Datenschutz bei Informations- und Kommunikationsdiensten

Alfred Büllesbach

Gutachten

Herausgeber: Stabsabteilung der Friedrich-Ebert-Stiftung

53170 Bonn (Briefanschrift)
Godesberger Allee 149, 53117 Bonn

Umschlag: Pellens Kommunikationsdesign GmbH, Bonn
Layout: PAPYRUS – Schreib- und Büroservice
Gesamtherstellung: Druckerei Plump, Rheinbreitbach
Printed in Germany 1997

Vorwort

Die Notwendigkeit eines sicheren Datenschutzes in einer sich verändernden Informationsgesellschaft wirft umfangreiche Fragestellungen auf. Die Entwicklung der Informations- und Kommunikationstechnologien ändert zwar nichts an den verfassungsrechtlich begründeten und gesetzlich abgesicherten Grundsätzen zu Datenschutz und Datensicherheit, zwingt aber dazu, die Möglichkeiten ihrer Verwirklichung zu überprüfen. Die neuen Technologien zeichnen sich durch Vernetzung und dezentrale Anwendung aus. Dabei fallen – oft ohne Wissen des Betroffenen – große Mengen personenbezogener Daten an, deren weitere Nutzung nicht nachvollziehbar ist.

Voraussetzung für hohe Akzeptanz bei Nutzern und Anbietern ist Vertrauen. Deshalb sollten Datenschutz und Datensicherheit integrale Bestandteile von Dienstleistungen, Produkten und Beratungen im Netz sein. Ziel von Datenschutzgesetzen und Datenschutztechniken sollte sein, so wenig wie möglich personenbezogene Daten zu produzieren, deren Verarbeitung transparent zu gestalten und auf vereinbarte Vorgänge zu beschränken. Je besser dies gelingt, desto mehr dürfte sich die Bereitschaft erhöhen, auf die Informations- und Kommunikationstechniken zurückzugreifen und ihre Vorteile zu nutzen. Das heißt, diese als Basistechnologie für eine neue wirtschaftliche Wertschöpfung zu etablieren.

Die im Informations- und Kommunikationsdienstegesetz (IuKDG) gefundenen Regelungen zum Datenschutz sind die derzeitige rechtliche Grundlage, auf der sich deutsche Anbieter und Nutzer im weltweiten Netz bewegen. Reichen diese Gesetze aus? Sind Lücken geblieben und weiterer Handlungsbedarf für die Politik vorhanden?

Die Friedrich-Ebert-Stiftung hat Prof. Dr. Alfred Büllesbach, Leiter Datenschutz in der debis Systemhaus GmbH, gebeten, ein Gutachten anzufertigen, in dem er die Entwicklungen und Gefahren darstellt und die gesetzlichen Bestimmungen hinsichtlich ihrer Wirksamkeit untersucht.

Dr. Jürgen Burckhardt
Geschäftsführendes Vorstandsmitglied
der Friedrich-Ebert-Stiftung

Problemstellung

Die moderne Informationstechnologie gilt als Basistechnologie für neu erwartete wirtschaftliche Wertschöpfung. Im Zentrum stehen die Integration bisher getrennter Informationstechniken, interaktive Tele- und Mediendienste, die Verbreitung im privaten und geschäftlichen Bereich und schließlich die weltumspannende universelle Erreichbarkeit von Individuen. Es liegt auf der Hand, daß dieser Prozeß vielfältige Neuerungen für Datenschutz und Datensicherheit verlangt. Wichtig ist, zu erkennen, daß bei der Nutzung der modernen Informations- und Kommunikationstechnologie große Mengen personenbezogener Daten anfallen, die ohne großen Aufwand gespeichert, vorgehalten und abgerufen werden können. Je nach Nutzungsart sind dies personenbezogene Daten über Kreditwürdigkeit, Gesundheit, Reiseverhalten, Kaufstile, sexuelle Orientierung, Mediennutzung etc. Es liegt auf der Hand, daß diese Daten ökonomisch hoch bedeutsam sind. Sie werden Gegenstand von zielgruppenorientierten Marketingstrategien, sie können aufbereitet, zusammengeführt, abgeglichen, kontrolliert und in vernetzten Systemen überwacht werden.

Einige Beispiele mögen dies verdeutlichen:

– Heute ist es einem Verbraucher möglich, sich das Angebot eines Händlers im Internet anzusehen und diesem dort auch direkt seine Bestellung zu übermitteln. Die Bezahlung erfolgt elektronisch. Das bedeutet datenschutzrechtlich, daß die gesamten Daten eines Geschäftsvorfalls gesammelt über ein Medium versandt werden. Dem Provider des Netzzuganges wäre es möglich, ein umfassendes Kommunikations- und Konsumprofil seiner Kunden zu erstellen, das sowohl verschiedene finanzielle Transaktionen (z.B. Begleichung einer Rechnung, bevorzugte Art der Bezahlung) als auch deren Inhalte (z.B. Aufstellung der bestellten Produkte, Geschäftspartner) enthält. Bisher lagen diese Daten eines Geschäftsvorfalls bei verschiedenen Stellen (Versandhaus, Bank, Telefongesellschaft) vor.

– Das interaktive Fernsehen unterscheidet sich von der herkömmlichen Form des Fernsehens dadurch, daß es Individualkommunikation anstelle von Massenkommunikation ermöglicht. Der Verbraucher hat also die Möglichkeit, über den Rückkanal gezielte Dienste und Inhalte abzurufen, die ihn persönlich interessieren. Diese Vorgänge erzeugen personenbezogene Daten. Diese können für unterschiedliche Zwecke gespeichert werden: für die Erbringung und die Abrechnung der erbrachten Leistungen, zur Definition und Bildung persönlicher Interessenprofile und deren Speicherung. Aufgrund dieses Interessenprofils erhält der Verbraucher alle relevanten Informationen und Angebote bei jeder Nutzung schneller (z.B. TV-Guide). Es liegt auf der Hand, daß solche Datenspeicherungen sensible Datensammlungen sind, die für mehrere Zwecke genutzt und mißbraucht werden können. So können Stamm-, Verbindungs- und Nutzungsdaten zu Persönlichkeitsprofilen verknüpft werden. Der Nutzer kann bestimmten Gruppen zugeordnet, eingeordnet und ausgegrenzt werden. Die Daten können an Dritte preisgegeben und zweckentfremdet, z.B. staatlicher Überwachung oder nicht erwünschter kommerzieller Manipulation und Nutzung zugeführt werden. Ein denkbares Szenario wäre z.B. eine Meinungsumfrage durch einen interaktiven Mediendienst. Dem Diensteanbieter stünde dann neben der Identität des Kunden auch seine Entscheidung – möglicherweise im Zusammenhang mit früher geäußerten Meinungen – zur Verfügung. Dies würde nicht nur die Erstel-

lung von Konsumprofilen, sondern auch von Meinungsprofilen des Kunden ermöglichen.

– Mit der zunehmenden Verbreitung von Internet-Anschlüssen nicht nur am Arbeitsplatz, sondern auch im privaten Haushalt bestellen viele Bürger bei Versandhäusern, Reiseveranstaltern oder im lokalen Pizzaservice via Internet. Diese Informationen werden gegenwärtig unverschlüsselt übertragen. Datenschutzrechtlich hat dies zur Konsequenz, daß nicht nur die erforderlichen Geschäftsdaten, sondern zunehmend auch Daten über die private Netznutzung entstehen. Manche dieser Daten könnten sogar zu kriminellen Zwecken weiterverwendet werden (z.B. bei Angabe der privaten Kreditkartennummer als Zahlungsform).

– Softwarekomponenten erlauben bei bestimmten Protokollen Besonderheiten, so daß Server spezielle Einstellungen auf dem Rechner des Benutzers speichern und später wieder abrufen können. Davon weiß der Nutzer nichts und bemerkt es auch nicht. Solche Anbindungen, die sogenannten „Cookies“, haben ambivalenten Charakter. Sie könnten beispielsweise als elektronische Rabattmarke im elektronischen Commerce fungieren, sie können aber auch dazu benutzt werden, um die Seiten, die ein Benutzer beim Besuch des Servers ausgesucht hat, zu speichern. Würden verschiedene solcher Cookies eines Benutzers zusammen abgerufen, so wären Rückschlüsse über seine Interessen und Neigungen möglich. Eine datenschutzrechtliche Speicherung und Verarbeitung dieser Daten ist nur bei informierter Zustimmung zulässig.

  Wie treffend von einem Richter am Bundesverfassungsgericht formuliert worden ist, ist auf die Abwesenheit des Staates in der modernen Kommunikationstechnologie kein Verlaß. Das wäre schon angesichts der virulenten staatlichen Kontrollbedürfnisse eine naive Erwartung. In der Tat zeigt der Entwurf zum Telekommunikationsbegleitgesetz unangemessene Erweiterungen staatlicher Überwachungsbedürfnisse auf die Gesamtheit der modernen Kommunikationstechnologie. Es handelt sich deshalb nicht nur um die lineare Erstreckung bisher bekannter Überwachungsmöglichkeiten nach G 10 Gesetz, §§ 100 a und b StPO sowie § 39 Außenhandelsgesetz gegenüber dem öffentlichen Fernmeldeverkehr, sondern um die Überwachung der gesamten kommerziellen Mediennutzung im privaten und geschäftlichen Bereich. Ein solcher staatlicher Eingriff in den gesamten privaten und geschäftlichen elektronischen Verkehr ist einmalig. Er muß politisch und gesellschaftlich umfangreich erörtert werden.

Die Beispiele zeigen, daß auf dem Weg in die Informationsgesellschaft, zur Förderung vielfältiger Anwendungs- und Nutzungsformen im Umgang mit Informations- und Kommunikationstechnologie, zur Nutzung von Multimedia, zur Nutzung des Electronic Commerce und auf dem Weg zum digitalen Fernsehen vielfältige Kommunikations- und Konsumprofile von Nutzern erstellt werden. Die Privatsphäre der Benutzer muß hergestellt bzw. gewahrt werden. Der Handlungsbedarf ist offensichtlich. Das vorgelegte IuKDG als Gesetzespaket, der Mediendienstestaatsvertrag und das TKG auf der Basis vorhandener allgemeiner Datenschutzregelungen muß durchdacht, erprobt und nach einer Erfahrungszeit auf einen einheitlichen, für den Bürger verständlichen Nenner gebracht werden. Unverhältnismäßige und nicht erforderliche Überwachungen sind zu unterlassen; der Kunde/Bürger muß Vertrauen in die Informationsgesellschaft setzen können.

Kurzfassung

Die Bedeutung von Datenschutz und Datensicherheit in der Informationsgesellschaft steigt mit der globalen Vernetzung und den damit verbundenen Datenspuren, der umfangreichen Erweiterung der Anwendungsmöglichkeiten, der Kombination verschiedener Dienste, der Erschließung neuer Märkte und der damit verbundenen Filigranisierung von Marketing-Strategien und nicht zuletzt mit der Erstreckung polizeilicher und geheimdienstlicher Befugnisse, auf die durch diesen Prozeß umfangreich neu entstandenen bzw. entstehenden personenbezogenen Daten. Parallel zu dieser Entwicklung spielen Fragen der Entmonopolisierung, der Deregulierung, der Entstaatlichung und damit verbunden der Privatisierung bisher öffentlich wahrgenommener Aufgaben eine Rolle, da sie zu Verlagerung von Datenverarbeitungsprozessen führen. Das Prinzip der Selbstbestimmung, das politisch, gesellschaftlich und individuell nicht zuletzt durch die Rechtsprechung des Bundesverfassungsgerichts im Volkszählungsurteil herausgearbeitet wurde, bildet im deutschen Datenschutzrecht einen Meilenstein. Die Auseinandersetzung mit dem Thema Datenschutz in der Informationsgesellschaft ist vor diesem Hintergrund zu sehen.

Die rechtliche und gesellschaftskritische Diskussion um Datenschutzgefährdungen setzt die grobe Skizzierung von Entwicklungslinien in der Informationstechnik voraus.

I. Entwicklungslinien in der Informationstechnik

1. Die Rechner- und Netzstrukturen entwickelten sich von proprietären und regionalen Systemen zu offenen und globalen Infrastrukturen.
2. Die bisher getrennten Informationstechniken und Medien wie Fernsehen/Rundfunk, Computer, Telefon, Zeitung, Versandhandel etc. wachsen zusammen und führen zu neuen multimedialen Anwendungen.
3. Die Nutzung der klassischen Medien war passiv, d.h., man kannte aktive Anbieter und passive Verbraucher. Die heutigen Teledienste erlauben dialogisches und interaktives Verhalten aller Teilnehmer.
4. Während die bisherige technische Netzinfrastruktur zwischen Wirtschaft, öffentlichem Dienst, Forschung und privater Anwendung unterschied, nutzen heute alle diese Anwendungen eine technische Infrastruktur.
5. Die digitale Technik ist heute mit wachsender Tendenz auch in privaten Haushalten vorhanden. Weltweit wird heute bereits von 50 Millionen Internet-Anwendern gesprochen.
6. Weltumspannende, extraterrestrische Funknetze erlauben eine universelle Erreichbarkeit des Individuums unter einem Anschluß, in dem gleichzeitig alle multimedialen Nutzungen möglich sind.
7. Die Softwaregestaltung erlaubt es Fachleuten wie Laien, Massenanwendungen mit einheitlichen Standards und Oberflächen zu nutzen.
8. Die moderne Softwaretechnologie erlaubt Interaktionen zwischen Softwarekomponenten auf verschiedenen Plattformen und in verschiedenen Lokationen (z.B. Client Server, aktive Inhalte etc.).

II. Datenschutz- und IV-Sicherheitsgefährdungen

Die oben dargestellte informationstechnische Entwicklung führt dazu, daß personenbezogene Daten weltweit – teilweise ohne Wissen des Nutzers – anfallen. Hierbei handelt es sich um Nut-

zungs- und Verbindungsdaten, die für Zwekke der Abrechnung, der Fehlersuche und der Leistungsverbesserung benötigt werden, aber auch für Zwecke verschiedener Auswertungen wie Kommunikations- und Nutzungsprofile, Verhaltens- und Leistungskontrollen etc. mißbraucht werden können. Darüber hinaus wachsen die öffentlichen und privaten Telekommunikationsnetze zu komplexen Multibetreibernetzen zusammen und erhöhen für die Nutzer die Unübersichtlichkeit der Verantwortung.

Neben den datenschutzrechtlichen Gefährdungen erfordert die zuverlässige Nutzung die Beachtung der Anforderungen für sichere Kommunikationssysteme. Dies umfaßt die Identifikation und Authentisierung von Sender und Empfänger, die Zuordnung der verteilten Rechte, deren Prüfung, die korrekte Übertragung der vom Absender freigegebenen, autorisierten und an den ausgewählten Empfänger zu übertragenen Nachricht und deren Sicherung sowie die Nachweisbarkeit des Empfangs, die Gewährleistung der Vertraulichkeit von Empfänger, Sender und Nachricht. Für ausgewählte Verfahren sind Kontrollmechanismen erforderlich, z.B. zur Beweissicherung, Protokollierung für Zwecke der Datenschutz- und Sicherheitskontrolle.

