Symposium

Das Internet –
Ende des Datenschutzes?

The Internet –
Privacy at an End?

1. September 1997

Impressum

Herausgeber: Berliner Datenschutzbeauftragter
verantwortlich: Claudia Schmid
Pallasstraße 25/26, 078 Berlin
Telefon: (0 30) 78 76 88 44
Telefax: (0 30) 2 16 99 27

Internet http://www.datenschutz-berlin.de
E-Mail: mailbox@datenschutz-berlin.de

Redaktion,
Layout: Volker Brozio

Druck: Verwaltungsdruckerei Berlin

1. Auflage: August 1998

Inhaltsverzeichnis

Vorwort

Während das Internet ursprünglich überwiegend dem Informationsaustausch im Wissenschaftsbereich diente, wird es heute zunehmend auch für kommerzielle Zwecke genutzt. Die Datenübermittlung gerade auch personenbezogener Daten gilt jedoch nach wie vor als höchst unsicher: Elektronisch unverschlüsselt versandte Informationen können abgefangen, mitgelesen, gespeichert und verfälscht werden, ohne daß der Absender dies bemerkt. Kreditkartennummern können von Dritten für betrügerische Zwecke genutzt werden. Der Kunde im globalen virtuellen Kaufhaus ist bisher gezwungen, sehr viel mehr Spuren zu hinterlassen als in einem realen Kaufhaus.

Wie regelmäßig anläßlich der Internationalen Funkausstellung in Berlin hat der Berliner Datenschutzbeauftragte auch 1997 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 1. September 1997 beim Symposium „Das Internet – Ende des Datenschutzes?“ gehalten wurden.

Die verschiedenen Beiträge stellen einerseits die vielfältigen Probleme für die Privatsphäre dar, die mit der Nutzung des Internet verbunden sind; andererseits werden verschiedene nationale und internationale Regulierungsansätze zur Sicherung der Privatsphäre bei der Nutzung von modernen Kommunikationsdiensten beschrieben.

Mein Dank für die fruchtbare Zusammenarbeit beim Symposium 1997 gilt wiederum allen, die an der Vorbereitung und Durchführung der Veranstaltung beteiligt waren.

Hansjürgen Garstka

Berliner Datenschutzbeauftragter

Eröffnungsansprache zum Symposium Das Internet - Ende des Datenschutzes? beim Internationalen Mediendialog Internationale Funkausstellung Berlin

Hansjürgen Garstka

Sehr geehrte Damen und Herren,

Ich begrüße Sie herzlich zum siebten Datenschutzsymposium, das der Berliner Datenschutzbeauftragte seit 1985 im Rahmen der Internationalen Funkausstellung in Berlin durchführt.

Als wir vor eineinhalb Jahren begannen, die Thematik dieses Symposiums zu planen, war uns zwar klar, daß die Wahrung der Persönlichkeitsrechte in globalen Netzen eines der großen Themen der nächsten Jahre werden würde. Welche Aktualität das Thema aber genau zum jetzigen Zeitpunkt haben würde, konnte von uns nicht geahnt werden.

Seither sind weltweit die Telekommunikationsnetze explosionsartig gewachsen, das Internet und andere Träger von Telekommunikationsdiensten werden inzwischen von Hunderten von Millionen Menschen genutzt. Dienste wie E-mail, WorldWide-Web oder Newsgroups sind nicht mehr Spielwiese von Studenten, Wissenschaftlern oder Technofreaks. Vielmehr zählen sie inzwischen auch zum jederzeit präsenten Kommunikationsmedium in Wirtschaft und – wenn auch zu Recht zögernd – öffentlicher Verwaltung. Das Zusammenwachsen von Telekommunikationsnetzen und Fernsehtechnik, wie es ja als eines der Hauptneuerungen auf dieser Funkausstellung demonstriert wird, wird die Dienste an die Wohnzimmersofas heranführen und ihnen auch diejenigen Bevölkerungsschichten erschließen, die bislang große Teile ihrer Freizeit dem Hin- und Herzappen zwischen mehr oder weniger erhebenden Fernsehsendungen verbrachten.

In eigenartigem Gegensatz zu der Euphorie bei der Nutzung der Neuen Medien steht die Sorglosigkeit, mit der die meisten Beteiligten über die Konsequenzen für ihre Persönlichkeitsrechte hinweggehen.

Kaum jemand, der E-mail nutzt, macht sich Gedanken darüber, daß an einer Vielzahl von Stellen, über die die Informationen ihren Weg nehmen, die Nachricht abgefangen und gespeichert, inhaltlich verändert, ja umgeleitet werden kann. Kaum jemand, der sich über WWW-Hyperlinks durch alle Sexangebote dieser Welt hangelt, ist besorgt, daß irgendwo ein Catcher sein könnte, der sein Verhalten genau aufzeichnet. Wer mag darüber nachdenken, daß sein elektronisches Geschwätz einmal gegen ihn verwandt werden könnte? All dies ist möglich, und, so hört man von vielen Seiten, auch durchaus Praxis. Interessenten für das Verfolgen von Kommunikationsspuren und -inhalten finden sich zuhauf.

Am harmlosesten natürlich ist zunächst pure Neugier: Das beginnt bei Web- und Postmasters, die nicht nur die Inanspruchnahme der Dienste mitverfolgen, sondern auch protokollieren, wer wann welche Informationen abgerufen hat. Es liegt auf der Hand, daß aus mit statistischem Interesse begründeter Neugier schnell Verhaltenskontrolle werden kann.

Schon beeinträchtigender sind die Eingriffe derjenigen, die die bei der Nutzung entstandenen Daten für wirtschaftliche Zwecke nutzen wollen: Betriebsorganisation, Netzoptimierung, Eigenwerbung, schließlich Fremdwerbung, Kommerzialisierung der Verkehrsdaten für unkontrollierbare Zwecke. Hier entsteht die Begierde nach der Erstellung von Persönlichkeitsprofilen, die schon von jeher im Datenschutz als die Ursünde betrachtet wurden: Das Zusammenführen von Daten über die verschiedensten Lebensbereiche mit dem Ziel, den Menschen für die eigenen – lauteren oder unlauteren – Zwecke transparent zu machen. Daß die so nützlichen Suchmaschinen im Internet hier ihre häßliche Seite zeigen, wird uns morgen auf der Tagung des Internationalen Arbeitskreises Datenschutz bei der Telekommunikation beschäftigen, deren Teilnehmer ich bei dieser Gelegenheit im Publikum begrüßen möchte.

Schließlich das kriminelle Interesse: Wirtschaftsspionage, die geschädigten Unternehmen schon Milliardenverlust gebracht hat; der Versuch, Ausgangsmaterial für Erpressungen jeder Art zu erlangen; die Erschleichung von Informationen, beginnend mit der Kreditkartennummer, zur Begehung von Betrügereien jeder Art.

Häufig können diejenigen, die Zugang zu den Daten haben, diese nicht nur zur Kenntnis nehmen, sondern sie auch manipulieren. Die Lösung dieses Problems ist nicht nur unabdingbare Voraussetzung für die Nutzung der Netze für Electronic Commerce, wie Bankgeschäfte und Vertragsabwicklung, oder nichtkommerzielle vertrauensabhängige Dienste wie Telemedizin.

Sie ist auch die Voraussetzung dafür, daß die virtuelle Welt der Telekommunikation die reale Welt adäquat abbildet: Vor zwei Jahren haben wir an dieser Stelle die Probleme der „Plastizität“ der virtuellen Information bei Multimedia-Diensten diskutiert.

Ist damit das Ende des Datenschutzes im globalen Netz gekommen? Der Titel unserer Veranstaltung endet mit einem Fragezeichen – um das wir im übrigen im Laufe der Herstellung der verschiedenen Prospekte heftig kämpfen mußten.

Die Antwort auf diese Frage ist ganz offensichtlich davon abhängig, in welchem Umfang die Nutzung der Telekommunikationsnetze – und zwar sowohl hinsichtlich der Verkehrs- als auch hinsichtlich der Inhaltsdaten – vor dem Zugriff Dritter verborgen werden kann.

Drei Lösungswege sehe ich:

- Priorität vor allem hat die anonyme Nutzung: Wer sich dem System gegenüber nicht zu identifizieren hat, muß keine Folgen befürchten. Der Kauf der Zeitung am Kiosk (in einer fremden Umgebung), das Telefonat in der Telefonzelle, die Internetnutzung von einem öffentlichen Internetzugang aus hinterlassen zwar möglicherweise Spuren von Inhalten, aber keine der Nutzer. Das vor einigen Tagen in Kraft getretene deutsche Teledienstegesetz schreibt ebenso wie der entsprechende Staatsvertrag für die Mediendienste vor, daß derartige anonyme Nutzungsmöglichkeiten angeboten werden müssen. Die auf dieser Funkausstellung propagierte d-Box für den Empfang digitaler Fernsehsendungen weist nach allen Informationen eine derartige Funktion nicht auf – ein Verstoß gegen dieses gesetzliche Gebot, wenn nicht entsprechend nachgerüstet wird. Auch werden sich viele Internetanbieter daran gewöhnen müssen, daß die bislang weitgehend sorglose Protokollierung der Abfragen künftig nicht mehr möglich ist.
- Die pseudonyme Nutzung verschafft Vorteile der Anonymität in den Fällen, in denen eine anonyme Nutzung nicht möglich ist. Allerdings setzt sie einen Makler voraus, der die Zuordnung zwischen Pseudonym und echtem Namen herstellt; dieser setzt sich dem Angriff (oder Anreiz) interessierter Dritter aus.

- Die Verschlüsselung setzt nicht am Teilnehmer, sondern am Inhalt an: Nicht die Kommunikationspartner bleiben geheim (wenn sie sich nicht der obigen Methoden bedienen), sondern die Nachrichten selbst. Die dafür zur Verfügung stehenden Instrumente sind so mächtig, daß sie mehrere Funktionen auf einmal erfüllen: Vertraulichkeit, Authentizität der Kommunikationspartner, Authentizität der Informationsinhalte, ohne die globale Kommunikation zu beeinträchtigen.

Diese Wege setzen das Engagement beider Seiten voraus: der Anbieter von Netz- und Dienstleistungen, aber auch der Teilnehmer. Ich betrachte es als Anliegen dieses Symposiums, alle Beteiligten zu diesem Engagement aufzurufen.

Ein besonderes Problem wirft die Frage auf, welche Eingriffsrechte den staatlichen Ermittlungsbehörden gegenüber dem Geschehen im Netz zustehen sollen. Niemand bestreitet, daß Telekommunikation zur Begehung von Straftaten genutzt werden kann – sei es durch Nutzung des Netzes als Hilfsmittel, sei es, daß das Netz selbst zum Gegenstand der Straftat wird – und daß Straftaten angemessen verfolgt werden müssen. Deshalb richtet sich das Interesse der Strafverfolgungsbehörden wohl von Anfang an darauf, Umstände und Inhalt von Telekommunikation nachvollziehen zu können. Das POT, das Pretty Old Telephone, ist Al Capone bereits zum Verhängnis geworden, als er leichtfertig nicht etwa über seine Morde, wohl aber über steuerlich relevante Sachverhalte geplaudert hat. Auch der berühmte Berliner Erpresser Dagobert ist aufgrund von Verbindungsdaten, die von der belgischen Telefongesellschaft aus einer Telefonzelle aufgezeichnet worden waren, gefaßt worden. Jüngst erst gelang es an einer Berliner Hochschule, aufgrund der – staatsanwaltschaftlich genehmigten – Protokollierung der Inanspruchnahme eines Internetservers sowie der ausgetauschten Informationen den Datenaustausch von strafbarer Kinderpornografie nachzuweisen.

Die Grenzfläche zwischen menschenrechtlich gesicherter Privatheit der Kommunikation und dem Gefahrenabwehr- und Strafverfolgungsinteresse des Staates gehört, wenn ich recht sehe, nicht nur in unserem Staat, sondern weltweit, zu den derzeit am heftigsten diskutierten Themen der Rechtspolitik.

Nicht nur meine, sondern die Position vieler an der Wahrung der Grundrechte Interessierter ist, daß auch vor dem Hintergrund der Möglichkeiten der modernen Informationsgesellschaft dem Menschenrecht auf unbeobachtete Kommunikation kategoriale Bedeutung zukommt. Ich meine damit nicht nur, daß ein Kernbestand an Lebensbereichen übrig bleiben muß, die dem Zugriff jeder Instanz, auch des strafenden Staates entzogen sein müssen – die Rettung von Menschenleben mag eine Ausnahme bilden. Die in unserem Staat anscheinend bevorstehende Niederreißung eines solchen Bereiches durch die verfassungsmäßige Verankerung des „Großen Lauschangriffs“ zeigt, daß dies angesichts der herrschenden politischen Situation nicht mehr wahrgenommen wird.

Vielmehr müssen die technischen und organisatorischen Grundbedingungen der künftigen globalen Telekommunikationsstruktur so ausgestaltet sein, daß der Zugriff Interessierter dadurch verhindert wird, daß er keinen Ertrag mehr bringt. Dies schließt es aus, daß bei der Gestaltung von Netzen und Diensten von vornherein dienstefremde Interessen mit eingebaut werden. Ich meine dies sowohl im Hinblick auf „betriebsbedingte Interessen“ der Betreiber als auch im Hinblick auf Interessen der Sicherheitsbehörden.

Ich bin davon überzeugt, daß es hierfür geeignete Architekturen und Instrumente gibt. Wir wollen hierzu unseren Anteil leisten – unser Symposium möge hierzu beitragen.

Privacy on the Internet: Everyone a Data Protection Officer? Keynote Presentation

Alan F. Westin

Introduction

It has been said that a keynote speech should have the same relationship to the conference as the fan does to the fan dancer of earlier strip-tease days. That is, it should go before the subject and stir audience interest but it should not try to cover the subject completely.

In that spirit, let me try to stir your interest in today's proceedings by exploring four main themes:

1. **How should we think about the Internet as a new medium, and how do privacy issues here compare with our experiences with and the dynamics of privacy in the hard-copy, off-line worlds?**
2. **Who are today's Internet users, and what does survey research in 1997 tell us about the experiences, concerns, and attitudes of U.S. Net users about online communication, commerce, and privacy?**
3. **What is government doing in the United States to examine these online privacy issues, and what effects are these activities having?**
4. **What are the possible roles of individual Net users in asserting their own privacy boundaries, and is it possible that the Net may turn out to be the most individually-responsive privacy medium in history?**

Now, to stir your interest...

1. How should we think about the Internet as a new medium, and how do privacy issues here compare with our experiences with and the dynamics of privacy in the hard-copy, off-line worlds?

The Internet now reaches well over 100 nations, and has somewhere between 50-75 million global users (depending on whose estimates you are most comfortable with). There are over 16 million hosts, of which four million are commercial sites.

A current story in the U.S. illustrates how pervasive the Internet is becoming. A third grade geography teacher asked her class what the capital of the nation was. „Washington, D.C." one student volunteered. „Good," said the teacher, „and who knows what 'D.C.' stands for?" Another student quickly responded: „I know – dot com."

So how should we understand this increasingly pervasive activity in many organizational and personal lives, particularly in the advanced-technology democracies?

The Internet, it seems to me, should be recognized as an explosive new medium where the full array of human conduct plays out, and all the traditional tensions in democratic society over individual privacy, public disclosure, and society-protecting surveillance will have to be confronted in new settings.

- As a powerful new electronic medium, the Internet is reshaping patterns of communication, information exchanges, and – potentially – commerce. It has become a mass media preoccupation, and virtually everyone agrees that Internet development holds enormous potential for new and creative social, business, and political activity.
- But the Internet also replicates all the vices and pathologies of contemporary society, from consumer fraud and intrusive advertising to circulation of hate speech, soliciting obscene materials, promoting terrorist projects, and criminally stalking children and women. As in the earliest frontier days in America, the Internet abounds with modern day cattlemen, sheep-herders, farmers, saloon keepers, whores, and hacker-gunmen, with the influences of the schoolmarm, minister, sheriff, and judge also struggling to be heard and felt.
- The online and Net worlds also reproduce all the basic tensions about individual privacy, public disclosure, and society-protecting surveillance that democratic societies struggle with in the off-line world with new dangers and new opportunities just coming into focus.

With this general perspective, let me turn to a dose look at the Internet world and the privacy risks and opportunities it is generating.

2. Who are today's Internet users, and what does survey research in 1997 tell us about the experiences, concerns, and attitudes of U.S. Net users about online communication, commerce, and privacy?

In the Spring of 1997, Privacy & American Business commissioned Louis Harris & Associates to conduct the first statistically representative survey of the 42 million adult Americans (18 and older) currently using the Internet. The survey provided four U.S. populations for analysis and comparisons:

- total adult computer users (about 100 million);
- computer users on the Internet (about 42 million);
- computer users with online services but not on the Internet (about 28 million); and
- computer users not yet online or using the Net (about 49 million).

The survey report (written by Louis Harris, with an Interpretive Essay by myself) also compared the orientations of these four populations to the results on privacy-trend questions of the total U.S. adult public (about 190 million), based on 1995 and 1996 Harris-Westin privacy surveys.

First, who are the Computer users, both on and not yet on the Net?

- Demographically, Computer users are younger, have more education, and higher incomes than the general public. Net users are even younger, more affluent, and better educated than Computer users not on the Net.
- Computer users as a group, and the Net and Online user sub-groups, share overall business-privacy concerns at the same high levels as the general public. In 1995, 80 % of the total public felt that „Consumers have lost all control over how personal information about them is collected and used by companies." An identical 80 % of computer users agreed with this statement in 1997, with 82 % of Net users agreeing.
- On the other hand, Computer users are less fearful of technology than the general public. Where 63 % of the general public agreed in 1995 that „technology is almost out of control," only 55 % of 1997 computer users and 36 % of Net users shared that view.

- Computer and Net users are less distrustful of institutions (measured by the Harris-Westin Distrust Index) than the general public. Where the general public registered 71 % in High and Medium distrust in 1995, only 60 % of Computer users in 1997 registered such distrust, with Net users at 56 %.
- In another important overall comparison, U.S. Computer users and the general American public share a preference for voluntary over regulatory policies to protect consumer privacy. If businesses and industry associations adopt good privacy protection policies, 72 % of the general public said in 1995 they would prefer that approach; in 1997, 70 % of computer users and 72 % of Net users agreed with that view of voluntary being preferable to regulatory as a general matter. (However, as noted below, thc U.S. public often favors sector-specific legislation, when it feels problems are outpacing voluntary efforts.)
- Only 5 % of Net users and 7 % of Online-Service users say they have personally been the victim of what they thought was an invasion of their privacy. Receiving unwanted email advertising and having personal information required or captured at web sites were the intrusions most complained of. This is a low level of direct invasion when compared to the 25 % of the public that reported in 1995 that they have had their privacy invaded in thc off-line world, and 35 % is some particular consumer-information sectors.
- Moving from experiences to perceptions, online and Net users expressed a wide range of concerns over threats to the privacy and security of their activities online. Specifically:
  - 53 % of Net users and 57 % of Online-Service users say they are concerned that information about which sites they visit will be linked to their e-mail address and disclosed to some other person or organization without their knowledge or Consent. Not surprisingly, 55 % of Net users say the ability to choose not to give their real name is important to them in using the Internet.
  - 59 % of Net users who send and receive e-mail are concerned that the contents of what they communicate will be obtained by some Person or organization without their knowledge or consent.
  - 42 % of those receiving unsolicited e-mail advertising say „it's getting to be a real pain“ and want „to stop getting these messages.“ If there were a procedure for removing their e-mail addresses from unsolicited advertising, over a third (37 %) of e-mail users would want their names removed from all solicitations. (This compares with only 17 % of Computer users who would remove their names from all regular postal mailings.)
  - 75 % feel there are privacy problems in putting state and local government's public records with personally-identified information on the Internet , even though these are available today to anyone in manual form and organizations can buy computer tapes of such records for business, legal, and research purposes.
- Computer users divide about equally on whether there is a significant difference between collecting marketing information from children in the off-line and online worlds. But, many practices generally accepted in marketing to children in the off-line world are strongly rejected for online conduct. When asked to assume that the purpose for gathering the information cited was the only use that a company would make of various types of information about children presented in a series of questions, majorities of computer users rejected the acceptability of all the types of uses presented.

