



Unrevidierte Freelance-Übersetzung!!!

**5063/2000/DE-ENDG.
WP 37**

Originalfassung: Englisch

Arbeitsdokument

Privatsphäre im Internet

- Ein integrierter EU-Ansatz zum Online-Datenschutz -

Angenommen am 21. November 2000

Die Arbeitsgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingerichtet. Sie ist ein unabhängiges EU-Beratungsgremium zum Thema Datenschutz und Schutz der Privatsphäre. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG und in Artikel 14 der Richtlinie 97/66/EG festgelegt. Das Sekretariat wird gestellt von der:

Europäischen Kommission, GD Binnenmarkt, Referat Freier Informationsfluss und Datenschutz.
Rue de la Loi 200, B-1049 Brüssel / Wetstraat 200, B-1049 Brüssel - Belgien - Büro: C100-2/133
Internet-Adresse: www.europa.eu.int/comm/dg15/en/media/dataprot/index/htm

INHALTSVERZEICHNIS

KAPITEL 1: EINLEITUNG	1
KAPITEL 2: INTERNET – TECHNISCHE DARSTELLUNG	4
I. Grundlagen	4
Ausgefeiltere Protokolle auf der Grundlage des TCP/IP-Protokolls	6
II. Akteure im Internet	7
Telekommunikationsbetreiber	7
Internet-Zugangsanbieter	7
Internet-Diensteanbieter	8
Nutzer	8
III. Dienste im Internet	9
E-Mail	9
Newsgroups	9
Chatrooms	9
World Wide Web	9
IV. Gefahren für die Privatsphäre	10
Gefahren für die Privatsphäre bei der Verwendung des TCP/IP-Protokolls	10
Gefahren für die Privatsphäre bei der Verwendung höherer Protokolle	11
Gefahren für die Privatsphäre im Zusammenhang mit der Implementierung des HTTP-Protokolls in den marktgängigen Browsern	13
V. Einige wirtschaftliche Überlegungen	14
VI. Zusammenfassung	16
KAPITEL 3: ANWENDUNG DER DATENSCHUTZVORSCHRIFTEN	17
I. Allgemeine rechtliche Überlegungen	17
Personenbezogene Daten im Internet	17
Anwendung der Richtlinien	17
II. Die Überprüfung der Telekommunikations-Richtlinie: die Definition der "elektronischen Kommunikationsdienste"	22
III. Sonstige anwendbare Rechtsvorschriften	24
IV. Anwendung der einzelstaatlichen Datenschutzvorschriften und ihrer internationalen Auswirkungen	25
V. Zusammenfassung	25
KAPITEL 4: ELEKTRONISCHE POST	27
I. Einleitung	27
II. Beteiligte	27
III. Technische Beschreibung	27

Der Vorgang des Versendens einer E-Mail	28
E-Mail-Adressen	28
E-Mail-Protokolle	29
IV. Gefahren für die Privatsphäre	29
Sammlung von E-Mail-Adressen	29
Verkehrsdaten	30
E-Mail Inhalte	31
V. Analyse spezifischer Aspekte	33
Webmail	33
Teilnehmerverzeichnisse	34
Spam	34
VI. Vertraulichkeit, Sicherheitsaspekte	36
VII. Maßnahmen zur besseren Absicherung der Privatsphäre	36
VIII. Zusammenfassung	37
Unsichtbare Verarbeitung durch "Mail-Clients" und SMTP-Relais	37
Aufbewahrung von Verkehrsdaten durch Zwischenträger und E-Mail-Diensteanbieter	37
Überwachung	37
Speicherung und Überprüfung der Inhalte von E-Mails	38
Unerbetene E-Mails (<i>Spam</i>)	38
E-Mail-Verzeichnisse	38
KAPITEL 5: SURFEN AND SUCHEN	40
I. Einleitung	40
II. Technischer Ablauf und beteiligte Akteure	40
Der Vorgang des Websurfens	40
Das Surfen aus der Sicht des Internet-Nutzers	43
Überblick über die wichtigsten, in verschiedenen Abschnitten des Websurfens erzeugten und gespeicherten Daten	43
III. Gefahren für die Privatsphäre	44
Neue Überwachungssoftware	45
IV. Rechtliche Beurteilung	46
Hauptvorgaben der allgemeinen Richtlinie 95/46/EG: Grundsatz der Zweckentsprechung, der Verarbeitung nach Treu und Glauben und der Unterrichtung der Dateninhaber	47
Zentrale Bestimmungen der besonderen Richtlinie über den Schutz der Privatsphäre im Bereich der Telekommunikation	49
V. Maßnahmen zur besseren Absicherung der Privatsphäre	52
VI. Zusammenfassung	53
KAPITEL 6: VERÖFFENTLICHUNGEN UND FOREN	55
I. Einleitung	55
II. Technische Beschreibung	55
Öffentliche Diskussionsforen	55
Veröffentlichungen und Verzeichnisse	56

III. Gefahren für die Privatsphäre	57
Öffentliche Diskussionsforen	57
Veröffentlichungen und Verzeichnisse	58
IV. Rechtliche Beurteilung	59
Öffentliche Foren	59
Veröffentlichungen und Verzeichnisse	60
V. Maßnahmen zur besseren Absicherung der Privatsphäre	62
Anonymität in öffentlichen Foren	62
Systematische Indexierung von Daten	62
Onlinezugang zu öffentlichen Informationsangeboten	63
VI. Zusammenfassung	64
KAPITEL 7: ELEKTRONISCHER GESCHÄFTSVERKEHR IM INTERNET	65
I. Einleitung	65
II. Akteure	65
III. Sichere Zahlungssysteme	67
IV. Gefahren für die Privatsphäre	69
V. Rechtliche Beurteilung	71
Rechtmäßigkeit der Verarbeitung: Grundsatz der Zweckentsprechung (Artikel 5 bis 7 der Richtlinie 95/46/EG)	72
Unterrichtung der betroffenen Personen (Artikel 10 der Richtlinie 95/46/EG)	73
Aufbewahrung von personenbezogenen Daten bzw. von Verkehrsdaten (Artikel 6 der Richtlinie 95/46/EG bzw. Artikel 6 der Richtlinie 97/66/EG)	73
Automatisierte Einzelentscheidungen (Artikel 15 der Richtlinie 95/46/EG)	74
Rechte der betroffenen Personen (Artikel 12 der Richtlinie 95/46/EG)	74
Verpflichtungen der für die Verarbeitung Verantwortlichen: Vertraulichkeit und Sicherheit (Artikel 16 und 17 der Richtlinie 95/46/EG bzw. 4 und 5 der Richtlinie 97/66/EG)	74
Anwendbares einzelstaatliches Recht (Artikel 4 der Richtlinie 95/46/EG)	74
VI. Zusammenfassung	75
KAPITEL 8: CYBERMARKETING	76
I. Einleitung	76
II. Technische Beschreibung	76
Online-Erstellung von Datenprofilen und Werbung	76
Elektronische Post	77
III. Rechtliche Beurteilung	78
Datenschutzrichtlinie	78
Richtlinie zum Fernabsatz	79
Besondere Richtlinie zum Schutz der Privatsphäre im Bereich der Telekommunikation	79
Die Richtlinie über den elektronischen Geschäftsverkehr	79
IV. Zusammenfassung	80
Online-Erstellung von Datenprofilen und Werbung	80
Elektronische Post	81

KAPITEL 9: MASSNAHMEN ZUR BESSEREN ABSICHERUNG DER PRIVATSPHÄRE	83
I. Einleitung	83
II. Technologien zur besseren Absicherung der Privatsphäre	84
<i>Cookie-Killer</i>	84
<i>Proxy-Server</i>	85
Anonymisierungs-Software	86
E-Mail-Filter und anonymen E-Mail-Versand	87
Informationsmittler	87
III. Weitere Maßnahmen zur besseren Absicherung der Privatsphäre	89
P3P	89
Kennzeichen für den Schutz der Privatsphäre	90
IV. Zusammenfassung	91
KAPITEL 10: ZUSAMMENFASSUNG	93
Trends und Gefahren	93
Leitlinien und Empfehlungen	94
2.1 Bewusstseinsbildung bei den Internet-Nutzer	94
2.2 Konsequente und koordinierte Anwendung der vorhandenen Rechtsvorschriften	95
2.3 Entwicklung und Verwendung von Technologien, die den Datenschutz gewährleisten, fördern und verbessern	95
2.4 Schaffung vertrauensbildender Verfahren für Kontrolle und Feedback	96
GLOSSAR DER FACHAUSDRÜCKE	98

GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN



KAPITEL 1: EINLEITUNG

Mit diesem Dokument soll ein integrierter EU-Ansatz für die Problematik des Online-Datenschutzes geboten werden. Mit dem Ausdruck "integriert" wird der Sachverhalt betont, dass die Untersuchung in der Hauptsache von den beiden Texten der allgemeinen Datenschutzrichtlinie (Richtlinie 95/46/EG) und der Richtlinie über den Schutz der Privatsphäre im Bereich der Telekommunikation (Richtlinie 97/66/EG) ausgeht, aber auch alle bislang von der Arbeitsgruppe vorgelegten Stellungnahmen und Dokumente zu bestimmten strittigen Fragen berücksichtigt und zusammenstellt, die mit der genannten Problematik zu tun haben¹.

Die Arbeitsgruppe hat bei der Erörterung ihrer künftigen Arbeit bei verschiedenen Gelegenheiten auf die Notwendigkeit hingewiesen, die Datenschutzproblematik im Zusammenhang mit der Nutzung des Internets zu behandeln. Um diese Fragen systematisch und effizient bearbeiten zu können, wurde 1999 die Task Force 'Internet' (ITF) gegründet. Hauptaufgabe dieser Task Force ist es, die Ressourcen und Wissensbestände der verschiedenen einzelstaatlichen Datenschutzbehörden zusammenzutragen, um zu einer einheitlichen Auslegung und Anwendung des vorhandenen rechtlichen Rahmens in diesem Bereich beizutragen.