III. Folgerungen

1. Multimedia und globale Datennetze bilden die Basis für technologische und wirtschaftliche Entwicklung in der Informationsgesellschaft. Voraussetzung für hohe Akzeptanz bei Verbrauchern, Bürgern und kommerziellen Nutzern ist Vertrauen. Vertrauen wird nicht nur durch zentrale Regulierung herstellbar, sondern durch die Bereitstellung vertrauenswürdiger Dienstleistungen, die jeder nutzen kann. Daraus folgt, daß es umfangreicher Konzepte für Dienstleistungen und Produkte zum Schutz gegen Mißbrauch des Netzes, zum Schutz gegen persönlichkeitsverletzende und kriminelle Dienstleistungen und für sichere und vertrauenswürdige Verfahren bedarf. Datenschutz muß nicht nur rechtlich und organisatorisch, sondern insbesondere auch technisch verstärkt umgesetzt werden.
2. Entscheidender Grundsatz für die politischen und rechtlichen Rahmenbedingungen ist die Erbringung der vertrauenswürdigen Dienstleistungen durch Private im freien Wettbewerb. Datenschutz und Datensicherheit werden so zum Bestandteil des Wettbewerbs.
3. Eine Regulierung des Einsatzes kryptographischer Verfahren zum Zwecke des Abhörens durch Ermittlungs- und Sicherheitsbehörden ist unverhältnismäßig. Die deutsche Wirtschaft braucht den freien Zugang zu kryptographischen Verfahren, denen sie vertrauen kann.
4. Politisch ist die Standardisierung von technischen Komponenten und Dienstleistungen zu fördern, um die Kompatibilität der Verfahren und die Qualität auf einem angemessenen Niveau sicherzustellen.
5. Die vertrauenswürdigen Dienstleistungen auf Basis von kryptographischen Verfahren haben globale Bedeutung. Es müssen zügig multi- und bilaterale Vereinbarungen über die gegenseitige Anerkennung dieser Verfahren abgeschlossen werden.

IV. Empfehlungen

1. Die zergliederten bereichsspezifischen Regelungen – einschließlich der neuen Gesetze – schaffen für Datenschutz und IV-Sicherheit teilweise überschneidende Überregulierung und eine strukturelle Unübersichtlichkeit für Nutzer, Verbraucher und Normadressaten. Für den Bürger und für die Anwender sollten nach kurzer Erfahrungszeit klarere Regelungen geschaffen werden.
2. Die Eigenverantwortung der Bürger für ihren Datenschutz und die Sicherheit ihrer Anwendung ist durch öffentliche Diskussionen zu fördern und das Bewußtsein für Selbstschutz und eigenen Systemschutz zu stärken.
3. Die Kompetenzverteilung zwischen Bund und Ländern ist vor dem Hintergrund der internationalen Entwicklung der Informationstechnologie zu überdenken.

Inhaltsverzeichnis

Vorbemerkung

Die Auseinandersetzung um Datenschutz in einer sich verändernden Informationsgesellschaft, die von den Stichworten Multimedia, Dienstleistung, Informationstechnik als neuer Wertschöpfer, veränderte Abbildung, verändertes Rollenverhalten von Menschen, Entwicklung neuer Märkte und neuer Marktdynamiken begleitet wird, wirft umfangreiche Fragestellungen zum Verhältnis des einzelnen Bürgers im Umgang mit der neuen Informationstechnik national wie international auf. Neben der informationstechnologischen Entwicklung sind gleichzeitig Fragen der Entmonopolisierung, der Deregulierung, der Entstaatlichung und der Privatisierung[1] bisher öffentlich wahrgenommener Aufgaben verbunden. In dieser hier nur tendenziell aufgezeigten globalen Entwicklung zeigt sich, daß politisch, gesellschaftlich und individuell das Prinzip der Selbstbestimmung in den Vordergrund getreten ist.

Das Bundesverfassungsgericht hat dies im Volkszählungsurteil mit der Herausarbeitung des Rechts auf informationelle Selbstbestimmung deutlich gezeigt und damit – nicht nur für die deutsche Datenschutzrechtsentwicklung – einen Meilenstein gesetzt. Die Auseinandersetzung mit dem Thema „Datenschutz in der Informationsgesellschaft“ ist nur vor diesem Hintergrund vernünftig zu führen.

Ich gehe zunächst von der technischen, wirtschaftlichen und gesellschaftlichen Entwicklung aus, um auf dieser Basis die Datenschutzgefährdungen zu erkennen und die vorhandenen datenschutzrechtlichen Regelungen zu messen und schließlich zu weiteren politischen Forderungen zu gelangen.

1 Vgl. Büllesbach, Alfred (Hrsg.): Staat im Wandel – mehr Dienstleistung, weniger Verwaltung, Köln 1995.

Entwicklungslinien in der Informationstechnik

Die Entwicklung von rechnergestützten Informationssystemen zielt nicht nur auf eine Verbesserung der bisherigen Merkmale ab, vielmehr werden neue Systeme und Anwendungen entwickelt, die – miteinander kombiniert – eine neue Qualität in der Datenverarbeitung ausmachen. Durch diesen technischen Fortschritt ergeben sich auch neue Anforderungen an Datenschutz und IV-Sicherheit.

Im folgenden werde ich zunächst die wichtigsten Entwicklungslinien in der Informationstechnik erläutern, um dann auf die daraus resultierenden Gefährdungen für Datenschutz und Datensicherheit einzugehen.

1. Die Rechner- und Netzstrukturen entwikkelten sich von proprietären und regionalen Systemen zu offenen und globalen Infrastrukturen.

Die bisher verfügbaren Rechnersysteme waren weitgehend unabhängig voneinander. Kommunikation zwischen ihnen fand über herstellerabhängige Protokolle statt. Eine Vernetzung „nach außen“ war nur in seltenen Fällen gegeben. Die meisten Rechnerverbundsysteme bestanden aus Computern, die räumlich nahe beieinander angesiedelt waren. Wurde über mehrere Standorte hinweg kommuniziert, so geschah dies in den meisten Fällen über Leitungen, die von den lokalen Telekommunikationsunternehmen angemietet worden waren. Zudem fand eine Rechnerkommunikation oft nur innerhalb eines Unternehmens statt.

Heute werden zur standortübergreifenden Kommunikation zumeist öffentliche Netze genutzt, d.h., Leitungen werden nicht mehr exklusiv durch eine Firma, sondern von vielen Teilnehmern verwendet. Statt verschiedenen proprietären Kommunikationsprotokollen wird heute zunehmend der Standard des Internets (TCP/IP[2]) verwendet. Darüber hinaus haben sich die Ansprüche an die Kommunikationsmöglichkeiten verändert. Rechnerkommunikation soll zunehmend auch zwischen verschiedenen Unternehmen (z.B. im Rahmen einer Händler-Kunden-Beziehung) möglich sein. Dies verlangt nach einer leistungsfähigeren Infrastruktur, die jederzeit eine standort- und herstellerunabhängige Kommunikation ermöglicht. Dies wird durch den allgemeinen Trend hin zu den Internet-Standards begünstigt.

Dies bedeutet allerdings auch, daß „jeder mit jedem“ vernetzt sein muß, was auch das „Eindringen“ von Unberechtigten in die firmeneigenen Rechnersysteme potentiell ermöglicht. Insbesondere da die Schwächen der meisten im Internet verbreiteten Systeme bekannt sind (und neue Schwächen über dasselbe Netz schnell bekannt gemacht werden[3]), werden hohe Anforderungen an die Sicherheitsadministration gestellt.

2 Transmission Control Protocol/Internet Protocol: Die Standards des Internets werden in sog. RFCs (Request for Comment) niedergelegt. Eine Beschreibung der Kommunikationsstandards der TCP/IP-Serie findet sich im RFC 1180 „*A TCP/IP Tutorial*“. Alle RFCs können beim Network Information Center via Internet abgerufen werden. *http://www.internic.net/ds/dspg1intdoc.html*
Im Rahmen einer Protokoll-Neugestaltung wurde der neue Internet-Standard IP Version 6 entwickelt. Dieser ist im RFC 1883 unter dem Titel „Internet Protocol, Version 6 (IPv6) Specification“ niedergelegt.

3 Sicherheitsschwächen sowie die Beschreibung aktueller Sicherheitsprobleme bei bestimmten Systemen werden im Internet über verschiedene sog. Mailing-Lists verteilt. Ein Beispiel hierfür ist die Mailing-List des DFN-CERT *win-sec-ssc*, über die Warnungen und Informationen des DFN-CERT verschickt werden.

2. Die bisher getrennten Informationstechniken und Medien wie Fernsehen, Rundfunk, Computer, Telefon, Zeitung, Versandhandel etc. wachsen zusammen und führen zu neuen multimedialen Anwendungen.

Bisher besaßen die Informationstechniken jeweils eigene „Übertragungswege" vom Anbieter zum Verbraucher. Fernsehsendungen wurden über Hochfrequenzwellen verbreitet, Computer kommunizierten über Koaxialkabel, Kataloge wurden in gedruckter Form verteilt. Verschiedene Anwendungen führten daher zwangsläufig zu „Medien-Brüchen", die in dieser Art mit modernen Informationssystemen nicht mehr notwendig sind. So ist es z.B. einem Verbraucher möglich, sich das Angebot eines Händlers im Internet anzusehen und diesem dort auch direkt seine Bestellung zu übermitteln. Sogar die Bezahlung kann unter Verwendung von „elektronischem Geld"[4] im Internet stattfinden.

Dies bedeutet, daß die gesamten Daten eines Geschäftsvorfalls gesammelt über ein Medium versandt werden. Dem Provider des Netzzuganges wäre es daher möglich, ein umfassendes Kommunikations- und Konsumprofil seiner Kunden zu erstellen, das sowohl verschiedene finanzielle Transaktionen (z.B. Begleichung einer Rechnung, bevorzugte Art der Bezahlung) als auch deren Inhalte (z.B. Aufzählung der bestellten Produkte, Geschäftspartner) enthält. Bisher lagen jeder Stelle (z.B. Versandhaus, Bank, Telefongesellschaft) nur diejenigen Daten vor, die sie zu Zwecken der Abrechnung (eventuell Fehlerbehebung o.ä.) brauchte. Die Gesamtheit der bei einem Geschäftsvorfall angefallenen Daten war also auf verschiedene Stellen verteilt. Jetzt liegen sie zusammengefaßt bei einer Stelle vor.

3. Die Nutzung der klassischen Medien war passiv, d.h., man kannte aktive Anbieter und passive Verbraucher. Die heutigen Teledienste erlauben dialogisches und interaktives Verhalten aller Teilnehmer.

Während der Verbraucher bei der Nutzung klassischer Medien – wie Fernseher oder Zeitung – nur passiv konsumieren konnte, machen moderne Teledienste eine aktive Teilnahme am Geschehen möglich. Dies kann das Verhalten oder die Präferenzen eines Kunden widerspiegeln.

Ein denkbares Szenario wäre z.B. eine Meinungsumfrage durch einen solchen Teledienst. Dem Diensteanbieter stünden dann neben der Identität des Kunden auch seine Entscheidung – möglicherweise im Zusammenhang mit früher geäußerten Meinungen – zur Verfügung. Dies würde die Erstellung nicht nur eines Konsumprofils, sondern auch eines Meinungsprofils des Kunden ermöglichen.

4. Während die bisherige technische Netzinfrastruktur zwischen Wirtschaft, öffentlichem Dienst, Forschung und privaten Anwendungen unterschied, nutzen heute alle diese Anwendungen eine technische Infrastruktur.

Große Wirtschaftsunternehmen besaßen bisher eigene Telekommunikationsinfrastrukturen (oder hatten diese im Bereich der Deutschen Telekom angemietet) und betrieben darauf eigene „Firmennetze". Aus dem „Forschungsnetz" zwischen Universitäten hat sich das heutige „Internet" entwickelt. Auch im öffentlichen Dienst gab es eigene Netzinfrastrukturen, d.h., diese Anwendungsbereiche waren schon durch die unterliegende Infrastruktur voneinander abgetrennt.

Heute sehen viele Unternehmen und Behörden ein Einsparungspotential darin, keine eigenen Leitungen – also ein privates Netz – zu besitzen, sondern die Infrastruktur des Internets zu nutzen. Innerhalb des Internets entstehen also verschiedene „virtuelle private Netze", d.h., daß Daten aus völlig unterschiedlichen Anwendungsbereichen und Quellen „vermischt" über eine Infrastruktur übermittelt werden. Es muß

4 Konzepte zu „elektronischem Geld" finden sich im Internet unter *http://www.digicash.com/*oder bei *http://www.cybercash.com/*.

also technisch und organisatorisch sichergestellt werden, daß die gesendeten Daten einerseits den gewünschten Empfänger erreichen und andererseits auf dem allgemeinen Übertragungsweg nicht ausgespäht werden. Eine mögliche Lösung ist hier der Einsatz kryptographischer Methoden. Zusätzlich muß gewährleistet werden, daß die unterliegende Kommunikationsinfrastruktur so leistungsfähig ist, daß sie dem wachsenden Kommunikationsverkehr zuverlässig standhält.

5. Die digitale Technik ist heute mit wachsender Tendenz auch in privaten Haushalten vorhanden. Weltweit wird bereits heute von über 50 Millionen Internet-Anwendern gesprochen.

Bis in die 70er Jahre war Rechnertechnologie alleine großen Firmen und Organisationen vorbehalten, die Computer als Rationalisierungsmittel nutzten. Die Anschaffungskosten für diese Geräte machten es Privatleuten unmöglich, Rechner zu Hause zu verwenden. Der Computer hatte also lediglich Einzug in die Arbeitswelt – jedoch nur an ausgewählten Arbeitsplätzen – gehalten.

Dies änderte sich, als Hardware-Hersteller zu Beginn der 80er Jahre kleine, nicht sehr leistungsfähige Geräte zu Konsumentenpreisen auf den Markt brachten. Der „Home-Computer“ hielt – zuerst als reines Spielzeug, später auch als Arbeitsmittel – zunächst zögerlich Einzug in den Privatbereich. Später drängte der leistungsstärkere und universell einsetzbare PC in immer mehr Haushalte. Auch an nicht-technischen Arbeitsplätzen und in den Büros hielt der PC (zumeist vernetzt mit anderen) Einzug.

Mittlerweile besitzen viele dieser Rechner sogar einen Anschluß ans weltumspannende Internet, und die Anwender können so die Vielzahl der Angebote nicht nur am Arbeitsplatz, sondern auch privat nutzen. Zudem zielen die Angebote im Internet immer mehr auf Privatpersonen ab. So werben dort beispielsweise Reiseveranstalter und Versandhäuser. Aber auch Pizza kann beim lokalen Pizza-Service via Internet bestellt werden.

Da darüber hinaus die meisten im Internet übertragenen Informationen unverschlüsselt versendet werden, könnten beim Netzanbieter auch Inhalte der privaten Kommunikation gesammelt werden. Dies hat zur Konsequenz, daß nicht nur „Geschäftsdaten“, sondern zunehmend auch Daten über die private Netznutzung entstehen. Manche dieser Daten könnten sogar zu kriminellen Zwecken „weiterverwendet“ werden (z.B. die private Kreditkarten-Nummer).

6. Weltumspannende, extraterrestrische Funknetze erlauben eine universelle Erreichbarkeit des Individuums unter einem Anschluß, in dem gleichzeitig alle multimedialen Nutzungen möglich sind.

