie der Kommission zur Änderung der Richtlinie 90/388/EWG betreffend die mobile Kommunikation und Personal Communications, ABl. Nr. C 197, 01. 08. 95, S. 5.
16 Grünbuch über ein gemeinsames Konzept für Mobilkommunikation und Personal Communications in der Europäischen Union, KOM (94) 145 endg., 27. 04. 94.

nie und der Telekommunikationsnetze, bis 1998 festgelegt wird.[17] In dieser Richtlinie werden auch die Anforderungen präzisiert, die aufgrund der EG-Wettbewerbsregeln bei der Ausgestaltung der Reformgesetze in den Mitgliedstaaten zu beachten sind. Die Richtlinie wird dabei helfen, die Reformdebatte in den Mitgliedstaaten zu strukturieren und die Diskussion auf die wesentlichen noch offenen Fragen, wie etwa die der Ausgestaltung der Einzelheiten eines Systems zur Finanzierung des öffentlichen Dienstes, zu konzentrieren.

Der im Juli vorgelegte Entwurf sieht weiterhin auch die Liberalisierung bereits bestehender Telekommunikationsinfrastruktur Dritter zum 1. Januar 1996 vor. Dieser Punkt war von der Kommission in ihren Schlußfolgerungen aus der Konsultation zum Infrastruktur-Grünbuch noch offengelassen worden. Inzwischen hat sich jedoch gezeigt, daß die von der Kommission erhoffte Flexibilität bei der Behandlung von Einzelanträgen in den Mitgliedstaaten ausgeblieben ist, so daß ein Tätigwerden der Kommission erforderlich wurde.

Die Richtlinie zur Festlegung des gemeinschaftsrechtlichen Rahmens für das Zieldatum 1998 wird ebenfalls vor ihrer endgültigen Annahme durch die Kommission, die noch vor Ende dieses Jahres erfolgen soll, als Entwurf zur Konsultation publiziert werden.

Mit diesen Ergänzungen der Dienste-Richtlinie soll noch in diesem Jahr ein Koordinatensystem für die weitere Liberalisierung geschaffen werden, das dann durch nationale Gesetzgebung und ergänzende Harmonisierungsmaßnahmen auf Gemeinschaftsebene ausgefüllt werden kann.

2. Flankierende Maßnahmen

Die schrittweise Öffnung der Telekommunikationsmärkte in der Europäischen Union durch die vorgesehenen Ergänzungen der Dienste-Richtlinie wird von einer Reihe flankierender Maßnahmen auf Gemeinschaftsebene begleitet, die das Ziel haben, den Liberalisierungsprozeß abzustützen und unerwünschte Auswirkungen der Marktöffnung zu verhindern.

a) Universeller Dienst

Angesichts der ständig wachsenden Bedeutung des Zugangs zu Kommunikationsdiensten muß auch unter Wettbewerbsbedingungen sichergestellt sein, daß jeder Zugang zu einer Grundversorgung mit Telekommunikationsdiensten zu erschwinglichen Preisen erhält. In diesem Zusammenhang ist die Frage nach der Definition und der Finanzierung eines universellen Dienstes im Bereich der Telekommunikation von entscheidender Bedeutung.

Das Infrastruktur-Grünbuch geht davon aus, und diese Position wurde auch in der Konsultation bestätigt, daß zur Zeit der Sprachtelefondienst den Kern des universellen Dienstes bildet, sich die Anforderungen jedoch mit dem Herannahen der Informationsgesellschaft auch ändern können. Die Kommission hält jedoch in jedem Falle eine enge Definition des universellen Dienstes für erforderlich, um keine unüberwindbaren Marktzutrittsschranken für neu in den Markt eintretende Unternehmen zu schaffen.

Hinsichtlich der Finanzierung des universellen Dienstes sieht die im Entwurf vorgelegte Richtlinie zur Einführung vollständigen Wettbewerbs vor, daß grundsätzlich alle Marktteilnehmer, die öffentlichen Sprachtelefondienst oder öffentliche Telekommunikationsnetze betreiben, zur Finanzierung und Bereitstellung des universellen Dienstes herangezogen werden können. Die Kommission legt insbesondere Wert darauf, daß die Finanzierung transparent, nichtdiskriminierend und entsprechend dem Grundsatz der Verhältnismäßigkeit ausgestaltet wird.

Die Kosten der Universaldienstverpflichtung sollte auf der Grundlage der einem Betreiber durch die Erfüllung von Universaldienstverpflichtungen entstehenden Nettokosten, insbesondere für die Bereitstellung von Telefondiensten in nicht einträglichen Gebieten oder für wirtschaftlich nicht interessante Kunden in sonstigen Gebieten, berechnet werden. Es wird Aufgabe der nationalen Regulierungsbehörden sein, die geeigneten Verfahren hierfür zu entwickeln. Bei der Berechnung der Kosten des universellen Dienstes darf nicht vergessen werden, daß auch ertragsschwächere Kunden einen Wert für ein privatisiertes Telekommunikationsunternehmen haben. Es dürfen nicht nur die von einem Anschluß abgehenden Gespräche betrachtet werden, sondern es muß auch berücksichtigt werden, daß jeder Anschluß auch dadurch, daß er angerufen werden kann, zusätzlichen Verkehr erzeugt. So können auch solche Anschlüsse für einen Betreiber wirtschaftlich interessant sein, von denen aus nur wenige oder keine Anrufe getätigt werden.

Die aus den EG-Wettbewerbsregeln folgenden Grundsätze der Finanzierung des universellen Dienstes sind in dem Richtlinienentwurf zur Einführung vollständigen Wettbewerbs auf den Telekommunikationsmärkten konkretisiert. Der gemeinsam mit diesem Entwurf im Juli vorgelegte Vorschlag für eine ONP-Richtlinie über Zusammenschaltung legt darüber hinaus einen harmonisierten Rahmen für die Ausgestaltung der Finanzierungssysteme für den universellen Dienst in den Mitgliedstaaten fest.[18] Die Kommission prüft zur Zeit, ob darüber hinausgehende Maßnahmen im Bereich des universellen Dienstes auf Gemeinschaftsebene erforderlich sind, und wird Ende dieses Jahres oder Anfang des nächsten Jahres dazu in einer Mitteilung Stellung nehmen.

b) Zusammenschaltung und Interoperabilität

Ein weiteres Kernproblem im Zusammenhang mit der Liberalisierung ist die Regelung der Zusammenschaltung von Netzen und Diensten.