Die Task Force hat in den vergangenen zwei Jahren verschiedene Papiere vorgelegt, die von der Arbeitsgruppe angenommen wurden. Seit Anfang des Jahres 2000 hat die Task Force die Häufigkeit ihrer

¹ Vor allem folgende: **Stellungnahme** 1/98 "Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)", von der Arbeitsgruppe 'Schutz von Einzelpersonen bei der Verarbeitung ihrer personenbezogenen Daten' am 16. Juni 1998 angenommen. **Arbeitsdokument** "Processing of Personal Data on the Internet", von der Arbeitsgruppe am 23. Februar 1999 angenommen, WP 16, 5013/99/EN/final. **Empfehlung** 1/99 zum Thema: "Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware", von der Arbeitsgruppe am 23. Februar 1999 angenommen, 5093/98/EN/final, WP 17; **Empfehlung** 2/99 zum Thema: "The respect of privacy in the context of interception of telecommunications", angenommen am 3. Mai 1999, 5005/99/final, WP 18; **Stellungnahme** 3/99 "Public sector information and the protection of personal data", von der Arbeitsgruppe angenommen am 3. Mai 1999; **Empfehlung** 3/99 zum Thema "Preservation of traffic data by Internet Service Providers for law enforcement purposes", angenommen am 7. September 1999, 5085/99/EN/final, WP 25; **Stellungnahme** 1/2000 zu bestimmten Datenschutzaspekten des elektronischen Handels, vorgelegt von der Task Force 'Internet', angenommen am 3. Februar 2000, 5007/00/EN/final, WP 28; **Stellungnahme** 2/2000 zur allgemeinen Überprüfung des rechtlichen Rahmens im Telekommunikationsbereich, vorgelegt von der Task Force 'Internet', angenommen am 3. Februar 2000, WP 29, 5009/00/EN/final; **Stellungnahme** 5/2000 zur Verwendung öffentlicher Verzeichnisse für die Rückwärtssuche oder die Suche nach Vielfachkriterien (Rückwärtsverzeichnisse), WP 33, angenommen am 13. Juli 2000 und **Stellungnahme** 7/2000 zum Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000, KOM (2000) 385 endg., angenommen am 2. November 2000, WP 36.

Die Arbeitsgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingerichtet. Sie ist ein unabhängiges EU-Beratungsgremium zum Thema Datenschutz und Schutz der Privatsphäre. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG und in Artikel 14 der Richtlinie 97/66/EG festgelegt. Das Sekretariat wird gestellt von der:

Sitzungen erhöht, um ein Synthesedokument zu erstellen, das als Bezugsrahmen für die Behandlung der derzeitigen und möglichst auch künftigen Fragen zum Thema Privatsphäre im Internet dienen kann.

Hauptziel dieses Dokuments ist es, einen ersten Ansatz zur Problematik des Online-Datenschutzes zu liefern, der dazu dienen kann, das Bewusstsein für die Gefahren für die Privatsphäre bei der Nutzung des Internets zu schärfen und gleichzeitig einen Leitfaden für die Auslegung beider einschlägigen Richtlinien zu bieten. Die Arbeitsgruppe weiß, dass der Datenschutz bei den Nutzern des Internets eine vorrangige Sorge ist². Deshalb misst sie der Behandlung dieser Frage große Bedeutung bei, ist sich aber darüber im klaren, dass noch manche strittigen Fragen, die Anlass zu speziellen Erörterungen geben, weitere Arbeiten erforderlich machen.

Dieses Dokument selbst kann nicht erschöpfend sein, aber es soll die typischsten Situationen behandeln, denen Internet-Nutzer gegenüberstehen können, wenn sie irgend einen der im Netz vorhandenen Dienste nutzen (z.B. E-Mails, Surfen, Suchen, Newsgroups usw.). Wegen seines allgemeinen Charakters behandelt das Dokument keine spezifischen Fragen, die eventuell verdienen, von der Arbeitsgruppe einmal untersucht zu werden, wie etwa die Überwachung von E-Mails am Arbeitsplatz. Dieses Arbeitsdokument beruht auf dem derzeitigen Stand der Internet-Technik, die sich allerdings von ihrem Wesen her sehr dynamisch entwickelt.

Um die Lektüre zu erleichtern, erfolgt in diesem Arbeitsdokument zunächst eine grundlegende technische Darstellung und Behandlung der allgemeinen rechtlichen Fragen. Danach werden sämtliche Internetdienste einzeln behandelt, wobei jeweils die anstehenden technischen und rechtlichen Fragen thematisiert werden. Den Maßnahmen und Techniken zur Verbesserung des Schutzes der Privatsphäre der Internet-Nutzer ist ein eigenes Kapitel gewidmet. Im letzten Kapitel wird eine Zusammenfassung vorgelegt.

Ein Glossar mit Fachausdrücken wurde am Ende des Dokuments eingefügt, um den Leser in die Lage zu versetzen, die technischen Ausdrücke zu verstehen, die in diesem Arbeitsdokument verwendet wurden. Alle kursiv gedruckten Ausdrücke werden im Glossar erläutert.

Die Task Force hat absichtlich gewisse Wiederholungen im Text dieses Dokuments in Kauf genommen, um den Lesern eine selektive Lektüre des Dokuments zu gestatten, die nur an einer bestimmten Frage interessiert sind. Zu diesem Zweck wurden auch einige zusätzliche – zuweilen sich wiederholende – Beschreibungen in den Text aufgenommen, um ein Nachschlagen in einzelnen Kapiteln zu ermöglichen.

Die Arbeit der Task Force 'Internet' wurde von Peter HUSTINX koordiniert, dem Vorsitzenden der niederländischen Datenschutzbehörde. Die konsolidierte Fassung des Arbeitsdokuments wurde von einer Redaktionsgruppe innerhalb der Task Force erstellt, die von Diana ALONSO BLAS (niederländische Datenschutzbehörde) und Ann-Christine LACOSTE (belgische Datenschutzbehörde) gebildet wurde. Die Arbeit der Redaktionsgruppe galt insbesondere der Strukturierung und Überprüfung der Konsistenz des gesamten Dokuments, der Einbeziehung und weiteren Ausarbeitung zusätzlicher rechtlicher Fragen und technischer Informationen sowie der Anmerkungen weiterer Delegationen und schließlich der Ausarbeitung des Glossars der Fachausdrücke und der Zusammenfassung dieses Dokuments.

An verschiedene Phasen der Arbeit der Task Force 'Internet' beteiligten sich die Vertreter der Datenschutzbehörden aus sechs Mitgliedstaaten, sei es durch Arbeitspapiere, die für verschiedene Kapitel den Ausgangspunkt bildeten, oder durch Anmerkungen zu den Beiträgen anderer Mitglieder der Task Force oder aber durch Diskussionsbeiträge in den fünf Sitzungen der Task Force, die sie im Jahr 2000 abhielt.

Insbesondere seien folgende Personen genannt: Anne-Christine Lacoste und Jean-Marc Dinant (Belgien), Ib Alfred Larsen (Dänemark), Marie Georges (Frankreich), Angelika Jennen und Sven Moers (Deutschland), Emilio Aced Féllez (Spanien) und Diana Alonso Blas, Ronald Hes und Bernard Hulsman

² Dies wird in einer sechsmonatigen Untersuchung unterstrichen, die kürzlich von der Markle-Stiftung vorgelegt wurde. Siehe Zeitungsartikel von AARON, D., *A Euro-American proposal for privacy on the Net*, Washington Post, 2. August 2000.

(Niederlande). Die Task Force dankt ferner Christine Sottong-Micas (Sekretariat der Arbeitsgruppe Datenschutz gemäß Artikel 29, Europäische Kommission) und Karola Wolprecht (Praktikumssemester 1999/2000 bei der Europäischen Kommission) für ihre Hilfe und Unterstützung.

KAPITEL 2: INTERNET – TECHNISCHE DARSTELLUNG

I. Grundlagen

Das Internet ist ein Netzwerk von Computern, die auf der Grundlage des Transport Control Protocol/Internet Protocol (TCP/IP) miteinander kommunizieren³. Es handelt sich dabei um ein internationales Netz von miteinander verbundenen Computern, das Millionen von Menschen in die Lage versetzt, in einem sogenannten "Cyberspace" miteinander zu kommunizieren und Zugang zu umfangreichen Mengen an Informationen aus allen Teilen der Welt zu erhalten⁴.

Historischer Vorläufer des Internets war das Militär-Netzwerk ARPAnet (1969), dem die Vorstellung zugrunde lag, ein US-weites elektronisches Netzwerk zu schaffen, durch das Computer von Militär, Waffenindustrie und Universitäten mit verteidigungsrelevanter Forschung über redundante Kanäle selbst dann miteinander kommunizieren können, wenn Teile des Netzwerks durch Kriegseinwirkung zerstört sind⁵.

Die ersten Programme zur Beförderung elektronischer Post erschienen 1972. Im Jahre 1985 schuf die nationale amerikanische Wissenschaftsstiftung das NSFNET-Netzwerk, mit dem sechs US-amerikanische Supercomputer-Zentren miteinander verbunden wurden. In den späten 80er Jahren wurde dieses Netzwerk, das nunmehr den Namen MERIT erhielt, einer Gruppe von Universitäten übertragen. Dieses Netzwerk öffnete sich allmählich auch nicht universitären und außeramerikanischen Einrichtungen. 1990 schuf Tim Berners Lee, der am CERN in Genf arbeitete, den ersten Browser und führte das Konzept des *Hyperlink* ein; seitdem wurden ständig neue Dienste und Funktionen hinzugefügt.