- 59 % of computer users say it is not acceptable to ask children for e-mail addresses for the purpose of gathering statistics on site visiting, and 58 % oppose asking for such addresses to improve a business's product.
- 73 % of computer users say it is not acceptable to obtain the real names and addresses of children when they register to use a site, or to purchase products.
- And, 90 % say it is not acceptable (74 % „not at all acceptable“) for companies to rent or sell the real names and addresses of their child registrants or customers to third parties for marketing.
- 75 % of computer users are NOT confident that companies on the net that are marketing to children would follow the policies they set forth on how they would handle the childrens information they collect.

  Reflecting these privacy concerns, especially where the potential safety of children are involved, a majority of Computer users say they favor legal action.
- 94 % of Computer users say that companies collecting information from children should he held legally liable for violations of their stated policies.
- When asked which of three roles „government“ should take in approaching „Internet privacy issues,“ a majority of all Computer users – at 58 % – favor „passing laws NOW for how personal information can he collected and used on the Internet.“ 24 % favor government recommending standards but not passing laws now, and 15 % say government should „let groups develop voluntary privacy standards but not take any action now unless real problems arise.“ However, only 47 % of Net users favor enacting government laws now, while those Computer users not using the Net or an online service favored government laws at 65 %.
- It should be noted that the question on government approaches came at the end of a detailed survey exploring potential threats to privacy and security, and especially after the series on children's privacy issues. Also to be noted is that the question did not specify whether state or federal governments should be the rule setters; just what kind of controls government would set, how these would be monitored, and which government agency would act as the enforcing agent; and what kinds of penalties and remedies would be installed. We can expect that the attitudes of computer users and especially Net users would be significantly affected by the alternatives presented on those matters.

  In comparative terms, it is useful to note that the views of computer users overall, and online and Net users specifically, generally follow the patterns that past privacy surveys have found to operate as driving factors in the off-line world.
- Past Harris-Westin surveys have found that two-thirds majorities of the American public (and computer users as a sub-group) oppose creation of a federal regulatory agency covering the entire private sector (as in the European data protection commissions' model). But strong majorities will favor sector-specific legislation at the state or federal levels when the perception is that serious breaches of privacy and confidentiality are taking place and voluntary controls by industry or private groups are either ineffective or not adopted widely enough. Examples have included legislation that would forbid employers or health insurers to use genetic tests for employment or underwriting purposes, and federal laws protecting privacy and confidentiality of medical records and the increased electronic movement of personally identified health information. Computer-user support for „government“ action on the Net suggests that the Net is seen as a „sector“ in which voluntary policies are not yet perceived as present.

- In past privacy surveys, trust in the practices of an industry in handling its customers' personal information in a „proper" or „responsible" way and „respecting its confidentiality" came through as a major factor in helping the majority of the public (our 55 % „Privacy Pragmatists") to decide whether to give their personal information for organizational uses under privacy-policy promises or whether they would favor passing legislation to mandate the rules. In the 1997 online privacy survey, with ten industries that handle consumer information presented for judgment, a majority of respondents gave high ratings (in the 68-80 % ranges) to employers, hospitals, banks, and Companies making Computer hardware and software. But online companies – those offering Online Services, direct Internet access, and marketing products on the Net–- received low confidence ratings, in the low 40 % levels. This placed them alongside credit bureaus and direct-mail marketers, two groups that have traditionally received low-confidence ratings in privacy surveys.
- The answers to most of the key questions relating to privacy concerns and policy preferences in our 1997 survey followed exactly the level of confidence in the three online businesses – the lower the confidence in online firms, the more privacy-oriented the positions. This was true, for example, with all the questions involving children's privacy; concern about the confidentiality of e-mail content; concern about putting public records on the Net; desire to remove their e-mail address from all unsolicited marketing; and support for passing government laws now on Internet privacy.

  Since 70 % of U.S. Computer users generally favor voluntary policies over legislative rules for consumer privacy protection, the explanations for a majority of total Computer users favoring government action now for the Internet he in a combination of factors (in addition to the effects of low confidence in online companies):
- There has been a steady drumbeat of largely alarming stories in both the mass and online/computer media about privacy and security risks on the Internet. These often present the situation as one in which no current tools or policies are available to protect users, and that staying off the Net, not using one's credit card for purchases, and never volunteering personal information are the sensible ways to proceed. Along with movies and TV programs depicting hackers and privacy invaders trolling the Net and finding helpless victims, the media coverage has sent a message to many millions of viewers and readers that Orwells progeny own the online world.
- Industry association policies and guidelines for collecting and using consumer information online and on the Net are in a very early stage of roll out. Most of them were developed in 1996, and the most important ones are 1997 products, some just issued in late May or early June, and some to be presented at the Federal Trade Commission's Workshop on Consumer Privacy Online in mid-June. These include policies from the Direct Marketing Association, the Interactive Services Association, and others it is highly doubtful that respondents to our survey in April of 1997 had heard about these, or had any experiences with them with which to decide how well they worked.
- The survey recorded remarkably low awareness by online service subscribers of the information-handling policies of their current service provider. Almost three out of four online service users (71 % plus 3 % don't know) said they were not aware of „any rules or policies [that their] online service has as to how it will use the information it maintains or collects about [their] online usage . . ."

- A series of questions about how web site visitors decide whether to give registration-type information when they visit sites documented that most web site visitors are NOT today encountering dear, up-front declarations of information policy from most sites they visit. Net users say getting such information would have a major effect on their decisions whether to provide personal information, but 79 % say they have declined to give information to sites not explaining their policies, and 8 % say they have given false information.
- There was also very low awareness of software tools for exercising individual control over information and communication practices.
  - 75 % of e-mail users said they weren't aware of any procedure or technique to remove their e-mail address from companies or organizations sending them advertising materials.
  - 45 % of parents with children using the Net said they were not aware of any software programs that let parents automatically limit the web sites their children visit or the personal information they can provide to sites.

It is also dear that very few members of the computer-using public have yet heard about new control approaches such as the e-Trust information labeling and independent- certification system for designating commercial web sites, or the privacy policies and preferences program being developed by the Center for Democracy and Technology, with strong business and public-interest group support.

Finally, strong interest was expressed by the privacy-concerned respondents in getting free and easy-to-use software tools that would allow them to state their preferences as to how they would wish their personal information to be used by business or organizational web sites, and even to conduct dialogues with such sites over just how such uses could be made acceptable. Similar strong interest was expressed by parents in getting and using software that would allow them to control what personal information their children could give to Internet sites or in chat rooms.

What are the implications of these survey results and their underlying explanations for the online and Internet industries, businesses marketing online, technologists, public-interest groups, government bodies, and individual online users.

Some surveys record confusion and indecision on the part of the public on controversial issues, or such low levels of knowledge or interest that the results offer little help to the public policy-making process. This survey, I believe, is just the opposite. It offers a dear call to all the communities sharing responsibility for the unique entity that is the Internet to hear and respond effectively to the concerns of Net and online users (and also computer users not yet online) that communication, information-exchange, and consumer commerce must be made more privacy-secure than either perception or reality make it today.

The results are certainly a summons to intensified action by the online and Internet industries and all companies hoping to create broad commerce on the Net. These groups must move guidelines and policies from paper to the daily online world. They must also give strong support to the development, distribution, and effectiveness-testing of personal privacy-enhancing tools: such as personal-information-control software tools; digital signatures and biometric identifiers to assure more secure personal identification; and easy-to-use encryption programs.

The low confidence that the survey results registered in the trustworthiness of online companies means that online business groups will have to engage in major educational and verification programs to demonstrate that the policies and tools they support do provide an effective platform for reasonable online privacy.

If – as this survey documents–- the growth of Internet use and especially Internet communication and commerce depend on increasing user confidence in the medium's ability to provide reasonable privacy protection, there is cause for careful optimism. When a mass market and a major societal resource of the scope of the Internet depends as much as users say it will on providing consumer and citizen confidence, the stake for business and government in making that happen is enormous.

3. What is government doing in the United States to examine these online privacy issues, and what effects are these activities having?

Clearly, government leaders in the U.S. are concerned about and intend to be active in examining online and Internet privacy issues.

Executive Branch Actions

At the Executive Branch level, the Federal Trade Commission held two important workshops in June of 1996 and 1997 examining the collection and uses of personal information in cyberspace. Several dozen witnesses appeared at each workshop–- from business and industry associations, the online technology communities, consumer and privacy advocates, and legal experts. And, the full array of online privacy issues were examined–- unsolicited advertising (spamming), online „lookup" Services offering location information on individuals, „cookie" technology for identifying and tagging visitors to web sites, harvesting the comments of participants in forums, collection and uses of information from children on the Net, the status of filtering tools and other personal control mechanisms for users, identification „marks" attesting to information collection practices of a web site, etc.

At both of its workshops, the FTC concluded that there were serious privacy issues that needed immediate attention, especially in light of the Louis Harris-*Privacy & American Business* survey findings of computer-user concerns reported at the 1997 hearing. But the FTC endorsed the development of voluntary standards by industry and wide dissemination of personal-control software as the measures to be taken now. However, the FTC emphasized that its legal authority covering deceptive practices would enable it to prosecute any organization that violated the online information policies that it advertised to online visitors or customers, as well as the power to endorse industry-developed privacy policies and immunize such industry enforcement from threats of anti-trust violation.

Another highly active executive agency, the National Telecommunications and Information Administration (NTIA), in the U.S. Department of Commerce, sponsored the production and has just published a collection of analyses on the uses, advantages, and problems with self-regulation in cyberspace. The report, Privacy and Self-Regulation in the Information Age, offers a sophisticated set of commentaries ranging across the ideological spectrum, and is a valuable addition to the U.S. dialogues on how to approach setting privacy standards in the online environments.

As for the Clinton Administration itself, the President, Vice President Gore, and several Cabinet Secretaries held a White House event in July announcing and endorsing a report on Electronic Commerce by Presidential Assistant Ira Magaziner. In its section of privacy, the Magaziner Report emphasized that assuring the proper handling of personal information online was both a policy requirement and a necessary condition for the growth of electronic commerce. In this area, the Administration believes, given the rapidly-changing nature of online development and the need to balance privacy interests with free speech and consumer-choice values, „the private

sector must lead." But the Clinton Administration said that government would watch closely for concrete progress, and would not hesitate to step in if voluntary efforts and technology tools were insufficient.

The Congressional Scene

Bills have been introduced in Congress to address half a dozen key online privacy issues – from spamming and junk email controls and protection against release of personal public-record information on the Internet to requirements for adult consent before information about children is gathered online. While Congressional committee hearings have been held on some of these issues, experts believe that only the childrens privacy bills have any serious prospects for floor action and enactment in the 1997-98 period.

What effects have these Executive and Congressional actions had so far? Actually, they have spurred considerable activity. First, they have fed the U.S. mass media, and provided the raw material for widespread public education on threats to privacy and possible responses in the online world, as well as giving consumer, privacy, and children's rights advocates an important platform for their positions. Second, they have energized businesses and industry groups to address the development and promulgation of voluntary actions, from Privacy Notices on Web Site Home Pages to detailed industry codes for online marketing. Third, they have prompted substantial funds being committed and a rising customer market for technology tools such as parental controls, information filters, and special „trust marks" to assure individuals (with third party verification processes) of how their personal information will be used if they visit or patronize businesses online.

Most important, these government steps and solid survey research findings have served notice on business and industry leaders that there will be no substantial use of electronic commerce by American online consumers if reliable and effective privacy policies are not enunciated and implemented. In a market economy, that claim on management attention has extraordinary force, and is already fueling serious business actions.

4. What are the possible roles of individual Net users in asserting their own privacy boundaries, and is it possible that the Net may turn out to be the most individually-responsive privacy medium in history?

Even though consumers have ultimate veto power over online economic activity, we might be pessimistic about the future of privacy in cyberspace were it not for the fortunate simultaneous arrival of what have come to be called „privacy-enhancing technologies." These include easy-to- use encryption software; the personal-control and parental-control software already mentioned; anonymous payment mechanisms (draw-down money cards, electronic purses, third-party payment systems, etc.); biometric identifiers for secure confidential transactions; and a wide variety of techniques for preserving anonymous communications and transactions online.

The fact that there are already both market-incentives and positive market responses for such personal-privacy technologies is a dramatic new development in information-technology and society relations since World War Two. Until now, virtually all inventions and applications supported organizational interests and enhanced organizational power, at the expense of „data subjects". Now, however, assuming that public demand, market incentives, and legal rules all are promoted to support individual-choice approaches online, there are good possibilities that a new balance of

information power can be achieved in the 21st century. We can envisage a situation in which every person signing onto the Internet will, in effect, be sitting at the control panel, indeed, serving as their own Data Protection Commissioner in cyberspace.

Conclusions

I began by saying that the Internet world is reproducing and will continue to reproduce all of the tensions among personal privacy, public disclosure, and protective surveillance that democracies face in the off-line world. Calling privacy a „human right“ and creating regulatory structures does not eliminate the hard choices that the enhanced communication and commercial opportunities of the Internet bring.

What makes me optimistic is that there seems to be such a firm sense among Computer users in the US and elsewhere that informational privacy must be addressed, and that individual notice-and-choice is the core principle to pursue.

It will take much passionate advocacy, collection of „horror stories“ and „cautionary tales“, and assembling of empirical experience with both voluntary and regulatory approaches if privacy values are to be installed in cyberspace. But, this is not beyond either the creative competence or the societal power of privacy supporters, and this meeting can help to start the process of finding our way.

Das Internet – ein „Datenschleppnetz“ für Personendaten?

The Internet – a Fishing Net for Personal Data?

Peter L. Heinzmann

Zusammenfassung

Das Internet wurde als „offenes Netz“ konzipiert. Eine Kontrolle oder Überwachung der Inhalte bzw. der übertragenen Informationen ist nicht denkbar. Man sollte sich ferner im klaren sein, daß in der gegenwärtigen Form Sender- und Empfängeradressen gefälscht werden können. Dasselbe gilt für die übertragenen Informationen.

Im vorliegenden Bericht werden technische Möglichkeiten aufgezeigt, welche in bezug auf Personendaten von Bedeutung sind. Es wird illustriert, wo und auf welche Art Informationen zugegriffen werden kann. Dabei zeigt es sich, daß in den meisten Fällen von unerwünschtem Zugriff auf Personendaten Unvorsichtigkeit oder klares Fehlverhalten vorliegt.

Einleitung

Welche Daten werden weshalb gesammelt?

Personenbezogene Daten, wie

- Einzelangaben über persönliche oder sachliche Verhältnisse,
- Persönlichkeitsprofile, soziale Beziehungen, Verhaltensweisen

lassen sich im Internet direkt oder indirekt über öffentliche oder geheime Datensätze (Paßwörter) gewinnen.

Als Zweck der Datensammlung ist an erster Stelle die Direktwerbung (1:1 Marketing, Bulk E-mail) zu nennen. Personenbezogene Daten fallen aber auch im Rahmen der Überwachung unberechtigter oder ungeeigneter, nicht sachgemäßer Systemnutzung an (Überwachung durch Rechenzentren bzw. Systemadministratoren). Wie bei allen Sicherheitsproblemen in Computersystemen sind auch beim Sammeln von Personendaten persönliche Profilierung oder technischer Spieltrieb mögliche Gründe. Schließlich kann auch Erpressung bzw. kriminelle Absicht als Motivation zum Datensammeln vorkommen.

Wo können Daten gesammelt werden?

Daten durchlaufen im Internet eine Vielzahl von Zwischenstellen bzw. „neuralgischen Punkten“ vom Kunden bis hin zum Endrechner (vgl. Figur 1).

Allerdings ist der eigentliche Übertragungsweg in der Regel nicht die heikelste Stelle. Bedeutend gezielter kann man Daten beim WWW-Server, beim daran angeschlossenen Rechner bzw. bei der Anwendung, oder beim Kundenrechner sammeln. Eine kritische Stelle ist ferner der Internet-Zugangsanbieter (Internet Service Access Provider, ISP), da dort eine genaue Identifikation des Kunden möglich ist. Schließlich sei erwähnt, daß man für eine gezielte Informationsbeschaffung häufig einfacher die „Umgebung“ anspricht (social engineering), d. h. über konventionelle Kanäle attackiert.

Dem technischen Zugriff auf Personendaten ist dennoch Beachtung zu schenken, da er automatisiert und daher in großem Stil eingesetzt werden kann (vgl. auch Data Mining). Im folgenden werden die „neuralgischen Punkte“ zur „technischen“ Datensammlung diskutiert.

Internet-Zugangsanbieter (Internet Service Provider, ISP)

Internet-Zugangsanbieter (Internet Service Provider, ISP) sind für die Verbindung zum Internet besorgt. Bei Privatanschlüssen ist der Internet-Zugangsanbieter eine Organisation, die man über Modemverbindungen erreicht. In Firmen wird der Internet-Zugang in der Regel durch die entsprechenden Rechenzentren betrieben und über die firmeneigenen Lokalnetze angeschlossen. Die wichtigsten Komponenten des Internet-Zugangssystems sind das Einwählsystem mit den Verrechnungsdaten (Accounting) und die verschiedenen Proxy-Systeme mit den zugehörigen Log-Daten (vgl. Figur 2).

Einwählsystem

Beim Einwählsystem wird normalerweise für Verrechnungszwecke die Nutzungszeit und Telefonnummer bzw. Benutzeridentifikation erfaßt (Accounting-Daten). Diese Daten sind in entsprechenden „Log-Files“ abgespeichert. Korreliert man diese Informationen mit den Adressen, welche in jedem Datenpaket enthalten sein müssen, so können Nutzungprofile Personen zugeordnet werden.

Proxy-Server

Beim Internet-Zugang gibt es in der Regel sogenannte Proxy-Rechner. Proxy-Rechner verhalten sich als Stellvertreter für andere Rechner auf dem Internet.

WWW-Proxies speichern beispielsweise Kopien bereits einmal abgefragter WWW-Seiten. Anfragen für WWW-Seiten werden zuerst an den Proxy-Rechner geschickt. Im Proxy wird kontrolliert, ob sich die entsprechende Seite bereits im Speicher befindet und in der Zwischenzeit nicht verändert hat. Ist das der Fall, so wird die Seite nicht vom Originalrechner, sondern nur vom Proxy zum Kunden übertragen, was sich positiv auf die Antwortzeiten auswirkt. Bei diesem Vorgehen kann aber auch aufgezeichnet werden, welche Kundenrechner in welchem Zeitpunkt welche WWW-Seiten anfordern. So kann beispielsweise in einem Rechenzentrum überwacht werden, ob „nicht-arbeitsrelevante“ Seiten während der Arbeitszeit abgerufen werden. Oder ein ISP kann das Nutzungsprofil seiner Kunden erfassen. Diese Daten sind in sogenannten „Log-Files“ gespeichert. Typische Resultate des Proxy-Systems sind Listen der am häufigsten abgefragten WWW-Seiten.

Neben den WWW-Proxies gibt es auch News-Proxies, welche den Newsgruppenverkehr bearbeiten. Weitere Proxy-Systeme sind in Zusammenhang mit Zugriffsschutz oder E-mail anzutreffen.

Verhalten der Zugangsanbieter

Internet-Service-Provider sind mit Telefongesellschaften vergleichbar. Wie die Telefongesellschaften, so haben auch die meisten ISP gelernt, mit den personenbezogenen Daten richtig umzugehen. Allerdings sind sie exponierter für allfällige Zugriffsversuche auf die „Log-Dateien“.