Während die vorgeschlagene Ergänzung der Dienste-Richtlinie zur Einführung vollen Wettbewerbs lediglich die wettbewerbsrechtlichen Grundsätze in bezug auf die Zusammenschaltung mit dem öffentlichen Telefonnetz der Telekommunikationsorganisationen spezifiziert, legt der bereits erwähnte Vorschlag für eine ONP-Richtlinie über Zusammenschaltung einen harmonisierten Rahmen für die auszuhandelnden Zusammenschaltungsbedingungen, die Entgelte sowie für die auf nationaler und europäischer Ebene zu schaffenden Schlichtungsmechanismen für öffentliche Telekommunikationsdienste und öffentliche Telekommunikationsnetze fest.

Nach der vorgeschlagenen ONP-Richtlinie sind die Grundsätze der Transparenz und Nichtdiskriminierung auf Zusammenschaltungsvereinbarungen anzuwenden. Grundsätzlich soll das Aushandeln der Zusammenschaltungsbedingungen jedoch Angelegenheit der betroffenen Unternehmen bleiben, wobei allerdings einige Bedingungen vorab von den nationalen Regulierungsbehörden festgelegt werden können.

Die vorgeschlagene ONP-Richtlinie wird das zentrale Element der spezifischen Regulierung im Bereich der Zusammenschaltung sein und einen der Kernpunkte der anstehenden ONP-Reform bilden. Allerdings kann eine solche ONP-Richtlinie die Anwendung

17 Entwurf – Richtlinie der Kommission zur Änderung der Richtlinie 90/388/EWG über die Einführung vollständigen Wettbewerbs auf dem Markt für Telekommunikationsdienste, ABl. Nr. C 263, 10. 10. 95, S. 6.

18 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Zusammenschaltung in der Telekommunikation zur Gewährleistung des Universaldienstes und der Interoperabilität durch Anwendung der Grundsätze für einen offenen Netzzugang (ONP), KOM (95) 379 endg., 19. 07. 95.

des EG-Wettbewerbsrechts nur ergänzen, aber keinesfalls ersetzen. Deshalb wird auch zu prüfen sein, inwieweit es notwendig ist, das Verhältnis von ONP-Vorschriften und EG-Wettbewerbsrecht im Bereich Zusammenschaltung und Zugangsbedingungen durch besondere Maßnahmen klarzustellen, um mögliche Mißverständnisse zu vermeiden. Gleichzeitig könnte dabei auch untersucht werden, inwieweit die Anwendung der Wettbewerbsregeln in diesem Bereich effizienter und einfacher gestaltet werden kann.

c) Lizenzierung

Die entscheidenden Fragen in diesem Bereich lauten: Wie werden Telekomnetze lizenziert? Welche Beschränkungen können im Hinblick auf die Zahl der zu erteilenden Lizenzen gerechtfertigt werden? Welche Lizenzbedingungen dürfen auferlegt werden?

Die Kommission vertritt die Auffassung, daß die Zahl der zu vergebenden Lizenzen für Infrastrukturanbieter und Diensteanbieter, und zwar einschließlich der Anbieter von Telefondiensten, nur aus Gründen, die mit grundlegenden Anforderungen gerechtfertigt werden können, eingeschränkt werden dürfen. Einschränkungen sind deshalb in erster Linie aus Gründen der Frequenzknappheit zulässig.

Hinsichtlich der Frage, welche Linzenzbedingungen Infrastrukturanbietern zulässigerweise auferlegt werden können, ist zwischen privater und öffentlicher Telekommunikationsinfrastruktur zu unterscheiden. Unter öffentlicher Telekommunikationsinfrastruktur ist in diesem Zusammenhang solche Infrastruktur zu verstehen, die für die Erbringung von Telekommunikationsdiensten für die Öffentlichkeit genutzt werden. Der Begriff der privaten Infrastruktur erfaßt dagegen solche Infrastruktur, die nicht für öffentliche Telekommunikationsdienste genutzt wird.

Im Fall von privater Telekommunikationsinfrastruktur sollten Bedingungen nur zum Schutz der Einhaltung der grundlegenden Anforderungen (wie etwa der Verfügbarkeit von Frequenzen) auferlegt werden dürfen. Bei öffentlicher Telekommunikationsinfrastruktur sollten zusätzlich noch Pflichten für die Erbringung öffentlicher Dienstleistungen in Form von gewerblichen Vorschriften, d. h. Regeln bezüglich der Qualität, Verfügbarkeit und Dauer von Telekommunikationsdiensten, die über lizenzierte Telekommunikationsinfrastruktur zur Verfügung gestellt werden, einbezogen werden können.

Sowohl hinsichtlich der Lizenzierungsverfahren als auch hinsichtlich der Lizenzierungsbedingungen ist die Einhaltung des Verhältnismäßigkeitsprinzips von entscheidender Bedeutung: Es muß vermieden werden, daß „mit Kanonen auf Spatzen geschossen" wird. Wenn mehrere wirksame Methoden zur Verfügung stehen, darf nur das den Lizenznehmer am wenigsten belastende Mittel gewählt werden. So sollte deshalb der Erteilung von Allgemeingenehmigungen oder „class licences" in allen Fällen der Vorzug gegeben werden, in denen eine individuelle Prüfung und Genehmigung eines Antrags nicht erforderlich ist.