Die Nummer, unter der Benutzer telefonisch erreichbar waren, wurde früher durch den Standort, an dem sie sich befanden, bestimmt. Konnte man also eine Führungskraft in ihrem Büro unter der Nummer A erreichen, so mußte man, wollte man sie zu Hause anrufen, die Nummer B kennen und wählen. Befand sich die Person auf dem Weg oder war ihr Aufenthaltsort nicht genau bekannt, so war es nicht möglich, sie zu erreichen.

Wurde durch die Mobilität einer Person früher ihre Erreichbarkeit erheblich eingeschränkt, so schließen sich diese beiden Begriffe heute nicht mehr aus. Teilnehmer können nun jederzeit und an jedem Ort unter einer einheitlichen Nummer erreicht werden. Es ist sogar für die Telefondienste feststellbar, wo sich der Benutzer zum Zeitpunkt eines Telefonats befindet. Hierdurch ist es möglich, ein Bewegungsprofil des Nutzers zu erstellen.

Zusätzlich können über diese einheitliche Nummer nicht nur Telefondienste, sondern (mit entsprechenden technischen Mitteln) auch Multimedia-Dienste jeglicher Art in Anspruch genommen werden, z.B. Internet und Versenden von elektronischer Post. D.h., daß die gesamte Kommunikation einer Person unter einer „Kommunikationsnummer“ bei einem Diensteanbieter anfällt. Durch Auswertung der hier auflaufenden Informationen kann ein komplettes Kommunikationsprofil des Nutzers gebildet werden.

7. Die Software-Gestaltung erlaubt es Fachleuten wie Laien, Massenanwendungen mit einheitlichen Standards und Oberflächen zu nutzen.

Die Benutzerschnittstellen von früheren Rechnersystemen waren meist textbasiert ausgelegt. Zur Bedienung mußte der Nutzer über intime Systemkenntnisse verfügen und meist kryptische Befehle über die Tastatur eingeben.

Moderne Benutzeroberflächen sind zumeist graphisch orientiert. Neben der Tastatur wurden neue Eingabegeräte (z.B. Maus) entworfen, die dem Nutzer die Handhabung vereinfachen und die Interaktion mit der Maschine intuitiv ermöglichen sollen. Damit wurde auch „Computer-Laien“ der Zugang zum Rechner erschlossen. Insbesondere die „Benutzung“ des Internets (das sog. „Surfen“) ist per Maus-Klick möglich. Die Eingabe von Befehlen über die Tastatur ist damit fast überflüssig geworden. Auf diese Weise wurde praktisch jedermann die Möglichkeit gegeben, kinderleicht das globale Informationsangebot zu nutzen. Das Internet stellt sich so für den Nutzer als ein großes System dar, aus dem er beliebig Informationen schöpfen kann („information at your fingertips“). Es wird für ihn schwer nachvollziehbar, von welchem Rechner in welchem Land er gerade Informationen empfängt.

Auch kommerzielle Anwendungen wie Textverarbeitungssysteme und Tabellenkalkulationsprogramme nutzen heute einheitliche Standards bezüglich einer graphischen Benutzeroberfläche. Dies resultiert in Zukunft in einem (leicht bedienbaren) „Nutzersystem“, das sowohl Netz- als auch Bürofunktionalitäten integriert. So werden künftig die Grenzen von Büro- und Netzanwendungen für den Benutzer nicht mehr sichtbar sein. Für den Nutzer wird es dadurch auch immer schwieriger zu unterscheiden, wann er sich auf welchem System (z.B. im Internet) befindet. Dadurch wird es für ihn undurchsichtiger, wer wo seine Daten speichert und diese auswerten kann.

8. Die moderne Software-Technologie erlaubt Interaktionen zwischen Softwarekomponenten auf verschiedenen Plattformen und in verschiedenen Lokationen.

In klassischen Systemen wurde Software auf denjenigen Rechnern ausgeführt, auf denen sie entwickelt und gespeichert wurde. Eine sogenannte „Portierung“ auf andere Systeme gestaltete sich aufgrund von Systemunterschieden äußerst schwierig. Durch neuartige Software-Konzeptionen und Architekturen wird die Barriere zwischen den verschiedenen Systemen jedoch durchbrochen. Sog. „aktive Komponenten“ und interpretierte Programmiersprachen erlauben die Ausführung von „heruntergeladenen“ Programmen auf dem Rechner des Nutzers – unabhängig von dessen Betriebssystemumgebung. Unter Umständen wird auf dem Rechner des Nutzers – ohne dessen Einverständnis, oder ohne daß er dies bemerkt – ein Programm ausgeführt. Schon heute ist es – aufgrund von Implementationsfehlern – möglich, die Festplatte eines Benutzersystems zu lesen und gegebenenfalls sogar Daten abzuziehen.

Auch erlauben es bestimmte Protokollbesonderheiten, daß Server spezielle Einstellungen auf dem Rechner des Benutzers speichern und später wieder abrufen können. Eine Anwendung dieser sog. „Cookies“ wäre es beispielsweise, als elektronische Rabattmarke zu fungieren. Sie können allerdings auch benutzt werden, um die Seiten, die ein Benutzer beim Besuch des Servers aufgesucht hat, zu speichern. Würden verschiedene solcher „Cookies“ eines Benutzers zusammen abgerufen, so wären Rückschlüsse über seine Interessen und Neigungen möglich.

Datenschutz- und IV-Sicherheitsgefährdungen

Die dargestellte informationstechnische Entwicklung hat nachhaltige Auswirkungen in Hinblick auf datenschutzrechtliche und sicherheitstechnische Belange.

1. Datenschutzgefährdungen

Datenschutzrechtlich ergeben sich z.B. Gefährdungen in Hinblick auf die Überwachung der Kommunikationstätigkeit, auf die Vertraulichkeit von Kommunikationsinhalten und auf die Verkettung verschiedener erfolgter Zugriffe im Internet.

1.1 Verlust der Unbeobachtetheit der Kommunikation

Die Kommunikation eines Nutzers kann beispielsweise bei der Verwendung von elektronischer Post leicht durch eine Auswertung von normalerweise geführten Log-Dateien beobachtet werden. Diese Logs können nicht nur bei dem Nutzer nächstgelegenen „elektronischen Postamt“ vorliegen, sondern bei jeder Station, über welche die elektronische Mail (eMail) transportiert wurde. Auch viele World Wide Web Server (WWW-Server) speichern, wann welche Seite von welcher Internet-Adresse aus aufgerufen wurde. Der Web-Master hat außerdem die Möglichkeit, anhand der Zeiten, die ein Nutzer auf einer bestimmten Web-Seite verweilt, auf die Neigungen des Nutzers zu schließen. Dies alles ermöglicht bereits die Analyse des Verhaltens und der Interessen des Abrufers[5]; durch die Verwendung der sog. „Cookies“ wird dieses Problem noch ausgeweitet. Durch „Cookies“ – kleine Textdateien mit Informationen, die besuchte WWW-Server auf dem Rechner des Benutzers speichern – wird es möglich, die Zugriffe von WWW-Nutzern auf verschiedenste Angebote miteinander zu verketten, um so Profile über die Nutzer zu erlangen. Dies wird z.B. verwendet, um den Nutzer gezielt „bewerben“ zu können.

1.2 Verlust der Vertraulichkeit der Kommunikation

Eine weitere Gefährdung der Privatsphäre des Nutzers liegt darin, daß der Inhalt der Kommunikation, z.B. der Text einer eMail oder die Bestellung bei einem WWW-Server, im allgemeinen unverschlüsselt übertragen wird, d.h., die Vertraulichkeit der übertragenen Information ist nicht gewährleistet. Ein Angreifer hätte so die Möglichkeit, den Inhalt einer Kommunikation „mitzuhören“ und zu speichern. Das „Briefgeheimnis“ kann nicht gewahrt bleiben. Über den Nutzer könnte ein umfassendes Kommunikationsprofil erstellt werden, das – neben Informationen über seine Kommunikationspartner – auch den Inhalt z.B. seiner Nachrichten enthält.

Die Nutzung von aktiven Komponenten und Skript-Sprachen wie JavaSkript erlauben es, vertrauliche Daten vom Rechner des Nutzers zu entfernten Servern zu übertragen. Es ist möglich, die eMail-Adresse des Nutzers, seine IP-Nummer sowie Informationen über die von ihm genutzte Software zu erlangen.[6] Mit Hilfe der oben genannten Programmiersprachen ist es auch möglich, dem Nutzer ein sog. „Trojanisches Pferd“ auf den Rechner zu laden, das dessen Paßwörter mitschneidet oder private Dateien zu entfernten Server-Systemen sendet.

5 Siehe auch *Verbraucherschutz im Internet*, Herbert Damker, Prof. Dr. Günter Müller, in Datenschutz und Datensicherheit 21 (1997) 1.

6 Eine Demonstration dieser Möglichkeiten wird auf dem WWW-Server des „Center for Democracy and Technology“ auf der Web-Seite *http://www.13x.com/cgi-bin/cdt/snoop.pl* geboten. Eine technische Erläuterung der hierbei genutzten Funktionen findet sich auf *http://www.cdt.org/privacy/how.html*.

1.3 Speicherung ohne Einwilligung

Der Verlust der Unbeobachtetheit und der Vertraulichkeit wird durch die Unübersichtlichkeit der Netze – insbesondere des Internets – verstärkt. Darüber hinaus wachsen die öffentlichen und privaten Telekommunikationsnetze zu komplexen Multibetreibernetzen zusammen und erhöhen für den Nutzer die Unübersichtlichkeit bezüglich des jeweilig Verantwortlichen für den Kommunikationsdienst. Da weder Systemgrenzen noch Ländergrenzen beim „Surfen" eine Rolle spielen, hat der Nutzer keine Möglichkeit, festzustellen, wo seine personenbezogenen Daten gespeichert werden. Es ist ihm im allgemeinen nicht möglich, eine derartige Speicherung zu verhindern. Die Speicherung seiner personenbezogenen Daten findet ohne seine Einwilligung statt. Für den Anbieter von Telekommunikationsdienstleistungen sowie die Betreiber von Servern ist die Erhebung personenbezogener Daten somit sehr einfach.[7] Der Nutzer hinterläßt seine Datenspuren geradezu „im Vorbeigehen". Dies kann durch technische Maßnahmen beim Server-Betreiber allerdings eingeschränkt werden. Dies ist im Teledienstedatenschutzgesetz (TDDSG) § 4 Abs. 2 auch vorgesehen.

Eine Möglichkeit, diese unerwünschte Speicherung zu umgehen, wäre die Verwendung eines Pseudonyms, bei der Verwendung von eMails über einen „anonymen Re-Mailer", beim „Surfen" durch den sog. „Anonymizer".[8]

1.4 Auswertung des Kommunikationsverhaltens

Suchmaschinen bieten heutzutage die Möglichkeit, gezielt Informationen im Internet zu suchen. Der Server Dejanews[9] beispielsweise bietet die Möglichkeit, alle News-Postings, die von einer bestimmten eMail-Adresse aus versandt wurden, aufzulisten, womit es möglich wird, die Vorlieben eines Nutzers zu bestimmen. Die eMail-Adresse einer Person kann ebenso einfach über spezialisierte Suchdienste[10] im Internet herausgefunden werden.

1.5 Teledienstanwendungen

Bei der Nutzung von kommerziellen Teledienstanwendungen können bei einem Anbieter umfangreiche Datensammlungen mit personenbezogenen Daten entstehen. Ein Beispiel dafür wäre das Betreiben einer „elektronischen Mall", in dem ein Anbieter verschiedenen Händlern Platz zur Verfügung stellt, auf dem diese ihre Waren und Dienstleistungen anbieten können. Alle befinden sich aber technisch auf demselben Server-System und werden vom selben Service Provider betrieben. Dieser Provider hätte dann theoretisch Zugriff auf eine Sammlung verschiedenster Daten einer Person, die deren Vorlieben aufs genaueste beschreiben. Es besteht demnach die Gefahr, daß der Diensteanbieter die Daten nicht getrennt speichert und verarbeitet, sondern seine „übergreifende" Datensammlung auswertet und diese „Komplett-Auswertung" seinen Händlern zur Verfügung stellt, die diese wiederum zur gezielten Kundenwerbung verwenden.

2. IT-Sicherheitsgefährdungen

Neben den datenschutzrechtlichen Gefährdungen erfordert die zuverlässige Nutzung die Beachtung der Anforderungen für sichere Kommunikationssysteme. Das Internet ist sowohl von der Technologie als auch von seinem ursprünglichen Zweck als Kommunikationsnetz für Wissenschaft und Forschung her als offenes System konzipiert. Im Gegensatz zu den herkömmlichen öffentlichen Telekommunikationsnetzen erhöht diese offene Systemkonzeption das Risiko von Angriffen und Manipulationen erheblich. Passive Angriffe wie das Abhören von Informationen und die Analyse von Verbindungsdaten sind, wie oben erläutert, sehr einfach möglich, da die Informationen über Rechner einer Vielzahl unbekannter Beteiligter lau-

7 Siehe auch *Data Mining und Datenschutz*, Erich Schweighofer, in: Datenschutz und Datensicherheit 21 (1997) 8.

8 *http://www.anonymizer.com/.*

9 *http://www.dejanews.com/.*

10 Suchmaschinen für eMail-Adressen sind beispielsweise der Internet Address Finder (*http://www.iaf.net*) und die Four11 Directory Services (*http://www.four11.com*).

fen. Diese können die übermittelten Informationen aber auch ebenso einfach und unbemerkt manipulieren (z.B. Wiedereinspielen von Informationen, Verzögern oder Löschen von Nachrichten, Modifikation von Informationen und Absender/Adressat, Stören der Nutzung).

2.1 Verlust der Integrität/Authentizität

Bei der Verwendung von elektronischer Post ist es einem Angreifer leicht möglich, einen beliebigen Absender vorzutäuschen. Ebenso können die Inhalte der versendeten Nachrichten manipuliert werden.

Auch die Authentizität der Angebote im WWW ist nicht gewährleistet. So ist es beispielsweise Hackern gelungen, die Inhalte der WWW-Server des amerikanischen Justizministeriums und auch des CIA zu verändern. Ebenso einfach ist es möglich, das Vertrauen eines Web-Surfers zu erlangen, indem man – unter Verwendung eines bekannten Namens, etwa eines Versandhauses – eine eigene Web-Seite betreibt und dort die Daten der Nutzer sammelt.

2.2 Verlust der Verfügbarkeit

Weiterhin kann nicht garantiert werden, daß die ins Internet eingestellten Angebote ständig verfügbar sind. Viele Server-Systeme sind so konfiguriert, daß es Hackern leichtfällt, sie anzugreifen und sie durch eine „Flut“ von Abfragen für andere Personen unerreichbar zu machen. Diese Art der Angriffe bezeichnet man als „Denial of Service Attacks“. Für einen Anbieter, der im Internet Waren und Dienstleistungen anbietet, ist dies fatal, da er so für seine Kunden nicht mehr erreichbar ist.

Eine weitere Möglichkeit, die Verfügbarkeit von Systemen zu attackieren, besteht darin, Programme mit maliziösem Inhalt auf dem angegriffenen System zur Ausführung zu bringen. Das bekannteste Beispiel hierfür ist der sog. Internet- oder Morris-Wurm, der – allerdings nicht in böser Absicht – im November 1988 große Teile des Internets lahmlegte.[11]

Um dies zu verhindern, ist ein umfassender Schutz gegen sog. „Malware“ (Viren, Würmer etc.) notwendig.