Es ist denkbar, daß ISP in Zusammenhang mit Strafverfolgung gezwungen werden könnten, Daten zu sammeln und weiterzugeben. Auch hier dürfte man sich an die Regelungen im Bereich der Telefonie anlehnen.

Rechenzentren können die Log-Dateien zur Überwachung unberechtigter oder ungeeigneter, nicht sachgemäßer Systemnutzung auswerten. Sie sind diesbezüglich mit einer neuen Fragestellung konfrontiert, was die Behandlung der personenbezogenen Daten anbelangt. Allerdings ist das Problem innerhalb der Firmen nicht neu, sondern vergleichbar mit der Behandlung personenbezogner Daten bei der Nutzung der privaten Telefonzentralen.

Übertragungsweg

Vom Datenproduzent (Server) zum Konsument (Client) durchlaufen die Datenpakete verschiedenste Abschnitte: Kabelsegmente, Vermittlungsrechner (Router), Zwischenrechner (Proxies). Figur 3 illustriert den Weg der Datenpakete von einem Rechner in Rapperswil zu einem Rechner in Berlin, wie er nach Eingabe des Befehls „traceroute“ auf einem Unix-System dargestellt wird.

Wie das Beispiel in Figur 3 zeigt, werden vom Interkantonalen Technikum Rapperswil (ITR) bis zur TU-Berlin 21 Zwischenstellen durchlaufen. Diese Zwischenstellen gehören verschiedenen Netzwerkanbietern. Im Prinzip könnten die Inhalte der Datenpakete bei all diesen Stellen untersucht oder aufgezeichnet werden, ähnlich wie man den Verkehr auf Telefonleitungen überwachen könnte. Der technische Aufwand, um an ganz bestimmte Daten zu gelangen, ist aber erheblich.

WWW-Server

Wie kommen Informationen auf WWW-Seiten

Anfang 1997 schätzte man, daß bei über 650 000 Organisationen WWW-Server vorhanden sind. Insgesamt dürften einige zig Millionen Informationsseiten auf WWW-Servern abgespeichert sein. Es ist sehr einfach, Informationen auf einem WWW-Server zu publizieren, und es existieren keine Kontrollen zur Überwachung der publizierten Inhalte bzw. Informationen.

Bei den WWW-Seiten unterscheidet man:

- statische WWW-Seiten, deren Inhalt einmal festgelegt und für längere Zeit fix ist;
- dynamische WWW-Seiten, deren Inhalt pro Abfrage oder in regelmäßigen Zeitabständen neu erstellt wird (z. B. aufgrund von Abfragen bei einer Datenbank oder Seiten, die den Zugriff auf Statistik/Log-Informationen ermöglichen);
- WWW-Seiten mit Eingabemöglichkeiten (Formulare, Guest-Books, Fragebogen . . .)
- WWW-Seiten mit Programmen: z. B. Java-Applets, welche beim Seitenaufruf zum Kunden übertragen und ausgeführt werden.

Die riesige Zahl von WWW-Seiten stellt eine Unmenge von Informationen verschiedenster Ausprägungen dar. Seien es Kopien oder Zitate von Zeitungsberichten, allgemeine Informationen zu Dingen oder Personen oder gar sehr spezifische Angaben.

WWW-Seiten werden normalerweise bewußt erstellt.

Vielfach werden aber auch relativ unbedacht Informationen an WWW-Server übergeben. Die WWW-Browser können zwar ein Warnfenster erscheinen lassen, welches darauf aufmerksam macht, daß nun Daten preisgegeben werden, aber häufig werden solche Warnungen nicht beachtet oder gar ausgeschaltet. In Zusammenhang mit unbedachten Eingaben sind vor allem sogenannte Guest-Books zu erwähnen, bei welchen man sich wie in einem Gästebuch bei einer Ausstellung „eintragen“ und beliebige Angaben machen kann.

Häufig gibt man bei WWW-Servern auch persönliche Informationen preis, um bestimmte Daten (z. B. Public-Domain-Programme) zu erhalten. Zwar sind diese Informationen dann nicht unbedingt allgemein zugänglich, aber immerhin sind sie irgendwo beim entsprechenden Server abgespeichert, wobei deren Weiterverwendung meist völlig offen ist. Figur 5 zeigt ein Beispiel einer solchen Anwendung zusammen mit der Alarmmeldung (Security Information) des Browsers. Es ist zu beachten, daß diese Alarmmeldung von vielen Benutzern ausgeschaltet wird.

Schließlich kann es auch vorkommen, daß aufgrund von Fehlern oder Unachtsamkeiten über WWW-Server auf nicht-öffentliche Daten zugegriffen werden kann.

HyperText Transfer Protokoll (HTTP) und Log-Files

Der Zugriff auf WWW-Server erfolgt über das HyperText Transfer Protokoll (HTTP). Darin wird in erster Linie die Adresse der gewünschten Seite angegeben. Mit dem HTTP-Protokoll kann aber auch angegeben werden, von wo aus man auf diese Seite verwiesen wurde oder beispielsweise welchen Browser man verwendet.

Natürlich müssen die Abfragen auch die Adresse des Abfragenden enthalten, damit diesem die gewünschten Informationen zurückgeschickt werden können. Entsprechend kann ein WWW-Server die Anzahl der Zugriffe zu bestimmten Seiten zusammen mit den Adressen oder Domainnamen der Abfragenden erfassen und in „Log-Files“ abspeichern. Gerade in Zusammenhang mit dem Einsatz von WWW als Marketing- und Werbe-Mittel ist die Kenntnis der Sequenz der besuchten Seiten (bzw. des „click streams“) oder der Herkunft der Interessenten von Bedeutung.

Cookies – Gedächtnis für WWW-Server

Das Hypertext-Protokoll beinhaltet keine Möglichkeit zur Kontrolle, ob bestimmte Informationen auf einem WWW-Server von einem bestimmten Kunden schon einmal abgerufen oder eingegeben wurden. Mit Hilfe sogenannter Cookies kann man aber eine solche Gedächtnisfunktion implementieren.

Das Internet – ein „Datenschleppnetz“ für Personendaten?

Zusammen mit der angeforderten WWW-Seite (Reply) schickt der Server ein Cookie an den Browser beim Kundenrechner (PC). Das Cookie enthält einen frei wählbaren Namen (z. B. mit Informationen darüber, in welcher Sprache oder zu welchem Zeitpunkt der Kunde die Informationen erbeten hat), eine Geltungsdauer und einen Geltungsbereich (Pfad im Filebaum). Das Browserprogramm kann den Benutzer über die Zusendung des Cookie informieren und fragen, ob das Cookie angenommen werden soll oder nicht. Wenn man das Cookie annimmt, so wird es auf dem lokalen System, d.h. beim Kunden, gespeichert. Bei der nächsten Anfrage beim selben Geltungsbereich (Server, Pfad) schickt dann der Browser das Cookie automatisch mit. Auf diese Weise kann man dem Server bestimmte Statusinformationen aus dem letzten Besuch (z. B. gewünschte Sprache) übergeben.

Cookies können sehr nützlich sein, indem sie beispielsweise auf komplexen Servern die Navigation erleichtern und den Kunden direkt an die ihn interessierenden Stellen führen oder auf entsprechende Spezialangebote aufmerksam machen. Cookies können helfen, das Benutzerverhalten zu erfassen. Allerdings ist allein wegen der Cookies die Identität des Benutzers noch nicht bekannt. Erst wenn ein Benutzer im Verlauf seines Besuchs bei einem bestimmten Server auch seine Identität bekanntgibt (z. B. durch Angabe seiner E-mail-Adresse), kann er aufgrund seines Benutzerverhaltens mit Werbesendungen bedient oder belästigt werden.

Suchmaschinen

Die Inhalte der WWW-Seiten sind mittels sogenannter Suchmaschinen in Volltext-Form erfaßt und werden für Abfragen zur Verfügung gestellt. Stellvertretend ist in Figur 7 eine Abfrage bei der Suchmaschine AltaVista dargestellt.

Suchmaschinen sind einerseits von großem Nutzen, wenn man feststellen will, welche Informationen zu bestimmten Themen oder auch Personen verfügbar sind: Versuchen Sie mal Ihr „persönliches elektronisches Profil“ zu erforschen, indem Sie mit Hilfe von Suchmaschinen nach Daten zu Ihrer Person oder Firma suchen!

Andererseits muß man sich bewußt sein, daß auch mit der Angabe von Suchbegriffen Informationen preisgegeben werden. Gewisse Suchmaschinen haben bereits begonnen, entsprechend den eingegebenen Suchbegriffen mit den Suchergebnissen die passenden Werbespots einzublenden. Man spricht in diesem Zusammenhang von „Content based advertisement“. Es gibt auch Suchmaschinen, welche die momentan am häufigsten gesuchten Begriffe anzeigen (vgl. http://www.eule.de).

News- und Mailserver

Personendaten, insbesondere E-mail-Adressen, werden notgedrungen immer dann abgegeben, wenn man Antworten zu bestimmten Themen erwartet. Dies ist der Fall bei E-mail-Verteillisten, Newsgruppen oder auch bei Systemadministratoren, welche für eine Internet-Domain verantwortlich sind. Bei Systemen, welche Kontakt-Informationen speichern, um sie später wieder verwenden zu können, speist man im Grunde genommen Datenbanken mit persönlichen Informationen (z. B. Newsgruppe, E-mail-Verteilliste, whois Datenbank, vgl. Figur 8). Das Problem ist nun, daß viele dieser Datenbanken öffentlich sind und keine Kontrolle darüber möglich ist, wer was wozu nutzt.

Kundenrechner (PC)

Im Normalfall sollten die auf dem Kundenrechner gespeicherten Daten nicht zugreifbar sein, nur weil man mit dem Internet verbunden ist. Durch Fehlmanipulationen oder Systemfehler ist jedoch auch das nicht völlig auszuschließen.

Die Gefahr wird etwas größer, wenn auf dem Kundenrechner nicht nur statische Seiten dargestellt, sondern auch Programme ausgeführt werden. Dies kann einerseits dann der Fall sein, wenn Programme vom Internet auf den Rechner kopiert und dort (durch den Benutzer) mehr oder weniger bewußt installiert und gestartet werden. Neben der Virenproblematik setzt man sich dabei auch der Gefahr aus, daß Programme neben den gewünschten auch irgendwelche versteckte Funktionen ausführen (man spricht in diesem Zusammenhang auch von „Trojan Horses“).

Mit dem Aufkommen von ActiveX und Java, d.h. von Programmen, welche mittels HTTP auf den Kundenrechner übertragen werden und eigentlich im Browser (mit beschränkten Zugriffsrechten) ablaufen sollten, hat sich eine neue Dimension der Gefahr des unbemerkten Zugriffs auf lokale Daten eröffnet. Ein Beispiel ist in Figur 9 dargestellt, wo man mit Hilfe eines Java-Applets auf einem Rechner ein sogenanntes „Finger-Programm“ starten konnte, welches Informationen zu den momentan aktiven Benutzern dieses Rechners erfaßt. (Wenn ein System richtig konfiguriert ist, kann der Fingerbefehl von extern nicht ausgeführt werden. Das hier gezeigte Beispiel funktioniert dann nicht.)

Ähnliche Probleme von unerwünschtem Zugriff auf Daten auf dem Kundenrechner (PC) treten in Zusammenhang mit sogenannten Mail-Makros auf.

Zusammenfassung

Die verschiedenen aufgeführten Möglichkeiten zur Beschaffung von Personendaten mögen den Anschein erwecken, das Internet sei der Alptraum der Datenschützer. Das Aufzeigen von Möglichkeiten ist noch lange nicht gleichzusetzen mit der beobachteten Nutzung. Don’t panic!

Zwar wird man gerade in jüngster Zeit immer häufiger durch unerwünschte Mails (sogenannte Bulk- oder SPAM-Mails) belästigt. Wie bei den Bulk E-mails, so ist man auch bei den in diesem Bericht aufgeführten Bereichen meist selbst schuld an der Weitergabe der Daten. Es geht daher in erster Linie um die Bewußtseinsmachung bei den Internet-Nutzern. Dazu gehört:

- Virtuelle Identität: Sind Sie sich bewußt, daß Bestimmungs- und Absenderadressen nicht unbedingt stimmen müssen.
- Geben Sie nicht leichtfertig persönliche Daten preis.
- Beachten Sie Alarm- und Sicherheitshinweise der Browser.

Ohne Bekanntgabe minimaler Personendaten (z. B. Adressen) ist der Internetbetrieb nicht möglich. Technisch sind Hilfen und Maßnahmen zur Verbesserung des Persönlichkeitsschutzes in Bearbeitung (Verschlüsselung, Authentisierung, Zertifikate, etc.). Organisatorisch und in bezug auf die Gesetzgebung sind ebenfalls Arbeiten im Gange, welche die Nutzung personenbezogener Daten besser regeln (z. B. Platform for Privacy References, P3P oder Gesetze betreffend SPAM-Mails in USA).

Letztlich wird man aber auch auf das „anständige Verhalten der Netznutzer“ – die Netiquette – appellieren müssen, um die Entwicklung des Internet nicht zu behindern.

Empowering the Citizen Through Cryptography

Marc Rotenberg

I would like to thank the Berlin Data Protection Commission for the opportunity to speak with you today. The future of privacy is an issue that concerns all people around the globe. l welcome the opportunity to describe for you recent developments in the United States.

Even as you consider whether the Internet will bring about the end of privacy, there is a new opportunity to protect privacy and to extend privacy safeguards for the world of the Internet. Across the Internet users of new communications technology are looking to new techniques–- and particularly cryptography–- to protect privacy, and they are hoping that their national governments will end the current crisis in policy.

The reason for the crisis in policy is not hard to understand. The current regulatory system is a relic of a different era, a time when cryptography was controlled by the military and there was little practical commercial use and little public interest in the use of encryption. National policies were developed in an era when encryption was largely the province of spies and soldiers. The policies of our governments, which emphasized secrecy and control, were appropriate in their day. But the world has changed.

Today cryptography is used for everything from communication to commerce, from electronic publishing to new payment systems. It protects not only the confidentiality of communications, but also provides for authentication and verification. Encryption can even provide techniques for anonymous transactions that may one day promote commerce and protect privacy.

The electronic communications infrastructure is clearly no longer the exclusive domain of governments. Today's network carries not only diplomatic communiqus and military plans as in an earlier day–- it is the conduit for global electronic commerce, private correspondence and the most sensitive bits of personal information, including medical and financial records.

Even though governments recognize the important role that cryptography plays in protecting privacy, some governments hope to limit its use. They fear that the widespread availability of cryptography will make it easy for criminals to evade detection. But cryptography is so fundamental to the growth of the information economy that any attempt to limit its use imposes great cost.

In such a world, the best policies are those that seek to adapt to changing circumstance. It would be foolhardy for any government not to anticipate that strong, unbreakable encryption will be widely available on the Internet. And it would be equally wrong to prevent citizens and businesses from making use of the best tools available to protect their sensitive information from potential criminal threats.

We are therefore in a period of transition when law must be updated to reflect new realities. Reforming the export control regime so that it reflects the need for good encryption in commercial products and to protect personal privacy is a sensible first step. Further delay is likely only to increase the risks to users and businesses.

The Lessons of Clipper

Cryptography was not always a matter of public debate. For many years, governments around the world classified all matters pertaining to cryptography. Research was limited and cryptographers were discouraged from publishing their analysis. This began to change in the 1970s with the development of public key cryptography and the growing realization that cryptographic techniques could no longer be controlled with central key management authorities. But still governments remained reluctant to allow publication of research and controls remained in place.

In the early 1990s cryptography became a matter of widespread public debate not because of innovation but because of politics. The United States government, responding to the need for a new cryptographic system but reluctant to give up the ability to wiretap private communications, proposed a new cryptographic standard called the „Escrowed Encryption Standard“ or Clipper. Clipper was a particularly type of cryptography that would require users to deposit copies of keys with agents of the government. The argument for this proposal was that it was necessary to ensure that government could maintain its ability to intercept messages in a criminal investigation and prosecute wrong-doing.

The response from the public was swift. At first industry groups and a few experts expressed opposition to the proposal. Then users across the Internet voiced their concern. A letter from 42 experts was sent to the President of the United States in January of 1994. Then in April a petition signed by 47,000 Internet users was delivered to the White House.

Internet users did not want government to restrict the freedom to use cryptography, the freedom to use new technologies to protect personal privacy. Eventually, the government withdrew the Clipper proposal. But „the ghost of Clipper“ lives û Commercial Key Escrow, Key Recovery, etc. We have named these new „upgrades“ Clipper 2.0 and Clipper 3.0.

Recent Developments

Over time, governments are beginning to understand the important role the cryptography will play in protecting privacy and promoting on-line commerce.

The International Working Group on Data Protection in Telecommunications was among the first international organizations to recognize the need for strong cryptography in new communications services. At the meeting here in Berlin in November 1996, the group adopted a report which said that:

> Technical means should also be used for the purpose of protecting confidentiality. In particular the use of secure encryption methods must become and remain a legitimate option for any user of the Internet.

In March, 1997 the Organization for Economic Cooperation and Development issued guidelines for the development of cryptography policy. The Guidelines follow from earlier week by the OECD on privacy and information security. The OECD Guidelines recognize that national and global information infrastructures are developing rapidly to provide a seamless network for world-wide communications and access to data and that this emerging information and communications network is likely to have an important impact on economic development and world trade. The OECD further recognized that that the users of information technology must have trust in the security of information and communications infrastructures, networks and systems; in the confidentiality, integrity, and availability of data on them; and in the

ability to prove the origin and receipt of data; and that data is increasingly vulnerable to sophisticated threats to its security, and ensuring the security of data through legal, procedural and technical means is fundamentally important in order for national and international information infrastructures to reach their full potential.

The OECD Guidelines speak very directly to the important relationship between cryptography and privacy protection. The fifth principles of the OECD Cryptography Guidelines states:

> THE FUNDAMENTAL RIGHTS OF INDIVIDUALS TO PRIVACY, INCLUDING SECRECY OF COMMUNICATIONS AND PROTECTION OF PERSONAL DATA, SHOULD BE RESPECTED IN NATIONAL CRYPTOGRAPHY POLICIES AND IN THE IMPLEMENTATION AND USE OF CRYPTOGRAPHIC METHODS.

This principle recognizes privacy in both communications and stored data. The OECD Guidelines note that „Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and communications and the protection of the identity of individuals. Cryptographic methods also offer new opportunities to minimize the collection of personal data, by enabling secure but anonymous payments, transactions and interactions."

The OECD Guidelines recognized also that cryptography will raise new privacy issues:

> At the same time, cryptographic methods to ensure the integrity of data in electronic transactions raise privacy implications. These implications, which include the collection of personal data and the creation of systems for personal identification, should be considered and explained, and, where appropriate, privacy safeguards should be established.

The OECD recognized that some government „may" choose to promote lawful access to encrypted communications but beyond this acknowledgment there was little support for the key escrow effort. Indeed, since adoption of the OECD Cryptography Guidelines there has been little indication that OECD member governments intend to pursue a policy based on key escrow or key recovery.

The OECD Guidelines came about through the work of an expert group. Non-governmental organizations also played a significant role. An international alliance of civil liberties groups, internet users, and consumer associations brought together by the Global Internet Liberty Campaign issued a resolution in support of the of the freedom to use cryptography at a Paris conference on September 25, 1966. The resolution urged the OECD to base its cryptography policies on „the fundamental right of citizens to engage in private communication", to resist a policy that would encourage the development of networks designed for surveillance, and recommended that the OECD „turn its attention" to the growing public concern about the use of surveillance technology and its implications on the fundamental right to communicate freely.