Ähnlich wie für die Fragen der Finanzierung des universellen Dienstes und der Zusammenschaltung sind auch die für die Lizenzierung von Telekommunikationsnetzen und -diensten bestehenden Anforderungen des EG-Wettbewerbsrechts in den Entwürfen für eine Ergänzung der Dienste-Richtlinie im Bereich der Mobilkommunikation und im Hinblick auf die volle Liberalisierung präzisiert. Darüber hinaus wird die Kommission jedoch in Kürze noch einen Vorschlag für eine Richtlinie zur Harmonisierung der Lizenzierungsverfahren der Mitgliedstaaten vorlegen, der an die Stelle der beiden bereits vorgelegten Vorschläge zur gegenseitigen Anerkennung von Telekommunikations- und Satellitenlizenzen treten wird.[19]

19 ABl. Nr. C 36, 04. 02. 94; ABl. C 108, 16. 04. 94.

d) Wettbewerbspolitik

Die Wettbewerbsregeln des EG-Vertrages sind für die Schaffung eines neuen ordnungspolitischen Rahmens in mehrfacher Hinsicht von Bedeutung:

Zum einen sind sie ein zentrales Instrument zur Öffnung des Marktes für neue Teilnehmer. Die Kommission hat die Wettbewerbsregeln mit großem Erfolg zur schrittweisen Liberalisierung des Telekomsektors eingesetzt und wird jetzt die vollständige Öffnung des Telekommunikationssektors mit den vorgeschlagenen Ergänzungen der Dienste-Richtlinie auf der Grundlage der Wettbewerbsregeln vollenden.

Zum anderen gewinnen die Wettbewerbsregeln in einem liberalisierten Umfeld auch zunehmend an Bedeutung im Hinblick auf die Gewährleistung eines effektiven und fairen Wettbewerbs zwischen den Marktteilnehmern. Die weitere Öffnung des Telekommunikationssektors, aber auch die fortschreitende technische Entwicklung wird in den nächsten Jahren zu einer vollständigen Neustrukturierung der Märkte führen. Dieser Prozeß, der bereits begonnen hat, sich in den kommenden Jahren aber noch weiter verstärken wird, führt unvermeidbar dazu, daß die Wettbewerbsaufsicht auf nationaler Ebene, vor allem aber auch auf Gemeinschaftsebene stark an Gewicht gewinnen wird.

Ein Beispiel für diese Entwicklung ist die Bildung von strategischen Allianzen, die zunächst allein unter den traditionellen Telekommunikationsbetreibern geschlossen wurden (z. B. BT/MCI, Atlas, Phoenix, Unisource), heute aber zunehmend auch unter Beteiligung von neuen Marktteilnehmern geschlossen werden (Beispiele auf dem deutschen Markt sind VEBA/Cable and Wireless oder VIAG/BT). Eine erste Entscheidung der Kommission betreffend solche Allianzen erging im Hinblick auf die Kooperation zwischen BT und MCI, welche die Kommission im vergangenen Jahr unter Auflagen genehmigte.[20] Diese Entscheidung fiel vor dem Hintergrund der Tatsache, daß die Heimatmärkte der beiden Betreiber bereits weitgehend liberalisiert sind, und die Kooperation überdies auf eine Tätigkeit auf einem globalen Markt abzielt.

Die Bildung von Allianzen bleibt allerdings nicht auf Unternehmen aus dem Telekommunikationssektor beschränkt. Im Vorfeld der Informationsgesellschaft werden jetzt auch immer häufiger joint ventures mit Beteiligten aus anderen Sektoren der Informations- und Kommunikationsindustrie, wie etwa der Film- und Verlagsindustrie, aber auch Softwareunternehmen, gegründet, um auf den neu entstehenden Kommunikationsmärkten tätig zu werden. In den vergangenen Monaten mußte die Kommission auf der Grundlage der Fusionskontrollverordnung zwei solcher joint ventures untersagen. Im vergangenen Jahr untersagte die Kommission in der Sache Mediaservice GmbH das geplante joint venture zwischen Deutscher Telekom, Bertelsmann und der Kirch-Gruppe, da es die marktbeherrschende Stellung der beteiligten Unternehmen in den gerade erst entstehenden pay-TV-Markt hinein verlängert hätte.[21] Im Juli untersagte die Kommission die Gründung des joint ventures Nordic Satellite Distribution (NSD) zwischen Norsk Telekom, TeleDanmark und Kinnevik, insbesondere da dieses joint venture den beteiligten Unternehmen eine Marktstellung verschafft hätte, die es ihnen ermöglicht hätte, den skandinavischen Markt für Satellitenfernsehen gegen Mitbewerber abzuschotten.[22] Die bisher getroffenen Entscheidungen liefern erste Elemente für die Entwicklung klarer Maßstäbe zur kartellrechtlichen Beurteilung solcher Kooperation. Eine Reihe weiterer Fälle wird jedoch noch zu prüfen sein, bevor ein klares Bild entstehen kann.

20 Entscheidung vom 27. 07. 1994, ABl. Nr. L 223, 27. 08. 94, S. 36.
21 Entscheidung vom 9. November 1994, ABl. Nr. L 364, 31. 12. 94, S. 1.
22 Pressemitteilung IP/95/801, 19. 07. 95.

Ein weiterer Bereich, der die Kommission auch in Zukunft beschäftigen wird, ist die wettbewerbsrechtliche Mißbrauchsaufsicht über marktbeherrschende Unternehmen im Telekommunikationssektor. Trotz der vollständigen Liberalisierung des Sektors bis zum Jahre 1998 werden die traditionellen Telekommunikationsbetreiber noch lange über diesen Zeitpunkt hinaus eine marktbeherrschende Stellung auf zahlreichen Märkten des Telekommunikationssektors haben. Es besteht die Gefahr, daß mit dem zunehmenden Wettbewerb auch die Versuchung wächst, diese Marktposition zu mißbrauchen. Die Kommission wird darüber wachen müssen, daß die Telekommunikationsbetreiber dieser Versuchung nicht erliegen.