Man muss sich aber vor Augen halten, dass TCP/IP weiterhin das zentrale *Protokoll* für die Datenübertragung im Internet ist und sämtliche Dienste darauf beruhen. Dieses *Protokoll* wurde so konzipiert, dass es sehr einfach eingerichtet werden kann und unabhängig von den einzelnen Computertypen und Betriebssystemen arbeitet.

Jeder einzelne Computer im Internet wird durch eine einmalige IP-Adressnummer in der Form A.B.C.D. identifiziert, wobei A, B, C und D Zahlen zwischen 0 und 255 sind (z.B. 194.178.86.66).

Ein *TCP/IP-Netzwerk* beruht auf der Übertragung von kleinen Informationspaketen. Jedes Paket enthält die IP-Adresse des Absenders und des Empfängers. Dieses Netzwerk ist verbindungslos, d.h., im Gegensatz etwa zu einem Telefonnetz setzt der Beginn einer Kommunikation zwischen zwei Geräten nicht voraus, dass sie bereits miteinander verbunden sind. Ferner bedeutet dies, dass gleichzeitig zahlreiche Kommunikationsverbindungen mit vielen Partnern möglich sind.

Das Bereichsnamen-System *DNS (Domain Name System)* ist ein System, mit dem Computern, die über eine IP-Adresse identifiziert sind, Namen verliehen werden können. Solche Namen haben die Form <Name>.<übergeordneter Bereich>, wobei <Name> eine Zeichenfolge ist, die von einer oder mehreren, durch Punkte voneinander getrennten Unterzeichenfolgen gebildet wird. Der übergeordnete Bereich kann entweder allgemeiner Art sein wie etwa "com" für kommerzielle Websites oder "org" für nicht

³ Die hier beschriebenen technischen Aspekte werden drastisch vereinfachend dargestellt, damit sie auch für Laien verständlich sind. Zu mehr Einzelheiten siehe: Mitteilung der Kommission an den Rat und das Europäische Parlament: Organisation und Verwaltung des Internet - Internationale und europäische Grundsatzfragen 1998 - 2000. KOM (2000) 202 endg., 11. April 2000. Im Internet abrufbar unter: <http://europa.eu.int/eur-lex/de/oj/index.html>

⁴ Siehe Entscheidung Reno versus ACLU (26. Juni 1997), Supreme Court of the United States, abrufbar unter: www2.epic.org/cda/cda_decision.html

⁵ Siehe Entscheidung Reno versus ACLU (26. Juni 1997).

gewinnorientierte Einrichtungen oder aber ein geographischer Bereich wie etwa "be" für Belgien. Eine Beteiligung am *DNS* muss bezahlt werden, und Unternehmen oder Einzelpersonen, die einen Bereichsnamen haben möchten, müssen sich ausweisen. Einige öffentlich im Internet zugängliche Tools ermöglichen es, die Verknüpfung zwischen dem Bereichsnamen und dem entsprechenden Unternehmen wie auch zwischen der IP-Adresse und dem Bereichsnamen herauszufinden. Ein Bereichsname als solcher ist nicht erforderlich, um einen Computer mit dem Internet zu verbinden.

Bereichsnamen sind dynamisch. Ein einzelner Internet-Computer kann einen oder viele - oder gar keinen - Bereichsnamen haben, aber jeder einzelne Bereichsname bezieht sich jeweils auf nur eine IP-Adresse.

Die Anzahl der IP-Adressen ist gegenwärtig begrenzt und hängt von der Größe des Feldes ab, das der IP-Adresse im *Protokoll* zugewiesen wurde⁶. Die IP-Adressen werden in Europa über ein internationales Verfahren⁷ an Internet-Zugangsanbieter vergeben, die sie sodann an ihre Kunden, Einrichtungen und Einzelpersonen, weitergeben. Benutzt man eine öffentlich zugängliche Suchmaschine wie etwa <http://www.ripe.net/cgi-bin/whois>, kann die für die Vergabe einer besonderen IP-Adresse zuständige Stelle ermittelt werden. In der Regel handelt es sich dabei um einen:

- Verwalter eines mit dem Internet verbundenen "Lokalen Netzes" (Local Area Network - LAN) (z.B. ein Privatunternehmen oder eine staatliche Behörde). In diesem Fall verwendet er wahrscheinlich ein festes IP-Adressierschema und verwaltet ein Verzeichnis der Entsprechungen zwischen den Computern der Teilnehmer und den IP-Adressen. Falls das *Dynamic Host Configuration Protocol* (DHCP⁸) verwendet wird, führt das *DHCP*-Programm in der Regel ein Logbuch, in das die Nummern der Ethernet-Karten eingetragen sind. Anhand dieser weltweit jeweils einmaligen Nummern kann ein einzelner Computer im Lokalen Netz identifiziert werden.
- Internet-Zugangsanbieter, der vertragliche Vereinbarungen mit Internet-Teilnehmern trifft. In diesem Fall führt der Anbieter ein Logbuch mit der zugewiesenen IP-Adresse, der Identität des Teilnehmers, dem Datum, dem Zeitpunkt und der Dauer der Adressenzuweisung. Falls der Internet-Nutzer ein öffentliches Telefonnetz benutzt (mobiles oder ortsfestes Telefon), wird darüber hinaus von der Telefongesellschaft für Zwecke der Telefonabrechnung die angerufene Nummer (mit Datum, Stunde und Dauer) aufgezeichnet.
- Inhaber eines Bereichsnamens; dies kann der Name eines Unternehmens, eines Beschäftigten eines Unternehmens oder eine Privatperson sein.

Das heißt, in diesen drei Fällen können mit Hilfe Dritter, die für die Zuweisungen der Adressen zuständig sind, ohne großen Aufwand Internet-Nutzer identifiziert werden (d.h. seine/ihre amtliche Identität: Name, Adresse, Telefonnummer usw.).

Ein *Router* ist ein wichtiges Gerät, mit dem Leitwege für *TCP/IP-Netzwerke* ermittelt werden. Dies bedeutet, dass die Routen beim *TCP/IP* dynamisch sind und je nach Ausfall oder Überlastung einiger Strecken oder Verbindungen verlaufen. Das Gerät kann auch als *Firewall*, also als "Brandmauer"

⁶ Die neuere Version (IPversion6) des IP-Adressiersystems wird derzeit auf der Grundlage von 128 Bit langen Zahlen entwickelt.

⁷ Die Internet Corporation for Assigned Names and Numbers (ICANN) ist eine Einrichtung ohne Erwerbscharakter, die mit der Zuständigkeit für die Vergabe der IP-Adressen gegründet wurde (<http://www.icann.org>). In Europa wird der Adresserraum von der Einrichtung RIPE (Réseaux IP Européens) verwaltet (<http://www.ripe.net>). Zu weiteren Einzelheiten der noch laufenden Entwicklung der Internet-Bereichsnamen siehe die in Fußnote 3 genannte Mitteilung der Kommission.

⁸ Das *Dynamic Host Configuration-Protokoll* (DHCP) ist ein Internet-Protokoll für die automatische Konfiguration der Computer, die das *TCP/IP*-Protokoll verwenden. DHCP kann für die automatische Zuweisung von IP-Adressen verwendet werden. (<http://www.dhcp.org>)

zwischen einer Organisation und dem Internet verwendet werden. Vor allem kann es gewährleisten, dass von einem bestimmten *ISP* nur autorisierte IP-Adressen ausgehen können.

Wichtig ist die Feststellung, dass das wichtigste Kriterium für die Wahl der Routen zwischen TCP/IP-Netzwerken die Übertragungsgeschwindigkeit ist. Da Informationen in einer Leitung nahezu mit Lichtgeschwindigkeit zirkulieren, kann es effizienter sein, TCP/IP-Pakete von London nach Madrid über New York zu schicken, wenn im Netzwerk von Paris ein Übertragungstau vorhanden ist. Es gibt Tools, die den Nutzer über die Route zwischen zwei Punkten informieren, aber sie kann sich theoretisch jederzeit, selbst bei der Übertragung einer einzelnen Dokumentenseite, wieder ändern.

Ausgefeiltere Protokolle auf der Grundlage des TCP/IP-Protokolls

Für bestimmte Dienste wurden neben TCP/IP einige andere *Protokolle* entwickelt. Die am meisten verbreiteten *Protokolle* sind:

- HTTP (**H**yper**T**ext **T**ransport **P**rotocol) für das Surfen im Netz,
- FTP (**F**ile **T**ransfer **P**rotocol) für die Übermittlung von Dateien,
- NNTP (**N**ews **N**etwork **T**ransport **P**rotocol) für den Zugang zu Newsgroups,
- SMTP (**S**imple **M**ail **T**ransport **P**rotocol) und POP3 (für den Versand und Empfang von E-Mails).