I was particularly gratified that the OECD gave such a strong endorsement of privacy and chose not to endorse key escrow. Promoting key escrow around the world may have a severe impact on the work of human rights organizations and threaten to shift a delicate balance between the rights of citizens and the authority of government in the wrong direction. The U.S. Department of State has reported each year on the growing use of electronic surveillance by governments against dissidents, journalists and human rights organizations. It is particularly important that democratic governments send a clear message that the technologies of the emerging information infrastructure should not be designed to facilitate government surveillance of private communications.

Then in July, at the meeting of the European Ministers on the Global Information Society it was reiterated by the European Commission that it is the view of the European nations to support the development and public availability of strong cryptography. Minister Rexrodt played a leading role in the July conference in Bonn in urging support for strong cryptography.

And recently, the two European governments that seemed prepared to support widespread controls on cryptography are now reconsidering their position. In France, Industry Minister Christian Pierret said on Friday that for electronic commerce to flourish France has to develop security, reliability and privacy on the Internet. He added further that France would allow the liberalisation of basic encryption techniques. According to one report, Minister Pierret said, „This liberalisation of encrypting technology will allow French companies to fully enter the market of electronic commerce currently dominated by U.S. companies." This development follows efforts by Microsoft Corp. chairman Bill Gates who argued in Paris with French President Jacques Chirac that encryption should be allowed for commercial purposes. France has apparently also decided to suspend its efforts to implement key escrow encryption. New difficulties have appeared with the proposal and France will not sign or publish the Common Criteria or authorize a TTP public encryption system.

In England, the election of a new government has also raised doubts out the Department of Trade and Industry's policy paper „Licensing of Trusted Third Parties for the Provision of Encryption Services." The Labor Party expressly opposed key escrow. And at a conference organized earlier this by Privacy International and the London School of Economics, there was strong public opposition to the DTI proposal.

In the United States it is clear that more work will need to be done to remove unjustified obstacles to the free use of cryptographic products and services. But progress is occurring on many friends. In Congress, legislation titled the Security and Freedom through Encryption Act has received support from a majority of the Members of the House of Representatives. This legislation, if enacted, affirms the freedom to use cryptography without restriction and would relax export controls. At the same, cases in the federal court system continue to test the constitutionality of the controls on cryptography. Last week a federal court in San Francisco ruled that US export controls on encryption and related publications are an unconstitutional prior restraint of expression under the First Amendment. It is my belief that over times, as the courts come to understand the public and commercial significance of encryption, the President's authority to regulate this technology in the name of national security will become increasingly suspect.

While there are clearly forces within the United States government that would prefer that current controls be kept in place and that new methods, such as key escrow encryption be adopted, it seems clear that the tide is turning.

Future Directions

Efforts are also underway by Non Governmental Organizations to form coalitions around issues of common concern and to develop appropriate policy frameworks for privacy, free speech and cryptography on the Internet. The Global Internet Liberty Campaign is one organization that will play an increasingly important role on behalf of netizens. GILC was formed in June, 1996 at the last INET conference in Montreal.

The GILC Statement of Principles is based on internationally recognized norms of political and human rights. On the issue of cryptography, GILC has said simply that users should have the right to „encrypt communications and information without constraint.“ The GILC promulgated the „Paris Resolution in Support of the Freedom to Use Cryptography“ and continues to work in support of privacy, free speech, and the unrestricted use of cryptography.

The Open Internet Policy Principles were adopted by a group of international experts and are are intended as a framework for government officials, parliamentarians, and non governmental organizations as they consider the impact of the Internet in their own and other countries. The experts included European and American parliamentarians, government officials, non-governmental organizations, and the academic and business communities.

The Principles emphasize that „The Internet is an inherently open, decentralized communications infrastructure which is ideally suited to support the free exchange of ideas, a rich political discourse, and a vibrant economy.“

With regard to policy making and the Internet, the Principles point out that policy making ought to be undertaken „by policy makers who are well informed about the unique nature of the net and have direct experience with its use; and, with substantial input and comment from the user community.“

Other matters of privacy, the Open Internet Policy Principles propose:

- Communications Privacy: „Users of the Internet should have the right to be free of unlawful government interception of or access to communication and information online.“
- Right of Anonymity: „Users should have the right to communicate without disclosing their identity.“
- Unfettered Right to Use Encryption: „Users should have the right to use any form of cryptographic technology they choose to protect the privacy of their communications.“

New Challenges

Cryptography standing alone is simply a technique. Until we understand how it is used we can actually say very little about whether it will help protect privacy or work to undermine privacy. But we recognize in cryptography the foundation for developing techniques that will protect privacy.

One of the most critical techniques is the development of anonymity in information environments. We need to find ways to protect anonymity in a wide range of social and political activities–- voting, commerce, transportation, and information access.

Ministers at the Bonn conference said that „where the user can choose to remain anonymous off-line, that choice should also be available on-line.“

The Working on Group on Data Protection in Telecommunications has also recognized the important role that anonymity will play in preserving online privacy.

> Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society.

Anonymity like cryptography may be seen as a threat by some governments. There is the real problem of money laundering and the need for accountable in a variety of

transactions. Personal information, properly obtained and used for lawful purposes, is also critical for many activities. But anonymity must be preserved in the on-line world.

We are still in the very early stages of developing techniques for anonymity. Robust anonymity will require ease of use, consumer acceptance, and a means to address law enforcement concerns.

We must also explore further discussion of „Technologies of Privacy,“ and in particular begin to assess the many technical proposals that are being put forward to protect personal privacy. My view is that it is critical in all of these proposals to focus on the collection and use of personal information, to understand the circumstances of disclosure, and the rights available to the data subject. Too few of the proposals that are being put forward actually enhance personal privacy. Too many will facilitate the growing data profiles of citizens in the information economy.

Conclusion

Technology and privacy have always had an uneasy relationship. At times technology is threat, at other times it is opportunity. It is clear today that we live in an era where technology is both threat and opportunity. We should find the path that allows us to minimize the risk and pursue the opportunity. In the information age, this path necessarily requires that we fully explore the terrain of cryptography.

This week has also humbled us by events larger than the Internet and technology itself. The death of Princess Diana reminds us that privacy is an enduring human value, a right that touches each one of us. When privacy is transgressed, we have seen that tragedy may result. Let us build the techniques and develop the policies that will preserve this most precious and sweeping of all rights for generations to come.

References

Ross Anderson, Crypto in Europe – Markets, Law and Policy [http://www.cl.cam.ac.uk/ftp/users/rja14/queensland.ps.Z]

Bernstein v. U.S. Department of State

Department of Trade and Industry, „Licensing of Trusted Third Parties for the Provision of Encryption Services“ (UK) [http://www.dti.gov.uk/pubs]

European Commission, Global Information Networks (July 199) [http://www2.echo.lu/bonn/pressrel.html]

Global Internet Liberty Campaign, The Paris Resolution in Support of the Freedom to Use Cryptography (September 1996) [http://www.gilc.org/gilc/resolution.html]

Ian Goldberg David Wagner Eric Brewer, „Privacy Enhancing Technologies for the Internet“ [http://www.cs.berkeley.edu7daw/privacy-compcon97-www/privacy-html.html]

Internet Society, „IAB and IESG Statement on Cryptographic Technology and the Internet“ (August 1996) [ftp://ftp.isi.edu/in-notes/rfc1984.txt]

National Research Council, „Cryptography's Role in Securing the Information Society“ (1996) [http://www.nap.edu/readingroom/books/crisis/]

Privacy International, „1996 Review of International Privacy Rights: Excerpts from the US State Department's „Country Reports on Human Rights for 1996“ (January 1997) [http://www.privacy.org/pi/reports/hr96−privacy−report.html]

Privacy International, Scrambling for Safety conference [http://www.privacy.org/pi/conference/dti/]

Recommendation of the Council of the OECD Concerning Guidelines for Cryptography Policy [http://www.oecd.org/dsti/iccp/crypto−e.html]

Report of the International Working Group on Data Protection in Telecommunications [Berlin, November 16, 1996) [http://www.datenschutz-berlin.de/diskus/13−15.htm]

Bruce Schneier, Appli ed Cryptography (2d ed. 1996) [http://www.amazon.com/exec/obidos/ISBN=0471117099/electronicprivacA]

Note: Many books on cryptography policy and cryptography technology are available for sale at the EPIC Bookstore [http://www.epic.org/bookstore/]

Organizations

Electronic Privacy Information Center [http://www.epic.org/]

Global Internet Liberty Campaign [http://www.gilc.org/]

Internet Privacy Coalition [http://www.privacy.org/ipc/]

Internet Society [http://www.isoc.org/]

Privacy International [http://www.privacy.org/pi/]

Initiativen der Europäischen Kommission zum Datenschutz in der globalen Informationsgesellschaft

Ulf Brühann

Die Europäische Kommission identifizierte die Informationsgesellschaft in Ihrem Weißbuch von 1993[1] als eine der Herausforderungen des 21. Jahrhunderts, als der amerikanische Vizepräsident Gore sich gerade die ersten Gedanken über die „Information Highways“ machte. Wie ein roter Faden durchzieht das vorgeschlagene Bündel von Maßnahmen zur schwerpunktmäßigen Entwicklung der Informationsnetze die Idee, daß die Entwicklung der rechtlichen Regelung mit der technischen Entwicklung Schritt halten müsse. Schon im allgemeinen Aktionsplan wurde der Datenschutz im Bereich der Privatsphäre als eines der Mittel zur kontinuierlichen Realisierung des ordnungsrechtlichen Rahmens ausdrücklich angesprochen[2] und diese Forderung konsequent durchgehalten und weiter ausgeführt in den Vorschlägen zur Entwicklung eines „gemeinsamen Informationsraums“[3].

In den oft als „Bangemann-Bericht“ apostrophierten Empfehlungen für den Europäischen Rat „Europa und die globale Informationsgesellschaft“ thematisiert eine vom Europäischen Rat in Brüssel beauftragte Gruppe von Persönlichkeiten in ihrem Bericht unter der Überschrift „Was noch zu tun bleibt“ den Schutz der Privatsphäre mit den Worten: „Nach Ansicht der Gruppe wird ohne die rechtliche Sicherheit eines unionsweiten Ansatzes der Vertrauensmangel auf seiten des Verbrauchers einer raschen Entwicklung der Informationsgesellschaft im Wege stehen.“

In ihrem Aktionsplan „Europas Weg in die Informationsgesellschaft“[4] ist sich die Kommission bewußt, „daß im einzelnen zu regeln ist, wie die allgemeinen Grundsätze auf spezifische Situationen anzuwenden sind, die sich aus der Einführung neuer Technologien ergeben“.

Der Datenschutz in öffentlichen Telekommunikationsnetzen wird in dem Vorschlag einer Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN)[5], angesprochen. Ziel des geänderten Vorschlags ist es, die allgemeinen Grundsätze des Schutzes personenbezogener Daten und der Privatsphäre im Hinblick auf die speziellen Anforderungen und Bedingungen moderner Telekommunikationstechnologien zu ergänzen und zu spezifizieren, um abweichende Entwicklungen in der Europäischen Union zu vermeiden, die den Binnenmarkt für Telekommunikationsdienstleistungen und Telekommunikationsgeräte in Frage stellen könnten. Der Vorschlag befindet sich gegenwärtig im Endstadium des gemeinschaftlichen Gesetzgebungsverfahrens. Die luxemburgische Präsidentschaft hat die formelle Einberufung des Vermittlungsausschusses angekündigt, in dem die zwischen Parlament und Rat noch bestehenden Divergenzen ausgeräumt werden sollen.

In ihrer Mitteilung einer Europäischen Initiative für den elektronischen Geschäftsverkehr[6] hat die Kommission die grundlegende Bedeutung des Rechts des einzelnen auf Datenschutz im Rahmen der vertrauensbildenden Maßnahmen unterstrichen. Der Schutz der Privatsphäre sei in den Bereichen der elektronischen Zahlungssysteme, der Besteuerung und elektronischer Systeme zur Verwaltung der Abgeltung von Urheberrechten von besonderer Bedeutung. Darüber hinaus verfolgt die Kommission das Ziel, angesichts der globalen Natur des elektronischen Handels eine Übereinkunft über globale verbindliche Regeln zum Datenschutz etwa im Rahmen der Welthandelsorganisation vorzubereiten[7].

Darüber hinaus hat sie Maßnahmen angekündigt zur Gewährleistung eines gemeinsamen rechtlichen Rahmens zur Anerkennung digitaler Unterschriften im Binnenmarkt sowie die Festlegung von Mindestkriterien für Zertifizierungsstellen. Ferner wird sich die Kommission um die Entwicklung einer Politik innerhalb der Gemeinschaft und international bemühen, die den freien Verkehr von Verschlüsselungstechnologien und -produkten bei gleichzeitiger Berücksichtigung der öffentlichen Sicherheit gewährleisten soll[8].

Im Vorschlag für ein 5. Rahmenprogramm der Europäischen Gemeinschaft im Bereich der Forschung und technologischen Entwicklung[9] hat die Kommission den Datenschutz sowohl als allgemeines Kriterium für die Auswahl und Bewertung von Forschungsvorhaben aufgenommen (Technikfolgenabschätzung)[10] als auch in der Maßnahme Informationsgesellschaft die Entwicklung datenschutzfreundlicher Technologien als förderungswürdig anerkannt[11].

Auf internationaler Ebene führt die Kommission einen Dialog mit unseren wichtigsten Handelspartnern über das gemeinsame Vorgehen zur Förderung der Verbreitung von Diensten in der Informationsgesellschaft. Der Datenschutz als eine der wichtigsten Bedingungen in dieser Hinsicht ist wesentlicher Teil dieses Dialogs vor allem mit den Vereinigten Staaten und Japan.

1 Wachstum, Wettbewerbsfähigkeit, Beschäftigung, Herausforderungen der Gegenwart und Wege ins 21. Jahrhundert, Weißbuch der Europäischen Kommission, Beilage 6/93 zum Bulletin der Europäischen Gemeinschaften, Luxemburg, 1993

2 a.a.O., S. 27

3 a.a.O., S. 106, 108

4 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. vom 19. 7. 1994, S. 9

5 Gemeinsamer Standpunkt (EG) Nr. 57/96, vom Rat festgelegt am 12. September 1996, ABl. C 315 v. 24. 10. 1996, 30.

6 Europäische Initiative für den elektronischen Geschäftsverkehr. Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen, KOM (97) 157 vom 14.4 1997

7 a.a.O., S. 28

8 a.a.O., S. 27

9 Vorschlag für einen Beschluß des Europäischen Parlaments und des Rates über das fünfte Rahmenprogramm der Europäischen Gemeinschaft im Bereich der Forschung, technologischen Entwicklung und Demonstration (1998-2002), KOM (97) 142 endg. vom 30.4 1997

10 a.a.O., Erwägungsgründe, S. 21

11 a.a.O., Anhang II, 2. Maßnahme, S. 32

The European Telecommunications Directive A Regional Approach to Solve Privacy Problems in International Networks

Giovanni Buttarelli

Mr. Brühann has provided us, as usual, with an exhaustive overview of the initiatives taken by the European Union. Nothing could actually be added to his interesting considerations on Information Society, apart from publicly expressing our gratitude for the commitment shown by Mr. Brühann himself and his service during the past few years – which resulted in concrete achievements and led European institutions and agencies to address privacyrelated issues in fruitful ways.

I feel slightly embarassed in mentioning these topics, partly because privacy legislation was enacted only recently in my country; indeed, You might wonder with reason what interest may be a lecture on this subject matter by an Italian speaker. In fact, and I cannot help feeling a bit proud about it, Italy was the focus of a lively debate on research and legislation applying to computer networks during the past two years; the quality of this debate was excellent, and we are planning to sum up its gist on the Web pages which the Italian Data Protection Supervisory Authority is preparing for the end of this year.

This lively debate underlies the commitment shown by Italy during its EU presidency period towards speeding up the finalization of an European directive aimed at solving a few problems related to privacy on telecommunications networks.

My task today is to describe this directive so as to enable You to decide whether a modest – though fundamental – European proposal may provide a suitable solution to world-wide problems.

However, a couple of words should be said on another issue before addressing European initiatives in detail. Indeed, one might wonder whether there is room at all for the law on the network – i.e., for legal rules applicable to a transnational phenomenon which by its very nature would not seem to be amenable to effective controls.

The debate on privacy protection and security within telecommunications networks has rapidly expanded to unprecedented dimensions. Scientific papers and governmental initiatives coming from all countries in the world during the last year did increase awareness and knowledge in this sector – especially as regards legal issues. As You are certainly aware, Internet is a source of lively debate and widely diverging positions exist on this matter: from police-like control arrangements which are envisaged as a tool to fight crime and paedophily and would in practice eliminate confidentiality of electronic correspondence – a principle laid down in a number of constitutional charts – up to the total rejection of any kind of legal rules.

There is another version of this approach – namely, that any national or international legal provisions for data protection are outdated or inapplicable, given the huge speed of data flows in many States where no privacy laws are in force. Therefore it is regarded as unavoidable that the 'Network' should remain outside the scope of any legislation – without prejudice to already existing international agreements such as those concluded by the WTO.

Both positions are actually the expression of a sort of technological fatalism, which does not take into account the fact that, despite Internet specific features, many other transnational information media (TV, radio, fax, telex, mail) do pose similar problems.

Recently, a third approach has been developing, which would appear to offer an alternative solution to those I have just mentioned. The basic concept is that the attempt to keep up with the latest technological advancements by issuing detailed legislation is meaningless, as such legislation may be made rapidly obsolete – which does not mean, however, that one should not seek the implementation of fundamental rights and freedoms on the network as well.

This 'third path' is followed by the recent EU initiatives and, if I may say so, by the Privacy Act recently adopted by Italy.

It is, no doubt, an ambitious solution which aims at enhancing the protection of individuals through general principles and rules which may also be implemented by means of: a) international cooperation among States and Data Protection Supervisory Authorities; b) the adoption of codes of conduct (especially as regards access and service providers); c) international model contracts to be used by businesses and public authorities in relationships entailing transnational data flows; d) encouraging businesses to develop privacy enhancing technologies so as to reduce the risk of a breach of privacy and security on account of technical flaws.

In other words, law and technology are not mutually exclusive, provided legal rules are devised in such a way as to be applicable in concrete and to respect the principle of free movement of ideas and information as well as individual rights.

Examination of a recent „Privacy Policy Chart", based on a 26-item questionnaire, showed that user policies of the four biggest US providers diverge on fundamental issues related to privacy and security – such as information to users; headers and contents of e-mail; use of other personal data; web-site browsing. These discrepancies, which are considerable in a few cases, are no longer accountable and the European initiatives which Mr. Brühann just mentioned may allow reducing them further.

I will not deal with the International Conference held in Bonn on 6–8 July last, which might be one of the topics to be discussed in the panel. I would rather draw Your attention to the first directive on privacy protection (95/46/EC) which was adopted by the European Union in 1995. It is of a general nature and, though not specifically concerning networks, it also applies to privacy breaches committed on the network. This first instrument – which for the sake of convenience I will refer to as 'the general directive ' – did not consider sensitive issues such as the right to anonymity, encryption, email access, etc.; still, it laid down a few principles which were also applicable to network providers and users – and, in particular, the right to a fair and transparent data processing, including the so-called 'invisible processings'.

Following the adoption of the directive, it was considered necessary to set forth, in a separate Act, additional principles applying only to telecommunications. Again, for the sake of convenience, I am referring to this subsequent directive – which is soon to be finally approved – as the 'European TLC Directive'. This Directive was developed through a lengthy process.

In 1986 and 1988, the European Parliament adopted two resolutions which required the Commission to submit specific proposals in the telecommunications sector by taking into account the envisaged opening of the markets and with a view to ensuring a level of privacy in respect of personal data as much adequate as possible to the modernisation of services.

In 1990, the European Commission put forward an initial draft which was not examined in detail until September 1995, as all efforts were focussed on the general Directive 95/46/EC.