Die zunehmende Zahl von Einzelfällen wird nur bei einer engen und effizienten Zusammenarbeit zwischen Kommission und nationalen Wettbewerbsbehörden sowie zwischen Kommission und nationalen Telekommunikationsregulierungsbehörden, aber auch der nationalen Wettbewerbs- und Telekommunikationsregulierungsbehörden untereinander zu bewältigen sein.

e) Datenschutz

Auch die Gewährleistung eines hinreichenden Schutzniveaus in bezug auf persönliche Daten und die Privatsphäre ist eine wesentliche Rahmenbedingung für den Übergang in die europäische Informationsgesellschaft. Nur wenn ein ausreichender Datenschutz sichergestellt ist und die Benutzer nicht befürchten müssen, daß ihre persönliche Daten mißbraucht werden könnten, werden die neuen Informations- und Kommunikationsdienste die Akzeptanz der Verbraucher finden.

Nachdem die allgemeine Richtlinie des Europäischen Parlaments und des Rates zum Datenschutz am 24. Juli im Grundsatz angenommen wurde, ist jetzt der Weg frei für die Beratung der bereichsspezifischen Datenschutz-Richtlinie für Telekommunikationsnetze und -dienste, für die die Kommission im vergangenen Jahr einen geänderten Vorschlag vorgelegt hat,[23] durch den EG-Ministerrat. Diese Richtlinie geht allerdings noch vom Fortbestehen besonderer und ausschließlicher Rechte der Telekommunikationsorganisationen aus und muß deshalb im Rahmen des weiteren Rechtsetzungsverfahrens an die Bedingungen einer vollständigen Liberalisierung angepaßt werden.

f) Die internationale Dimension: Wie kann Europa vergleichbaren und effektiven Zugang zu globalen Märkten sichern?

Im Rahmen der Welthandelsorganisation haben inzwischen die Verhandlungen über eine Liberalisierung der sogenannten Basistelekommunikationsdienste (u. a. Telefondienst, Datendienste, einfacher Wiederverkauf von Übertragungskapazität) begonnen.

Die politische Entscheidung des Rates vom 17. November 1994, die ordnungspolitisch eindeutigen Positionen des Infrastruktur-Grünbuchs sowie die jetzt vorliegenden Richtlinienentwürfe setzen für die Handelspartner der Europäischen Union klare Signale der Entschlossenheit zur konsequenten Liberalisierung. Damit wird die europäische Verhandlungsposition in internationalen Verhandlungen, insbesondere im Rahmen von WTO/GATS, erleichtert. Auch die Forderung nach einem chancengleichen Zugang europäischer Unternehmen zum US-amerikanischen Markt gewinnt vor dem Hintergrund eines festen Liberalisierungsfahrplans für die Union an Gewicht.

23 Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetze (ISDN) und digitalen Mobilfunknetzen, KOM (94) 128 endg., 13. 06. 94.

g) Die soziale und beschäftigungspolitische Dimension

Der sozialen und beschäftigungspolitischen Dimension der Vorbereitung auf die Informationsgesellschaft hat die Kommission im zweiten Teil ihres Infrastruktur-Grünbuchs breiten Raum gewidmet. Nach Auffassung der Kommission dürfen die Beschäftigungswirkungen der Liberalisierung nicht isoliert im Telekommunikationssektor betrachtet werden. Das entscheidende und übergeordnete Argument für die Liberalisierung der Telekommunikation ist, daß sie zu einer größeren Effizienz im Informationssektor im allgemeinen und zu einer wichtigen Standortverbesserung für die europäische Wirtschaft insgesamt führt. Sie soll damit einen wichtigen Beitrag zum Kampf gegen die Arbeitslosigkeit in allen Bereichen der europäischen Industrie leisten. Im Grünbuch wird aber zugleich hervorgehoben, daß die ordnungspolitische Reform von Maßnahmen auf Gemeinschaftsebene, vor allem aber auch auf Ebene der Mitgliedstaaten, etwa in den Bereichen, Aus-, Fort- und Weiterbildung, begleitet sein muß, die den Strukturwandel abstützen.

III. Maßnahmen der Kommission in anderen Bereichen

Auch wenn die Telekommunikationspolitik zur Zeit im Mittelpunkt der Initiative der Kommission zur Informationsgesellschaft steht, ergreift die Kommission jedoch auch in anderen Bereichen Maßnahmen zur Vorbereitung eines neuen ordnungspolitischen Rahmens im Hinblick auf die entstehende Informationsgesellschaft. Ich möchte hier nur auf zwei weitere Bereiche kurz hinweisen: den Urheberrechtsschutz und die audiovisuellen Medien.

1. Urheberrechtsschutz

Urheberrechte sind durch neue Technologien und insbesondere die Digitalisierung künftig bisher unbekannten Gefährdungen ausgesetzt. Ein wirksamer Urheberrechtsschutz ist jedoch andererseits eine der Grundbedingungen dafür, daß Informationsinhalte für die neue Dienstleistungen auf dem elektronischen Superhighway zur Verfügung gestellt werden.

Die Kommission hat die Problematik jetzt in einem Grünbuch zu „Urheberrecht und verwandten Schutzrechten in der Informationsgesellschaft“ aufbereitet, das am 19. Juli 1995 vorgelegt wurde.[24] Das Grünbuch enthält einen umfassenden Fragenkatalog, über den die interessierten Kreise konsultiert werden. Auf der Grundlage dieser Konsultation wird die Kommission dann über ihr künftiges Arbeitsprogramm in diesem Bereich entscheiden.

2. audiovisuelle Medien

Auch im Bereich der audiovisuellen Medien hat die Gemeinschaft wichtige ordnungspolitische Bausteine für einen neuen Regulierungsrahmen vorgelegt. So hat die Kommission im März einen Vorschlag zur Reform der Richtlinie „Fernsehen ohne Grenzen“ vorgelegt,[25] mit der einige strittige Fragen geklärt werden sollen und insbesondere das Teleshopping weitgehend liberalisiert wird. Andere fortgeschrittene audiovisuelle Dienste sind jedoch ausdrücklich ausgeklammert worden. Sie sollen zum Gegenstand eines Grünbuchs über neue audiovisuelle Dienste gemacht werden, das die Kommission im kommenden Jahr vorlegen wird.