Hierarchie der Schichten und Protokolle bei der Internet-Kommunikation

HTTP für Surfen und Suche im Netz	SMTP für die Versendung von E-Mails	POP3 für das Herun- terladen von E-Mails von Mail-Servern zum "Client"	NNTP für die Über- tragung von Nachrichten	FTP für das Herunter- und Hinaufladen von Dateien und Programmen	usw... Viele sonstige Protokolle der oberen Ebene können in Zu- kunft verwendet oder entwickelt werden
TCP/IP					
PPP für <i>Modems</i> an Telefonleitungen	X-75 für Terminal- adapter an ISDN- Leitungen	ADSL für ADSL- <i>Modems</i> an her- kömmlichen Telefonleitungen	ETHERNET für LAN-Platinen in Lokalen Netzwerken	usw... Viele sonstige Protokolle der unteren Ebene sind in Gebrauch oder können entwickelt werden	

• Diese *Protokolle* sind nötig, weil das TCP/IP-*Protokoll* lediglich die Übertragung der Grobinformationen von einem Computer zum anderen ermöglicht. Computer, die einen Dienst bieten, werden SERVER genannt. Computer, die einen Dienst in Anspruch nehmen, heißen CLIENT. Für die Übermittlung eines technischen Dienstes benutzen sowohl der CLIENT als auch der SERVER dasselbe *Protokoll*, das heißt, dieselben Kommunikationsregeln. Deshalb wird das Internet häufig auch als CLIENT/SERVER-Netz bezeichnet. Wichtig ist festzuhalten, dass unabhängig davon, welcher Dienst genutzt wird, das TCP/IP-*Protokoll* jedem der vorgenannten Dienste zugrunde liegt; dies bedeutet, dass jede Gefahr für die Privatsphäre, die im Zusammenhang mit dem TCP/IP-*Protokoll* auftreten kann, auch bei der Benutzung jedes beliebigen anderen Dienstes im Internet gegenwärtig ist.

• Um Missverständnisse mit der allgemeinen Bedeutung des Ausdrucks "Dienst" zu vermeiden, wird in diesem Dokument der Terminus *Protokoll* generell zur Bezeichnung der Dienste HTTP, FTP, NNTP und sonstiger Dienste im Internet verwendet.

Ein *Proxy-Server* ist ein zwischengeschalteter Server zwischen dem Internet-Nutzer und dem Netz. Er arbeitet als Zwischenspeicher im Netz (*Web cache*), wodurch die optische Darstellung der Informationen (das heißt die Darstellung von Dokumentenseiten) drastisch beschleunigt wird. Viele große Einrichtungen oder Internet-Zugangsanbieter haben diese Lösung bereits eingeführt. Jede Seite, jedes Bild oder jedes Logo, das Mitarbeiter einer Einrichtung von außerhalb heruntergeladen, wird in einem "Cache" des *Proxy-Servers* gespeichert und steht unmittelbar darauf anderen Mitarbeitern derselben Einrichtung zur Verfügung.

II. Akteure im Internet

Unternehmen oder Einzelpersonen können in bezug auf das Internet unterschiedliche Aufgaben wahrnehmen und folglich verschiedene Datenverarbeitungsoperationen durchführen (zum Beispiel als Telekommunikationsbetreiber Verbindungen herstellen oder als *ISP* besuchte Websites speichern), mit allen Konsequenzen, die dies für die Anwendung der Grundsätze des Schutzes der Privatsphäre hat.

Telekommunikationsbetreiber

In Europa war die Infrastruktur für Telekommunikation faktisch ein Monopol der traditionellen Betreiber der Fernmeldenetze. Diese Situation ist nunmehr im Wandel begriffen und das Monopol wird häufig auf Kupfer- oder Glasfaserkabelnetze eingeschränkt, während bei der drahtlosen Kommunikation und den sich neu herausbildenden Technologien wie *WAP*, *UMTS* usw. zwischen nationalen Betreibern Wettbewerb entsteht.

Die traditionellen Fernmeldeunternehmen bleiben allerdings wichtige Akteure, da sie die Datenkommunikation zwischen den Netzbenutzern und den Internet-Zugangsanbietern (IAP) herstellen.

Die Fernmeldeunternehmen verarbeiten für die Ausstellung der Gebührenrechnungen die sogenannten Verkehrsinformationen wie etwa die anrufende Telefonnummer und ihren Standort (bei Mobiltelefonen), die angerufene Nummer sowie Datum, Zeitpunkt und Dauer der Verbindung⁹.

Internet-Zugangsanbieter

Internet-Zugangsanbieter (IAP) bieten - in der Regel auf vertraglicher Basis - TCP/IP-Verbindungen zu:

- Einzelpersonen, die ein *Modem* oder Terminaladapter (ISDN) verwenden. In diesem Fall erhalten die Teilnehmer für die Dauer der Verbindung eine IP-Adresse, die sich wahrscheinlich bei der nächsten Einwahl wieder ändert. Dies wird dynamische TCP/IP-Adressierung genannt.

Bei Verbindungen über *ASDL* oder Videokabel sind die IP-Adressen in der Regel statisch, sofern eine ständige Verbindung besteht.

Um eine Verbindung zu erhalten, müssen die Teilnehmer¹⁰ einen Vertrag abschließen (selbst wenn die Teilnahme gratis ist) und Namen, Adresse und andere personenbezogene Daten angeben. Gewöhnlich erhalten Sie dann eine Nutzerkennung (UserId, die auch ein Pseudonym sein kann) sowie ein Passwort, um zu verhindern, dass Fremde ihr Abonnement benutzen. Anscheinend ist bei den Internet-Zugangsanbietern üblich, zumindest aus Sicherheitsgründen in Dateien systematisch Datum, Zeitpunkt, Dauer und dynamische IP-Adresse des Internet-Nutzers einzufügen. Solange ein solches *Protokoll* mit der IP-Adresse eines Nutzers verknüpft werden kann, muss diese als personenbezogene Datei betrachtet werden.

⁹ Die Verarbeitung und Speicherdauer solcher Daten unterliegt strikten Rechtsvorschriften; dies wird weiter unten erläutert.

¹⁰ Selbstverständlich können auch kleine Unternehmen solche Verträge schließen, aber auf diese besonderen Fälle wird in diesem Arbeitspapier nicht eingegangen.

– Organisationen, die Wählleitungen (dialup) oder häufiger gemietete Leitungen zu ihrer Unternehmensverwaltung benutzen. Solche Mietleitungen werden gewöhnlich von den traditionellen Fernmeldebetreibern zur Verfügung gestellt. Die Verbindungen können auch über Satellit oder über terrestrische Funkverbindungen hergestellt werden. Die IAP vergeben die IP-Adressen an Unternehmen und stellen durch *Router* sicher, dass die Adressen eingehalten werden.

Internet-Zugangsanbieter besitzen eine oder mehrere Mietleitungen (abgeschirmte Netzkabel, Glasfaser, Satellitenfunk), die mit anderen, größeren IAP verbunden sind.

Internet-Diensteanbieter

Internet-Diensteanbieter (ISP) bieten Einzelpersonen und Unternehmen Netzdienstleistungen. Sie besitzen oder mieten ständige TCP/IP-Verbindungen und benutzen Server, die ständig mit dem Internet verbunden sind. Ihre typischen Angebote sind "Web-hosting" (Speicherung von Webseiten auf ihren Webservern), Zugang zu Newsgroups, Zugang zu FTP-Server und elektronische Post. Dies setzt voraus, dass sie über einen oder mehrere Server mit den Protokollen HTTP, NNTP, FTP, SMTP und POP3 verfügen.

Häufig übernehmen Firmen, die Internet-Zugang bieten (IAP), auch die Funktionen von *ISP*. Aus diesem Grund wird der Terminus *ISP* häufig verwendet, um sowohl Zugangs- als auch Diensteanbieter zu bezeichnen. Aber unter konzeptionellem Gesichtspunkt handelt es sich um unterschiedliche Aufgaben. Die Zugangsanbieter bringen als Brücke zum Internet den gesamten Datenstrom der Internet-Teilnehmer auf den Weg, während die Diensteanbieter lediglich darauf achten, was auf ihren Servern geschieht¹¹. In diesem Arbeitspapier wird der Terminus *ISP* in seiner allgemeinen Bedeutung verwendet, die auch die Zugangsanbieter mit einschließt. Das Kürzel IAP wird nur dann verwendet, wenn deutlich ist, dass es ausschließlich um den Zugang zum Internet geht; in allen übrigen Fällen wird der Oberbegriff *ISP* verwendet.

Unter technischen Gesichtspunkten ist für die Erhebung personenbezogener Daten das Vorhandensein der Server entscheidend, die mit *Protokollen* operieren. So wird bei HTTP-Servern in der Regel automatisch ein "Logbuch" oder "Logfile" generiert, das sämtliche oder einige Daten enthält, die in der HTTP-Anfragezeile (Automatische Browsermeldungen) und in der IP-Adresse vorkommen. Das Generieren solcher Protokolle ist Standard und erfolgt in jedem Server.

Nutzer

Internet-Nutzer können Einzelpersonen sein, die von ihrer Wohnung aus das Internet aufsuchen und dabei in der Regel eine temporäre TCP/IP-Verbindung (also unter Verwendung einer dynamischen IP-Adresse) aufbauen, und zwar mit Hilfe eines Modems, eines Terminaladapters (ISDN) oder einer Standleitung (deshalb statische IP-Adresse) mit Hilfe eines ADSL- oder TV-Kabel-Anschlusses usw. Auch Verbindungen über Mobiltelefon sind möglich, wengleich in der Regel teurer.

Selbst wenn ein Teilnehmer eine falsche Identität oder die Identität eines anderen Nutzers angibt (in der Regel durch die Angabe der Nutzerkennung und des Passwortes eines Dritten), kann der eigentliche Eigentümer der Leitung, der eine bestimmte IP-Adresse zugewiesen worden war, ermittelt werden, da die angegebene Identität mit derjenigen im Logbuch des IAP verglichen wird. Dies ist tatsächlich auch, was die Polizei tut, um etwa strafbare Einbrüche in Computer zurückzuverfolgen, die mit dem Internet verbunden sind.

Dies gilt auch, wenn jemand ein lokales (LAN) oder ein internes Netzwerk (Intranet) benutzt.

¹¹ Hier wird auch nicht die Funktion der ISP als Inhalte-Anbieter behandelt, wengleich manche unter Umständen bestimmte Inhalte anbieten (so haben manche ISP ihre eigenen *Portal-Sites*).