Following the Edimburgh Conference, in June 1994, the Commission submitted a modified draft which had been simplified in light of the subsidiarity principle.

A political agreement was reached on this Directive in the first half of 1996, during the Italian EU Presidency period. On September 12, 1996, the Council was therefore able to issue a common position (no. 57/1996). Eleven amendments were proposed by the EU Parliament on 16 January 1997, and the conciliation procedure laid down in the Treaty is reaching its final stage. Thus, it can be said that very few issues remain to be addressed and it is expected that the Directive will be finally approved by the end of 1997 – given also the fact that there will not be much time left for European countries to transpose it into their national legal systems (the term being 24 October 1998).

One cannot help wondering whether the European TLC Directive will manage to achieve its goals. It is a legitimate doubt, given that the Directive does not expressly mention the prime network – i.e., Internet -, and in this regard it might appear outdated. Indeed the directive does not address the most important issue – i.e., Internet – directly; nevertheless, it deals more generally with privacy in the sector of telecommunications networks – whereas the initial draft concerned specifically the integrated services digital network (ISDN) and digital mobile networks.

The new directive weas considered necessary since digital telecommunications networks allow transmitting voice, data, pictures, texts and sound in the form of totally new services.

Network digitalization enhances the development of 'intelligent' activities and functions which impinge on privacy in totally new ways and warrant more specific provisions as compared with those of the general Directive; the objective was therefore that of ensuring a correct use of data and services as well as the social 'acceptance' of digital networks (only think, for instance, of video-on-demand and interactive television). If the development of all these services is not harmonized, this will probably jeopardize the free competition among service providers and the free market of the Information Society.

The scope of application of the Directive was subsequently extended so as to provide specific rules applying to the protection of privacy in the whole telecommunications sector – including both analog and digital networks as well as Internet, although this is not expressly referred to.

The aim of the telecommunications Directive is the same as that of the general directive: namely, to ensure an equivalent level of protection of fundamental rights and freedoms (in particular – but not only – the right to privacy), with regard to the processing of personal data in the telecommunications sector, and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

I would refer to the telecommunications Directive as a 'daughter directive', since it 'particularises' and 'implements' the general Directive.

The general Directive will further apply to the telecommunications sector, but it will be particularized by the telecommunications one in respect of specific issues.

In the big world of telecommunications there will be at least one sector in which only the general directive will apply rather than the telecommunications one: namely, the processing of personal data relating to telecommunications services provided within non-publicly available networks (as is the case with a company's internal network, in respect of which there arises the need to protect the employees' privacy). Still, the telecommunications Directive does not prevent Member States from choosing to apply the same directive to this category of services as well.

a) The telecommunications Directive will also apply to legal persons to the extent that they are subscribers (for instance, the directive will not apply, at least directly, to a legal person who is a service provider, whereas it will protect any collective body which is party to a contract with the provider of a publicly available telecommunications service);

b) in no case will the telecommunications Directive give rise to the obligation for Member States to include legal persons into the scope of application of the general directive, which will continue to apply to natural persons only;

c) the telecommunications Directive will protect the 'legitimate interests' of legal persons. This conventional wording is used on account of the fact that the rights conferred on legal persons are considered equivalent to personal rights in a few countries, whereas in others they are regarded as legitimate interests or interests of factual nature;

d) in the absence of a general definition of 'legal person', this concept will further be grounded on national law (in a few countries, legal persons are all bodies whether by fact or by law, businesses and any other collective agencies such as associations, foundations, committees, etc.).

There can be no doubt as to the fact that this approach was adopted following the concerns expressed by a few countries fearing a chain reaction – namely, the risk that following the adoption of the telecommunications Directive the scope of application of the general Directive could be extended so as to include legal persons as well.

These concerns were overcome based on three main considerations:

a) the telecommunications Directive protects subscribers and users of telecommunications services, and it would be quite difficult for service and network providers to distinguish between subscribers who are legal persons and subscribers who are natural persons;

b) there are legal persons who, including for commercial purposes, are interested in the protection of security and confidentiality of communications and not willing to receive unsolicited calls or communications;

c) a diversified approach by Member States might result in obstacles to the internal TLC market and to service liberalization – which will take effect starting from 1998.

The telecommunications Directive will not apply to radio and television broadcasting, provided these activities are performed according to traditional modalities (that is, as point-to-multipoint services). Conversely, the new point-to-point services such as interactive television and video on demand will also be governed by the telecommunications Directive.

One of the most controversial issues in the directive probably concerned the services (analog and/or digital) to which it should apply. Again, a compromise solution was found with some difficulty, by reconciling the concerns of those countries believing that the application of the directive to analog services would entail excessive costs with the considerations of those who correctly maintained that the protection of fundamental rights and freedoms should not differ on account of the nature of the networks involved (the general directive itself is applicable to all types of networks).

This balance was struck partly because it is not easy to identify clearcut differences between analog and digital networks; furthermore, a few services are offered by using both kinds of networks.

The directive will apply to any service (via ISDN; mobile digital networks; analog networks, etc.) independently of cost/benefit assessments.

Regarding security issues, article 4 of the TLC Directive does not add very much to article 17 in the general directive (which is referred to in a recital and in a declaration); it is nevertheless useful, as it provides that the security obligations conferred by the general directive on the controller are to be discharged, in public telecommunications networks, by the subject dealing most closely with subscribers – that is to say, by the service provider. Where measures concerning the security of the whole network are required to safeguard security of its services, such measures will have to be adopted in conjunction with the provider of the public telecommunications network – who will be jointly liable.

The service provider will have to inform subscribers concerning the specific risks of a breach of the security, the possible remedies and the costs involved.

Unfortunately, as a result of a lively debate, no mention is made in the Directive of encryption facilities, which are not to be offered on a mandatory basis (as was provided for in a compromise draft); still, the Directive lays down an implicit obligation to include them in the information which must be provided according to the modalities I have previously mentioned.

Actually, this was the out-of-date position of some countries which were concerned as to the need for possible changes to their national legislation regarding encryption facilities, or which feared that the costs for the implementation of such facilities by a limited number of subscribers would have to be re-distributed among all the subscribers, or which requested the elimination of any reference which might lead users to believe that mobile telephone networks were liable to risks as to the security of communications.

A specific obligation will be imposed on Member States, as also related to the European Convention of Human Rights: namely, ensuring the confidentiality of communications within the scope of application of the directive. Article 5 allows Member States to adopt a flexible approach: they will not be obliged to issue provisions governing the recording of a telephone conversation by any of the users making such conversation (e.g., for getting evidence of a commercial transaction or professional communications); however, they will have to prohibit listening to, recording, surveillance and interception of communications by third parties where they are performed without the consent of the users involved. One should only think, for instance, of the use of loudspeaker-equipped devices. A recital was included in which it is recognized that a few countries prohibit such interferences only when they are intentional, whereas they do not prohibit listening to a casually intercepted communication. It should be pointed out, however, that this part is likely to be modified in the final version of the text.

The telecommunications Directive basically 'particularizes' and complements the provisions of the general directive concerning the processing of traffic and billing data.

Traffic data relating to subscribers and users, processed to establish calls, shall be erased or made anonymous. However, the network or service provider may further process personal data for the purpose of subscriber billing and interconnection payments, up to the end of the period during which the bill may lawfully be challenged or payment may be pursued. Where the processing is carried out for the purpose of marketing its own services, the service provider will have to apply for the subscriber's consent: a simple 'optout' solution will therefore not be sufficient.

As to the form of such consent, the provisions of the general directive will further apply: the consent must be given freely and in a specific form; it must be informed consent and be expressed at least unambiguously.

The TLC Directive also includes less restrictive provisions in order to allow access to personal data by the authorities competent for the settling of disputes – particularly interconnection or billing disputes. It will be possible to derogate from these provisions to allow access to data for purposes relating to public security and crime prevention, as well as to ensure that the data are stored for a longer period of time in order to protect such interests.

The sensitive matter of itemized billing was dealt with by recognizing the right for subscribers not to receive this service. Member States may decide to allow service providers to offer such services either as a default option (according to an opt-out scheme in favour of subscribers), or only upon application. Furthermore, Member States will have to adopt the necessary measures in order to reconcile the right of subscribers to verify correctness of their bills with the right to privacy of calling users and called subscribers.

This reconciliation will be achieved either by requiring the deletion of a certain number of digits from the called numbers mentioned in itemized bills (the directive does not specify how many digits should be deleted) and/or encouraging the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services (for example calling cards and facilities by credit card or charging other subscribers or current accounts).

As you can see, privacy will be better protected even in work places, in the family and between spouses.

Subscribers and Netizens will have the right to decide if and to what an extent they are to be included into printed or electronic directories of subscribers which are available to the public or obtainable through directory enquiry services.

The directive takes into account the risk that total elimination of the address may cause troubles to those persons having common family names.

However, subscribers will be entitled:

a) to have only such data included as are necessary to identify them, and to give their consent to the publication of additional personal data (occupation, educational degree, etc.);

b) to be omitted from one or more directories, whether electronic or printed;

c) to be included into such directories only on condition that their data are not used for the purpose of direct marketing;

d) to have their address omitted in part (for instance, by omitting the street number);

e) not to have any reference revealing their sex (for instance, by abbreviating first names).

In this way, the TLC Directive takes also account of the need to prevent female subscribers from being harassed on account of their complete address being known.

Another major issue in the TLC Directive concerns the provisions applying to calling line identification and connected line identification. Where these services are offered, which is mainly, if not exclusively, the case with digital networks, there must be the possibility to eliminate, free of charge, the presentation of the calling line identification on the receiving equipment. This option will have to be offered on a per-call basis to the user, or on a per-line basis to the subscriber.

The called subscriber will further have the possibility:

a) 'to be unaware' (that is to say, to prevent the presentation of calling line identification);

b) to avoid nuisance calls (i.e., to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber);

c) to override the elimination of the presentation of the calling line identification, in the presence of malicious or nuisance calls;

d) to eliminate the presentation of the connected line identification to the calling user (particularly in case of call forwarding).

The activity of organisations (such as helplines) who have an interest in ensuring the anonymity of their callers will thus be protected.

Finally, along with other major principles concerning automatic call forwarding and monitoring of emergency calls, the TLC Directive includes provisions on marketing, by laying down the following principles:

a) the use of automated calling systems without human intervention (automatic calling machines) or facsimile machines (fax) for the purpose of direct marketing should only be allowed in respect of subscribers who have given their prior consent;

b) unsolicited calls for the purpose of direct marketing by means other than those I have just mentioned should not be allowed without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls. The choice between an opt-in system and an opt-out one should be left to national legislation.

The TLC Directive will have to be enacted by national legislation within 24 October 1998, that is, within the same term provided for in respect of the general directive. There are additionally a few transitional provisions, in particular concerning the editions of already published telephone directories.

The Commission will specify the technical details relating to the data which may be processed for the purpose of subscriber billing and interconnection payments; there will be no need to follow the usual Council procedures.

Let me apologize for this lengthy lecture; there is, however, one final remark I would like to make: the TLC Directive, together with the general one, may actually give a valuable contribution towards solving the problem of network privacy.

In telecommunications networks – especially telematics ones – space is virtual and potentially unlimited: a balanced system of rules should therefore fit in without major difficulties. Thus, I may suggest that a suitable answer for the question tabled in this Symposium (The Internet: Privacy at an End?) could be 'The Internet: The Beginning of Privacy!'.

Datenschutz bei Multimedia

Die Neukonzeption des Datenschutzes bei Informations- und Kommunikationsdiensten

Stefan Engel-Flechsig

1. Das Informations- und Kommunikationsdienste-Gesetz: Regelungsintention und Regelungsübersicht

Für neue Informations- und Kommunikationsdienste müssen rechtliche Rahmenbedingungen vorliegen, die einen Ausgleich zwischen dem Wunsch nach freiem Wettbewerb, berechtigten Nutzerbedürfnissen und staatlichen Interessen schaffen. Innovationen müssen gefördert sowie die informationelle Selbstbestimmung des Nutzers gestärkt werden. Mit dem vom Bundesminister für Bildung, Wissenschaft, Forschung und Technologie erarbeiteten Entwurf für ein Informations- und Kommunikationsdienste-Gesetz soll ein bundeseinheitlicher rechtlicher Rahmen für Multimedia geschaffen und in den Rechtsbereichen Datenschutz und Datensicherheit die Akzeptanz neuer Technologien gefördert werden.

Am 13. Juni 1997 hat der Deutsche Bundestag in zweiter und dritter Lesung das Informations- und Kommunikationsdienste-Gesetz (IuKDG) beschlossen und eine Entschließung zum IuKDG verabschiedet.[1] Das IuKDG ist – wie vorgesehen – am 1. August 1997 in Kraft getreten[2].

Das IuKDG war am 18. April 1997 als Regierungsentwurf in erster Lesung im Parlament behandelt worden und an den federführenden Ausschuß für Bildung, Wissenschaft, Forschung, Technologie und Technikfolgenabschätzung sowie an den mitberatenden Innenausschuß, den Rechtsausschuß, den Ausschuß für Wirtschaft, den Ausschuß für Familie, Senioren, Frauen und Jugend, den Ausschuß für Post und Telekommunikation sowie an den Ausschuß für Angelegenheiten der Europäischen Union überwiesen worden. Die Ausschüsse haben intensive Beratungen unternommen. Am 14. Mai hatte der federführende Ausschuß gemeinsam mit den mitberatenden Auschüssen eine Expertenanhörung zu den Artikeln des Gesetzes durchgeführt.[3]

Der Regierungsentwurf zum IuKDG ist in seiner Grundkonzeption vom Parlament bestätigt worden. Dies gilt sowohl im Hinblick auf seinen Aufbau als Artikelgesetz, seinen verfassungsrechtlichen Geltungsbereich für „Teledienste“, seine Erstregelungen für Teledienstedatenschutz und für digitale Signaturen sowie hinsichtlich der Ergänzungen und Änderungen bestehender Gesetze. Gegenüber dem Regierungsentwurf sind in einigen Artikeln Änderungen vorgenommen worden. Diese nehmen wichtige Anregungen aus den parlamentarischen Beratungen, aber auch aus der Stellungnahme des Bundesrates und der Gegenäußerung der Bundesregierung zum Regierungsentwurf[4] auf.[5]

[1] vgl. BT-Drs. 13/7934 sowie BT-Drs. 13/7935 vom 11. 6. 1997
[2] vgl. hierzu BGBl I, S. 1870
[3] Die Ergebnisse sind in BT-Drs. 13/7934 zusammengefaßt.
[4] vgl. hierzu insgesamt BT-Drs. 13/7385
[5] vgl. zu den einzelnen Änderungen Engel-Flechsig, IuKDG vom Bundestag verabschiedet, DuD 8/1997, S. 474 ff.

„Multimedia“ als Synonym für die Informations- und Kommunikationsgesellschaft ist eine Querschnittsmaterie. Dies gilt unter tatsächlichem und unter rechtlichem Blickwinkel: Die tatsächlichen Auswirkungen der Informations- und Kommunikationstechnologie sind in allen Lebenszusammenhängen festzustellen; sie reichen z. B. von der Inanspruchnahme von Dienstleistungen im Netz über die Abwicklung alltäglicher privater Bankgeschäfte bis hin zur Übermittlung vertraulicher medizinischer Daten zwischen Arzt, Krankenkasse und Patient.

Nicht zuletzt wegen des Querschnittscharakters von Multimedia ist das IuKDG ein sog. Artikelgesetz. Es vereinigt Erstregelungen mit Ergänzungen und Änderungen bereits bestehender bundesgesetzlicher Vorschriften in einem Mantelgesetz. Der Mantel wird dabei gebildet vom sachlichen Gegenstand des Gesetzgebungsvorhabens – Multimedia. Der Gesetzentwurf bezieht entsprechend dem Leitprinzip „Deregulierung geht vor Regulierung“ aber keineswegs alle denkbaren gesetzlichen Änderungen oder Anpassungen mit ein, die angesichts des Wandels in fast allen Rechtsbereichen festzustellen sind. Vielmehr beschränkt sich der Gesetzentwurf auf einige wesentliche Fragen, die jetzt geregelt werden müssen, um den für die wirtschaftliche Entwicklung notwendigen Handlungsrahmen zu beschreiben und damit bestehende Rechtsunsicherheit zu beseitigen.

Im Überblick enthält das IuKDG folgende Regelungen:

- Art. 1: Gesetz über die Nutzung von Telediensten („Teledienstegesetz“, TDG)
- Art. 2: Gesetz über den Schutz personenbezogener Daten bei Telediensten („Teledienstedatenschutzgesetz“, TDDSG)
- Art. 3: Gesetz zur digitalen Signatur
- Art. 4: Änderung des Strafgesetzbuches
- Art. 5: Änderung des Gesetzes über Ordnungswidrigkeiten
- Art. 6: Änderung des Gesetzes über die Verbreitung jugendgefährdender Schriften
- Art. 7: Änderung des Urheberrechtsgesetzes
- Art. 8: Änderung des Preisangabengesetzes
- Art. 9: Änderung der Preisangabenverordnung
- Art. 10: Rückkehr zum einheitlichen Verordnungsrang
- Art. 11: Inkrafttreten

Gesetzliche Neuregelungen enthalten insbesondere die Art. 1, 2 und 3:

- Art. 1 ist das Kernstück des IuKDG. Das „Gesetz über die Nutzung von Telediensten“ umfaßt die Regelungen, die für die wirtschaftliche Entwicklung neuer Informations- und Kommunikationsdienste wesentlich sind. Dabei handelt es sich um Regelungen zur Bestimmung des Geltungsbereichs der bundesgesetzlichen Regelung, zur Zugangsfreiheit der Informations- und Kommunikationsdienste und zur Verantwortlichkeit von Diensteanbietern bei Telediensten.
- Art. 2 befaßt sich mit dem Schutz personenbezogener Daten bei Telediensten. Als bereichsspezifische Regelung ergänzen diese Regelungen den allgemeinen Datenschutz im Bundesdatenschutzgesetz (BDSG). Sie enthalten eine Neukonzeption des vorhandenen Datenschutzes.

- Art. 3 regelt eine konkrete Informations- und Kommunikationsdienstleistung. Das „Gesetz zur digitalen Signatur“ umschreibt die Rahmenbedingungen für einen sicheren Einsatz digitaler Signaturen. Dabei beschränkt sich der Gesetzgeber auf die Formulierung eines gewerberechtsähnlichen Zulassungs- und Überwachungsverfahrens für die bei Einsatz und Nutzung digitaler Signaturen erforderliche Infrastruktur, die Beschreibung der Anforderungen an die verwendeten technischen Komponenten und an die datenschutzrechtlichen Anforderungen bei der Verarbeitung der anfallenden personenbezogenen Daten.[6]

Unter dem Blickwinkel der Anpassung an neue Informations- und Kommunikationsdienste werden mit den Art. 4, 5 und 6 die erforderlichen Änderungen in bereits vorhandenen Regelwerken vorgenommen; mit Art. 7 wird im Urheberrecht die EU-Datenbankenrichtlinie[7] in nationales Recht umgesetzt.