24 KOM (95) 382, 19. 07. 95.
25 KOM (95) 86, 22. 03. 95.

IV. Schlußbemerkung

Das Leben in den Industriegesellschaften wird durch neue digitale Informations- und Kommunikationsmöglichkeiten künftig stark geprägt werden. Ihre Einführung in Europa eröffnet nach der Überzeugung der Kommission die Chance zur Erreichung zahlreicher positiver Effekte, die weit über die genannten Sektoren hinausreichen.

Die ordnungspolitischen Initiativen der Gemeinschaft zielen darauf ab, diese Chance zu nutzen und das Entstehen eines neuen dynamischen Wirtschaftszweigs in Europa kontrolliert zu ermöglichen.

Marcel Haag, Europäische Kommission, Generaldirektion IV – Wettbewerb, Abteilung „Telekommunikation, Koordinierung Informationsgesellschaft".

Informationssicherheit für Multimedia Collaboration

Dr. Wolfgang Klasen

1 Einführung

Die aktuellen Entwicklungen in der Telekommunikation sind gekennzeichnet durch eine zunehmende Integration verschiedener Netztechnologien wie etwa Telefon- und Computernetze und Medien wie Text, Graphik, Audio und Video. Dabei ist die Gewährleistung von Informationssicherheit („IT-Sicherheit", „Security") sowohl für die Anbieter von Telekommunikationsdiensten oder Netzen, als auch für den Kunden ein wichtiges Qualitätsmerkmal. Unter IT-Sicherheit verstehen wir in diesem Kontext den Schutz gegen absichtliche Angriffe, die verarbeitete Informationswerte bedrohen. Abhängig von der Rolle innerhalb einer bestimmten Kommunikations- und Dienstleistungsbeziehung stehen dabei verschiedene Sicherheitsbedürfnisse im Vordergrund. So ist es zum Beispiel für den Anbieter eines Telekommunikationsdienstes von Interesse, daß der Dienst nur durch Berechtigte benutzt und diese Benutzung nachprüfbar belegt und abgerechnet werden kann. Für den Kunden zählt ebenfalls die korrekte Abrechnung; zusätzlich stellen die Aspekte Datenschutz und Verläßlichkeit im Sinne von Vertraulichkeit und Integrität ein vitales Interesse dar, d. h. der Dienst soll genau die vorgegebenen Aktionen ausführen und keine anderen oder zusätzlichen.

Das Querschnittsthema „IT-Sicherheit" spielt in den meisten Ausprägungen von Multimediaanwendungen eine wichtige Rolle. Dabei sind Mechanismen und Funktionen zur Informationssicherheit ein wesentliches Werkzeug zur technischen Durchsetzung von Datenschutzbelangen und bilden damit eine Voraussetzung für die Funktionsfähigkeit der Informationsgesellschaft. Oft ist die Bereitstellung bestimmter Sicherheitsdienste sogar eine Voraussetzung für den erfolgreichen kommerziellen Einsatz von Multimediaanwendungen, wie etwa die Forderung nach einer effizienten und betrugssicheren Abrechnung von Video on Demand-Diensten (VoD) zeigt.

In verschiedenen Standardisierungsgremien werden seit geraumer Zeit allgemeingültige Klassifikationsregeln und Bewertungskriterien für den Einsatz (kryptographischer) Sicherheitsfunktionen in der Informationstechnik erarbeitet. Das Ziel ist sowohl die Gewährleistung sicherer Interoperabilität (ISO OSI) als auch eine funktionale und qualitative Überprüfbarkeit der eingesetzten Sicherheitsdienste (ITSEC). Prinzipiell kann lediglich ein relativer Schutz gegen Bedrohungen der Informationssicherheit eingebracht werden, 100%ige Sicherheit ist nicht realisierbar. Im Rahmen einer Risikoanalyse werden dazu Aufwand und Nutzen von Sicherheitsmaßnahmen gegenübergestellt und die Erfordernisse identifiziert. Dabei muß für einen potentiellen Angreifer der Aufwand für eine Attacke stets weitaus höher sein als der erwartete Nutzen.

2 Anforderungen an MM-Sicherheit (Überblick)

Durch das Zusammenwirken verschiedener Übertragungsmedien und Darstellungstechniken werden komplexe Anforderungen an die Sicherheitsarchitekturen gestellt, deren Lösungen jedoch in vielen Fällen aus bereits bekannten Basisfunktionen generiert wer-

den können. So geht die digitale Integration einer Vielzahl von Dienstangeboten in Telekommunikationsnetzen mit der zügigen Standardisierung kryptographisch unterstützter Abrechnungs- und Zugriffskontrolldienste einher (DAVIC, DVB, . . .). Bedarf an neuen Sicherheitskonzepten entsteht zum Beispiel im Rahmen computerunterstützter kooperativer Arbeit (CSCW): beim gemeinsamen Benutzen traditioneller Anwendungen können hier lokal existierende Schutzmechanismen außer Kraft gesetzt werden, da die Aktionen einzelner Konferenzteilnehmer nicht mehr individuell zugeordnet werden können.

Unter dem Aspekt der Integration in Multimediaanwendungen ergeben sich einige typische Anforderungen an Funktionen für Informationssicherheit:

Multimedia-Sicherheitsdienste

- Authentifikations- und Abrechnungsdienste:

  Wie bei allen Value-Added-Services ist auch bei Multimediadiensten zu Abrechnungszwecken eine Zugriffskontrolle und dadurch auch eine Benutzerauthentifikation notwendig. Im Rahmen von Broadcast-Multimediadiensten wie Video on Demand werden neue Konzepte federführend entwickelt und eingesetzt. Andere wichtige Anwendungsfelder für eine sichere Gebührenerfassung sind Multimedia-Datenbanken und -Archive.

- Performante kryptographische Mechanismen und Algorithmen:

  Insbesondere bei synchronen Anwendungen erfordert der hohe Datendurchsatz eine performante Realisierung kryptographischer Verfahren. So benötigt eine sichere Breitbandkommunikation hochperformante Hardware zur schnellen Verschlüsselung, bei einigen Anwendungen ist zusätzlich die Fähigkeit zum häufigen Schlüsselwechsel erforderlich („key-agility“). Für Softwarelösungen werden geeignete Kompromisse zwischen der zu erzielenden Sicherheit und dem geforderten Durchsatz angestrebt. Zum Beispiel wird untersucht, in welchen Fällen eine Teilverschlüsselung von Audio-Video-Daten ausreicht.