3. Zusammenfassung

Es ist also technisch möglich, das Kommunikations- und Konsumverhalten von Nutzern zu überwachen und dies zu detaillierten Benutzerprofilen auszuwerten. Insbesondere im Internet ist heute die Wahrung der Privatsphäre der Benutzer nicht gegeben.

11 Spafford, Eugene H.: *The Internet Worm Incident*, Proceedings of the 1989 European Software Engineering Conference, Lecture Notes in Computer Science # 87.

Ein Anwendungsgebiet – Datenschutz schafft Vertrauen für den elektronischen Geschäftsverkehr

1. Elektronische Kommunikationskultur

Die Entwicklung des Internets hat zu einer starken Zunahme des elektronischen Geschäftsverkehrs national wie international geführt. Der elektronische Geschäftsverkehr ist natürlich nicht auf das Internet beschränkt. Er bietet eine Vielzahl von Anwendungsmöglichkeiten im Schmalbandbereich (Bildschirmtext), im Fernsehfunk (Teleshopping) und Offline (Katalogverkauf auf CD-ROM) sowie über firmeneigene Netze (Bankgeschäfte etc.). Allerdings werden im Internet rasch verschiedene Formen des Electronic Commerce miteinander verbunden. Firmennetze werden zu Intranets. Dieser Prozeß führt zu tiefgreifenden strukturellen Veränderungen. Der elektronische Geschäftsverkehr vereinfacht die Geschäftsabwicklung und beschleunigt die Reaktionsfähigkeit. Typischerweise ist der elektronische Geschäftsverkehr für internationale Geschäfte besonders geeignet und eröffnet den Anbietern neue Märkte. Electronic Commerce umfaßt so unterschiedliche Tätigkeiten wie Teleshopping, elektronischen Aktienhandel, kommerzielle Auktionen, öffentliche Auftragsvergabe, elektronische Frachtpapiere, Informations- und Finanzdienste. Die Einnahmen aus dem elektronischen Geschäftsverkehr im Internet sollen bis zum Jahr 2000 weltweit auf über 200 Mrd. ECU steigen.[12]

Die Unternehmen verlagern zunehmend Anwendungen auf das Internet, die bislang in getrennten Netzen von geschlossenen Benutzergruppen genutzt wurden. Globale Industriezweige wie die Automobil-, Computer- und Luftfahrtindustrie integrieren ihre Lieferketten über das Internet.

Sowohl Verbraucher als auch Unternehmen müssen darauf vertrauen können, daß ihre Transaktionen nicht abgefangen, ausgewertet oder verändert werden. Für die elektronische Kommunikationskultur sind Sicherungen der Integrität, der eindeutigen Urheberschaft und der Vertraulichkeit, wie sie in der Schriftkultur mit Briefumschlag, Unterschrift, Stempel und Siegel jahrhundertelange gepflegt wurden, noch nicht etabliert. Dabei birgt die elektronische Kommunikation neue und andere Risiken der Manipulation, des Bruchs der Vertraulichkeit und der Ausforschung des Kommunikationsverhaltens. Für die weitere Entwicklung des elektronischen Geschäftsverkehrs sind Lösungen für Fragen wie eindeutige Identifikation des Vertragspartners, vertrauliche Datenübermittlung, Verbindlichkeit und Beweisbarkeit einer elektronischen Willenserklärung und sichere Zahlungsverfahren wichtige Faktoren. Ein erster Schritt in diese Richtung ist das Gesetz zur digitalen Signatur (Artikel 3 des IuKDG). Es bedarf einer mehrseitigen Sicherheit als integralem Bestandteil der Kommunikationstechnik.[13]

12 ActivMedia, Romtec, *European Information Technology Observatory 97, in: EU-Kommission, Mitteilungen an das Europäische Parlament: Europäische Initiative für den elektronischen Geschäftsverkehr*, KOM(97) 157.

13 Müller, Günter, Pfitzmann, Andreas (Hrsg.): *Mehrseitige Sicherheit in der Kommunikationstechnik – Zusammenfassendes Resultat des von der Gottlieb-Daimler- und Karl-Benz-Stiftung geförderten Kollegs „Sicherheit in der Kommunikationstechnik“*, Juli 1997.

Neben einem Systemschutz (Firewall-Systeme) bedarf es Selbstschutztechniken (Zugriffsschutztools, Verschlüsselungstools), die die Nutzer selbstverantwortlich einsetzen.[14] Systemdatenschutz bedeutet hierbei auch z.B. das Prinzip der Datenvermeidung sowie anonyme und pseudonyme Nutzungsmöglichkeiten für elektronische Netze und Dienstleistungen. Ein Beispiel hierfür wäre das Angebot, in elektronischen Märkten mit anonymen, vorbezahlten Wertkarten elektronische Leistungen zu beanspruchen, ohne dabei Datenspuren durch den Nutzer zu hinterlassen. Das Interesse der Anbieter, das Verhalten der Nutzer auswerten zu können, wäre durch Pseudonyme gewährleistet, die einen gerechten Ausgleich der Interessen zwischen Dienstleister und Benutzer möglich machen. Es muß lediglich sichergestellt werden, daß im Konfliktfall die Zuordnung des Pseudonyms zur Person möglich ist.

Dem Nutzer müssen vertrauenswürdige Dienstleistungen angeboten werden, die dieser im eigenen Interesse einsetzen kann. Denn die Bereitschaft zur Selbstorganisation in einer globalisierten Informationsgesellschaft muß entwikkelt und gefördert werden. Um sich zu schützen, muß dem Nutzer auch die Möglichkeit gegeben werden, sich über die Gefahren in angemessener Weise zu informieren.

Daneben beinhaltet Selbstschutz nicht nur die Bereitstellung von einfach zu bedienenden Werkzeugen, wie beispielsweise Verschlüsselungswerkzeugen (PGP[15]) für das vertrauliche Versenden von elektronischer Post, sondern auch die Bereitstellung einer vertrauenswürdigen Infrastruktur, die ein verläßliches Management der verwendeten kryptographischen Schlüssel sicherstellt. Eine Genehmigungspflicht oder ein teilweises Verbot kryptographischer Verfahren würde dem Selbstschutz-Interesse der Bürger entgegenstehen.[16] Weitere Dienste, die die Vertraulichkeit der Kommunikation gewährleisten, müssen – für den Nutzer transparent – zum Selbstschutz zur Verfügung gestellt werden. Ein Beispiel hierfür ist das Protokoll SSL[17].

2. Vertrauenswürdige Kommunikationskultur

Die Rechtssicherheit bei der Kommunikation, der Persönlichkeitsschutz, die Vertraulichkeit, der Urheber- und Verbraucherschutz sind nicht nur eine Frage der Kultur, sondern auch des Wettbewerbs und bedürfen eines verbindlichen Ordnungsrahmens.

Sowohl der elektronische Geschäftsverkehr als auch neue Möglichkeiten der Kriminalität werfen weltweit Fragen nach neuen Gesetzen bzw. Regelungen für Teledienstleistungen auf. Mit der Verabschiedung des Informations- und Kommunikationsdienstegesetzes (IuKDG)[18] wurde in Deutschland erstmals ein gesetzlicher Ordnungsrahmen für Teledienste geschaffen, mit dem mehr Rechtssicherheit bei der Erbringung und Nutzung von Telediensten erreicht werden soll.

14 Büllesbach, Alfred, Garstka, Hansjürgen: *Systemdatenschutz und persönliche Verantwortung*, in: Müller, Günther, Pfitzmann, Andreas (Hrsg.), ebenda.

15 Das Programm PGP (Pretty Good Privacy) wurde vom Amerikaner Phil Zimmerman entwickelt. Die amerikanische Version von PGP ist bei *http://www.pgp.com* erhältlich. Eine internationale Version findet sich beispielsweise bei *http://www.heise.de/ct/pgpCA/download.html*. siehe auch: Zimmerman, Phil, *PGP – Pretty Good Privacy – Das Verschlüsselungsprogramm für Ihre private elektronische Post*, deutsche Übersetzung von: Deuring, A.; Creutzig, Ch., Bielefeld 1994.

16 Eine Übersicht über die rechtliche Situation und den Stand der politischen Diskussion über Kryptographie zusammen mit weiterführenden Links findet sich unter *http://www.fitug.de/ulf/krypto/verbot.html*.

17 Secure Socket Layer. Die aktuelle Spezifikation kann bei *http://home.netscape.com/eng/ssl3/index.html* eingesehen werden.

18 BGBl. I, 1870 ff., 1997.

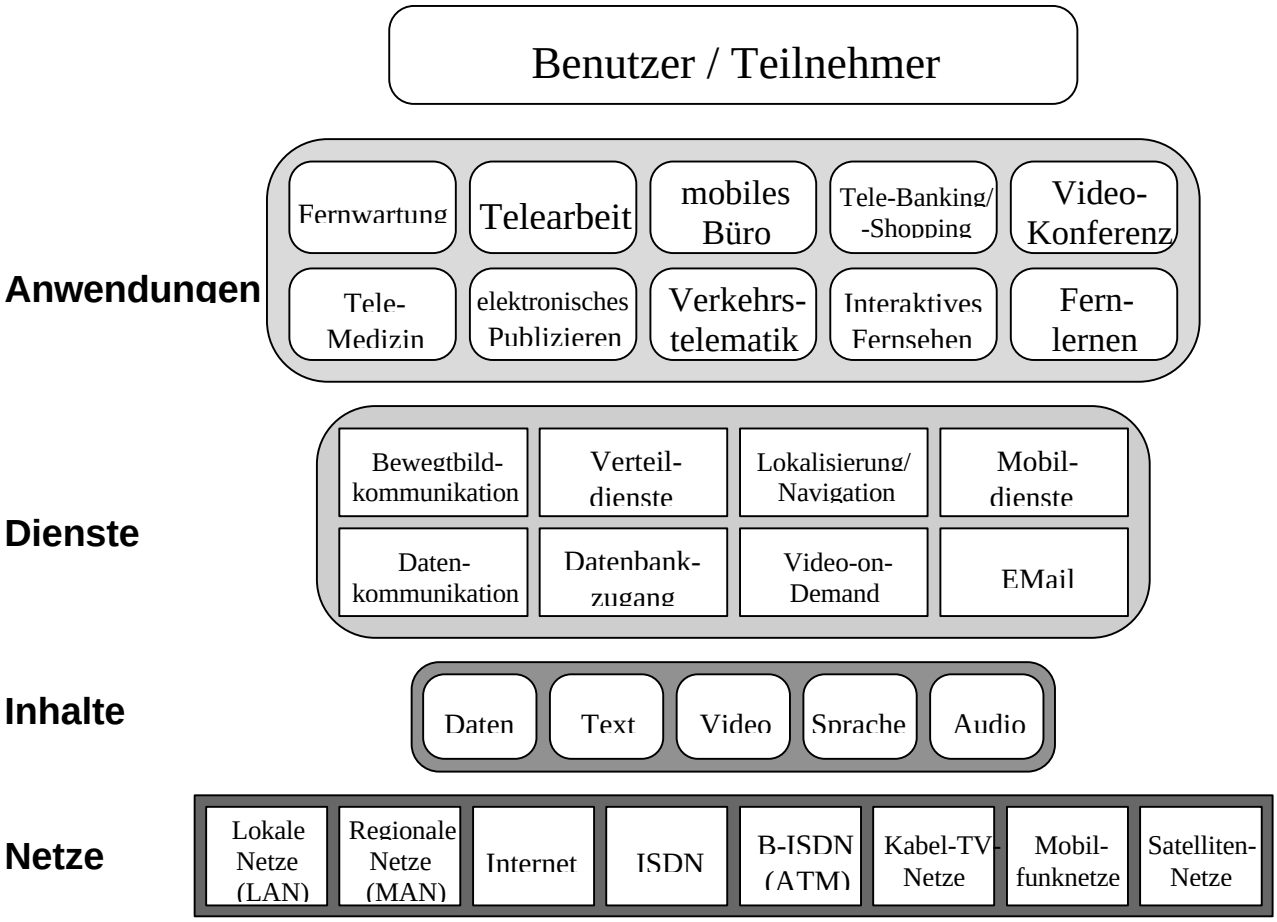

Abbildung 1: Der Informationsraum bei Multimedia[19]

Die Vielfalt der Dienste, die verschiedenen Netzstrukturen, die Verschiedenheit der Inhalte und nicht zuletzt die Vielfalt der Anwendungen haben dem Gesetzgeber große Schwierigkeiten bereitet, die Kategorien von Telediensten deutlich und klar abzugrenzen. Das IuKDG zeigt diese Schwierigkeiten. Telekommunikation, individuelle Computerkommunikation und Rundfunk wachsen zusammen. Dieser Prozeß ist rechtlich im historischen Ablauf nicht immer exakt bestimmbar. Zukünftig muß nach jetziger Regelungsstruktur zwischen den Telekommunikationsdiensten, den Telediensten und Mediendiensten unterschieden werden. Im Telekommunikationsgesetz (TKG) werden Dienste reguliert, die sich primär auf das Angebot von Telekommunikationsnetzen und Übertragungswegen beziehen (Netzbetreiber, Mobilfunkanbieter). Dagegen regelt das sog. Multimediagesetz den Inhalt von Informations- und Kommunikationsdiensten, die der individuellen Kommunikation dienen (Telebanking, Telespiele, Information über Waren- und Dienstleistungsangebote). Dienste, bei denen die allgemeine Meinungsbildung und die redaktionelle Gestaltung im Vordergrund stehen, z.B. Fernseheinkauf, Fernsehtext und Radiotext, fallen in Deutschland in die Zuständigkeit der Bundesländer. Um zu einheitlichen Rahmenbedingungen zu gelangen, haben die Bundesländer parallel zum IuKDG einen Mediendienstestaatsvertrag (MDStV) – im Kern mit gleichlautenden Regelungen – abgeschlossen. Für den Anbieter kann es dennoch zu relevanten unterschiedlichen Rechtsfolgen, z.B. Haftung, Presserecht, Jugendschutz, führen

19 Müller, Günter, Stoll, Frank: *Der Freiburger Kommunikationsassistent – Sicherheit in multimedialen Kommunikationsnetzen durch nutzerbezogene Dezentralisation*, in: *Symposium Multimedia und Datenschutz*, 28.08.1995, Materialien zum Datenschutz 22, Berliner Datenschutzbeauftragter.

Telekommunikations-dienste	Informations- und Kommunikations-dienste für die indivi-duelle Nutzung (Teledienste)	Informations- und Kommunikations-dienste, die an die Allgemeinheit gerich-tet sind (Medien-dienste)	Rundfunkdienste
Gesetzliche Regelungen: TKG Rechtsverordnung zum TKG TDSV	Gesetzliche Regelungen: IuKGD BDSG LDSG	Gesetzliche Regelungen: Mediendienstestaats-vertrag Landesmediengesetze Landesdatenschutz-gesetze	Gesetzliche Regelungen: Rundfunk-staatsvertrag Landesmediengesetze Landesdatenschutz-gesetze

Abbildung 2: Kategorien von Telediensten

– je nachdem, ob sein Dienst als Teledienst dem IuKDG oder als Mediendienst dem Staatsvertrag über Mediendienste unterliegt.

Die für solche geschäftlichen Anwendungen geltenden Gesetze sind also vielfältig und dazu zwangsläufig in der Abgrenzung unscharf in Hinblick darauf, wo exakt die Grenzen zwischen Telekommunikations-, Tele- und Mediendiensten für Anbieter liegen.