Nutzer können auch Einrichtungen, öffentliche Verwaltungen oder Unternehmen sein, die das Internet nicht nur nutzen, um Informationen zu liefern oder zu suchen, sondern auch, um für ihre Zwecke oder Tätigkeiten (Verwaltungsvorgänge, Verkauf von Produkten oder Bereitstellung von Dienstleistungen, Veröffentlichung von Verzeichnissen oder Kleinanzeigen, Versand von Fragebögen usw.) Daten zu sammeln.

III. Dienste im Internet¹²

Jeder, der Zugang zum Internet hat, kann eine Vielfalt von Kommunikationsformen und Informationssuchverfahren benutzen. Am meisten verbreitet sind elektronische Post (siehe Kapitel 4), "Newsgroups" und "Chatrooms" (siehe Kapitel 6) und das World Wide Web (siehe Kapitel 5).

Alle diese Verfahren können zur Übermittlung von Texten verwendet werden; die meisten können auch Klänge, Bilder und bewegte Bilder transportieren. Zusammen genommen bilden sie ein einzigartiges Medium, das bei seinen Nutzern als "Cyberspace" bekannt ist, ein "Raum", der jeder Person, die über einen Internet-Zugang verfügt, überall auf der Welt zugänglich ist.

E-Mail

Über die elektronische Post können elektronische Mitteilungen von Person zu Person oder zu Gruppen von Personen versandt werden. In der Regel wird die Nachricht elektronisch auf einem Server gespeichert, bis der Empfänger seinen "Briefkasten" leert; zuweilen wird die Ankunft einer Nachricht durch irgendeine Art von Zeichen gemeldet.

Newsgroups

Newsgroups werden genutzt, um Informationen auszutauschen oder Stellungnahmen zu bestimmten Fragen abzugeben. Sie dienen Gruppen von regelmäßigen Teilnehmern, aber deren Mitteilungen können auch von anderen gelesen werden. Es gibt Tausende solcher Gruppen, von denen jede den Informations- oder Meinungsaustausch zu einem bestimmten Thema fördert. Jeden Tag werden mehr als 100.000 neue Mitteilungen verschickt.

Chatrooms

Zwei oder mehr Personen, die unmittelbar miteinander kommunizieren möchten, können einen "Chatroom" betreten und sich in Echtzeit miteinander unterhalten, indem sie Mitteilungen schreiben, die nahezu unmittelbar auf dem Bildschirm des jeweils anderen erscheinen.

World Wide Web

Das am besten bekannte Kommunikationsmittel im Internet ist das World Wide Web, das den Nutzern gestattet, in entfernten Computern Informationen zu suchen und aufzufinden. Einfach gesagt besteht das Web aus großen Mengen von Dokumenten, die in weltweit verstreuten Computern gespeichert sind.

Das Navigieren im Web ist ziemlich einfach. Die Nutzer können entweder die Adresse einer bekannten Website oder aber ein oder mehrere Stichwörter in eine kommerzielle "Suchmaschine" eingeben, die zum interessierenden Thema Websites ausfindig macht. Die Nutzer bearbeiten gewöhnlich eine angezeigte Seite oder wechseln zu einer anderen, indem sie mit Hilfe einer "Computermaus" auf ein "Icon" oder eine Verknüpfung auf der angegebenen Seite klicken. Das Web ist also, vom Gesichtspunkt eines Lesers aus betrachtet, sowohl mit einer riesigen Bibliothek vergleichbar, die Millionen von sofort verfügbaren und

¹² Siehe Entscheidung Reno versus ACLU (26. Juni 1997).

indexierten Veröffentlichungen enthält, als auch mit einem immer größer werdenden Einkaufszentrum, das Waren und Dienstleistungen bereit hält (siehe Kapitel 7).

Jede Person und Einrichtung mit einem Computer, der ans Internet angeschlossen ist, kann Informationen "veröffentlichen" oder sammeln (siehe Kapitel 6, 7 und 8). Solche Informationsanbieter oder -sammler können staatliche Stellen, Bildungseinrichtungen, gewerbliche Körperschaften, Interessengruppen und Einzelpersonen sein. Sie können ihre Informationen entweder der Gesamtheit der Internet-Nutzer zur Verfügung stellen oder aber den Zugang auf eine bestimmte Gruppe beschränken.

IV. Gefahren für die Privatsphäre¹³

Gefahren für die Privatsphäre bei der Verwendung des TCP/IP-Protokolls

Da das Internet von Anfang an als ein offenes Netzwerk konzipiert wurde, weisen viele Merkmale der Kommunikationsprotokolle - eher aufgrund von Nebeneffekten als von absichtlichen Entscheidungen - Aspekte auf, die das Eindringen in die Privatsphäre der Internet-Nutzer möglich machen.

Was das TCP/IP-Protokoll betrifft, bieten drei Eigenschaften einen möglichen Eingriff in die Privatsphäre:

- Die von den TCP/IP-Datenpaketen verfolgte **Route** ist dynamisch und verläuft nach dem Kriterium der besten Leistung. Theoretisch kann sie sich während des Herunterladens einer Dokumentenseite oder der Übermittlung eines elektronischen Schreibens ändern, in der Praxis aber bleibt sie weitgehend statisch. Im Fernmeldewesen hängt die Leistung eher von Überlastungen im Netzwerk ab als vom physikalischen Abstand zwischen Netzknoten (*Router*). Dies bedeutet, dass der "kürzeste" Weg zwischen zwei Städten, die etwa im selben EU-Mitgliedstaat liegen, über Nicht-EU-Staaten verlaufen kann, die unter Umständen keinen angemessenen Datenschutz gewährleisten¹⁴. Der durchschnittliche Internet-Nutzer hat keine akzeptable Möglichkeit, diese Strecke zu ändern, selbst wenn er weiß, welche zu einem bestimmten Zeitpunkt eingeschlagen wird.
- Weil die Übersetzung zwischen einem Domain-Namen und der entsprechenden numerischen IP-Adresse über **DNS-Server** erfolgt, deren Aufgabe es ist, diese Übersetzung zu gewährleisten, verzeichnen und speichern diese DNS-Server die Namen sämtlicher Internet-Server, zu denen ein Internet-Nutzer Kontakt herstellen wollte. In der Praxis stehen solche DNS-Server meistens bei den Internet-Zugangsanbietern, die die technischen Möglichkeiten haben, erheblich mehr als nur dies zu erfahren, wie in den folgenden Kapiteln dargestellt wird.
- Der **ping**-Befehl, den es bei allen Betriebssystemen gibt, erlaubt es jedermann im Internet, zu erkennen, ob ein bestimmter Computer eingeschaltet und an das Internet angeschlossen ist. Es handelt sich um einen Befehl, der aus der Folge der Buchstaben PING und anschließender IP-Adresse (oder dem entsprechenden Namen) eines ausgewählten Computers besteht. Der so angewählte Computer-Nutzer bemerkt in der Regel nicht, dass und zu welchem Zweck jemand versucht hat zu erfahren, ob er zu einem bestimmten Zeitpunkt im Netz war.

Ständige Internet-Verbindungen über Kabel oder ADSL-Leitungen sind denselben Gefahren ausgesetzt.

Selbst wenn solche Datenverarbeitungsvorgänge legitim und je nach Umständen sogar für ein reibungsloses Funktionieren des Internets unvermeidlich sind, müssten die Internet-Nutzer darüber informiert werden, dass solche Vorgänge stattfinden und welche Sicherheitsmaßnahmen möglich sind.

¹³ Die französische Datenschutzbehörde CNIL bietet auf ihrer Website unter der Rubrik 'Internet' ein Link "vos traces" (Ihre Spuren), über den Internet-Nutzer ihre eigenen Spuren verfolgen können, die sie bei der Nutzung des Internet hinterlassen. Die Erläuterungen lassen sich auf französisch, englisch und spanisch abrufen. Siehe www.cnil.fr

¹⁴ Zu mehr Einzelheiten über dieses Thema siehe Kapitel 2.

Gefahren für die Privatsphäre bei der Verwendung höherer Protokolle

In diesem Abschnitt werden drei Merkmale behandelt, die bei fast jeder Implementierung des HTTP-Protokolls in den am häufigsten verwendeten Browsern vorkommen. Die Kombination dieser Merkmale kann schwerwiegende Konsequenzen für die Privatsphäre der Internet-Nutzer haben.

Das HTTP-Protokoll ist von zentraler Bedeutung, da es das wichtigste im Web verwendete Protokoll ist und das Angebot von Diensten wie etwa E-Mails und Diskussionsforen erlaubt, die bislang gewöhnlich mit Hilfe spezieller höherer Protokolle wie POP3, SMTP oder NNTP¹⁵ übermittelt wurden.

Browsermeldungen

Es ist allgemein bekannt, dass etwa die Zeichenfolge "<http://www.website.org/index.htm>" soviel bedeutet wie: "Zeige mir unter Verwendung des HTTP-Protokolls die Seite namens 'index.htm' auf dem Server 'www.website.org". Nun könnte man denken, dass nur die IP-Adresse des Surfers und die Datei, die er sehen möchte, der Website übermittelt wird. Dies ist jedoch nicht der Fall.