- Copyright Protection:

  Viele Multimediaanwendungen erfordern neue Konzepte und Mechanismen für die Wahrung von Urheberrechten. Ein Beispiel dafür ist der Schutz von auf CD-ROM gespeicherten Informationen (Software, Verlagspublikationen, . . .) gegen Mißbrauch und Kopierbetrug. Hier können kryptographisch unterstützte Freischaltungsmechanismen angewendet werden. Die leichte Wiederverwertbarkeit digitaler Dokumente macht zusätzliche Mechanismen erforderlich. So sind in MM-Datenbanken oder auf CD-ROMs digitalisierte Einzeldokumente schnell zugänglich und können leicht weiterverarbeitet werden. Die Identität des ursprünglichen Dokumentenherausgebers muß daher „möglichst untrennbar“ mit dem ursprünglichen Dokument verbunden werden, um später finanzielle Forderungen rechtlich durchsetzen zu können („Digitales Wasserzeichen“).

- Digitale Signaturen in Multimediaanwendungen:

  Digitale Signaturen spielen eine zentrale Rolle für die Bereitstellung sicherer und verläßlicher Dienste. Sie garantieren den Schutz vor unbemerkter Manipulation beim Datentransport und sind häufig wichtiger Bestandteil „kryptographisch sicherer“ Produkte. Es existieren verschiedene, teilweise bereits standardisierte kryptographische Mechanismen zur Realisierung einer digitalen Signatur. (Als Beispiel für ein Softwareprodukt zur Realisierung verbindlicher Datenkommunikation unter MS-Windows sei SICRYPT®SIDEX von SNI genannt.)

- Gruppenbasierte Sicherheitsarchitekturen:

  Die traditionelle Punkt-zu-Punkt-Kommunikation wird durch allgemeinere gruppenbasierte Modelle abgelöst; dadurch werden neben einem „sicheren Multicasting“ Erweiterungen von Managementfunktionen erforderlich. Zu nennen sind hier die gruppenbasierte Authentifikation und Zugangskontrolle oder die Notwendigkeit eines gruppenorientierten Key-Managements.

- Hierarchische Zugriffskontrolle:

  Zugriffskontrollmechanismen müssen skalierbar und abgestuft eingesetzt werden können. So ist es zum Beispiel bei Audio-Video-Verteildiensten erwünscht, potentiellen Benutzern einen zeitlich oder qualitativ begrenzten Zugang zum Produkt zu ermöglichen, um so „Appetit“ auf diese Leistungen zu erzeugen. Diese Anforderungen können durch den Einsatz neuer digitaler Kryptomechanismen oder durch organisatorische Maßnahmen erfüllt werden.

- Key-Management Infrastruktur / Zertifizierungs- und Directory-Dienste:

  Kryptographische Sicherheitsfunktionen für Kommunikationsanwendungen stützen sich auf die (gelegentliche) Verteilung von Zertifikaten und geheimen Schlüsseln („Key-Management“). Die Schaffung einer unterstützenden Infrastruktur garantiert den Anwendern einen leichten Zugang zum erforderlichen Adress- und Schlüsselmaterial. Entsprechende Vorarbeiten sind von Standardisierungsgremien wie ITU, ISO oder ETSI bereits geleistet (z. B. X.509-Authentifikationsstandard). Wer in welchen Ländern Zertifizierungs- und Directory-Dienste bereitstellen wird ist noch unklar.

Für die produktmäßige Integration von Informationssicherheit in Multimediaanwendungen und Kommunikationsdienste gelten einige wichtige Randbedingungen:

Integrationsaufgaben

- Benutzerfreundlichkeit:

  Sicherheitsfunktionen sollen möglichst wenige und übersichtliche Benutzeraktionen erfordern; sie müssen auch für Laien anwendbar sein; nur durch hohe Bediensicherheit und Durchschaubarkeit der Aktionen (z. B. beim Anwenden einer digitalen Signatur) kann die erforderliche Benutzerakzeptanz erreicht werden;

- Konsistentes Sicherheitsniveau:

  Kommunikation zwischen unterschiedlichen Sicherheitsdomänen muß möglich sein; ebenso ist ein sicheres Interworking verschiedender Anwendungen und Dienste zu gewährleisten; die Beherrschbarkeit unterschiedlicher Kommunikationsplattformen ist sicherzustellen;

- Skalierbarkeit und Wirtschaftlichkeit:

  Die Lösungen müssen differenzierten Sicherheitsanforderungen genügen und in preiswerten, auf den Bedarf des Kunden abgestimmten Modulen angeboten werden; eine Verwendung von möglichst generischen Mechanismen ist anzustreben um eine vielseitige Einsetzbarkeit zu erreichen.

Sicherheitsniveau

Die Güte eines Sicherheitsdienstes, die dem Benutzer einer Multimediaanwendung zur Verfügung steht, wird prinzipiell von der schwächsten Einzelkomponente bestimmt, die an der Diensteerbringung beteiligt ist, d. h. von der Stelle, die nach dem „Prinzip des schwächsten Gliedes einer Kette“ von einem potentiellen Angreifer am ehesten überwunden werden kann. Um das dem Benutzer verfügbare Sicherheitsniveau einer komplexen Multimediaanwendung festlegen zu können, müssen sowohl die verschiedenen funktionalen Einzelkomponenten als auch deren Zusammenwirken analysiert werden. Den identifizierten Bedrohungen der Informationssicherheit werden dann Sicherheitsmaßnahmen gegenübergestellt, die in ihrer Gesamtheit eine Sicherheitsarchitektur definieren. In den deutschen IT-Sicherheitskriterien wurden für die Stärke von Sicherheitsmaßnahmen im Sinne ihrer Überwindbarkeit fünf verschiedene Stufen definiert[1]:

Schutzmaßnahmen der Stufe „nicht überwindbar“ sind extrem wirksam gegen gezielte Angriffe und mit den zur Zeit vorhandenen Methoden nicht zu brechen. „Sehr starke“ Maßnahmen sind sehr gut wirksam gegen gezielte Angriffe und nur mit sehr hohem Aufwand zu brechen.