2. Datenschutz bei Multimedia-Diensten: Anforderungen an seine gesetzliche Umsetzung im IuKDG

Zum Verständnis des mit Art. 2 vorliegenden Gesetzentwurfs sind die Empfehlungen des Rates für Forschung, Technologie und Innovation von grundlegender Bedeutung. Sie wurden am 21. Dezember 1995 der Öffentlichkeit vorgestellt und enthalten insbesondere in den Empfehlungen Nr. E 22 bis E 27 Aussagen zu Datenschutz und Datensicherheit.[8] Der Technologierat geht von vier wesentlichen Prämissen aus:

1. Ein konsequenter Datenschutz zählt zu den zentralen Akzeptanzvoraussetzungen der Informationsgesellschaft.
2. Die Entwicklung der Informations- und Kommunikationstechnologie ändert nichts an den verfassungsrechtlich begründeten und gesetzlich abgesicherten Grundsätzen: Sie zwingt aber dazu, den Schwerpunkt ihrer Verwirklichung mehr und mehr von rein normativen Vorgaben auf eine besondere technische Infrastruktur zu verschieben.
3. Vernetzung und dezentrale Anwendung und Nutzung sind typische Kennzeichen der modernen Informations- und Kommunikationstechnologien; die normative Ausgestaltung des Datenschutzes muß ergänzt werden durch eine Verstärkung des technologischen Aspektes.
4. Zu den erforderlichen technischen Sicherheitsmaßnahmen zählt der Einsatz von Kryptoverfahren, die als digitale Signaturverfahren die Authentizität und die Urheberschaft von Dokumenten und als Verschlüsselungsverfahren die Vertraulichkeit von Dokumenten sicherstellen können.

Der Technologierat leitet aus diesem Befund eine Korrektur der vorhandenen Datenschutzkonzeption ab. Dabei sind nach seiner Auffassung folgende Grundsätze zu berücksichtigen, die für die Konzeption des Datenschutzes im IuKDG grundlegende Ausgangspunkte sind:

6 Eine Übersicht zu den geplanten Regelungen auf der Grundlage eines Arbeitsentwurfs vom September 1996 findet sich in W. Bieser, CR 9/96, S. 564 ff.; vgl. auch Paul Mertes, Gesetz und Verordnung zur digitalen Signatur – Bewegung auf der Datenautobahn, CR 12/1996, S. 769 ff.

7 Richtlinie 96/9/EG des Europäischen Parlamentes und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken

8 Der Text der Empfehlungen des Rates für Forschung, Technologie und Innovation kann unter http://www.bmbf.de oder http://www.iid.de abgerufen werden.

- Vermeidung der Verarbeitung personenbezogener Daten,
- enge Zweckbindung der Verarbeitung personenbezogener Daten,
- Gewährleistung einer hohen Transparenz der Datenverarbeitung für den Nutzer,
- Kontrolle der Datenverarbeitung durch eine unabhängige Instanz,
- Entwicklung eines Grundstandards von technischen und organisatorischen Sicherheitsmaßnahmen, die ein Höchstmaß an Anonymität für den Nutzer sichern sowie
- Sicherstellung einer internationalen Zusammenarbeit, insbesondere im europäischen Rahmen.

3. Datenschutz bei Multimedia: Abgrenzung zu vorhandenen Regelungen

Das Datenschutzrecht in der Bundesrepublik Deutschland ist im Grundsatz durch eine klare Systematik gekennzeichnet: Die generelle Regelung wird im BDSG getroffen, während eigenständige bereichsspezifische Regelungen die besonderen Bedingungen und Eigenarten des jeweiligen Datenverarbeitungsbereichs berücksichtigen – zum Beispiel im Bereich des Sozialdatenschutzes oder im Bereich der Statistik. Damit kann den Besonderheiten des konkreten Verarbeitungskontextes am besten Rechnung getragen werden.[9]

Im Bereich von Information und Kommunikation gibt es eine Reihe von bereits geltenden bereichsspezifischen Regelungen: Zu nennen sind hier in erster Linie das Telekommunikationsrecht, die Landesdatenschutzgesetze und die staatsvertraglichen Regelwerke der Bundesländer im Rundfunkbereich.

Datenschutz bei Informations- und Kommunikationsdiensten folgt der grundsätzlichen Systematik des Datenschutzrechts: Das TDDSG stellt unter systematischem und inhaltlichem Blickwinkel eine bereichsspezifische Regelung dar, die außerhalb des BDSG getroffen wird, jedoch an dessen Regelungen anknüpft. Das TDDSG befaßt sich mit den besonderen Bedingungen des Umgangs mit personenbezogenen Daten bei Telediensten. Nur dort, wo das TDDSG eine besondere Bestimmung enthält, geht diese Bestimmung dem allgemeinen BDSG vor. Enthält das TDDSG keine Aussage, gelten die Bestimmungen des BDSG.

Mit der Frage der Abgrenzung zu vorhandenen datenschutzrechtlichen Bestimmungen ist die allgemeine Frage des Geltungsbereichs des TDDSG eng verbunden. Die Abgrenzung des TDDSG stellt sich dabei im Hinblick auf

- Telekommunikationsrecht, insbesondere im Hinblick auf das Telekommunikationsgesetz[10] und im Hinblick auf die Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsleistungen erbringen[11]; und im Hinblick auf

9 vgl. hierzu Simitis in Simitis u.a., BDSG, § 1, Rdnr. 16

10 vgl. BGBl. 1996 I, S. 1120 ff.; abgedruckt auch in epd, Kirche und Rundfunk, Nr. 59 vom 31. Juli 1996, S. 2 ff.

11 TDSV vom 12. Juli 1996, vgl. BGBl. 1996 I Nr. 34

- Landesrecht, insbesondere hinsichtlich der rundfunkrechtlichen Datenschutzbestimmungen[12] und hinsichtlich des geplanten Mediendienste-Staatsvertrages[13].

Hinsichtlich beider Abgrenzungsfelder ergibt sich die Antwort aus § 1 Abs. 1 TDDSG i.V.m. § 2 Abs. 1 TDG. § 2 Abs. 1 TDG lautet:

> *„Die nachfolgenden Vorschriften gelten für alle Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder und Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).“*

Das Gesetz regelt damit nur sog. Teledienste; dies sind insbesondere die neuen, vom Nutzer individuell im Wege der neuen Informations- und Kommunikationstechnologien nutzbaren Dienste. Die Nutzung der IuK-Dienste macht neue Wege wirtschaftlicher Betätigung und eine verbilligte Geschäftskommunikation (z. B. Ergänzung/Ersatz bisheriger Vertriebsformen) möglich. Prägend für die IuK-Dienste sind insbesondere die hierdurch möglichen autonomen und selbstbestimmten Anwendungen im Sinne eines individuellen und frei kombinierbaren Umgangs mit digitalisierten Informationen verschiedener Darstellungsformen (z. B. Text, Grafik, Sprache, Bild, Bildfolgen usw.).

Teledienste setzen die Übermittlung von Inhalten mittels Telekommunikation im Sinne des § 3 Nr. 16 TKG voraus. Das IuKDG regelt die Nutzung der mittels Telekommunikation übermittelten Inhalte, nicht die Telekommunikation selbst. Der telekommunikationsrechtliche Datenschutz bleibt also unberührt; Telekommunikationsdatenschutz und Teledienstedatenschutz stehen nebeneinander und sind daher in der Praxis gleichermaßen zu berücksichtigen. Dies trägt den verschiedenen denkbaren technischen Vorgängen am ehesten Rechnung. In der Praxis kann bereits heute zwischen dem (technischen) Telekommunikationsvorgang und dem (inhaltlichen) Informations- und Kommunikationsdiensteangebot unterschieden werden; in beiden Vorgängen sind unterschiedliche Vertragspartner – das Telekommunikationsunternehmen und mindestens ein Diensteanbieter – tätig; diese erfüllen unterschiedliche vertragliche Aufgaben; die von ihnen benötigten Daten sind nach unterschiedlichen Kriterien zu bestimmen. Im Ergebnis setzt diese Parallelität der Vorschriften eine differenzierte Analyse der jeweiligen Informationsschritte voraus. Eine Ergänzung der datenschutzrechtlichen Vorschriften des TKG, die sich auf telekommunikationsrechtliche Fragen beschränken, würde jedoch den vielfältigen inhaltlichen Nutzungsformen der neuen Informations- und Kommunikationsdienste nicht gerecht.

Teledienste sind nicht auf öffentliche Meinungsbildung angelegte massenmediale Veranstaltungen, sondern durch den Nutzer bestimmbare Kommunikation. Damit bleiben die rundfunkrechtlichen Regelungen, aber auch die Bestimmungen des Mediendienste-Staatsvertrages der Bundesländer unberührt. Soweit es sich also um einen Teledienst handelt, gelten nur die Bestimmungen des Teledienstedatenschutzgesetzes. In der Praxis ist auch insoweit eine genaue Analyse zur Einordnung eines einzelnen Dienstes als Teledienst oder Mediendienst erforderlich. Bei Mediendiensten folgen jedoch die datenschutzrechtlichen Bestimmungen der vom Teledienstedatenschutzgesetz vorgegebenen Grundkonzeption – sie sind also inhaltsgleich, zum überwiegenden Teil sogar wortgleich. Datenschutzrechtlich unterschiedliche Regelungen gibt es nur dort, wo mediendienstspezifische Fragestellungen (Beispiel: Auskunftsrecht des Nutzers bei Verwendung personenbezogener Daten zu journalistisch-redaktionellen Zwecken, § 16 Abs. 2 MDStV) im Vordergrund stehen. Diese inhaltliche Parallelität erlaubt so im Einzelfall eine im Ergebnis gleiche Bewertung eines Sachverhaltes bei Telediensten und bei Mediendiensten.[14]

[12] vgl. im einzelnen die Mediengesetze der Länder, z. B. LRG NW v. 24. 8. 1996, dort insbesondere §§ 45-50

[13] vgl. Mediendienste-Staatsvertrag, z. B. Bayerischer Landtag, 13. Wahlperiode, Drucksache 13/7716 v. 21. 03. 1997, S. 1 ff.

4. Datenschutz bei Multimedia: Umsetzung im Teledienstedatenschutzgesetz – TDDSG

Die Fortentwicklung des Datenschutzstandards, der mit dem geltenden Datenschutzrecht in der Bundesrepublik Deutschland erreicht worden ist, ist bei der Gestaltung der gesetzlichen Rahmenbedingungen eine wesentliche Zielbestimmung. Dabei gilt:

- Die gesetzlichen Rahmenbedingungen müssen auf die Risiken der neuen Informations- und Kommunikationsdienste eine Antwort finden: Personenbezogene Informationen können bei der Nutzung von Informations- und Kommunikationsdiensten in vielfältiger Weise anfallen, beliebig kombiniert, verändert oder ausgewertet werden; die Datenverarbeitung findet nicht mehr nur in einer Datenverarbeitungsanlage statt, sondern im Netz mit einer Vielzahl von Beteiligten; die Kontrollmöglichkeiten des Nutzers sind angesichts der zunehmenden Vernetzung erheblich eingeschränkt.

- Die gesetzlichen Rahmenbedingungen müssen auch die neuen technischen Möglichkeiten in ihren Blickwinkel einbeziehen. Ein Beispiel dafür, daß durch technische Innovationen Datenschutz verwirklicht werden kann, ohne höhere inhaltliche Zulässigkeitsvoraussetzungen zu formulieren, sind vorbezahlte Wertkarten, mit denen bereits gegenwärtig eine anonyme Inanspruchnahme von Dienstleistungen im Rahmen neuer Informations- und Kommunikationsdienste möglich ist[15]. Für die Konzeption des Datenschutzes im Bereich der neuen Dienste bietet sich damit ein technischer Ansatzpunkt, um das Recht auf informationelle Selbstbestimmung wirksam zu gewährleisten. Bereits durch die Gestaltung der Technik, mit der personenbezogene Daten erhoben und verarbeitet werden, kann so einer übermäßigen Datenverwendung vorgebeugt werden. Durch dateneinsparende Organisation der Übermittlung, der Abrechnung und Bezahlung sowie der Abschottung von Verarbeitungsbereichen kann dieser „Systemdatenschutz“ wirksam unterstützt werden.[16]

- Die gesetzlichen Rahmenbedingungen müssen schließlich dem veränderten Datenschutzbewußtsein von Unternehmen Rechnung tragen. Zahlreiche Unternehmen wissen, daß ihre Akzeptanz beim Kunden vom Umgang mit den personenbezogenen Daten des Kunden abhängt. Bei einem Online-Dienst z. B. ist der Umgang mit den zum Teil sehr sensiblen personenbezogenen Daten wie Abrechnungsdaten oder Nutzungsdaten für seine Akzeptanz beim Nutzer von wesentlicher Bedeutung. Die vorhandenen Kontrollmöglichkeiten durch den Nutzer oder die zuständigen Einrichtungen müssen deshalb um neue Möglichkeiten, die bereits bei der Vorbereitung und Entwicklung von Datenschutzkonzepten greifen können, ergänzt werden.

[14] vgl. zur Abgrenzung: Engel-Flechsig, ZUM 4/1997, S. 231 ff.; Kuch, ZUM 4/1996, S. 225 ff.

[15] vgl. z. B. den Einsatz vorbezahlter Wertkarten beim Abo-Sender „Premiere“, bei dem pro Film etwa 6 DM von einer vorbezahlten Karte abgebucht werden; vgl. auch den Hinweis von H. Schrader in seinem Schlußwort zur Sommerakademie ’96 (DuD 11/96, S. 679) auf die anonyme Computer-Quittung beim Online-Lotto in Hamburg und Schleswig-Holstein, bei der Name und Adresse der Teilnehmer nicht aufgenommen werden.

[16] vgl. auch John Borking, Der Identity-Protector, DuD 11/96, S. 654 ff.

Unter Berücksichtigung dieser Zielvorgaben sind im TDDSG die wesentlichen bereichsspezifischen Regelungen formuliert. In der Übersicht ergibt sich folgende Systematik:

- § 1 befaßt sich mit dem Anwendungsbereich.
- § 2 stellt die Begriffe „Diensteanbieter“ und „Nutzer“ klar. Er weicht dabei von der Begrifflichkeit im allgemeinen Datenschutzrecht ab, das insoweit von der „speichernden Stelle“ und dem „Betroffenen“ spricht. Das Gesetz folgt dem Sprachgebrauch des Teledienstegesetzes (Art. 1 IuKDG). Die Abweichung vom Sprachgebrauch rechtfertigt sich aus dem engen sachlichen Zusammenhang mit dem Teledienstegesetz. Der „Nutzer“ umfaßt dabei nicht nur natürliche Personen, sondern auch juristische Personen oder Personenvereinigungen, die Teledienste nachfragen. Damit will das Gesetz nicht den persönlichen Schutzbereich der datenschutzrechtlichen Bestimmungen erweitern, sondern es trägt den veränderten Nutzungsformen bei Telediensten Rechnung. Es sichert so die Geltung der datenschutzrechtlichen Bestimmungen für personenbezogene Daten auch dann, wenn als „Nutzer“ eine juristische Person oder Personenvereinigung auftritt.
- § 3 formuliert allgemeine Grundsätze für die Verarbeitung personenbezogener Daten, enthält eine umfassende Unterrichtungspflicht und führt erstmalig normative Voraussetzungen für eine „elektronische“ Einwilligung in die Verarbeitung personenbezogener Daten ein. Das TDDSG ergänzt insoweit die allgemeinen Regelungen des Datenschutzrechts.
- § 4 stellt die technischen und organisatorischen Voraussetzungen für Datenschutz bei Einsatz und Nutzung von Telediensten auf und setzt das Konzept des Systemdatenschutzes um; auch insoweit stellt das TDDSG zusätzliche Anforderungen an die Datenverarbeitung durch Diensteanbieter.
- § 5 und § 6 regeln die bereichsspezifischen Voraussetzungen für die Verarbeitung sog. Bestands-, Nachfrage- und Abrechnungsdaten bei Telediensten.
- § 7 spezifiziert das Auskunftsrecht des Nutzers nach § 34 BDSG und
- § 8 schließlich bietet eine Grundlage für eine erweiterte Kontrollmöglichkeit der Aufsichtsbehörden nach § 38 BDSG.

4.1. Anwendungsbereich

Die Regelungen des TDDSG gelten für den Schutz personenbezogener Daten bei Telediensten (§ 1 Abs. 1).

„Personenbezogene Daten“ sind – im Sinne von § 3 Abs. 1 BDSG – Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Hinsichtlich der Bestimmung dieser Einzelangaben kann auf das BDSG Bezug genommen werden. Nicht erfaßt werden daher Angaben über juristische Personen und Personenmehrheiten oder Personenvereinigungen, die aus dem Anwendungsbereich des BDSG ausgenommen sind.[17] Damit wird dem Charakter des informationellen Selbstbestimmungsrechtes als Ausgangspunkt für die datenschutzrechtliche Konzeption des TDDSG Rechnung getragen.[18]

[17] vgl. hierzu Dammann in Simitis u.a., BDSG, § 3 , Rdnr. 17 ff.

[18] Ob angesichts der dynamischen Entwicklung der neuen Informations- und Kommunikationsdienste zu einem späteren Zeitpunkt der Schutz von Einzelangaben über juristische Personen oder Personenvereinigungen einzubeziehen ist, ist abzuwarten; in § 89 Abs. 1 Satz 4 TKG wird nur eine Gleichstellung von Einzelangaben über juristische Personen, die dem Fernmeldegeheimnis unterliegen, mit personenbezogenen Daten vorgenommen.

Der Schutz personenbezogener Daten greift bei „Telediensten“ im Sinne des Teledienstegesetzes. Das TDDSG beschränkt sich nicht auf eine bestimmte Verarbeitungsstufe, sondern gilt generell beim Umgang mit personenbezogenen Daten bei Telediensten. Damit wird a priori kein Nutzungsschritt ausgeschlossen. Erfaßt sind also Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Vorgesehen ist aber auch die Einbeziehung neuartiger Nutzungen wie z. B. bei automatisierten Verfahren, die erst eine Erhebung, Verarbeitung oder Nutzung vorbereiten – z. B. bei sog. „cookies“.[19]

„Teledienste“ sind Dienste im Sinne des Teledienstegesetzes – Art. 1 IuKDG. Dies sind entsprechend § 2 Abs. 1 TDG alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Diese abstrakte Definition wird ergänzt durch die Bestimmungen in § 2 Abs. 2 TDG; konkret handelt es sich bei „Telediensten“[20] insbesondere um:

- Angebote im Bereich der Individualkommunikation: Hier geht es um Dienste, bei denen die Nutzung von Inhalten mittels Individualkommunikation im Vordergrund steht. Beispielhaft kann Telebanking für den wirtschaftlich geprägten Bereich der Individualkommunikation genannt werden. Darüber hinaus ist ein breites Spektrum von individuell nutzbaren Inhalten in den neuen Diensten wie Meinungsforen oder neue Formen der Zusammenarbeit wie beispielsweise Telearbeit, Telemedizin, Telelernen, Telematik und andere erweiterte Formen der Individualkommunikation zu nennen.
- Angebote zur Information und Kommunikation: Hier geht es um Dienste, die sehr unterschiedliche Informationen zum Inhalt haben können. Beispielhaft aufgeführt sind die für eine individuelle Nutzung auf Abruf vorgehaltenen Datendienste wie Verkehrs-, Wetter-, Umwelt- und Börsendaten; hierzu zählen zum Beispiel aber auch Einzelwerbeangebote über Waren und Dienstleistungen sowie sonstige Angebote und Anzeigen (z. B. homepages). Nicht erfaßt sind Datendienste, die mit dem Ziel der Meinungsbildung für die Allgemeinheit redaktionell aufbereitet sind, beispielsweise Textdienste im Rundfunk und in der elektronischen Presse.
- Angebote zur Nutzung des Internets oder anderer Netze; hier werden die von den Zugangsvermittlern – insbesondere Online-Anbietern – bereitgestellten Angebote zur Nutzung der neuen Dienste erfaßt (z. B. Navigationshilfen).
- Telespiele: Hier handelt es sich um eine besondere Form von Angeboten von Bewegtbilddarstellungen (video-on-demand). Mit der fortschreitenden technischen Entwicklung wird diesem Bereich erhebliche wirtschaftliche Bedeutung zukommen.
- Angebote von Waren und Dienstleistungen: Mit dieser Regelung wird ein breites Spektrum wirtschaftlicher Betätigung mittels der neuen Dienste erfaßt. Dies betrifft sowohl die elektronischen Bestell-, Buchungs- und Maklerdienste als auch interaktiv nutzbare Bestell- und Buchungskataloge, Beratungsdienste und ähnliche Formen wirtschaftlicher Betätigung. Wesentliches Kennzeichen dieser Dienste ist, daß diese Angebote unmittelbar in Anspruch genommen werden können.