Der Übersicht ist zu entnehmen, daß es keine Einheitlichkeit der Datenschutzregelungen für verschiedene Teledienste gibt. Bezüglich der Regelungskompetenz läßt sich zwischen den Bundesregelungen (TKG, Bundesdatenschutzgesetz, bereichsspezifische Bundesdatenschutzregelungen, IuKDG) und den Datenschutzregelungen der Länder (MDStV, Landesmediengesetze, Landesdatenschutzgesetze, Rundfunkstaatsvertrag, bereichsspezifische Landesdatenschutzregelungen) unterscheiden.[20]

Insgesamt sind im Bereich der Telekommunikation durch das TKG, das am 01.08.1996 in Kraft trat, und durch die beiden weiteren Regelungen – das IuKDG und den MDStV, die am 01.08.1997 in Kraft traten – neue Strukturen geschaffen worden. Der bisher geltende BTX-Staatsvertrag vom 31.08.1990 ist zum 31.07.1997 außer Kraft getreten. Mit dem TKG sind die europäischen Richtlinien zur Liberalisierung der Telekommunikationsmärkte umgesetzt worden. Das TKG löst das Fernmeldeanlagen-Gesetz[21] und das Gesetz über die Regulierung der Telekommunikation und des Postwesens vom 14.09.1994 (PTRegG)[22] ab.

Im Multimediagesetz werden im einzelnen die Verantwortlichkeit, der Datenschutz, der Einsatz digitaler Signaturverfahren und der Urheberrechtsschutz von Datenbanken geregelt sowie das Straf- und Jugendrecht angepaßt. Das IuKDG findet auch Anwendung auf Teledienste, die in einem Intranet innerhalb eines Konzerns angeboten werden. Wesentlich ist der

20 Vgl. Roßnagel, Alexander, Bitzer, Johann: *Multimediadienste und Datenschutz*, Akademie für Technikfolgenabschätzung in Baden-Württemberg, Stuttgart 1995.

21 Vgl. Fernmeldeanlagen-Gesetz in der Fassung der Bekanntmachung vom 03.07.1989 (BGBl. I S. 1455); vgl. aber § 97 Abs. 2 TKG, der für den Bereich des Sprachtelefondienstes eine Fortgeltung dieses Gesetzes bis zum 31.12.1997 vorsieht.

22 Vgl. BGBl. I S. 2325, 2371, 1996 I S. 103); vgl. auch insoweit § 97 Abs. 2 TKG, der für den Bereich des Sprachtelefondienstes eine Fortgeltung dieses Gesetzes bis zum 31.12.1997 vorsieht.

Grundsatz, daß Teledienste zulassungsfrei angeboten werden können.

Teledienste sollen so gestaltet werden, daß keine oder so wenig personenbezogene Daten wie möglich verarbeitet oder genutzt werden (Prinzip der Datensparsamkeit). Besondere datenschutzrechtliche Anforderungen werden an die Einwilligung, Unterrichtung, getrennte Verarbeitung von Nutzungsdaten und die Erstellung von Nutzungsprofilen gestellt. Der Diensteanbieter muß dem Nutzer die Inanspruchnahme und Bezahlung seiner Teledienste auch anonym oder pseudonym ermöglichen, wenn es technisch möglich und zumutbar ist.

Mit dem Signaturgesetz werden neue Wege beschritten. In dem Gesetz werden die Anforderungen festgelegt, um sichere digitale Signaturen in Verkehr zu bringen. Mit Hilfe kryptographischer Verfahren lassen sich heute sowohl die Integrität und Urheberschaft als auch die Vertraulichkeit von elektronischen Dokumenten sicherstellen. Die sichere Übermittlung von Dokumenten zwischen unbekannten Partnern wird durch Public-Key-Verfahren ermöglicht. Diese Verfahren sind auf eine vertrauenswürdige Infrastruktur angewiesen.[23]

Die Einführung einer digitalen Signatur, die den Beweiswert elektronischer Dokumente deutlich erhöhen soll, hat auch für die Weiterentwicklung des Electronic Commerce erhebliche Bedeutung. Eine wichtige Grundentscheidung des Gesetzgebers besteht darin, daß die für die digitale Signatur erforderlichen Schlüsselzertifikate und alle damit zusammenhängenden Dienstleistungen durch private Anbieter erbracht werden können. Dies ermöglicht eine schnelle und kostengünstige Durchdringung des Marktes mit digitalen Signaturen. Erst ab einer bestimmten kritischen Masse ist es für alle Marktbeteiligten interessant, sich auf diese Verfahren einzustellen und damit die Sicherheit des elektronischen Geschäftsverkehrs insgesamt zu erhöhen. Diese Sicherheit führt wiederum zu neuen Anwendungen im elektronischen Geschäftsverkehr.

23 Horster, Patrick (Hrsg.): *Digitale Signaturen*, Braunschweig/ Wiesbaden 1996.

3. Der elektronische Geschäftsverkehr ist global

Bei den Bemühungen des deutschen Gesetzgebers zur Schaffung von mehr Rechtssicherheit kann nicht übersehen werden, daß nationale Regelungen angesichts der Globalität der Netze zu kurz greifen. Zudem besteht durch neue nationale Vorschriften in unterschiedlichen Bereichen (digitale Signaturen, Datenschutz, Verantwortlichkeit, elektronische Zahlungsmittel, Verschlüsselung, Strafrecht) das Risiko, daß über die Gestaltung der erforderlichen Rahmenbedingungen hinaus neue Handelshemmnisse geschaffen werden, die die Entwicklung des elektronischen Geschäftsverkehrs auf globaler Ebene behindern. Deshalb sind die Anbieter und Nutzer des elektronischen Geschäftsverkehrs in einem zersplitterten ordnungspolitischen Umfeld tätig. Es müssen Lösungen gefunden werden, um zu einem weltweit akzeptierten ordnungspolitischen Rahmen für den elektronischen Geschäftsverkehr zu kommen. Die EU-Rahmenrichtlinie über den Schutz personenbezogener Daten vom 24.10.1995 stellt einen Rahmen für vertrauensbildende Maßnahmen hinsichtlich des Rechtes auf Datenschutz dar. Für die Globalisierung sind weitere Maßnahmen und Initiativen erforderlich. Die Europäische Union hat mit der Initiative für den elektronischen Geschäftsverkehr vom 14.04.1997 Ziele formuliert. Die Vorschläge umfassen den Zugang zum globalen Markt, rechtliche und ordnungspolitische Rahmenbedingungen und die Förderung eines günstigen politischen Umfeldes.[24] Mit der „Bonner Erklärung zur gemeinsamen Nutzung des Internet“ – verabschiedet von 29 Ministern auf der Konferenz „Globale Informationsnetze – Nutzung neuer Chancen“ am 07./08.07.1997 in Bonn – wurde der gemeinsame Wille formuliert, international den erforderlichen rechtlichen Rahmen zu vereinbaren und sich mit staatlichen Eingriffen in das Internet zurückzuhalten.

24 EU-Kommission, Mitteilungen an das Europäische Parlament: *Europäische Initiative für den elektronischen Geschäftsverkehr*, KOM(97) 157.

Von den Unternehmen und Wirtschaftsverbänden sollte die Möglichkeit genutzt werden, im Sinne einer verantwortlichen Selbstregulierung zu Vereinbarungen zu kommen, die allgemein akzeptiert und anerkannt werden. Dies gilt insbesondere für die Festlegung von Normen und Standards und die gegenseitige Anerkennung von Konformitätsbewertungen, um die weltweite Kompatibilität der Technologien und Verfahren, z.B. für digitale Signaturen, die technologische Gewährleistung von Datenschutz und IV-Sicherheit, zu erreichen. Darüber hinaus kann die Wirtschaft durch Festlegung und Einhaltung von Verhaltenscodices für Vertrauen sorgen. Verantwortliches Handeln fördert die Nutzung und Akzeptanz und kann staatliche Vorgaben zum Teil entbehrlich machen.

Regierungen, internationale Organisationen, Unternehmen und nicht zuletzt die Bürger müssen sich der Herausforderung einer „Bill of Rights“ für die globale Informationsgesellschaft stellen.

Prinzipien des Teledienstdatenschutzgesetzes

Das Teledienstdatenschutzgesetz (TDDSG) ist während der Beratungszeit vielfältig kritisiert worden. Nahezu in allen Stellungnahmen zur Anhörung des Deutschen Bundestages ist insbesondere das TDDSG, so z.B. in den Stellungnahmen des BDI, des Zentralen Kreditausschusses, der GDD, der Deutschen Telekom AG, der Daimler-Benz AG und CompuServe, bemängelt worden. Bevor ausgewählt auf die einzelnen Kritikpunkte eingegangen werden kann, soll die Struktur des TDDSG vorgestellt werden.

Innerhalb der datenschutzrechtlichen Regelungen ist besonders hervorzuheben:

a) Ziel ist der Schutz personenbezogener Daten unabhängig davon, ob sie in Dateien verarbeitet oder genutzt werden (§ 1 Abs. 2).

b) Festlegung von Grundsätzen für die personenbezogene Datenverarbeitung (§ 3):
   - Rechtsvorschrift oder Einwilligung
   - Zweckbindung
   - Prinzip der Autonomie des Nutzers
   - Prinzip der Datensparsamkeit
   - Unterrichtungspflicht vor Erhebung
   - Einführung der elektronischen Einwilligung

c) Datenschutzrechtliche Pflichten des Diensteanbieters:
   - Der Diensteanbieter muß anonyme oder pseudonyme Inanspruchnahme von Telediensten und ihrer Bezahlung ermöglichen, soweit dies technisch möglich und zumutbar ist.
   - Die Gewährleistung eines informationstechnischen Systemschutzes mit einzelnen Anforderungen (§ 4 Abs. 2).
   - Das Verbot der personenbezogenen Nutzungsprofile (zulässig bei Verwendung von Pseudonymen) beachten.

d) Regelung der Bestands-, Nutzungs- und Abrechnungsdaten einschließlich Löschungsfristen

e) Verbot der Übermittlung von Nutzungs- und Abrechnungsdaten an andere Diensteanbieter oder Dritte.

f) Erlaubnis des Diensteanbieters, an einen Dritten, der entsprechend eines Vertrages die Entgeltabrechnung vornimmt, die Abrechnungsdaten zu übermitteln.

f) Auskunftsrecht des Nutzers auch zu seinem Pseudonym, Auskunft kann auch elektronisch verlangt werden.

h) Abkehr von der Anlaßkontrolle nach § 38 BDSG

Das Gesetz hat einerseits datenschutzrechtliche Sonderregelungen für Anbieter von Telediensten getroffen, die begrifflich von der akzeptierten Sprache des BDSG abweichen, und hat andererseits bereits eine Reihe von Anforderungen aufgrund der EU-Richtlinie zum Datenschutz, die spätestens bis Ende 1998 übernommen werden müssen, vorweggenommen. Im Gegensatz zu vielen Kritiken besteht hier durchaus auch die Chance, Erprobungen für die Fortentwicklung des Datenschutzes zu machen.

Das TDDSG baut auf das Teledienstegesetz (TDG) auf.

Inhalt des Teledienstegesetzes

Das Teledienstegesetz (TDG) geht von der Zulassungs- und Anmeldefreiheit aus und regelt insbesondere in § 5 die Verantwortlichkeit für Inhalte von Telediensten. In § 5 Abs. 2 bringt es eine haftungsrechtliche Privilegierung der Provider. Zivilrechtliche und strafrechtliche Haftung tritt danach nur dann ein, wenn die Provider von den rechtswidrigen fremden Inhalten, die sie zur Nutzung bereithalten, Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Kenntnis im Sinne des Gesetzes bedeutet hierbei positives Wissen, d.h., die Diensteanbieter müssen nachweislich von Dritten auf bestimmte Inhalte hingewiesen worden sein.

Die reine Vermittlung des Zugangs zu fremden Inhalten führt nach § 5 Abs. 3 TDG nicht zu strafrechtlichen oder haftungsrechtlichen Konsequenzen.

Für geschäftsmäßige Angebote bei Telediensten schreibt § 6 TDG vor, daß Name und Anschrift sowie bei Personenvereinigungen und -gruppen auch Name und Anschrift der Vertretungsberechtigten angegeben werden müssen. Geschäftsmäßigkeit in diesem Sinne bedeutet, Tätigkeit mit oder ohne Gewinnerzielungsabsicht auf einen längeren Zeitraum angelegt und nicht nur gelegentlich. Nur gelegentliche Angebote auf virtuellen „Schwarzen Brettern“ erfordern nicht diese Angaben. Homepages beispielsweise, die für eine gewisse Zeit ins Internet eingestellt werden, verlangen jedoch Name und Anschrift.

Abgrenzungsfragen zum TDDSG

In vielen Stellungnahmen zur Vorbereitung des TDDSG wurde der Einwand erhoben, daß dieses Gesetz nicht auf die Systematik des Bundesdatenschutzgesetzes (BDSG) abgestimmt ist. So übernimmt es nicht die Struktur des BDSG und unterscheidet nicht klar zwischen technischen und organisatorischen Maßnahmen, Rechtmäßigkeitsvoraussetzungen und Ansprüchen der Betroffenen. Nicht klar ist das Verhältnis von TDDSG und BDSG geklärt.

Das Verhältnis TDDSG/BDSG ist in der Praxis offensichtlich ein Problem. Dies zeigen schon jüngere Anwendungsfälle. So beispielsweise, wenn ein Unternehmen Teledienste für einen Händler anbietet, der wiederum diesen Teledienst seinem Kunden anbietet. Wenn der Teledienst nur ein Teil des Verhältnisses ist, endet der Anwendungsbereich des TDDSG, sobald die Daten für Zwecke außerhalb des reinen Teledienstes verwendet werden. In diesem Fall kann kein datenschutzfreier Raum entstehen, sondern gilt das allgemeine Datenschutzrecht. In der Praxis wird dies mit dem Beispiel belegt, daß eine Bank bei der Nutzung ihrer Datenbestände sonst unterscheiden müßte, ob sie Daten über Telebanking oder am Schalter erhalten hat.

1. Umsetzung der europäischen Datenschutzrichtlinie

Die Bundesrepublik Deutschland hat bis zum 24.10.1998 die EU-Datenschutzrichtlinie vom 24.10.1995 in nationales Datenschutzrecht umzusetzen. Das TDDSG hat eine Reihe von bereichsspezifischen Regelungen geschaffen, die mit der Umsetzung auch in eine Novelle des BDSG eingeführt werden müssen. So beispielsweise die Einbeziehung der Erhebung von Daten unter die Rechtmäßigkeitsvoraussetzungen, die ausdrückliche Festlegung des Zweckbindungsgrundsatzes, der Wegfall der Ausnahme für Auskunfts- und Informationspflichten bei kurzfristigen Speicherungen und der Wegfall der Begrenzung der Aufsichtsrechte auf die Anlaßkontrolle.

Entgegen vielfältig in der Literatur geäußerter Bedenken kann nicht erkannt werden, worin hier ein wesentliches Problem liegt. Die Tatsache, daß mit der Novelle zum BDSG diese Bestimmungen ins BDSG kommen, macht sie für das TDDSG deshalb nicht überflüssig. Inwieweit im Rahmen der BDSG-Novelle das TDDSG angepaßt und bestimmte doppelte Regelungen überarbeitet werden, ist eine kodifikatorische Frage. Freilich ist es jedoch sinnvoll, die zerklüfteten und nicht immer aufeinander abgestimmten Regelungen bei nächster Gelegenheit zu vereinheitlichen.