„Starke“ Maßnahmen sind gut wirksam gegen gezielte Angriffe und mit hohem Aufwand zu brechen. „Mittelstarke“ Maßnahmen sind wirksam gegen gezielte Angriffe und mit mittelhohem Aufwand zu brechen. „Schwache“ Maßnahmen sind lediglich wirksam gegen unbeabsichtigte Verstöße, nicht aber gegen gezielte Angriffe.

Wenn man davon ausgeht, daß in Zukunft die Attraktivität von Angriffen gegen die Informationssicherheit mit kriminellem Hintergrund steigen wird, und wenn man den rasanten Anstieg der allgemein verfügbaren Rechnerleistung in Betracht zieht, dann hat die Wirkung einer „starken“ Maßnahme sicherlich nur zeitlich begrenzten Charakter. Eine

1 vgl. „IT Sicherheitskriterien“, Zentralstelle für Sicherheit in der Informationstechnik, Bonn 1989

tragfähige Sicherheitsarchitektur für Multimediadienste und -anwendungen muß also mindestens durch „sehr starke“ Maßnahmen geprägt sein. Die Realisierung „sehr starker“ und „nicht überwindbarer“ Maßnahmen kann durch kryptographische Verfahren mit entsprechend langer „Lebensdauer“ erfolgen. Für den „Multimedia Collaboration Teledienst“ der DeTeBerkom wird bei Siemens eine nach diesen Prinzipien gestaltete Sicherheitsarchitektur entworfen die im folgenden kurz erläutert werden soll.

3 Das Beispiel „Sicherheit für Multimedia Collaboration – MMCSec“

Unter „Multimedia Collaboration“ – kurz MMC – versteht man die informationstechnische Unterstützung verteilter Arbeitsgruppen unter Einbeziehung von Audio-, Video- und Datenkommunikation. Die Kommunikation findet dabei „synchron“ statt, d. h. es geht um gleichzeitiges Arbeiten an verschiedenen Orten. Die zusammenarbeitenden Personen haben dabei die Möglichkeit, im Rahmen einer Videokonferenz auf eine Rechneranwendung gemeinsam zuzugreifen, um so zum Beispiel einen Bericht zu erstellen, einen Konstruktionsplan zu bearbeiten oder Kalkulationen durchzuführen.

Die Vorteile dieser Systeme liegen zum einen in der Ersparnis von Zeit und Reisekosten, zum anderen befindet sich jedes Konferenzmitglied in seiner gewohnten Arbeitsumgebung mit dem entsprechenden Zugriff auf die eigenen Ressourcen.

Einzelne Anforderungen an die Informationssicherheit von MMC-Systemen ergeben sich zwangsläufig, wenn man die üblichen „Regeln“ einer klassischen Besprechungssituation analysiert und anschließend im virtuellen, elektronisch realisierten Sitzungsraum die gewohnten Kontrollmechanismen durch technische Funktionen ersetzt. So muß der vertrauliche Charakter eines geschlossenen Besprechungszimmers innerhalb einer verteilten Multimediaanwendung durch Mechanismen für Zugangskontrolle und Verschlüsselung nachgebildet werden. Dabei können kryptographische Integritätsmechanismen die Korrektheit und Authentizität von Adressinformationen und Daten garantieren. Es können so Angriffe abgewehrt werden, die durch gezieltes Vortäuschen einer falschen Identität (z. B. Absenderadresse) nichtkryptographische Sicherheitsmechanismen überwinden oder etwa unbemerkt auf der Übertragungsstrecke digitalisierte Nachrichteninhalte ändern.

Durch die unterschiedliche Rollenzuweisung der Teilnehmer einer Konferenz können sogenannte „Insiderbedrohungen“ entstehen: zum Beispiel hat der Besitzer einer Applikation, die mit den anderen Partnern geteilt wird, ein vitales Interesse daran, daß er den Zugriff seiner Kommunikationspartner auf seine eigenen Systemressourcen, die über die geteilte Applikation erfolgen könnte, kontrollieren kann. Sind mehr als zwei „Endsysteme“ an einer Multimediakonferenz beteiligt, dann können durch die unterschiedlichen Möglichkeiten von Rollenzuweisungen innerhalb der Konferenz Interessengruppen entstehen, deren Zusammensetzung zeitlich variabel sein kann: Beispiele für Rollen innerhalb einer Konferenz sind:

> Reguläres Konferenzmitglied, Konferenzadministrator, Initiator einer Konferenz/ Sitzung, Besitzer der geteilten Applikation, Gast, Third Party bzw. Trusted Third Party.

Insiderbedrohungen können durch dynamische, kryptographisch unterstützte Zugangskontrollmechanismen wirksam begegnet werden, wobei die verschiedenen Interessengruppen mit Hilfe des Key-Managements wirksam separiert werden müssen.

Basierend auf einer Bedrohungsanalyse wurde für den Berkom Multimedia-Collaboration-Service eine generische Sicherheitsarchitektur entwickelt. Durch die angedachte Dienstegranularität können MMC-Kontrollprotokolle, Shared Applications und Audio-Video-Daten je nach erforderlicher Sicherheitspolitik differenziert gegen Bedrohungen geschützt werden. Die Sicherheitsdienste sollen bezogen auf eine Benutzergruppe fest vorgewählt, beim Aufbau der Gruppenbeziehung ausgehandelt oder innerhalb einer Sitzung vom Benutzer in Abstimmung mit den Kommunikationspartnern dynamisch konfiguriert werden können. Dabei berücksichtigen das Key-Management und die Sicherheitsdienste die speziellen Erfordernisse der Gruppenkommunikation wie „Insiderbedrohungen“, „Gruppenbasierte Authentifikation“, „Sicheres Multicasting“ und anderes mehr.