In der folgenden Tabelle sind einige Daten aufgelistet, die bei einer HTTP-Anfrage (Automatische Browsermeldungen) im HTTP-Vorspann systematisch übermittelt werden und somit dem Server zugänglich sind:

<i>HTTP- Variablen</i>	<i>Opera 3.50</i>	<i>Netscape 4.0 Fr</i>	<i>Microsoft- Explorer 4.0 UK</i>
GET	GET /index.html HTTP/1.0	GET /index.html HTTP/1.0	GET /index.html HTTP/1.0
User-Agent:	Mozilla/4.0 (compatible; Opera/3.0; Windows 95) 3.50	Mozilla/4.04 [fr] (Win95; I ;Nav)	Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)
Accept :	image/gif, image/x- xbitmap, image/jpeg, /	image/gif, image/x-xbitmap, image/jpeg	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/msword, application/vnd.ms- powerpoint, /
Referer :		Where.were.you/doc.htm	Where.were.you/doc.htm
Language :		fr	fr-be

Die technische Definition dieser Felder lässt sich im Standard RFC 1945 für HTTP 1.0 oder RFC 2068 für HTTP 1.1 nachschlagen. Diesbezüglich sind folgende Anmerkungen zu machen:

- GET: Allein die erste Zeile ist unerlässlich.
- User-Agent: In dieser Zeile gibt jeder Browser bekannt, dass der Internet-Nutzer Windows 95 verwendet. Man könnte sich fragen, warum. Netscape fügt hinzu, dass der Browser eine französische Version ist. Jeder Browser gibt seinen eigenen Namen, seine Versions- und Unterversions-Identifikation an.

¹⁵ Siehe DINANT, Jean-Marc, Law and Technology Convergence in the Data Protection Field? *Electronic threats to personal data and electronic data protection on the Internet*, ESPRIT-Projekt 27028, Electronic Commerce Legal Issues Platform.

- Accept: Bei der Angabe der akzeptierten Formate unterrichtet der Microsoft-Explorer jede Website, dass auf dem Computer des Internet-Nutzers die Anwenderprogramme Powerpoint, Excel und Word installiert sind.
- Referer: Opera lässt nicht die Dokumentenseite erkennen, über die der Internet-Nutzer weiterverwiesen wurde (Referenzseite).
- Language: Opera gibt die verwendete Sprache nicht bekannt. Netscape gibt bekannt, dass der Nutzer Französisch verwendet. Der Microsoft-Internet-Explorer teilt mit, dass der Internet-Nutzer aus Belgien stammt und Französisch verwendet.

Unsichtbare Hyperlinks

Hyperlinks sind der Mehrwert des Internets. Sie gestatten mit einem einzigen Mausklick das Blättern von einem Kontinent zum anderen. Was den normalen Nutzern verborgen bleibt, ist die Möglichkeit der üblichen Browser-Software, die HTTP-Anfrage zum Herunterladen von Bildern in den *HTML*-Seitencode aufzunehmen. Solche Bilder müssen nicht auf demselben Server abgelegt sein, der die ursprüngliche Anfrage nach einer bestimmten Dokumentenseite erhalten hat.

In diesem Falle enthält die HTTP-Variable "Referer" den Hinweis auf die Dokumentenseite, über die der Internet-Nutzer weiterverwiesen wurde ("Referenzseite"), das heißt, die Hauptseite, auf der die Bilder abgelegt werden. Mit anderen Worten: Wenn eine Website auf ihrer Dokumentenseite im *HTML*-Format eine unsichtbare Verknüpfung zu einem Bild enthält, das sich auf der Website eines Online-Handelsunternehmens befindet, erkennt letztere die "Referenzseite", bevor sie ihre Werbeeinblendung (*banner*) verschickt. Bei einer Suche vermittelt eine Suchmaschine enthält der Name der Dokumentenseite die eingegebenen Stichwörter.

Cookies

Cookies sind Datensequenzen, die in Textdateien abgelegt und auf der Festplatte des Internet-Nutzers gespeichert werden können, während eine Kopie davon auf der Website verbleiben kann. Sie sind eine regulärer Bestandteil des HTTP-Verkehrs und können als solche ungehindert im IP-Verkehr mitgeführt werden.

Cookies befinden sich auf der Festplatte des Internet-Nutzers und enthalten Informationen über ihn, die von der Website, die sie dort abgelegt hat, oder jedem anderen, der das Datenformat dieser Website kennt, wieder ausgelesen werden können. *Cookies* können alle Informationen enthalten, die eine Website darin aufnehmen möchte: besuchte Seiten, angeklickte Werbespots, Kennnummer des Nutzers usw.¹⁶ In manchen Fällen können sie sinnvoll sein, um einen bestimmten Dienst über Internet liefern zu können oder den Nutzern das Surfen im Internet zu erleichtern. So stützen sich etwa bestimmte Kunden-Websites auf *Cookies*, um ihre Besucher bei jeder Wiederholung des Kontakts zu identifizieren und ihnen damit zu ersparen, sich bei jeder Durchsicht des neu eingegangenen Materials bei der Website erneut anmelden zu müssen.

Das SET-COOKIE wird in die HTTP-Antwortzeile platziert¹⁷, und zwar in unsichtbare *Hyperlinks*. Falls es von Dauer sein soll¹⁸, wird das *Cookie* auf der Festplatte des Internet-Nutzers gespeichert und während dieser Dauer an die Website zurückgeschickt, die das *Cookie* erzeugt hat (oder an andere Websites

¹⁶ Siehe HAGEL III, J. und SINGER, M., *Net Worth: the emerging role of the infomediary in the race for customer information*, Harvard Business School Press, 1999, p. 275.

¹⁷ Technisch gesehen lassen sich *Cookies* auch in JavaScript oder in die HTML-Zeilen im Bereich <META-HTTP EQUIV> einfügen.

¹⁸ *Cookies* ohne festgelegte Dauer werden "Session *Cookies*" genannt; sie verschwinden wieder, wenn der Browser oder die Anwendung abgeschaltet wird.

desselben Unterbereichs). Diese Rückmeldung nimmt die Form eines COOKIE-Felds in den automatischen Browsermeldungen an (siehe Schema weiter oben).

Werden Browsermeldungen und die unsichtbaren *Hyperlinks* miteinander verknüpft, kann ein Online-Unternehmen automatisch alle Stichwörter ablesen, die ein Internet-Nutzer in eine Suchmaschine eingegeben hat, auf der dieses Unternehmen Werbung betreibt, ferner Computertyp, Betriebssystem, Browsermarke des Internet-Nutzers, seine IP-Adresse sowie Zeit und Dauer der HTTP-Sitzung. Mit solchen Rohdaten können durch Kombination mit anderen Daten, die dem Unternehmen zugänglich sind, einige weitere Daten erschlossen werden wie etwa¹⁹:

1. Land, in dem sich der Internet-Nutzer befindet;
2. Internet-Bereich, zu dem er gehört;
3. Tätigkeitsbereich des Unternehmens, das den Internet-Nutzer beschäftigt;
4. Umsatz und Größe dieses Unternehmens;
5. Funktion und Stellung des Nutzers innerhalb dieses Unternehmens;
6. Internet-Zugangsanbieter;
7. Art der gewöhnlich besuchten Websites.

Ein *Cookie* gestattet den systematischen Versand einer bleibenden und einmaligen Kennung bei jeder Informationsabfrage, wogegen die IP-Adresse ein relativ unwirksames Identifizierungszeichen ist, da sie durch *Proxy-Server* unkenntlich gemacht werden kann und wegen ihres dynamischen Charakters bei Nutzern, die das Internet über ein *Modem* erreichen, nicht zuverlässig ist. Viele Online-Unternehmen haben bereits unsichtbare Merkmalsprofile erstellt²⁰.

Gefahren für die Privatsphäre im Zusammenhang mit der Implementierung des HTTP-Protokolls in den marktgängigen Browsern

Die Kombination von Browsermeldungen, unsichtbaren *Hyperlinks* und *Cookies* gibt die Möglichkeit an die Hand, von allen Internet-Nutzern, die ihren Browser so verwenden, wie er automatisch installiert wurde, unsichtbare Merkmalsprofile zu erstellen. Diese Erstellung "an sich" ist nicht im HTTP-Protokoll verankert, wie es vom World Wide Web Consortium (W3C) festgelegt wurde²¹. Vielmehr wurde bei der Definition des HTTP 1.1-Protokolls die Wirtschaft ausdrücklich auf Probleme im Zusammenhang mit dem Schutz der Privatsphäre bei der Implementierung des HTTP-Protokolls hingewiesen²²:

- *"Das Medium des Nutzers zu veranlassen, bei jeder Anfrage seine Systemanforderungen zu melden, kann sowohl sehr ineffizient sein (da nur ein geringer Prozentsatz der Antworten*

¹⁹ GAUTHRONET, Serge, "On-line services and data protection and the protection of privacy", Europäische Kommission, 1998, pp. 31 und 92, abrufbar unter:
<http://europa.eu.int/comm/dg15/en/media/dataprot/studies/servint.htm>

²⁰ Allein die Firma DoubleClick erklärte im März 1997, dass sie in weniger als einem Jahr mehr als eine Milliarde Werbebanner an ca. 26 Millionen Internet-Nutzer versandt habe (GAUTHRONET, op. cit., p. 84), und mehr als 100 Millionen ihrer Werbebanner jeden Monat außerhalb der USA angeklickt werden (ibid., p. 94). Derzeit werden für ein einziges Internet-Unternehmen täglich mehr als 500.000 Werbebanner versandt. Siehe
http://www.doubleclick.net/company_info/investor_relations/financials/analyst_metrics.htm

²¹ Das World Wide Web Consortium ist eine Organisation ohne Erwerbscharakter, die in den Einrichtungen Inria (Frankreich), MIT (USA) und Universität von Keio (Japan) untergebracht ist. Mitglieder dieses Konsortiums sind insbesondere Microsoft, AOL, Netscape, und das Center for Democracy and Technology (<http://www.w3.org/Consortium/Member/List>). W3C stellt unverbindliche, *de facto* aber doch obligatorische Normen auf, die die Zusammenarbeit der Computer im Internet gewährleisten sollen.