2. Abgrenzung Teledienste und Mediendienste

Es ist nicht leicht, Teledienste und Mediendienste, die im Einzelfall in der Wirtschaft durchaus wichtig sind, klar zu unterscheiden. Es ist keineswegs auszuschließen, daß in bestimmten Fällen beide Begriffe zutreffen. Die grundsätzliche Abgrenzung, wenn die individuelle Nutzung der Dienste im Vordergrund steht, handelt es sich um sogenannte Teledienste (§ 2 TDSG), wenn hingegen Dienste an die Allgemeinheit gerichtet sind, handelt es sich um Mediendienste (§ 2 MDStV), ist nicht sehr differenziert. Der Geltungsbereich des TDDSG bzw. des MDStV wird durch die Begrifflichkeit Teledienst und Mediendienst eröffnet. Es ist deshalb durchaus bedeutsam, wo die private Homepage im WWW, wo ein Online-Dienst wie beispielsweise AOL oder CompuServe, wo Verbraucherkommunikation, die neben Produktwerbung ein interaktiv nutzbares Angebot an Information und Kommunikation bietet und die weit über die reine

Produktinformation hinausgeht, einzuordnen ist.

So läßt sich sicher für viele angebotenen Dienste sowohl eine Einordnung nach § 2 Abs. 2 Nr. 4 MDStV als auch nach § 2 Abs. 2 TDDSG vornehmen. Werden beispielsweise im WWW über eine Homepage Wetterdaten weitergegeben, so kann es sich sowohl um Teledienste nach § 2 Abs. 2 Nr. 2 TDDSG („Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, Datendienste, z.B. Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote“) als auch um Abrufdienste nach § 2 Abs. 2 Nr. 4 MDStV handeln.

Die Unschärfe der Begriffe ist in den Beratungen bekannt gewesen und wurde in vielen Gesprächen zwischen Bund und Ländern zu klären versucht. Die permanente technologische Fortentwicklung, die tägliche Erweiterung elektronischer Nutzungsformen, die dynamische Marktentwicklung sollten durch enge korsettartige Begrifflichkeiten nicht behindert werden. Es wird deshalb auf die künftigen Erfahrungen in der Praxis ankommen, wie die Abgrenzung erfolgen kann und inwieweit die gemeinsame Erklärung des Bundeskanzlers und der Ministerpräsidenten der Bundesländer vom 18.12.1996 trägt:

„1. Bund und Länder haben sich am 01.07.1996 darauf verständigt, im Rahmen der Zuständigkeitsverteilung des Grundgesetzes einen in der Sache einheitlichen Rechtsrahmen in Form eines Bundesgesetzes und eines Länderstaatsvertrages zu schaffen. Es bestand Einigkeit darüber, die notwendigen Regelungen nicht an unterschiedlichen Auffassungen in Kompetenzfragen scheitern zu lassen.

2. Bund und Länder haben in wichtigen Fragenkomplexen einvernehmliche Ergebnisse erzielt. Dies gilt für die zentrale Frage der Zugangsfreiheit, die wortgleich geregelt ist; gleiches gilt für den Datenschutz sowie für die Grundzüge der Verantwortlichkeit der Diensteanbieter.

3. Bund und Länder stimmen darin überein, daß eine abschließende, alle Dienste umfassende Festlegung der jeweiligen Anwendungsbereiche zur Zeit nicht sinnvoll möglich ist. Durch die Zuordnung von einzelnen, heute bekannten Diensten im Teledienstegesetz und im Mediendienste-Staatsvertrag haben Bund und Länder die Aufteilung nach dem gegenwärtigen Erkenntnisstand vorgenommen.

4. Bund und Länder werden die Entwicklung neuer Dienste sowie die Anwendung der beiderseitigen gesetzlichen Regelungen fortlaufend beobachten und hierüber weiterhin im Gespräch bleiben. Sie vereinbaren, die Gespräche mit dem Ziel zu führen, eine Verständigung über notwendige Anpassungen unverzüglich und auf politischer Ebene herbeizuführen.

5. Bund und Länder werden beide Regelungswerke mit dem Ziel des gemeinsamen Inkrafttretens zum 01.08.1997 den jeweiligen Parlamenten zuleiten.“

Die Interpretations- und Abgrenzungsprobleme werden deshalb in der Praxis zunächst pragmatisch zu lösen sein, wobei unter dem Aspekt des Datenschutzes die Differenzierung (siehe spätere Abgrenzung) nicht von letztlich entscheidender Bedeutung ist, da die datenschutzrechtlichen Formulierungen im TDDSG und MDStV nahezu wortgleich sind. Entschieden werden muß jedenfalls, ob es sich entweder um einen Teledienst oder um einen Mediendienst handelt. Eine Kumulation ist ausgeschlossen. Engel-Flechsig weist auf eine Prüfungsreihenfolge hin, die vernünftig ist. So schlägt er vor:[25]

a) Handelt es sich um einen elektronischen Informations- und Kommunikationsdienst (mittels Telekommunikation)?

b) Kann der Dienst anhand der in § 2 Abs. 2 TDDSG oder in § 2 Abs. 2 MDStV genann-

25 Engel-Flechsig, Stefan: *Zusammenarbeit und Abgrenzung von Telekommunikationsgesetz, Informations- und Kommunikationsdienste-Gesetz des Bundes und Mediendienstestaatsvertrag der Länder*, in: Büllesbach, Alfred (Hrsg.): Datenschutz in der Telekommunikation, Deregulierung und Datensicherheit in Europa, Köln 1997.

ten konkreten Anwendungsbereiche eingeordnet werden?

c) Ist letzteres zu verneinen:
Kann der Dienst nach der abstrakten Zuordnung gemäß § 2 Abs. 1 TDDSG oder gemäß § 2 Abs. 1 MDStV eingeordnet werden?

3. Datenschutzrechtliche Unterschiede TDDSG/MDStV

Durch § 3 Abs. 3 TDDSG und § 12 Abs. 4 MDStV soll verhindert werden, daß die Nutzung von Telediensten bzw. Mediendiensten von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig gemacht wird. In den Ausschußberatungen ist § 3 Abs. 3 TDDSG mit dem Zusatz erweitert worden „wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in nicht zumutbarer Weise möglich ist". Diese Regelung öffnet Optionen für den Diensteanbieter, solange es für den Nutzer andere Zugänge zu diesen Telediensten gibt. Die fehlende Öffnung im Mediendienstestaatsvertrag ist unter diesem Aspekt sicherlich freundlicher für den Nutzer.

Es ist zu begrüßen, daß in der Schlußphase der Beratungen zum IuKDG § 5 Abs. 3, der die Übermittlung von Bestandsdaten an staatliche Stellen vorsah, gestrichen wurde, nachdem im MDStV eine solche Regelung nicht vorgesehen war. Die Auffassung des Hamburger Datenschutzbeauftragten in seinem 15. Tätigkeitsbericht über das Berichtsjahr 1996 (S. 19 Abs. 2) und auch des Bundesbeauftragten für den Datenschutz in seinem 16. Tätigkeitsbericht (BT-Drucksache 13/7500 vom 16.04.1997, S. 58), daß die Regelung in § 5 Abs. 3 TDDSG problematisch sei, wird geteilt. Die 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 22./23.10.1996 eine Entschließung über die Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich gefaßt. In dieser Entschließung weisen die Datenschutzbeauftragten darauf hin, daß die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs durch die neuen Dienste, wie Teleworking, Telebanking, Teleshopping, digitale Videodienste und Rundfunk im Internet etc., eine neue Dimension erhalten. Die Dimension liegt darin, daß immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, die mit geringem Aufwand kontrolliert und ausgewertet werden können. Diesem Datenwachstum auf der einen Seite stehen auf der anderen Seite Gefahren, die durch die Nutzung der neuen Technik zu kriminellen Zwecken entstehen, gegenüber. Die Datenschutzbeauftragten haben zu Recht darauf hingewiesen, daß die vielfältigen neuen Dienste erheblich umfangreichere Anwendungen und deshalb erheblich weitgestreutere personenbezogene Daten verarbeiten. Die einfache Übertragung der herkömmlichen Eingriffsbefugnisse auf die neuen Formen der Individual- und Massenkommunikation würde deshalb zwangsläufig zu einer Erweiterung der Eingriffsbefugnisse führen. Die Thesen, die die Konferenz zur Abwägung dieses Spannungsverhältnisses entwickelt hat, seien hier wiedergegeben.

„Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunikationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten, ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z.B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten

fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwendet werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z.B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen – insbesondere im weltweiten Datenverkehr – ohnehin leicht zu umgehen und kaum kontrollierbar wären."

Abelson et al. weisen zudem darauf hin, daß der Aufbau einer Infrastruktur zur Schlüsselhinterlegung oder Key Recovery aufgrund der hohen Komplexität kaum machbar wäre.[26]

§ 17 MDStV sieht ein Datenschutz-Audit vor, das im Zuge der Beratungen aus dem TDDSG gestrichen wurde. Nach der Regelung im MDStV dient das Datenschutz-Audit der Verbesserung von Datenschutz und Datensicherheit. Anbieter von Mediendiensten können ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter überprüfen und bewerten lassen sowie das Ergebnis der Überprüfungen veröffentlichen. Mit der Möglichkeit, ein solches Datenschutz-Audit[27] durchführen zu lassen, ist dem Gedanken, daß Datenschutz Qualitäts- und Wettbewerbsbestandteil[28] im privaten Bereich auf freiwilliger Grundlage ist, Rechnung getragen worden. Dieser Gedanke spiegelt das Bedürfnis vieler Wirtschaftsunternehmen, auch auf diesem Gebiet Wettbewerbs- bzw. Alleinstellungsmerkmale zu entwickeln, wider.

Im übrigen ist die Datenschutzregelung im TDDSG und im MDStV wortgleich.

4. Geltungsbereich in TDG und TDDSG zu weit

Der Geltungsbereich in § 2 Abs. 1 TDG erstreckt sich auf 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 (Teledienste). Dieser Geltungsbereich erstreckt sich damit grundsätzlich auf Teledienste ohne Rücksicht auf privaten, unternehmensinternen oder öffentlichen Bereich. Die Erfahrungen aus der Praxis zeigen, daß der Geltungsbereich sich nur auf Teledienste beziehen sollte, die der Öffentlichkeit angeboten werden. Die Regelungsstruktur des TDG und des TDDSG passen in der vorliegenden Form nicht für unternehmensinterne Kommunikationsnetze. LAN- und Internet-/Intranet-Anwendungen innerhalb von Organisationen unterliegen den Anforderungen dieser Gesetze. Teledienste, die innerhalb von Organisationen angeboten werden, sind aus dem Geltungsbereich dieses Gesetzes auszuklammern.

Die Regelungen in § 1 Abs. 1 TDDSG sind aus den gleichen Gründen ebenfalls zu weit. Er sollte sich nur auf Teledienste beziehen, die der Öffentlichkeit angeboten werden, da auch hier die Bestimmungen für Teledienste innerhalb von Organisationen nicht geeignet sind.

26 Abelson et. al: *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption*, Final Report, 27 May 1997, http://www.crypto.com/key.study.

27 A. Roßnagel, *Datenschutz-Audit*, Datenschutz und Datensicherheit 9/1997.

28 Vgl. Büllesbach, Alfred: *Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor*, Tagungsband, 20. DAFTA (1996), Köln 1997.

5. Verschiedene Begriffsbestimmungen zum Begriff „Diensteanbieter“

Der Begriff „Diensteanbieter“ in § 3 Nr. 1 TDG unterscheidet sich vom Begriff „Diensteanbieter“ in § 2 Nr. 1 TDDSG dadurch, daß beim Bereithalten von Telediensten zur Nutzung zwischen eigenen oder fremden Telediensten im TDG zusätzlich unterschieden wird. Eine wesentliche Aufklärung der Unterschiedlichkeit ergibt sich auch nicht aus der Begründung. Inhaltlich scheint mir die Differenz jedoch unwesentlich zu sein, da die Begrifflichkeit des Diensteanbieters im TDDSG sich ebenfalls auf eigene oder fremde Teledienste zur Nutzung erstreckt. Dennoch ist die Differenz sprachlich verwirrend und schafft Unsicherheit in der Anwendung.

6. Anmerkung zu § 4 Abs. 2 Nr. 4 TDDSG

Dort ist geregelt, daß personenbezogene Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden; eine Zusammenführung dieser Daten ist unzulässig, soweit dies nicht für Abrechnungszwecke erforderlich ist. Der Schutz, der mit dieser Regelung für den Nutzer erreicht werden soll, ist unklar. Die Trennung der Abrechnungsdaten der Nutzung verschiedener Teledienste durch einen Anbieter schränkt die Dienstleistungsgestaltung, die Preisgestaltung, z.B. die Gewährung von Rabatten bei der Nutzung mehrerer Teledienste, erheblich ein. Zudem erwartet der Kunde in aller Regel eine Abrechnung von einem Anbieter, auch wenn er verschiedene Dienste dieses Anbieters in Anspruch genommen hat. Die Erstellung einer Abrechnung erfordert EDV-technisch die Zusammenführung der Datenbestände. Für die Gestaltung der Abrechnungssysteme und die Rechnungsstellung ist die getrennte Abrechnung desselben Kunden sehr aufwendig und kostenintensiv. Dem Datenschutz des Nutzers kann bei der Erstellung teledienstübergreifender Nutzungsprofile durch die Ermöglichung der Verwendung eines Pseudonyms besser Rechnung getragen werden.

7. Hinweise auf nichtkonsistente Begriffe

a) § 3 Abs. 2 TDDSG führt dort den Begriff „verwenden“ ein. Besser wäre es gewesen, diesen Begriff durch die im BDSG akzeptierte Terminologie „verarbeiten und nutzen“ zu ersetzen.

b) Zur Verbesserung und Klarstellung und damit zum Schutz des Nutzers gegen Dritte sollte in § 4 Abs. 2 Nr. 3 TDDSG der Hinweis auf das Fernmeldegeheimnis in § 85 TKG angebracht werden.

c) § 5 Abs. 2 TDDSG sieht für die Verarbeitung und Nutzung von Bestandsdaten für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste die ausdrückliche Einwilligung als Zulässigkeitsvoraussetzung vor. Diese Vorschrift entspricht zwar – wie es sich auch aus der Begründung ergibt – § 89 Abs. 7 TKG, der ebenfalls eine Einwilligung vorsieht, sie ist jedoch nicht konkordant mit der TDSV in § 4 Abs. 2, wo für denselben Sachverhalt eine Widerspruchsklausel geregelt wird.