Die Systemarchitektur faßt sicherheitsspezifische Protokoll- und Datenelemente wie etwa Kryptoalgorithmen und Key-Management zu einem universellen Sicherheitssubsystem zusammen. Bei Siemens ZFE wird dieses Sicherheitssubsystem als hardwarebasierter Sicherheitsserver implementiert. Einerseits können somit hochperformante Verschlüsselungsdienste für sensible Datenströme unterstützt werden, andererseits wird eine auf Krypto-Hardware basierte Kontrolle über das Key-Management und die damit verbundenen Sicherheitsdienste realisiert.

4 Ausblick

Kooperative Multimediaanwendungen erfordern zunehmend komplexere Konzepte zur Kommunikationssicherheit. Im Handel erhältliche Produkte beschränken sich meist auf die Unterstützung von Punkt-zu-Punkt-Kommunikation, d. h. sind für die Kommunikation zwischen zwei Partnern ausgelegt, und weisen oft keine ausreichenden Sicherheitsfunktionen auf. Für die allernächste Zukunft ist die Etablierung von Standardwerkzeugen für computergestützte Gruppenarbeit in heterogenen Netzen zu erwarten. Hier entstehen durch die verteilte Systemarchitektur im besonderen Maße Gefahren für die Vertraulichkeit und Integrität der Daten sowie für die Verfügbarkeit der angeschlossenen Systeme. Durch kryptographische Sicherheitsfunktionen können diese Gefahren abgewehrt und kooperierende Systeme und Netze geschützt werden. Neben umfassenden Authentifikations- und Zugangskontrollmechanismen werden dabei sichere und schnelle Übertragungsmechanismen für Text-, Graphik-, Audio- und Videoinformation zum Einsatz kommen.

Die rasche Integration von Sicherheitsdiensten als Standardfunktionalität in Kommunikationsanwendungen erfordert eine umfassende Infrastruktur für Key-Management und Zertifizierung. Auch hier entscheidet nicht zuletzt der Kunde: durch sein gestiegenes Sicherheitsbewußtsein sind gute Voraussetzungen für die Akzeptanz sicherer Lösungen gegeben.

Hier folgen 18 Seiten Film!

Erfahrungen aus dem Pilotprojekt „Interaktive Videodienste“ in Berlin

Dr. Siegfried Hermann – Deutsche Telekom AG, Dir Potsdam/Dir Berlin

Pilotprojekt Interaktive Videodienste Berlin

1. Ziele der Pilotprojekte
2. Dienstebeschreibung
3. Übersicht der Elemente
4. Versorgungsbereich des Pilotprojekts
5. Gesamtarchitektur
6. Systemübersicht
7. Blockschaltbild Server und Vermittlung
8. Struktur des Echtzeit Encoders
9. Technische Daten des Echtzeit Encoders
10. Blockschaltbild der Übertragungstechnik in der Zentrale
11. Teilnehmereinrichtung
12. Diensteanbieter (4 Blatt)
13. Position der DTAG zum Datenschutz
14. Grundsätze der DTAG zum Datenschutz bei Multimedia (1)
15. Grundsätze der DTAG zum Datenschutz bei Multimedia (2)
16. Öffentlich zugängliche Terminals (1)
17. Öffentlich zugängliche Terminals (2)

Hier folgen 20 Seiten Film!

Programmanbieter im Berliner Pilotprojekt
Interaktive Videodienste

1. Digital-TV

1.1 Kostenfrei
- Deutsche Welle TV
- Landscape Channel
- European Bussiness News (EBN)
- n-tv
- Südwest 3
- Panoramablick auf Berlin (Live-Kamera) SFB

1.2 Pay per Channel
- Cartoon Channel
- Sophisticated music

1.3 Pay per view
- ORB (Ostdeutsche Rundfunk Brandenburg)
  (Chronik der Wende)

2. Top-Filme

(Near Video on demand)
- RTL
- PRO 7
- SFB
- SDR

jeweils 4 Filme im Zeitraster von 15 Minuten blockierungsfrei für alle Teilnehmer (8 NVOD-Module)

3. Video on demand

Kategorien
- Spielfilme
- Kinderprogramm
- Magazine / Talkshows
- Quiz / Unterhaltung
- Dokumentarfilme

als Programmveranstalter sind beteiligt: RTL, PRO 7, SFB, SDR, ORB

4. Pay-Radio
- DMX bieter über Satellit DMX Konverter/Audiocoder mehr als 50 Musikfarben, die über zwei Audioausgänge der Set Top Box zur Stereoanlage des Teilnehmers geführt werden.

5. Homeshopping
- Otto-Versand bietet 4 Produktgruppen:
  Damen, Wäsche, Herren, Heim/Haushalt.

  Teleshop hat 6 Produktgruppen mit insgesamt 48 Produkten im Angebot

  Bei beiden Anbietern ist die Bestellung über eine alphanumerische Eingabe (Adresse, Kunden-/Kreditkarten) möglich.

6. Gesundheitskanal
- Ferenczy Media präsentiert Gesundheitstips

7. Infodienste
- Bercos (Stadtinformationsdienste)
- Zweite Hand Verlags GmbH (Anzeigen)
- n-tv (Information on demand)
- tss Kommunikationstechnik / MIG
- BerlinInfo (Info Surf)

8. Homelearning
- FWU (Institut für Film und Bild in Wissenschaft und Unterricht)
  Lernwelt Television 2000

Autorenverzeichnis

Prof. Dr. Carl-Eugen Eberle,
Justitiar des Zweiten Deutschen Fernsehens

Dr. Hansjürgen Garstka,
Berliner Datenschutzbeauftragter

Marcel Haag,
Generaldirektion IV der Europäischen Kommission

Dr. Siegfried Hermann,
Deutsche Telekom AG, Berlin

Dr. Wolfgang Klasen,
SIEMENS AG, München

Prof. Dr. Joel Reidenberg,
Fordham University, School of Law, New York

Frank Stoll,
Institut für Informatik und Gesellschaft, Universität Freiburg