[19] vgl. hierzu § 3 Abs. 5 Satz 2, der eine Unterrichtung des Nutzers in diesen Fällen vorsieht.

[20] Grauzonen zu den Mediendiensten im Sinne des von den Ländern geplanten Mediendienste-Staatsvertrages lassen sich angesichts der dynamischen Entwicklung der Technik nicht ausschließen. Um diese Grauzonen zu minimieren, sind die Regelwerke von Bund und Ländern aufeinander abgestimmt; dies gilt insbesondere für die datenschutzrechtlichen Regelungen; Regelungslücken können so vermieden werden.

4.2. Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

§ 1 Abs. 2 und § 3 Abs. 1 TDDSG formulieren die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten. Zur Zulässigkeit der Datenverarbeitung wird in § 1 Abs. 1 TDDSG klargestellt, daß die allgemeinen datenschutzrechtlichen Vorschriften für die Verarbeitung personenbezogener Daten fortgelten, soweit das TDDSG keine besondere Regelung trifft. Abweichend vom BDSG wird der Schutz dabei auf Daten ausgeweitet, die nicht in Dateien verarbeitet oder genutzt werden. Mit dieser Ergänzung soll eine Umgehung der Datenschutzvorschriften im TDDSG verhindert werden, wenn die Sammlung der Daten den Dateibegriff des § 3 Abs. 3 BDSG nicht erfüllt – z. B. durch eine entsprechende Aufbereitung der Daten oder die Beschränkung auf nur ein Merkmal.

§ 3 Abs. 1 TDDSG enthält die Befugnisnorm für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Diensteanbieter. Sie entspricht im Grundsatz den in § 4 Abs. 1 BDSG festgelegten Voraussetzungen. Eine Verarbeitung und Nutzung ist nur dann zulässig, wenn das TDDSG oder eine andere Rechtsvorschrift dies erlaubt oder wenn der Nutzer eingewilligt hat. Das TDDSG bezieht darüber hinaus jedoch auch die Erhebung, also das Beschaffen von Daten über den Nutzer, in die Geltung des Gesetzesvorbehalts mit ein. Dies entspricht den Vorgaben der EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 23. November 1995.

§ 3 Abs. 2 TDDSG führt eine enge Zweckbindung für die Verwendung von erhobenen personenbezogenen Daten bei der Nutzung von Telediensten für andere Zwecke ein. Weitere Datenverarbeitungsschritte (Speichern, Ändern, Übermitteln und Nutzen) für andere Zwecke sind nur zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift diese Verwendung erlaubt oder der Nutzer eingewilligt hat. Rechtsvorschriften und Einwilligung stehen damit auch im TDDSG auf einer Stufe und sind rechtlich gleichwertige Anknüpfungspunkte für eine zulässige Verarbeitung personenbezogener Daten.

4.3. Unterrichtung des Nutzers

Der Nutzer ist vor der Erhebung umfassend zu unterrichten. Nur so kann er sich einen umfassenden Überblick über die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten verschaffen[21]. Nur so ist eine wirksame Einwilligung in die Verarbeitung personenbezogener Daten möglich. Die in § 3 Abs. 5 TDDSG vorgesehene Unterrichtung trägt diesen Grundsätzen Rechnung.

Die Anforderungen an die Unterrichtung gehen über die in § 4 Abs. 2 Satz 1 BDSG für eine Einwilligung vorgesehenen Anforderungen hinaus. Der Nutzer ist in allen Fällen über die Erhebung, Verarbeitung und Nutzung zu unterrichten, die Unterrichtung ist also unabhängig von einer eventuellen Einwilligung des Nutzers; die Funktion der Unterrichtung ist die Schaffung von Transparenz für den Nutzer. Auch hinsichtlich Zeitpunkt, Umfang und Form der Unterrichtung ergeben sich Unterschiede zum geltenden Datenschutzrecht: Den besonderen Risiken der Datenverarbeitung im Netz entsprechend ist der Nutzer über Art, Umfang, Ort und Zweck der Verarbeitung der personenbezogenen Daten zu unterrichten; die Unterrichtung ist zu protokollieren, und sie muß vom Diensteanbieter so abgelegt werden, daß der Nutzer sich jederzeit über den Inhalt der Unterrichtung informieren kann.

[21] vgl. hierzu die Ausführungen zu den Begriffsbestimmungen: Hier zeigt sich sehr deutlich, daß eine vom Begriff des „Betroffenen“ im BDSG unterschiedliche Sichtweise angebracht ist.

Von der Unterrichtung mit umfaßt werden automatisierte Verfahren, die quasi auf Vorrat beim Nutzer, z. B. auf dessen Festplatte, zu einer Ablage personenbezogener Daten bei der Nutzung von Telediensten führen, aber erst zu einem späteren Zeitpunkt vom Diensteanbieter abgerufen werden, z. B. sog. cookies[22]. In diesen Fällen erfolgt durch das bloße Ablegen der Daten in einem Datenspeicher beim Nutzer noch keine Verarbeitung oder Nutzung durch den Diensteanbieter. Ob damit bereits in jedem Falle schon eine „Erhebung“ im Sinne von § 3 Abs. 4 BDSG vorliegt, ist zweifelhaft und im Ergebnis davon abhängig, ob der Diensteanbieter zum Zeitpunkt der Ablage der Daten beim Nutzer bereits objektiv und subjektiv seine Verfügungsgewalt über die Daten begründet hat[23]. In jedem Falle entsteht jedoch eine vom Nutzer nicht ohne weiteres erkennbare Datensammlung. Auf diese soll er hingewiesen werden. Werden solche Daten vom Diensteanbieter erhoben, verarbeitet oder genutzt, gelten die allgemeinen Zulässigkeitsvoraussetzungen des TDDSG.

Ein Verzicht auf die Unterrichtung ist möglich, darf aber nicht als Einwilligung in eine Erhebung, Verarbeitung oder Nutzung gedeutet werden. In diesen Fällen sind vielmehr die gesetzlichen Zulässigkeitsvoraussetzungen in § 3 Abs. 1 und 2 TDDSG zu beachten.

4.4. Einwilligung in die Verarbeitung personenbezogener Daten

Die Einwilligung ist im Datenschutzrecht gleichwertiger Anknüpfungspunkt für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Im TDDSG wird dieser Grundsatz übernommen.[24]

Im Online-Bereich wird die Einwilligung eine erhebliche praktische Bedeutung erhalten. Dies gilt im öffentlichen Bereich ebenso wie im nicht-öffentlichen Bereich, da Online-Dienste im Bereich der intelligenten Dienstleistungen für den Nutzer individuell zugeschnittene Dienstleistungen vorbereiten und anbieten werden. Diese Möglichkeit kennzeichnet die wirtschaftlichen Entwicklungsmöglichkeiten neuer Informations- und Kommunikationsdienste, sie erleichtert die jederzeitige Nutzungsmöglichkeit der Teledienste für Dienstleistungen und Informationen jeder Art durch den Nutzer. Unter Berücksichtigung dieser praktischen Bedeutung widmet sich das TDDSG der Einwilligung hinsichtlich der Formerfordernisse und der Koppelung der Einwilligung mit der Erbringung von Telediensten[25].

In der Regel bedarf die Einwilligung nach § 4 Abs. 2, Satz 2 BDSG der Schriftform, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist. Eine schriftliche Einwilligung würde jedoch die nutzerorientierte Online-Nutzung für den Diensteanbieter wie auch für den Nutzer erschweren.

Hier sieht das TDDSG erstmalig die Möglichkeit einer elektronischen, also: nicht schriftlichen Einwilligung des Nutzers vor. Das mit der Schriftform gegebene besondere Schutzerfordernis soll für den Bereich der Teledienste grundsätzlich beibehalten werden; schriftlich erklärte Einwilligungen sollen weiterhin möglich sein. Daneben soll aber auch die elektronische Einwilligung ermöglicht werden. Wegen der besonderen Risiken, denen elektronische Erklärungen mangels Verkörperung (keine

[22] vgl. Beschreibung in Beat Leuthardt, Leben online, S. 143 ff.
[23] vgl. dazu Dammann in Simitis u.a., BDSG, § 3, Rdnr. 108 ff.
[24] vgl. § 3 Abs. 1 und 2
[25] Die Voraussetzungen für die wirksame Einwilligung durch einen Dritten, z. B. den Nutzer als juristische Person, richten sich nach den allgemeinen Grundsätzen; vgl. zur rechtlichen Einordnung Simitis, a.a.O., § 4, Rdnr. 28 ff.

Schriftform) und mangels biometrischer Kennzeichen (keine eigenhändige Unterschrift) ausgesetzt sind, bedürfen sie besonderer Verfahren, die ihre Wirksamkeit sicherstellen. Im einzelnen ist zu beachten[26]:

- Der Schutz der Nutzer vor einer übereilten Einwilligung ist sicherzustellen. Dieser Schutz ist in Anbetracht der besonderen technikspezifischen Gefahren, nämlich der Anwendung eines flüchtigen Mediums (Bildschirm) und des Handelns durch einfachen Knopfdruck oder Mausklick, das nicht zwischen wichtigen und unwichtigen Handlungen unterscheidet, von Bedeutung. In diesem Sinne autorisiert ist eine Einwilligung beispielsweise durch eine bestätigende Wiederholung des Übermittlungsbefehls, während gleichzeitig die Einwilligungserklärung mindestens auszugsweise auf dem Bildschirm dargestellt wird.
- Zum Nachweis von Authentizität und Urheberschaft der Einwilligung ist als geeignetes technisches Verfahren die Verwendung von digitalen Signaturen denkbar. Dabei kann es sich um digitale Signaturen im Sinne von § 1 Abs. 1 des Art. 3 IuKDG handeln. Es sind aber auch andere Verfahren denkbar. Die Vorschrift ist bewußt auch für die Anwendung anderer geeigneter technischer Verfahren offen, soweit die Authentizität und Urheberschaft entsprechend sichergestellt sind. Maßgebend ist dabei, ob die im Einzelfall verwendeten Verfahren die vom TDDSG vorgegebene Funktionalität erfüllen.
- Die Transparenz der vom Nutzer erlaubten Datenverarbeitung seiner personenbezogenen Daten wird durch eine Protokollierung und die jederzeitige Abrufmöglichkeit durch den Nutzer gewahrt. Sie schafft Akzeptanz für die Anwendung elektronischer Einwilligungen und sichert zugleich das informationelle Selbstbestimmungsrecht des Nutzers, der nachprüfen kann, wann, wem und in welchem Umfang er eine Einwilligung in die Verarbeitung seiner personenbezogenen Daten erteilt hat.

Der Katalog der allgemeinen Prinzipien wird in § 3 Abs. 3 um eine weitere Vorschrift ergänzt, die sich mit der Koppelung der Einwilligung und der Erbringung von Telediensten befaßt.

Die Einwilligung in die Verarbeitung personenbezogener Daten für andere Zwecke darf nicht zur Vorbedingung der Erbringung des Teledienstes gemacht werden. Damit trägt das TDDSG der Bedeutung der Einwilligung als eigenständiger Willensäußerung des Nutzers in eine bestimmte Art der Verarbeitung und Nutzung seiner personenbezogenen Daten Rechnung. Im allgemeinen Datenschutzrecht wird diese Bedeutung durch die besondere Hervorhebung der Einwilligung, z. B. im äußeren Erscheinungsbild bei mehreren Erklärungen, betont. Mit dem Koppelungsverbot will das TDDSG diesen Entscheidungsspielraum des Nutzers auch bei Telediensten in vollem Umfange erhalten und sicherstellen.

In der parlamentarischen Diskussion wurde diese Bestimmung im Sinne ihres Zwecks präzisiert: Mit diesem Koppelungsverbot wollte der Regierungsentwurf verhindern, daß Monopolstellungen von Diensteanbietern ausgenutzt werden, Dienstleistungen von Diensteanbietern also nur erhältlich sind, wenn der Nutzer seine Einwilligung für die Verarbeitung seiner Daten für andere Zwecke gibt. An dieser Intention hält auch das Parlament zwar fest, bezieht jedoch im Wortlaut der Bestimmung jetzt die Ausnutzung einer Monopolstellung ausdrücklich mit ein.

[26] vgl. die wortgleichen Voraussetzungen der ursprünglich in den beiden ersten Referentenentwürfen geplanten Änderung des Fernunterrichtsschutzgesetzes; der Kabinettentwurf hat diese Neuregelung zugunsten einer in Kürze zu erwartenden Änderung des BGB im Bereich der Formvorschriften zurückgestellt.

4.5. Grundsatz des Systemdatenschutzes

Der Grundsatz des Systemdatenschutzes im TDDSG[27] besagt: Bereits durch die Gestaltung der Systemstrukturen, in denen personenbezogene Daten erhoben und verarbeitet werden, soll einer unzulässigen Datenverwendung vorgebeugt und die Selbstbestimmung der Nutzer sichergestellt werden. Dies kann durch dateneinsparende Organisation der Übermittlung, der Abrechnung und Bezahlung sowie der Abschottung von Verarbeitungsbereichen unterstützt werden.

Der Diensteanbieter soll daher das Angebot seiner Teledienste an dem Ziel ausrichten, keine oder jedenfalls so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Normadressat ist der einzelne Diensteanbieter, unabhängig davon, ob er eigene oder fremde Dienste zur Nutzung bereithält oder ob er „nur“ den Zugang zur Nutzung von Telediensten vermittelt.

Dieser Grundsatz des Systemdatenschutzes findet seine Ausprägung in § 4 Abs. 1 mit der Verpflichtung zur Ermöglichung der Inanspruchnahme von Telediensten in anonymer oder pseudonymer Form. Diensteanbieter haben – im Rahmen der technischen Möglichkeiten und soweit ihnen individuell zumutbar[28] – den Nutzern anonymes oder pseudonymes Handeln zu ermöglichen. Dies gilt für die gesamte Nutzungsbeziehung. Der Nutzer ist entsprechend zu unterrichten.

Bestimmte technische Verfahren werden im Hinblick auf die zukünftige technische Entwicklung nicht vorgeschrieben. Denkbar ist z. B. das Angebot an den Nutzer, Teledienste mit vorbezahlten Wertkarten oder Chipkarten in Anspruch nehmen zu können. Für das Erfordernis der Anonymität ist die faktische Anonymität im Sinne von § 3 Abs. 7, 2. Alternative BDSG ausreichend. Pseudonymes Handeln ermöglicht nicht anonymes, sondern quasi-anonymes Handeln. Ein Pseudonym kann ein Name oder eine Kurzbezeichnung sein, die aus sich heraus die Identität des Nutzers nicht preisgeben, aber über eine Referenzliste beim Diensteanbieter mit der Identität des Nutzers zusammengeführt werden können.

4.6. Nutzungsprofile

Das TDDSG befaßt sich an verschiedenen Stellen mit der Möglichkeit, daß Daten über das Nutzungsverhalten eines bestimmten Nutzers erhoben, verarbeitet oder übermittelt werden. Angesichts der vielfältigen technischen Möglichkeiten in einer Netzstruktur ist dem Risiko der Entstehung von Nutzungsprofilen, die im Ergebnis zu einer vom Nutzer nicht kontrollierbaren Zusammenstellung aller seiner bei der Inanspruchnahme von Telediensten anfallenden Daten führen können, besondere Beachtung zu schenken. Gemeinsames Ziel der Vorschriften im TDDSG ist es daher, dieser Gefährdung der informationellen Selbstbestimmung des Nutzers Rechnung zu tragen.

§ 4 Abs. 2 Nr. 4 TDDSG enthält ein technisch und organisatorisch zu gewährleistendes Trennungsgebot. Die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer sind getrennt zu verarbeiten und eine Zusammenführung dieser Daten unzulässig. Mit dieser Regelung soll verhindert werden, daß der Diensteanbieter personenbezogene Daten über die Inanspruchnahme von verschiedenen Telediensten zusammenführt und auf diese Weise personenbezogene Nutzerprofile entstehen. Im Kabinettentwurf vom 11. Dezember 1996

[27] vgl. § 3 Abs. 4, § 4 Abs. 1 und 2

[28] Mit der individuellen Zumutbarkeit will das Gesetz die unterschiedliche subjektive Leistungsfähigkeit von Unternehmen berücksichtigen; diese kann je nach Größe des Unternehmens stark variieren.

wird jetzt die Möglichkeit, die Daten zu Abrechnungszwecken zusammenzuführen, berücksichtigt. Damit trägt der Entwurf einem wesentlichen Kritikpunkt der Unternehmen Rechnung, die mit den ursprünglichen Regelungen keine Möglichkeit hatten, eine einheitliche Abrechnung für die Inanspruchnahme von verschiedenen Diensten vorzunehmen.

Gemäß § 4 Abs. 4 TDDSG sollen Nutzungsprofile nur bei der Verwendung von Pseudonymen zulässig sein. Die Regelung trägt damit dem wirtschaftlichen Interesse des Diensteanbieters, die Inanspruchnahme der Teledienste auszuwerten, Rechnung, indem sie Nutzungsprofile nicht generell für unzulässig erklärt. Sie trägt aber auch dem Interesse des Nutzers an weitgehender Anonymität seines Konsumentenverhaltens Rechnung.

Ergänzt werden diese Vorschriften schließlich von § 6 Abs. 3 TDDSG, der die Übermittlung von Nutzungs- oder Abrechnungsdaten an andere Diensteanbieter oder Dritte nur in Ausnahmefällen vorsieht. Hinsichtlich der Übermittlung von Nutzungsdaten sieht das TDDSG eine Ausnahme z. B. für Diensteanbieter vor, die den Zugang zur Nutzung von Telediensten vermitteln. Voraussetzung ist, daß die Daten anonymisiert sind.

4.7. Bestands-, Nutzungs- und Abrechnunsgdaten

Mit zwei Vorschriften widmet sich der Entwurf des TDDSG den Voraussetzungen bestimmter im Rahmen von Telediensten anfallender Datenarten: Bestands-, Nutzungs- und Abrechnungsdaten. Welche personenbezogenen Daten jeweils zu diesen Daten zu zählen sind, ergibt sich nicht abschließend aus den Vorschriften in §§ 5 und 6. Dies ergibt sich vielmehr aus dem Zweck des jeweiligen Vertragsverhältnisses.

- **Bestandsdaten**

  Als Bestandsdaten sind nur solche Daten anzusehen, die für das Begründen, inhaltliche Ausgestalten oder Ändern des Vertrages über die Inanspruchnahme von Telediensten mit dem Diensteanbieter unerläßlich sind; es handelt sich dabei in der Regel um die Grunddaten des Vertragsverhältnisses; eine Verarbeitung und Nutzung der Bestandsdaten für andere Zwecke als den Vertragszweck ist nur mit ausdrücklicher Einwilligung des Nutzers zulässig.

  Im Regierungsentwurf war die Befugnis des Diensteanbieters vorgesehen, personenbezogene Bestandsdaten im Einzelfall auf Ersuchen zum Zwecke der Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes zu übermitteln[29]. Ob die genannten Behörden zu einem Ersuchen befugt sind, ergab sich nicht aus dieser Vorschrift. Sinn und Zweck der Regelung war allein die Berücksichtigung der vom Zweck des Vertragsverhältnisses zwischen Nutzer und Diensteanbieter nicht mehr erfaßten Übermittlung von Bestandsdaten an die genannten Behörden. Die Befugnis mußte sich daher – zusätzlich zu § 5 Abs. 3 TDDSG – aus anderen Vorschriften ergeben.[30]

  Der Deutsche Bundestag hat diese Vorschrift gestrichen. Mit der Streichung hat er eine wichtige inhaltliche Änderung des Regierungsentwurfs vorgenommen, deren Wirkung sich nicht nur auf den Datenschutz bei Telediensten beschränkt.