8. Die Begriffe „Bestands-, Nutzungs- und Abrechnungsdaten“ (§§ 5, 6 TDDSG)

§ 5 Abs. 1 TDDSG regelt zunächst die Befugnis zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Auf einen Katalog der Bestandsdaten wurde ausdrücklich verzichtet, weil – so laut Begründung – sich aus dem Zweck des jeweiligen Vertragsverhältnisses der Umfang ergibt; Bestandsdaten sind in jedem Fall nur solche Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung des Vertrages über die Inanspruchnahme von Telediensten mit dem Diensteanbieter unerläßlich sind. Eine ähnliche Abgrenzung enthält § 89 Abs. 2 Nr. 1 a, b und c TKG und auch die TDSV. Die Begriffe sind schwer voneinander abzugrenzen. Unklar ist, in welchem Umfang es daneben noch andere Daten gibt. Dies mag ein Beispielsfall verdeutlichen: Wenn ein Unternehmen Internet

Business Solutions für Händler anbietet und der Händler wiederum dem Endkunden die zur Verfügung gestellte Internet Business Solution als Teledienst vorhält, entstehen Bestelldaten, die über die Bestandsdaten hinausgehen und im Laufe der Geschäftsverbindungen vielfältig anwachsen. Nimmt man die jetzige, nicht ganz klare Regelung im TDDSG, so bedeutet es für diesen Fall, daß hinsichtlich der Bestandsdaten – soweit keine Regelung getroffen ist – zusätzlich die Vorschriften des BDSG – auch soweit sie nicht auf in Dateien verarbeitete personenbezogene Daten Anwendung finden – gelten (§ 1 Abs. 2 TDDSG). Für die über die Bestandsdaten hinausgehenden sog. Bestelldaten würde dann § 28 Abs. 1 Nr. 1 BDSG gelten. Daraus folgt, daß auch die weiteren Bestimmungen in den §§ 28, 29 BDSG nicht verdrängt sind. Die Regelungen zur Zweckänderung bzw. zur Verarbeitung und Nutzung für Beratung, Werbung, Marktforschung und bedarfsgerechte Gestaltung sind dann jedoch mit denen des TDDSG nicht mehr deckungsgleich.

Hier liegt ein systematischer Konflikt zwischen dem allgemeinen Datenschutzrecht und dem bereichsspezifischen Teledienstedatenschutzrecht vor.

In § 6 TDDSG ist das Prinzip des Verbotes mit Erlaubnisvorbehalt (§ 4 BDSG) geregelt, wonach personenbezogene Daten über die Inanspruchnahme von Telediensten nur erhoben, verarbeitet und genutzt werden dürfen, soweit dies für die nachfolgenden Nr. 1 und 2 erforderlich ist. Eine Einwilligungsregelung wie sie § 4 Abs. 2 BDSG vorsieht, fehlt in § 6 TDDSG. Es stellt sich rechtssystematisch und verfassungsrechtlich die Frage, ob eine solche Regelung mit dem Recht auf informationelle Selbstbestimmung vereinbar ist, da sie dem Nutzer das Recht zur Einwilligung in die Verarbeitung und Nutzung personenbezogener Daten nimmt.

9. Erfahrungsbericht in zwei Jahren

Insgesamt bewertet bilden die Artikel im IuKDG einen durchaus positiven Einstieg in die Bemühungen, den Standort Deutschland auf dem Weg in die globale Informationsgesellschaft rechtlich und politisch zu gestalten. Die einzelnen Kritikpunkte sind durchaus bedeutsam, jedoch darf nicht verkannt werden, daß hier prinzipiell Neuland beschritten wird, und daß alle Beteiligten sich nach bestem Wissen und Gewissen bemühen, die vernünftigsten und besten Regelungen zu finden. Gerade in einer Informationsgesellschaft, in der Visionen und Kreativität für die zukünftige Gestaltung verlangt sind, möchte ich eine abschließende Bewertung mit der allgemeinen Erkenntnis zitieren: „Das Bessere ist des Guten Feind."

Der Entschließungsantrag, der zum IuKDG vorgelegt und vom Bundestag mehrheitlich beschlossen wurde, greift insbesondere unter II. Forderungen des Bundestages an die Bundesregierung auf, die abschließend noch einmal zu betonen sind. Insbesondere der Anpassungs- und Ergänzungsbedarf bei den rechtlichen Rahmenbedingungen für neue Dienste soll spätestens nach Ablauf von zwei Jahren nach Inkrafttreten des IuKDG in einem Bericht der Bundesregierung an den Bundestag vorgelegt werden.

In einen solchen Bericht kann die in zwei Jahren zu erwartende Erfahrung einfließen und das IuKDG neu bewerten lassen.

Fernmeldegeheimnis, Telekommunikationsgeheimnis und Abhörrechte

Während Art. 5 Abs. 1 GG die Öffentlichkeitswirkung der Kommunikation schützt, gewährleistet Art. 10 GG die Geheimhaltung und Abschottung der Kommunikation. Das Fernmeldegeheimnis (das entsprechend der rechtlichen Fortentwicklung zum Telekommunikationsgeheimnis zu entwickeln ist) schützt ebenfalls die Offenheit des Meinungs- und Willensbildungsprozesses in der Gesellschaft durch das Recht des einzelnen, mit Hilfe eines Übermittlers kommunizieren zu können, ohne mit der Kenntnisnahme Dritter rechnen zu müssen. Die Freiheitsräume für diese beiden Handlungsformen der Kommunikation genießen einen besonderen verfassungsrechtlichen Schutz, der konstitutiv für eine demokratische Gesellschaft ist.[29] Die Resonanz dieses Grundrechtes für die demokratische Verfaßtheit der Gesellschaft wird angesichts der Erfahrungen mit seiner Suspendierung im nationalsozialistischen Staat[30] und in der DDR deutlich.[31] Die aktuelle Bewältigung der jüngsten deutschen Vergangenheit führt deutlich vor Augen, welchen Schaden die gesellschaftliche und politische Kultur insgesamt nimmt, wenn in der Gesellschaft dieser Freiraum nicht gewährleistet wird.

Ohne eine breite öffentliche Diskussion wird ein Gesetzentwurf der Bundesregierung für ein Begleitgesetz zum Telekommunikationsgesetz eingebracht, das noch in dieser Legislaturperiode verabschiedet werden soll. Als Zielbestimmung wird angegeben, daß die Ermittlungs- und Abhörbefugnisse des Staates entsprechend der Telekommunikations-Neuregulierung angepaßt werden müssen. Tatsächlich werden jedoch die Abhörmöglichkeiten ausgeweitet. Nach dem Entwurf des Begleitgesetzes zum TKG soll jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt, dazu verpflichtet werden, auf eigene Kosten die technischen Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Überwachungsmaßnahmen zu gestalten und vorzuhalten (§ 88 Abs. 1 TKG). Bislang waren nach § 100 b Abs. 3 StPO, Art. 10, Abs. 2 G10 und § 39 Abs. 1 Außenwirtschaftsgesetz nur Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, zur Bereitstellung der technischen Vorrichtungen für Abhörmaßnahmen verpflichtet. Zukünftig sollen alle, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung mitwirken – das ist sehr weit gefaßt – präventiv entsprechende Überwachungseinrichtungen in ihre Telekommunikationseinrichtungen einbauen. Diejenigen, die Telekommunikationsdienste geschäftsmäßig anbieten, sind verpflichtet, Kundendateien zu führen, auf die die Ermittlungs- und Sicherheitsbehörden über die Regulierungsbehörde online Zugriff haben. Die Abrufverfahren müssen so gestaltet werden, daß die Anbieter von den Zugriffen auf ihre eigenen Kundendaten keine Kenntnis erlangen können. Die Kosten für die Überwachungseinrichtungen müßten von den Betreibern getragen werden. Diese Art des unmittelbaren behördlichen Zugriffs auf private Daten ist einmalig.

29 Rieß: *Regulierung und Datenschutz im europäischen Telekommunikationsrecht*, Braunschweig/Wiesbaden, S. 187 f.

30 Der nationalsozialistische Staat beseitigt den grundsätzlichen Schutz des Brief- und Postgeheimnisses mit einer Verordnung des Reichspräsidenten zum Schutz von Volk und Staat am 28.02.39 (RGBl. I, 83), vgl. AK-GG, Schupert/ Art. 10 Rz 5.

31 Art. 31 der Verfassung der ehemaligen DDR vom 07.10.74 wurde faktisch nicht beachtet; ein Verstoß war nicht strafrechtlich sanktioniert; vgl. Reuter, Neue Justiz ´91, 383 ff.; OLG Dresden: Beschluß vom 22.03.93/1WS 100/92 –, RDtZ 93, 287.

So soll das Gesetz zu Artikel 10 Grundgesetz einen neuen Absatz 2 erhalten und § 100 b StPO einen neuen Absatz 3. Zu beiden Änderungsvorschlägen führt die Begründung übereinstimmend aus: „In Entsprechung zu der im Telekommunikationsgesetz vom 25. Juli 1996 enthaltenen Terminologie hat danach jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. Auf diesem Wege wird Telekommunikation wieder in die Überwachbarkeit einbezogen, die nach der neuen Terminologie nicht mehr unter dem Begriff der öffentlichen Telekommunikation zu subsumieren ist. Diese Anpassung ist insbesondere im Hinblick auf geschlossene Benutzergruppen (bisher als sog. Corporate Networks bezeichnet) und die neuartigen Vermarktungsmethoden von Telekommunikationsdiensten erforderlich“[32]. Mit dieser Formulierung ist klar, daß dies nicht nur eine sprachliche Anpassung an die bisherige Regelung ist, sondern eine Ausweitung. Bisher sind Corporate Networks von staatlichen Überwachungsmaßnahmen nicht betroffen gewesen, weil ihre Systeme keine für die Öffentlichkeit bestimmte Fernmeldeanlagen darstellten. Miterfaßt von der staatlichen Überwachungsbefugnis werden in Zukunft aber auch Corporate Networks sein, die durch Dritte geschäftsmäßig erbracht werden, beispielsweise bei Outsourcing oder innerhalb von Großunternehmen. Mit der Übernahme der Regelungen des TKG, hier insbesondere die Begriffsbestimmung nach § 3 Nr. 5 TKG (geschäftsmäßiges Erbringen von Telekommunikationsdiensten ist das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht) wird deutlich, daß sich die Überwachungsbefugnisse auch auf Nebenstellenanlagen in Hotels und Krankenhäusern, Clubtelefonen und Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind, erfaßt werden.[33]

Wenn diese Regelung beschlossen wird, was – nachdem auch der Bundesrat dies nicht beanstandet hat – zu erwarten ist, bedeutet dies, daß die herkömmlichen Befugnisse zur Überwachung des Fernmeldeverkehrs durch die neuen Dienste wie Teleworking, Telebanking, Teleshopping, digitale Videodienste und Rundfunk im Internet, die vielfältigsten Anwendungen des Electronic Commerce in diese Überwachung einbezogen werden. Eine solche Überwachungsdimension gab es in der bisherigen nicht-elektronischen Form nicht. Die Dimension hat zwei Auswirkungen: zum einen werden immer mehr personenbezogene Daten elektronisch übertragen und gespeichert, zum anderen nutzt der Bürger immer mehr Formen des Electronic Commerce, wodurch gleichzeitig die umfangreichere Erstreckung der Überwachungsmöglichkeiten auf die ausgeweiteten Nutzungsformen inbegriffen ist. Die lineare Übertragung bisher geregelter Eingriffsbefugnisse auf diese neuen Formen der Individual- und Massenkommunikation ist auch verfassungsrechtlich bedeutsam, da sie zu einer Erweiterung der Eingriffsbefugnisse durch Erweiterung der technischen Anwendungs- und Nutzungsmöglichkeiten führt. Diese Diskussion muß intensiver und differenzierter geführt werden, um einerseits die erforderlichen Eingriffsbefugnisse der Sicherheitsorgane zu gewährleisten, aber andererseits die Freiräume des Geschäftsverkehrs und der individuellen Rechte nicht unverhältnismäßig zu beschränken.[34]

32 Bundesratsdrucksache 369/97 vom 23.05.97, S. 43 u. S. 46.

33 (Vgl. hierzu auch Bundestagsdrucksache 13/3609 vom 30. Januar 1996, S. 53.

34 Vgl. auch hierzu die Entschließung der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23.10.96 über die Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich.

Schlußfolgerungen

1. Akzeptanz

Multimedia und globale Datennetze bilden die Basis für die technologische und wirtschaftliche Entwicklung in der Informations- und Kommunikationsgesellschaft. Voraussetzung für eine häufige Nutzung dieser Technologie ist das Erreichen einer hohen Akzeptanz bei Verbrauchern, Bürgern und kommerziellen Nutzern. In psychologischen Erhebungen wurde festgestellt, daß zentrale Gesichtspunkte für die Nutzungsbereitschaft der Informationstechnologien die Übertragungsintegrität, die informationelle Selbstbestimmung und die Mißbrauchskontrolle sind. Datenschutz muß nicht nur rechtlich und organisatorisch, sondern insbesondere auch technisch verstärkt umgesetzt werden.

2. Bereitstellung vertrauenswürdiger Dienstleistungen

Vertrauen ist nicht durch zentrale Regulierung herstellbar, sondern durch Bereitstellung vertrauenswürdiger Dienstleistungen, die jeder nutzen kann. Der einzelne soll nach seinem Bedarf vertrauenswürdige Dienstleistungen nutzen können.

Im einzelnen besteht ein Bedarf nach Konzepten, Dienstleistungen und Produkten für folgende Fälle:

a) Der Schutz des Netzes gegen externe Hakker muß ermöglicht werden. Hier sind moderne Firewall-Systeme gefragt, die die Netzübergangspunkte wirkungsvoll und zuverlässig gegen Hacker- und Malware-Attacken von außen schützen, ohne dabei die Funktionalität für den berechtigten Nutzer einzuschränken und die Kommunikation inakzeptabel zu verzögern. Für den Erbringer von Telekommunikationsleistungen oder anderen Dienstleistungen z.B. auf elektronischen Märkten muß gewährleistet werden, daß die Erschleichung von Dienstleistungen oder Kommunikationskosten nachhaltig verhindert wird. Dies kann beispielsweise durch Teilnehmer-Identifikation auf Basis starker kryptographischer Verfahren erfolgen.

b) Weiterhin müssen Personen gegen persönlichkeitsverletzende und kriminelle Dienstleistungen geschützt werden. Dies kann den Inhalt von Web-Seiten betreffen, auf denen z.B. Persönlichkeiten des öffentlichen Lebens beleidigt oder in Fotomontagen dargestellt werden, aber auch Seiten, auf denen dem Verbraucher betrügerische Angebote unterbreitet werden.

c) Dem Nutzer müssen sichere Verfahren angeboten werden, die eine sichere Kommunikation und eine sichere Abwicklung von Geschäftsvorfällen in Online-Diensten ermöglichen. Dies umfaßt Verfahren, die Integrität und Vertraulichkeit des Kommunikationsinhaltes sicherstellen, sowie die Urheberschaft von Dokumenten unstreitig beweisbar machen.

   Auch ohne den direkten Kontakt zwischen Händler und Kunden muß beiden Seiten ein Mittel an die Hand gegeben werden, daß verläßlich Zahlungsvorgänge ermöglicht. Das kann durch „elektronisches Geld“ oder durch die Möglichkeit der vertraulichen Übertragung einer Kreditkartennummer geschehen. Weitere evtl. pseudonymisierte Zahlungsarten sind denkbar.

   Schließlich beinhaltet dies noch qualitativ hochwertige und sorgfältig getestete Software, da die meisten der neugefundenen Sicherheitsschwächen nicht auf fehlerhaften Konzepten, sondern auf Implementationsfeh-

lern in der eingesetzten Software beruhen. Ein weiteres Qualitätsmerkmal für Software ist eine schnelle Behebung von neu gefundenen Schwächen, da diese schnell über das Internet bekanntgemacht werden und daher potentiell leicht ausgenutzt werden können.

d) Darüber hinaus bedarf es nachvollziehbarer Qualitätskriterien und Verfahren für vertrauenswürdige Dienstleistungen wie beispielsweise „Trust Center“, die eine sichere Infrastruktur und ein verläßliches Schlüsselmanagement für den Einsatz kryptographischer Verfahren anbieten und somit die Basis für die digitale Signatur und Vertraulichkeitsdienstleistungen bilden.