²² <http://www.w3.org/Protocols/rfc2068/rfc2068>. Die Zahlenangaben in Klammern beziehen sich auf die Nummerierung von W3C.

mehrere Darstellungsmöglichkeiten aufweist) als auch zu einer potentiellen Verletzung der Privatsphäre des Nutzers führen" [Seite 68]

- *"Es kann der Erwartung der Nutzer bezüglich der Gewährleistung ihrer Privatsphäre zuwiderlaufen, den Header 'Accept-Language' mit sämtlichen Sprachpräferenzen des Nutzers in jeder einzelnen Anfrage zu senden" [Seite 98]*
- *"Der Client-Computer sollte ohne Einwilligung des Nutzers den Inhalt des Headers 'From'²³ nicht senden, da dies dem Interesse des Nutzers an seiner Privatsphäre oder seinen Sicherheitsmaßnahmen zuwiderlaufen kann. Es wird nachdrücklich empfohlen, dem Nutzer die Möglichkeit zu geben, jederzeit vor einer Anfrage den Wert dieses Feldes zu deaktivieren, zu aktivieren oder zu ändern." [Seite 118]*
- *"HTTP-Client-Computer enthalten häufig umfangreiche Bestände an personenbezogenen Informationen (z.B. Name, Standort, E-Mail-Adresse, Passwörter, Verschlüsselungen usw. des Nutzers) und müssen sehr sorgfältig bewacht werden, damit über das HTTP-Protokoll kein unbeabsichtigter Abfluss dieser Informationen zu anderen Quellen erfolgt. Wir empfehlen nachdrücklich, den Nutzern ein geeignetes Interface zur Verfügung zu stellen, mit dem sie die Verbreitung solcher Informationen kontrollieren können, und den Entwicklern und Implementierern von Programmen, in diesem Bereich besonders sorgfältig zu sein. Die Erfahrungen zeigen, dass Irrtümer in diesem Bereich häufig ernste Probleme für Sicherheit und Privatsphäre zur Folge haben und äußerst nachteilige Publicity für die Firmen der Implementierer." [Seite 143]²⁴*

V. Einige wirtschaftliche Überlegungen

Das Internet hat in den vergangenen Jahren einen außerordentlichen Zuwachs erlebt. Die Anzahl der "Host"-Computer, also solche, die Informationen speichern und Mitteilungen übertragen, nahm von ca. 300 im Jahre 1981 auf etwa 9,4 Millionen im Jahre 1996 zu. Grob 60 Prozent dieser "Host" befinden sich in den Vereinigten Staaten. 1996 nutzten ca. 40 Millionen Menschen das Internet und man geht davon aus, dass es bis zum Jahre 2000 ca. 200 Millionen Teilnehmer sein werden²⁵. Voraussichtlich wird bis zum Jahre 2005 die Hälfte der europäischen Bevölkerung Anschluss ans Internet haben²⁶.

In vielen europäischen Staaten ist die Teilnahme am Internet für Einzelpersonen gratis, doch müssen die Teilnehmer die Telefongebühren bezahlen. Die IAP oder ISP erhalten von den Fernmeldebetreibern Entgelte entsprechend der Dauer des Ortsgesprächs des Internet-Teilnehmers. Das heißt, selbst in den Fällen, in denen die Nutzer freien Zugang zum Internet haben, müssen sie doch die Kosten für die Telefongebühren tragen. Davon profitieren sowohl der IAP/ISP als auch der Fernmeldebetreiber.

Softwarehersteller profitieren ebenfalls von der Nutzung des Internets, denn selbst wenn sie den Verbrauchern ihre Produkte kostenlos zur Verfügung stellen (Freeware, Browser usw.), erhalten sie doch von den Website-Servern Entgelte für die Verwendung ihrer Software.

Eine der einträglichsten Aktivitäten im Netz ist das Direkt-Marketing. Online-Handelsunternehmen platzieren Werbeeinblendungen auf den Dokumentenseiten, häufig auf eine Weise, dass die Erhebung von personenbezogenen Daten für die Nutzer weitgehend unsichtbar bleibt. Mit Hilfe von unsichtbaren Verknüpfungen in Verbindung mit den Browsermeldungen und den *Cookies* können unbekannte

²³ Das Feld "From Header" wird verwendet, um die Referenzseite zu nennen.

²⁴ Das Wort "privacy" (Privatsphäre) kommt in RFC 2068 achtzehn Mal vor.

²⁵ Siehe Entscheidung Reno versus ACLU (26. Juni 1997).

²⁶ Pressemitteilung der Europäischen Kommission, *Kommission begrüßt den neuen Rechtsrahmen zur Gewährleistung der Sicherheit von elektronischen Signaturen*, 30. November 1999.

Handelsunternehmen Merkmalsprofile von jedem einzelnen Internet-Nutzer erstellen. Ein einziges Online-Unternehmen könnte so täglich eine halbe Milliarde personenbezogener Werbeeinblendungen in das Web senden. Direkt-Marketing-Unternehmen finanzieren viele Suchmaschinen.

Über unsichtbare *Hyperlinks* auf ihren eigenen Dokumentenseiten, die zu Online-Unternehmen führen, beauftragen gewöhnliche Websites (und vor allem Suchmaschinen) weitverbreitete Browser wie Netscape und Internet Explorer, zu einem HTTP-Server des Online- Unternehmens eine eigene HTTP-Verbindung herzustellen. Bei der Ausführung der HTTP-Anfrage wird der Browser, wie weiter oben dargestellt, automatisch verschiedene Daten "ausplaudern", insbesondere die IP-Adresse, die Referenzseite (im Falle einer Suchmaschine enthält diese Variable die vom Sucher eingegebenen Stichwörter), die Marke, Version und Sprache des verwendeten Browsers (z.B. Internet Explorer 4.02, Niederländisch), das verwendete Betriebssystem (Windows 2000, Linux 2.2.5, Mac OS 8.6 usw.) und schließlich das die Identität bekanntgebende *Cookie* (z.B. UserId=342ER432), das von dem Online-Unternehmen mittels früherer unsichtbarer *Hyperlinks* möglicherweise bereits platziert ist.

Dem gewöhnlichen Internet-Nutzer ist im allgemeinen nicht bekannt, dass die Einblendungen, die er nach dem Eingeben der Zieladresse (URL – Unified Resource Locator) sieht, nicht von der Website stammen, die er gerade besucht. Auch merken die Nutzer nicht, dass ihr Browser beim Herunterladen eines *Werbemanners* systematisch eine einmalige Kennung, die IP-Adresse und die vollständige URL der Dokumentenseite übermittelt, die sie gerade besuchen (dazu gehören auch die Stichwörter, die Nutzer in Suchmaschinen eingeben, und der Name der Presseartikel, die sie Online lesen). Alle diese Daten können aufgrund der in einem *Cookie* gespeicherten einmaligen Kennung zusammen gestellt werden, um ein globales Profil eines einzelnen Teilnehmers zu erstellen, der von einer Website zu nächsten surft.

Die Erhebung von Informationen über Nutzer in Online-Umgebungen wird aus wirtschaftlichen und strategischen Gründen für sehr wichtig gehalten. Das folgende Zitat aus einer bekannten amerikanischen Zeitschrift²⁷ illustriert diese Überlegung: *Zu viele Firmen, die im Internet vertreten sind, darunter auch führende Spitzenunternehmen, beachten nicht ausreichend den Wert von Verbraucherprofilen. Wer die Rechte über die Online-Verbraucherprofile hält, entscheidet darüber, wer Gewinner oder Verlierer in dieser neuen Ära sein wird.*

Es ist erwähnenswert, dass die Sammlung von Daten über die Internet-Nutzer für ein Unternehmen gewöhnlich völlig kostenfrei ist, da die Verbraucher häufig selbst die Informationen liefern, z.B. beim Ausfüllen von Formularen. Websites nutzen häufig sogenannte Loyalty-Programme wie etwa Spiele, Fragebogen, Newsletters, bei denen die Besucher der jeweiligen Website Auskunft über personenbezogene Daten geben.

Neuere Fälle bestätigen den zunehmenden Wert, den die Wirtschaft Verbraucherprofilen beimisst. Verzeichnisse werden verkauft oder ausgetauscht, meistens über Versteigerungen der IT-Unternehmen, die auf diese Weise die Details und die Anzahl der Profile, die sie nutzen können, vermehren.

Es wird möglicherweise Erwerbungen auf der Grundlage der Daten über die Verbraucher geben, bei denen also der vorrangige Unternehmenswert, der aufgekauft wird, die Verbraucherdaten sind. (...) Verbraucherdaten sind auf vielfältige Weise geradezu die Währung des elektronischen Handels. Es geht um Verbraucher, die wertvoll sind, weil sie gezeigt haben, dass sie Käufer sind und dass sie bei einer konkurrierenden Firma eingekauft haben. (...) Namen in einer Datenbank ersparen den Unternehmen die Marketing-Ausgaben für den Erwerb eines Kunden - gewöhnlich ca. hundert Dollar pro Kunde²⁸.

²⁷ Siehe "Net Worth" (op cit), Seite xiii (Vorwort).

²⁸ Zitiert aus M. HALPERN und HARMON, "E-mergers trigger privacy worries" von Deborah KONG, <http://www.mercurycenter.com/svtech/news/indepth/docs/consum012400.htm>

Verbraucherdaten wurden auch bei Zusammenbrüchen von Internet-Unternehmen zum Verkauf angeboten. Vor kurzem hat ein Spielwarenhändler den Verkauf seiner Verbraucherprofile als Teil des Liquidationswerts seines Unternehmens betrieben. Solche Verbraucherprofile wurden allerdings von den Nutzern unter der Bedingung eingeholt, dass ohne die ausdrückliche Einwilligung der Nutzer die Informationen über sie nicht an Dritte weitergegeben werden dürfen. Die Profile enthalten Namen, Adresse, Informationen über die Rechnungen und das Einkaufsverhalten sowie Familienprofile mit den Namen und Geburtsdaten der Kinder.