[29] vgl. entsprechende Regelung in § 89 Abs. 7 TKG
[30] vgl. hierzu: Engel-Flechsig, DuD 1/1997, S. 14 , RDV 2/1997, S. 65

Die Regelung zur Übermittlung von Bestandsdaten an Strafverfolgungs- und Sicherheitsbehörden war während der parlamentarischen Debatte umstritten. Der Bundesrat hatte in seiner Stellungnahme bereits auf sein Bedenken hingewiesen, Datenschutzbeauftragte, Wirtschaft und Wissenschaft haben übereinstimmend auf verfassungsrechtliche Bedenken im Hinblick auf den Grundsatz der Verhältnismäßigkeit und im Hinblick auf den ungehinderten Zugriff der Sicherheitsbehörden auf personenbezogene Bestandsdaten bei Diensteanbietern hingewiesen. Die Vorschrift – im Wortlaut entsprechend wie bereits geltende Bestimmungen im TKG (§ 89 Abs. 6) oder im Entwurf des Postgesetzes (§ 41) formuliert – wurde darüber hinaus nicht nur als Befugnisnorm für den Diensteanbieter zur Übermittlung der Bestandsdaten[31], sondern als eigenständige Ermächtigungsgrundlage für Strafverfolgungs- und Sicherheitsbehörden aufgefaßt.

Die Bestimmung des § 5 Abs. 3 TDDSG ist vom Deutschen Bundestag zu Recht gestrichen worden. Die Weitergabe personenbezogener Daten an Sicherheitsbehörden soll nicht im Informations- und Kommunikationsdienste-Gesetz geregelt werden. Es bedarf der grundsätzlichen Klärung der Frage, ob und wieweit private Unternehmen Auskunftsverpflichtungen gegenüber im Vorfeld der Strafverfolgung ermittelnden Diensten nachkommen müssen. Die Sicherheitsbehörden dürfen bei Ausübung ihrer Tätigkeiten im Rahmen ihrer Befugnisse nicht durch neue technologische Entwicklungen behindert werden, aber die Befugnisse der Sicherheitsbehörden dürfen auch nicht in Abhängigkeit von den technischen Möglichkeiten gestaltet werden.

Die grundsätzliche Frage nach den Befugnissen der Sicherheitsbehörden ist damit nicht gelöst. Diese Frage muß vielmehr grundlegend geprüft werden. Gegebenenfalls kann sie dann in einem generellen Gesetz, zum Beispiel dem BDSG, oder in den jeweiligen Spezialgesetzen der Sicherheitsbehörden geregelt werden. Der Weg zurück in das TDDSG ist angesichts der rechtlichen und politischen Problematik nicht möglich.

- **Nutzungsdaten**

  Als Nutzungsdaten sind solche Daten anzusehen, die dem Nutzer die Nachfrage nach Telediensten ermöglichen; es handelt sich dabei um Daten, die während der Nutzung eines Teledienstes, z. B. Interaktionen des Nutzers mit dem Diensteanbieter, entstehen; Beispiel: clickstream. Nutzungsdaten sind nach Ende der jeweiligen Nutzung des Teledienstes zu löschen, soweit sie nicht zu Abrechnungszwecken erforderlich sind.

  Vom TDDSG nicht erfaßt werden sog. Verbindungsdaten im Sinne von § 5 Abs. 1 der Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsleistungen erbringen (TDSV), d. h. Daten, die zur Bereitstellung von Telekommunikationsdienstleistungen dienen. Nur bestimmte Verbindungsdaten dürfen nach diesen telekommunikationsrechtlichen Vorschriften erhoben und verarbeitet werden. Soweit bei der Inanspruchnahme von Telediensten Verbindungsdaten im Sinne der TDSV anfallen, findet diese Anwendung.

- **Abrechnungsdaten**

  Als Abrechnungsdaten sind solche Daten anzusehen, die für die Abrechnung der Inanspruchnahme von Telediensten erforderlich sind. Abrechnungsdaten dürfen nicht länger gespeichert werden, als es für die Abrechnung erforderlich

[31] vgl. so die Begründung zum Regierungsentwurf, BT-Drs. 13/7385, S. 24: „Die Vorschrift erlaubt dem Diensteanbieter eine zweckändernde Nutzung der Bestandsdaten; die Befugnisse der genannten Behörden werden davon nicht berührt."

ist; Abrechnungsdaten sind daher grundsätzlich nach Erfüllung der Forderung zu löschen. Das Gesetz geht davon aus, daß auch Abrechnungsdaten grundsätzlich beim jeweiligen Diensteanbieter verbleiben. Abs. 3 schließt daher eine Übermittlung von personenbezogenen Abrechnungsdaten an andere Diensteanbieter oder Dritte prinzipiell aus. Ausnahmen gelten nur für den Diensteanbieter, der den Zugang zur Nutzung von Telediensten vermittelt; dieser darf anderen Diensteanbietern oder Dritten Nutzungsdaten zu Zwecken der Marktforschung dieser Diensteanbieter in anonymisierter Form übermitteln, und er darf Abrechnungsdaten, soweit diese für die Einziehung einer Forderung dieses Diensteanbieters erforderlich sind, übermitteln. Dem Interesse der Diensteanbieter an einer Abrechnung durch dritte Unternehmen wird im Kabinettentwurf Rechnung getragen: Hat der Diensteanbieter mit einem Dritten einen Vertrag über die Abrechnung geschlossen, so darf er diesem Dritten Abrechnungsdaten zum Zwecke der Abrechnung übermitteln. Eine Übermittlung zu einer anderen Zweckbestimmung oder eine weitergehende Nutzung durch den Dritten ist unzulässig. Der Diensteanbieter hat den Dritten auf die Einhaltung des Fernmeldegeheimnisses (§ 85 TKG) zu verpflichten.

4.8. Auskunftsrecht des Nutzers

Der Nutzer soll – über das nach dem BDSG geltende Auskunftsrecht hinaus – die über ihn oder sein Pseudonym gespeicherten Daten unentgeltlich elektronisch einsehen können. Dies gilt in Abweichung von den hier ergänzend anwendbaren Vorschriften des BDSG, soweit es sich um Dateien handelt, die nur kurzfristig im Sinne von §§ 34 Abs. 4, 33 Abs. 2 Nr. 5 BDSG vorgehalten werden. Die Gewährleistung dieses Einsichtsrechts erübrigt sich, wenn die Inanspruchnahme von Angeboten anonym – beispielsweise mit Hilfe von vorbezahlten Wertkarten – ermöglicht wird.

4.9. Datenschutzkontrolle und Datenschutz-Audit

§ 8 TDDSG rundet den Katalog der Neuregelungen im Bereich der Teledienste ab. Das TDDSG ändert die vom BDSG vorgenommene Aufsichts- und Kontrollstruktur nicht.

Angesichts der überregionalen Ausdehnung zahlreicher Dienste hätte sich eine ähnliche Regelung wie in § 91 Abs. 4 TKG auch für den Bereich der Teledienste angeboten. Diese Vorschrift überträgt dem Bundesbeauftragten für den Datenschutz für die geschäftsmäßige Erbringung von Telekommunikationsdienstleistungen die Aufgaben der Aufsichtsbehörden bei Unternehmen. Bei Telediensten ist jedoch zu beachten, daß Diensteanbieter nicht nur überregional tätig sind (Beispiel: AOL, Compuserve etc.), sondern auch regional oder lokal beschränkte Teledienstangebote (Beispiel: Handwerksbetrieb) möglich sind. Kann die Effizienz der Kontrolle im Datenschutz – im nicht-öffentlichen wie im öffentlichen Bereich – bei überregional tätigen Teledienstanbietern durch eine eindeutige Zuordnung dieser Aufgaben zu einer Stelle gewährleistet werden, sind die datenschutzrechtlichen Vorschriften bei den Angeboten kleiner und mittelständischer Diensteanbieter, die ihre Teledienste regional oder lokal begrenzt anbieten, durch eine zentrale Stelle kaum noch effektiv zu kontrollieren. Im Ergebnis hat sich der Gesetzentwurf deshalb für eine Lösung entschieden, die an dem vorhanden Kontrollsystem festhält. Die Erfahrungen mit diesem Kontrollsystem sind abzuwarten. Es ist zu hoffen, daß die Datenschutzbeauftragten von Bund und Ländern sowie die Aufsichtsbehörden zu einem abgestimmten Vorgehen kommen werden, um gleiche Regeln und Verfahren für wirksame Kontrollen zu finden. Dies ist besonders wichtig für die Planungssicherheit ausländischer Unternehmen, die einheitliche Rahmenbedingungen in der Bundesrepublik Deutschland für Investitionen und einheitliche Ansprechpartner für Datenschutzkontrollen vorfinden müssen.

Der Deutsche Bundestag hat die Frage der einheitlichen Kontrolltätigkeit der Aufsichtsbehörden sehr ernst genommen. Er hat deshalb einen neuen Absatz angefügt, der dem Bundesbeauftragten für den Datenschutz im Bereich der Teledienste eine beobachtende Rolle zuweist. Mit dieser Ergänzung der datenschutzrechtlichen Vorschriften soll die allgemeine Beobachtung der Entwicklung des datenschutzrechtlichen Instrumentariums bei Telediensten gewährleistet werden. Der Bundesbeauftragte für den Datenschutz soll diese Entwicklung in seinen Tätigkeitsberichten aufzeigen. Praktische Bedeutung kommt dieser Aufgabe des Bundesbeauftragten für den Datenschutz bei der Entwicklung einheitlicher Maßstäbe für die Kontrolle oder die datenschutzrechtlichen Bestimmungen bei Telediensten zu. Durch die Entschließung des Deutschen Bundestages, die eine Prüfung der Akzeptanz der datenschutzrechtlichen Bestimmungen bei Nutzern und Unternehmen durch die Bundesregierung fordert,[32] erhält diese Aufgabe zusätzlichen praktischen Wert.

Der Gewährleistung einer wirksamen Kontrolle dient der Verzicht auf die aufgrund hinreichender Anhaltspunkte vorzunehmende Aufsichtstätigkeit der Aufsichtsbehörden gemäß § 38 BDSG. Dieser Verzicht trägt im Ansatz der Datenschutzkonzeption Rechnung, die den Aufsichtsbehörden eine aktive Rolle bei der Umsetzung des Grundsatzes des Systemdatenschutzes zuweist.

De lege ferenda wird das System der Datenschutzkontrolle jedoch um einen weiteren Gedanken zu ergänzen sein: das Datenschutz-Audit.

Funktion des Datenschutz-Audits könnte es sein, die Ziele der Datenvermeidung und eines hohen Datenschutzniveaus durch Stärkung und Unterstützung der unternehmerischen Selbstverantwortung zu erreichen. Das Datenschutz-Audit könnte sich nach Auswertung entsprechender Erfahrungen als ein geeignetes Instrument erweisen, im Wege der Selbstregulierung und der Schaffung marktgerechter Anreize ein hohes Datenschutzniveau sicherzustellen.[33]

Erfahrungen mit dem Mittel des Audits bestehen bislang noch nicht. Lediglich im Bereich der Umweltpolitik ist durch eine Verordnung der Europäischen Gemeinschaft[34] und ein Ausführungsgesetz des Bundes[35] ein Umweltaudit-Verfahren vorgesehen.

Das Datenschutz-Audit bedarf einer gesetzlichen Grundlage, wenn damit in den Schutzbereich von Art. 12 GG eingegriffen wird. Dies könnte sowohl durch die Festlegung der Anforderungen an die Prüfung und Bewertung als auch an das Verfahren sowie die Auswahl und Zulassung möglicher Gutachter geschehen. Damit würde das Datenschutz-Audit dem verfassungsrechtlichen Vorbehalt des Gesetzes in Art. 12

---

32 vgl. hierzu BT-Drs. 13/7935

33 vgl. auch positive Wertung in Roland Bachmeier, Datenschutz-Audit, DuD 11/96, S. 680; ders., Vorgaben für datenschutzgerechte Technik, DuD 11/96, S. 672 ff. (673); ebenso: Otto Ulrich, Leitbildwechsel. Dem (sicherheits-)technologisch aktivierten Datenschutz gehört die Zukunft, DuD 11/96, S. 664 ff. (668); vgl. jetzt grundlegend: Roßnagel, DuD 9/1997, S. 505 ff.

34 EWG 1836/93 vom 29. 6. 1993, ABl. L 168 vom 10. 7. 1993

35 Umweltauditgesetz vom 7. 12. 1995, BGBl I, S. 1591

Abs. 1 Satz 2 GG unterliegen. Eine Regelung dieser Fragen bleibt – wenn das Datenschutz-Audit diese Gestalt annehmen sollte – einem besonderen Gesetz vorbehalten[36]. Ohne diesen berufsbeschränkenden Charakter kann das Datenschutz-Audit bereits jetzt praktiziert werden – allerdings nur auf freiwilliger Basis und ohne vom Gesetzgeber vorgegebene Verfahren.

Das Audit ist angesichts der technischen Entwicklungen im Bereich der neuen Informations- und Kommunikationsdienste eine Antwort auf das gestiegene Datenschutzbewußtsein bei der Verarbeitung personenbezogener Daten bei Anwendern und Nutzern. Der Grundsatz richtet sich in erster Linie an Diensteanbieter, die bei der Konzeption ihres Angebots – eventuell auch bei der Entwicklung von Soft- und Hardware – datenschutzrechtliche Belange berücksichtigen wollen. Dem kann z. B. durch die Schaffung von Gütesiegeln Rechnung getragen werden. Damit bietet das Audit die geeignete Grundlage für ausländische Diensteanbieter, die vom Ausland aus ihre Teledienste in Deutschland anbieten wollen, ohne auf den in der Bundesrepublik hohen Datenschutzstandard zu verzichten, und die damit ihre Akzeptanz bei deutschen Nutzern erhöhen können. Das Audit kann schließlich auch die Rolle des betrieblichen Datenschutzbeauftragten unterstützen, der im nicht-öffentlichen Bereich gemäß § 37 BDSG die Aufgabe der Überwachung der Einhaltung datenschutzrechtlicher Vorschriften hat.

5. Die Entschließung des Deutschen Bundestages zum IuKDG

Bei der Verabschiedung des IuKDG hat der Deutsche Bundestag einen Entschließungsantrag der Fraktionen der CDU/CSU und der F.D.P. angenommen.[37] Dieser beruht auf dem parteiübergreifenden Gedanken, daß mit dem IuKDG Neuland betreten wird. Dies gilt vor allem für die Regelungen zum bereichsspezifischen Datenschutz sowie für die Regelungen der digitalen Signaturen. Durch diese Regelungen werden innovative Entwicklungen im Recht und bei den neuen Technologien angestoßen und gefördert; sie leisten einen wichtigen Beitrag zu einer breiten Akzeptanz der neuen Dienste und stellen darüber hinaus Weichen für die Entwicklung von Leitlinien für die internationale Diskussion. Die künftigen Entwicklungen bei den neuen Diensten und die Erfahrungen mit dem IuKDG müssen deshalb sorgfältig, auch durch begleitende wissenschaftliche Forschung, beobachtet werden, um gegebenenfalls erforderliche Anpassungen bzw. Ergänzungen des Rechtsrahmens in geeigneter Form aufgreifen zu können.

Der Deutsche Bundestag fordert deshalb die Bundesregierung auf, die Entwicklung bei den neuen Informations- und Kommunikationsdiensten zu beobachten und darzulegen, ob und gegebenenfalls in welchen Bereichen Anpassungs- bzw. Ergänzungsbedarf bei den rechtlichen Rahmenbedingungen für die neuen Dienste besteht, und hierüber dem Deutschen Bundestag einen Bericht nach Ablauf von zwei Jahren nach Inkrafttreten des IuKDG vorzulegen.

[36] vgl. hierzu die ursprünglich im 1. Referentenentwurf des IuKDG vom 28. 6. 1996 vorgeschlagene Regelung für ein Datenschutz-Audit: „Zur Verbesserung von Datenschutz und Datensicherheit können Diensteanbieter ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt." Der MDStV enthält noch diesen ursprünglichen Hinweis auf ein Datenschutz-Audit, vgl. § 17 MDStV; vgl. jetzt dazu Roßnagel, DuD, 9/1997, S. 505 ff.

[37] vgl. BT-Drs. 13/7935; es lagen auch Entschließungsanträge von Abgeordneten der SPD, BT-Drs. 13/7936, und der Fraktion BÜNDNIS 90/ DIE GRÜNEN, BT-Drs. 13/7937, vor, die keine Mehrheit fanden.

Mit dieser Entschließung wird dem in den Beratungen immer wieder geäußerten Wunsch nach Beobachtung und Evaluierung der weiteren technischen und rechtlichen Entwicklung Rechnung getragen. Fehlentwicklungen kann so rechtzeitig begegnet werden. Dies gilt in besonderem Maße im Bereich des Datenschutzes, aber auch bei der Verantwortlichkeit und bei digitalen Signaturen.

Mit der Entschließung wird darüber hinaus vom Bundestag dokumentiert, daß er die offengebliebenen Fragen weiterverfolgen will. Zu diesen Fragen rechnet er im Bereich der digitalen Signaturen ausdrücklich die Frage nach der Haftung der Zertifizierungsstellen gegenüber Dritten, die in den parlamentarischen Beratungen kontrovers diskutiert worden war.[38]

6. Ausblick

Global wirksame Regelungen können im Bereich des Datenschutzes bei neuen Informations- und Kommunikationsdiensten nicht ausbleiben.

Die Diskussion mit inländischen und ausländischen Diensteanbietern wird bei den Diskussionen zum Teldienstedatenschutz vorrangig sein. Dabei wird es darauf ankommen, die vielgestaltigen Informations- und Kommunikationsbeziehungen datenschutzrechtlich sachgerecht zu bewerten und rechtlich einzuordnen. Es wird auch darauf ankommen, technische Innovationen mit dem Ziel der Verwirklichung des Systemdatenschutzes zu fördern, die auch grenzüberschreitende Wirkung entfalten. Darüber hinaus müssen schließlich die Möglichkeiten eines wirksamen Informationsschutzes durch den Nutzer berücksichtigt werden, wie sie digitale Signaturverfahren und sichere kryptographische Verfahren bieten.

In der Europäischen Union sind Anknüpfungspunkte durch die Verabschiedung der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[39] geschaffen worden. Auch im Bereich der digitalen Signaturverfahren gibt es Überlegungen der Europäischen Kommission, um die Voraussetzungen für den europaweiten Einsatz der digitalen Signatur zu schaffen. Damit könnte in Europa eine einheitliche Sichtweise von Datenschutz und Datensicherheit bei neuen Informations- und Kommunikationsdiensten möglich werden.

[38] vgl. hierzu den Bericht des federführenden Ausschusses in BT-Drs. 13/7934, S. 37

[39] ABl. EU C 93 vom 13. 4. 1995

Autorenverzeichnis

Dr. Ulf Brühann,

Leiter der Abteilung „Freier Verkehr von Informationen, Datenschutz und die damit verbundenen internationalen Aspekte“, Generaldirektion XV der Europäischen Kommission, Brüssel

Dr. Giovanni Buttarelli,

Generalsekretär der Italienischen Datenschutzkommission, Rom

Stefan Engel-Flechsig,

Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, Referat M 1 „Multimedia – Rechtliche Rahmenbedingungen“, Bonn

Dr. Hansjürgen Garstka,

Berliner Datenschutzbeauftragter

Prof. Dr. Peter L. Heinzmann,

Leiter des Interkantonalen Technikums Rapperswil, Schweiz

Marc Rotenberg,

Director, Electronic Privacy Information Center (EPIC), Washington, DC

Prof. Dr. Alan F. Westin,

Professor emeritus of Public Law and Government, Columbia University, New York; Herausgeber der Zeitschrift „Privacy & American Business“