3. Politische und rechtliche Rahmenbedingungen

a) Entscheidender Grundsatz für die politischen und rechtlichen Rahmenbedingungen ist die Erbringung der vertrauenswürdigen Dienstleistungen durch Private im freien Wettbewerb.

b) Der Gesetzgeber soll sich auf Rahmenregelungen beschränken. Die Politik soll die Entwicklung international anerkannter und einsetzbarer Verfahren fördern.

c) Kryptographische Verfahren haben sich zu einer zentralen zivilen Technologie für vertrauenswürdige Dienstleistungen entwickelt. Eine Regulierung des Einsatzes kryptographischer Verfahren zum Zwecke des Abhörens durch Ermittlungs- und Sicherheitsbehörden ist unverhältnismäßig; sie ist zum wirksamen Schutz der Rechtsgüter der inneren Sicherheit ungeeignet. Eine Schlüsselhinterlegung oder ein „Key Recovery“ beeinträchtigen das erforderliche Vertrauen erheblich. Demgegenüber kann dem Einsatz unzulässiger Verschlüsselungsverfahren nicht wirksam begegnet werden. Die deutsche Wirtschaft braucht den freien Zugang zu kryptographischen Verfahren, denen sie vertrauen kann. Der Staat sollte dies im Interesse der gesamten Gesellschaft fördern und unterstützen.

d) Politisch ist die Standardisierung von technischen Komponenten und Dienstleistungen zu fördern, um die Kompatibilität der Verfahren und die Qualität auf einem angemessenen Niveau sicherzustellen.

e) Die vertrauenswürdigen Dienstleistungen auf Basis von kryptographischen Verfahren haben globale Bedeutung. Es müssen zügig multi- und bilaterale Vereinbarungen über die gegenseitige Anerkennung dieser Verfahren abgeschlossen werden.

Empfehlungen

a) Die Fortentwicklung der Informationsgesellschaft verlangt danach, Prinzipien des Datenschutzes und der Sicherheit der Informationsverarbeitung schon bei der Erforschung und der Fortentwicklung von Dienstleistungen und Produkten mit zu berücksichtigen, um sie so zum integralen Bestandteil der Produkte, Dienstleistungen und Beratungen zu machen.

b) Die zergliederten bereichsspezifischen Regelungen – einschließlich der neuen Gesetze – schaffen für Datenschutz und IV-Sicherheit teilweise eine überschneidende Überregulierung und eine strukturelle Unübersichtlichkeit für Nutzer, Verbraucher und Normadressaten. Für den Bürger und für Anwender sollten nach kurzer Erfahrungszeit klarere Regelungen geschaffen werden.

c) Die Eigenverantwortung der Bürger für ihren Datenschutz und die Sicherheit ihrer Anwendungen ist durch öffentliche Diskussionen zu fördern und das Bewußtsein für Selbstschutz und eigenen Systemschutz zu stärken.

d) Die Kompetenzverteilung zwischen Bund und Ländern ist vor dem Hintergrund der internationalen Entwicklung der Informationstechnologie zu überdenken.

e) Es sollten klare Grenzen bei Recht und Umfang der Eingriffsbefugnisse zu Zwecken der Strafverfolgung, der Gefahrenabwehr und des Zugriffs durch die im einzelnen zu benennenden Sicherheitsbehörden gezogen werden.

f) Es ist notwendig, die Selbstregulierung auch durch „Codes of Conduct“, erweiterte „Netiquette“ und datenschutzfreundliche Technologien im nationalen und internationalen Raum zu stärken.

g) Das Fernmeldegeheimnis ist entsprechend der technologischen und auch telekommunikationsrechtlichen Entwicklung zum Telekommunikationsgeheimnis fortzuentwickeln.

Weiterführende Literatur

Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption*, Final Report, 27 May 1997, http://www.crypto.com/key.study

ActivMedia, Romtec, European Information Technology Observatory 97, in: EU-Kommission, Mitteilungen an das Europäische Parlament: Europäische Initiative für den elektronischen Geschäftsverkehr, KOM(97) 157

Bartmann, Dieter, *Die elektronische Geldbörse*, Gutachten der Friedrich-Ebert-Stiftung, Bonn November 1997

Bizer, Johann, *Verschlüsselung und staatlicher Datenzugriff – Die deutsche Debatte*, in: Büllesbach, Alfred (Hrsg.), *Datenschutz in der Telekommunikation, Deregulierung und Datensicherheit in Europa*, Köln 1997

Brühan, Ulf, *Der Gemeinsame Standpunkt des Rates der EU zur Telekommunikationsrichtlinie*, in: Büllesbach, Alfred (Hrsg.), Datenschutz in der Telekommunikation, Deregulierung und Datensicherheit in Europa, Köln 1997

Büllesbach, Alfred (Hrsg.), *Datenschutz in der Telekommunikation, Deregulierung und Datensicherheit in Europa*, Köln 1997

Büllesbach, Alfred, *Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor*, Tagungsband, 20. DAFTA (1996), Köln 1997

Büllesbach, Alfred (Hrsg.) *Staat im Wandel – mehr Dienstleistung, weniger Verwaltung*, Köln 1995

Büllesbach, Alfred; Müller, Roland, *Schutz weltweiter Corporate Networks*, in: *Jahrbuch Telekommunikation und Gesellschaft 1996 – Öffnung der Telekommunikation: Neue Spieler – Neue Regeln*, Heidelberg 1996

Büllesbach, Alfred; Garstka, Hansjürgen, *Systemdatenschutz und persönliche Verantwortung*, in: Müller, Günter, Pfitzmann, Andreas (Hrsg.), *Mehrseitige Sicherheit in der Kommunikationstechnik* – Zusammenfassendes Resultat des von der Gottlieb-Daimler- und Karl-Benz-Stiftung geförderten Kollegs „Sicherheit in der Kommunikationstechnik", Juli 1997

Büllesbach, Alfred; Garstka, Hansjürgen, *Rechtlicher Regelungsbedarf und rechtliche Gestaltung der Sicherheit in der Kommunikationstechnik*, in: *it+ti – Informationstechnik und technische Informatik 38* (1996) 4

Bundesnotarkammer (Hrsg.), *Elektronischer Rechtsverkehr. Digitale Signaturverfahren und Rahmenbedingungen*, Köln 1995

Cheswick, William R.; Bellovin, Steven M., *Firewalls und Sicherheit im Internet*, Addison-Wesley 1996

Damker, Herbert; Müller, Günter, *Verbraucherschutz im Internet*, in: *Datenschutz und Datensicherheit* 21 (1997) 1

Datenschutz bei Multimedia und Telekommunikation, Hamburger Datenschutzhefte, Der Hamburgische Datenschutzbeauftragte, Hamburg 1997

Engel-Flechsig, Stefan, *Zusammenarbeit und Abgrenzung von Telekommunikationsgesetz, Informations- und Kommunikationsdienste-Gesetz des Bundes und Mediendienstestaatsvertrag der Län-*

der, in: Büllesbach, Alfred (Hrsg.*), Datenschutz in der Telekommunikation, Deregulierung und Datensicherheit in Europa*, Köln 1997

Engel-Flechsig, Stefan, *Teledienstedatenschutz,* in: *Datenschutz und Datensicherheit* 21 (1997) 1

EU-Kommission, Mitteilungen an das Europäische Parlament, *Europäische Initiative für den elektronischen Geschäftsverkehr*, KOM(97) 157

Fangmann, Helmut, *Das neue Telekommunikationsgesetz – Texte und Kommentierung für die Praxis*, Hüthig GmbH, Heidelberg 1997

Horster, Patrick (Hrsg.), *Digitale Signaturen*, Braunschweig/Wiesbaden 1996

Horster, Patrick; Portz, *Privacy Enhanced Mail – Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet*, in: *Datenschutz und Datensicherheit* (1994) 8

Janson, Phil, Waidner, Michael, *Electronic Payment Systems*, in *Datenschutz und Datensicherheit* 20 (1997) 6

Knorr, Michael, Schläger, Uwe, *Datenschutz bei elektronischem Geld*, in: Datenschutz und Datensicherheit 21 (1997) 7

Kress, Carl B., *The 1996 Telekommunikationsgesetz and the Telecommunications Act of 1996: Toward More Competitive Markets in Telecommunications in Germany and the United States*, http://www.law.indiana.edu/fclj/v49/no3/kress.html

Kubicek, Herbert, *Duale Informationsordnung als Sicherung des öffentlichen Zugangs zu Informationen*, in: *Computer und Recht*, 11. Jg., 1995

Kubicek, Herbert, *Der Schutz des Fernmeldegeheimnisses auf dem Telekommunikationsmarkt*, in: *Datenschutz und Datensicherheit* 11 (1995)

Müller, Günter; Pfitzmann, Andreas (Hrsg.), *Mehrseitige Sicherheit in der Kommunikationstechnik – Verfahren, Komponenten, Integration*, Addison-Wesley 1997

Müller, Günter, Stoll, Frank, *Der Freiburger Kommunikationsassistent – Sicherheit in multimedialen Kommunikationsnetzen durch nutzerbezogene Dezentralisation*, in: *Symposium Multimedia und Datenschutz*, 28.08.1995, Materialien zum Datenschutz 22, Berliner Datenschutzbeauftragter

Petersen, Holger, *Anonymes elektronisches Geld*, in: Datenschutz und Datensicherheit 21 (1997) 7

Rieß, Joachim, *Regulierung und Datenschutz im europäischen Telekommunikationsrecht*, Braunschweig/Wiesbaden 1996

Roßnagel, Alexander; Bizer, Johann, *Multimediadienste und Datenschutz*, Akademie für Technikfolgenabschätzung in Baden-Württemberg, Stuttgart 1995

Roßnagel, Alexander, *Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger*, ZRP, 1997

Roßnagel, Alexander, *Die Infrastruktur sicherer und verbindlicher Telekommunikation*, Gutachten der Friedrich-Ebert-Stiftung, Bonn 1996

Roßnagel, Alexander, *Datenschutz Audit*, in: *Datenschutz und Datensicherheit* 21 (1997) 9

Ruiz, Blanc R., *Privacy in Telecommunications – A European and an American Approach*, Kluwer Law International, 1997

Schaar, Peter, *Datenschutz in der liberalisierten Telekommunikation*, in: *Datenschutz und Datensicherheit* 21 (1997) 1

Schlickmann, Theodor W., *Daten- und Kommunikationssicherheit in den Forschungsprogrammen der Europäischen Kommission*, in: Büllesbach, Alfred (Hrsg.*), Datenschutz in der Telekommunikation, Deregulierung und Datensicherheit in Europa*, Köln 1997

Schweighofer, Erich, *Data Mining und Datenschutz*, in: *Datenschutz und Datensicherheit* 21 (1997) 8

Schwartz, Paul M.; Reidenberg, Joel R., *Data Privacy Law*, Michie, Charlottesville 1996

Simitis, Spiros, *Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung*, (1984) NJW 398

Simitis, Spiros, *Datenschutz und Europäische Gemeinschaft*, RDV 90

Tauss, Jörg; Kollbeck, Johannes; Mönikes, Jan (Hrsg.), *Deutschlands Weg in die Informationsgesellschaft – Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik*, Baden-Baden 1996

Telekommunikationsrecht: Telekommunikationsgesetz, Rechtsverordnungen, EG-Richtlinien, München 1997

Widmer, Ursula; Bähler, Konrad, *Rechtsfragen beim Electronic Commerce – Sichere Geschäftstransaktionen im Internet*, Orell Füssli, Zürich 1997

Zimmerman, Phil, *PGP – Pretty Good Privacy – Das Verschlüsselungsprogramm für Ihre private elektronische Post*, deutsche Übersetzung von: Deuring, A.; Creutzig, Ch., Bielefeld 1994

Gesetzestexte zum Datenschutz im Internet

Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990, http://www.datenschutz-berlin.de/gesetze/bdsg/inhbdsg.htm

Telekommunikationsgesetz (TKG) vom 25. Juli 1996, http://www.bundesregierung.de/inland/ministerien/post/tkg.html

Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz IuKDG) in der Fassung des Deutschen Bundestages vom 13. Juni 1997, http://www.iid.de/rahmen/iukdgbt.html

Gesetz zur digitalen Signatur (Signaturgesetz – SigG), http://www.netlaw.de/gesetze/sigg.htm

Verordnung zur digitalen Signatur (Signaturverordnung – SigV) in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997, http://www.iid.de/rahmen/sigv.html

Gesetz über die Nutzung von Telediensten (Teledienstegesetz – TDG), http://www.netlaw.de/gesetze/tdg.htm

Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz – TDDSG), http://www.netlaw.de/gesetze/tddsg.htm

Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag) vom 1. August 1997, http://www.datenschutz-berlin.de/gesetze/berlin/medien/medst.htm

Europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995, http://www.datenschutz-berlin.de/informt/heft24/dde.htm oder http://www2.echo.lu/legal/de/datenschutz/datensch.html

Gemeinsamer Standpunkt (EG) Nr. 57/96 im Hinblick auf den Erlaß der Richtlinie 96/…/EG des Europäischen Parlaments und des Rates vom … über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im dienste-integrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen (96/C 315/06), http://www.datenschutz-berlin.de/gesetze/europa/eg5796.htm

Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Telekommunikationsdiensteunternehmen-Datenschutzverordnung – TDSV) vom 12. Juli 1996, http://www.datenschutz-berlin.de/gesetze/medien/tdsv.htm

Verordnung über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind (Fernmeldeverkehr-Überwachungsverordnung – FÜV) vom 18. Mai 1995, http://www.datenschutz-berlin.de/gesetze/medien/fernmel.htm

Der Autor

Prof. Dr. Alfred Büllesbach

war am Institut für Rechtsphilosophie und Rechtsinformatik an der Universität München bis Ende Februar 1979. Bis August 1990 war er Landesbeauftragter für den Datenschutz des Landes Bremen und wechselte dann zum debis Systemhaus. Er leitete dort die Bereiche Datenschutz und IV-Sicherheit sowie Rechts- und Vertragswesen. Er ist Datenschutzbeauftragter der Daimler-Benz Inter-Services (debis) AG und deren juristische Töchter sowie Professor für angewandte Informatik/ Rechtsinformatik an der Universität Bremen.

Heute ist Prof. Dr. Büllesbach als Konzernbeauftragter für den Datenschutz für die Daimler-Benz Aktiengesellschaft einschließlich ihrer Beteiligungen verantwortlich.

Prof. Dr. Büllesbach beschäftigt sich seit über zwei Jahrzehnten mit Fragen der technischen, organisatorischen, gesellschaftlichen und rechtlichen Gestaltung der Informations- und Kommunikationstechnik.

Sein besonderes Augenmerk richtete er dabei auf die Integration der Sicherheitsanforderungen und die Organisation der Geschäftsprozesse. Nicht zuletzt geht es ihm darum, die Anforderungen aus der IV-Sicherheit, der Qualitätssicherung und des Datenschutzes in ein integriertes Gesamtkonzept zusammenzuführen.

Prof. Dr. Büllesbach hat in einschlägigen Fachzeitschriften zu diesen Themen veröffentlicht.