Die Firma TRUSTe, die die Bedingungen jener Firma bezüglich der Privatsphäre genehmigt hatte, gab am 8. August 2000 bekannt, dass sie beim Konkursgerichtshof der Vereinigten Staaten (United States Bankruptcy Court) Einspruch gegen die Vereinbarung der US-Handelskommission (FTC) mit jenem Unternehmen bezüglich der Bedingungen der Liquidation der Unternehmenswerte eingelegt habe²⁹.

Eine umfassende Datenschutzpolitik muss eine ausgewogene Wahl zwischen den Wirtschaftsinteressen und den Menschenrechten treffen. Zwei wichtige Fragen sind dabei noch nicht geklärt:

Bislang sind im Internet beträchtliche Mengen an Einzeldaten über viele Internet-Nutzer ohne deren vorherige Kenntnis oder Einwilligung gesammelt worden, insbesondere dank der unsichtbaren Nebeneffekte der Internet-Technologie. Es lässt sich voraussehen, dass in den kommenden Jahren personenbezogene Daten immer häufiger gegen materiellen Gewinn getauscht werden³⁰. Aber wie weit können Internet-Nutzer dabei gehen? Welche Art von personenbezogenen Daten kann von den Dateninhabern selbst mitgeteilt werden, für welchen Zeitraum und unter welchen Umständen?

Wenn die Finanzierung bestimmter Websites (zum Beispiel von Suchmaschinen) vorwiegend durch die Online-Wirtschaft erfolgt, ist die Versuchung groß, dass mit Hilfe der personenbezogenen Profilerstellung Dienstleistungen, die bislang gratis waren, Personen vorenthalten werden, die entweder nicht genügend Einkünfte haben oder auf Hunderte von vorher versandten Werbeeinblendungen nicht reagiert haben oder aber einfach ihre Privatsphäre erhalten wollen.

VI. Zusammenfassung

- Das Internet wurde als offenes Netzwerk für den Austausch von Informationen in weltweitem Maßstab (www) konzipiert. Es muss aber ein Gleichgewicht zwischen der "Offenheit" des Internets und dem Schutz der personenbezogenen Daten der Internet-Nutzer hergestellt werden.
- Im Internet werden gewaltige Datenmengen über die Internet-Nutzer gesammelt, häufig ohne dass sie davon erfahren. Dieser Mangel an Transparenz gegenüber den Internet-Nutzern muss behoben werden, um ein gutes Schutzniveau für die personenbezogenen Daten und die Verbraucher zu erreichen.
- Protokolle sind technische Mittel, mit denen festgelegt wird, wie Daten erhoben und verarbeitet werden. Browser und Software-Programme spielen ebenfalls eine wichtige Rolle. In manchen Fällen enthalten sie ein Identifizierprogramm, das eine Verbindung zwischen Internet-Nutzern und ihren Aktivitäten im Internet herstellen kann. Deshalb ist es Pflicht derjenigen, die solche Programme konzipieren und entwickeln, Produkte herzustellen, die den Schutz der Privatsphäre der Nutzer gewährleisten. In diesem Zusammenhang ist der Hinweis auf Artikel 14 des Entwurfs der Telekommunikations-Richtlinie vom 12. Juli 2000 wichtig, in dem es heißt, dass die Kommission erforderlichenfalls Maßnahmen trifft, um sicherzustellen, dass Endgeräte mit allen Sicherheitsfunktionen ausgestattet sind, die notwendig sind, um den Schutz personenbezogener Daten und der Privatsphäre zu gewährleisten.

²⁹ http://www.truste.org/users/users_investigations.html

³⁰ Siehe beispielsweise Erörterung der Informationsmittler in Kapitel 9.

KAPITEL 3: ANWENDUNG DER DATENSCHUTZVORSCHRIFTEN

I. Allgemeine rechtliche Überlegungen

Die rechtliche Beurteilung, die in den folgenden Kapiteln durchgeführt wird, muss vom Sachverhalt ausgehen, dass beide Datenschutz-Richtlinien (Richtlinien 95/46/EG und 97/66/EG) im Prinzip für personenbezogene Daten gelten, die im Internet verarbeitet werden³¹.

Alle rechtlichen Beurteilungen in diesem Dokument beruhen auf der Auslegung dieser beiden Richtlinien und der von der Arbeitsgruppe angenommenen Dokumente sowie in einigen (gekennzeichneten) Fällen auf der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte.

Personenbezogene Daten im Internet

Wie in diesem Arbeitspapier bereits erwähnt wurde, können Internet-Zugangsanbieter und Verwalter von lokalen Netzwerken ohne großen Aufwand Internet-Nutzer identifizieren, denen sie IP-Adressen zugewiesen haben, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internet-Nutzer zugeteilte dynamische IP-Adresse einfügen. Dasselbe lässt sich von den *Internet-Dienstanbietern* sagen, die in ihren HTTP-Servern Protokolle führen. In diesen Fällen besteht kein Zweifel, dass man von personenbezogenen Daten im Sinne von Artikel 2 Buchstabe a) der Richtlinie 95/46/EG reden kann³².

In anderen Fällen können Dritte zwar die dynamische IP-Adresse eines Nutzers erfahren, sind aber nicht in der Lage, sie mit anderen Daten bezüglich dieser Person so zu verknüpfen, dass sie identifiziert werden könnte. Es liegt also auf der Hand, dass solche Internet-Nutzer leichter identifiziert werden können, die eine statische IP-Adresse verwenden.

Dennoch besteht in vielen Fällen die Möglichkeit, die IP-Adresse von Nutzern mit anderen personenbezogenen Daten (egal, ob öffentlich zugänglich oder nicht) so zu verknüpfen, dass sie identifiziert werden können, insbesondere dann, wenn jemand unsichtbare Verarbeitungsverfahren zur Erhebung von zusätzlichen Daten über die Nutzer verwendet (etwa *Cookies*, die eine einmalige Kennung enthalten, oder aber moderne Datenerschließungsmethoden (*datamining*) in Verbindung mit großen Datenbanken, die personenbezogene Daten über Internet-Nutzer enthalten.

Selbst wenn also nicht in allen Fällen und nicht von allen Internet-Akteuren ein Nutzer aufgrund der im Internet verarbeiteten Daten ermittelt werden kann, wird in diesem Arbeitspapier davon ausgegangen, dass in vielen Fällen die Möglichkeit zur Erkennung der Internet-Nutzer gegeben ist, also große Mengen von personenbezogenen Daten im Internet verarbeitet werden, für welche die Datenschutzrichtlinien gelten.

Anwendung der Richtlinien

Wie die Arbeitsgruppe bereits bei früheren Gelegenheiten festgestellt hat, gilt die allgemeine Datenschutzrichtlinie 95/46/EG innerhalb ihres Geltungsbereichs für jegliche Verarbeitung von personenbezogenen Daten, unabhängig von den verwendeten technischen Verfahren. Die Verarbeitung von personenbezogenen Daten im Internet muss also im Lichte dieser Richtlinie betrachtet werden³³. Die

³¹ Siehe Arbeitsdokument WP 16: *Verarbeitung personenbezogener Daten im Internet*, von der Arbeitsgruppe am 23. Februar 1999 angenommen, 5013/99/EN/final.

³² Siehe auch Erwägungsgrund 26 in der Begründung der Richtlinie.

³³ Mit dem Ausdruck "die Richtlinie" soll in diesem Papier immer Richtlinie 95/46/EG verstanden werden.

allgemeine Richtlinie gilt also für alle Fälle und alle unterschiedlichen Beteiligten, die im ersten Abschnitt dieses Kapitels (technische Beschreibung) behandelt wurden.

Die **besondere** Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation spezifiziert und ergänzt die **allgemeine** Richtlinie 95/46/EG durch Festlegung der besonderen rechtlichen und technischen Vorschriften. Richtlinie 97/66/EG gilt für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste in öffentlichen Telekommunikationsnetzen der Gemeinschaft. Internet-Dienste sind Telekommunikationsdienste. Deshalb ist das Internet Teil des öffentlichen Telekommunikationsbereichs.

Für alle Fälle, die nicht ausdrücklich von der Richtlinie 97/66/EG erfasst sind, etwa die Pflichten der für die Datenverarbeitung Verantwortlichen und die Rechte von Einzelpersonen oder die nicht öffentlichen Telekommunikationsdienste, gilt Richtlinie 95/46/EG³⁴. Personenbezogene Daten, die von den Internet-Nutzern während ihrer Verbindung mit dem Internet aus freien Stücken preisgegeben werden, fallen immer unter diese Richtlinie.

In der folgenden Tabelle wird versucht, zu systematisieren, welche Fälle unter die besondere Richtlinie 97/66/EG fallen, und gegebenenfalls die wichtigsten einschlägigen Grundsätze zu nennen. Dabei ist allerdings zu berücksichtigen, dass sich Überschneidungen ergeben, wenn Betreiber unterschiedliche Aufgaben parallel wahrnehmen.

³⁴ Siehe Erwägungsgrund 11 der Richtlinie 97/66/EG.

Betreiber	Aufgabe	Mögliche Verarbeitung personen-bezogener Daten	Einschlägige Bestimmungen der Telekom-Richtlinie
<i>Telekommunikations-Anbieter</i> (z.B. AT&T)	Herstellung der Verbindung zwischen Internet-Nutzern und <i>ISP</i>	Protokollierung der Verbindungen Internet-Nutzer/ <i>ISP</i> Übermittlung der Anruferkennung des Internet-Nutzers an den <i>ISP</i>	Telekommunikations-Richtlinie, insbesondere: Vertraulichkeit der Kommunikation, der Verkehrsdaten und der Daten für die Gebührenabrechnung, Anzeige bzw. Unterdrückung der Rufnummer und des Anschlusses
<i>Internet-Diensteanbieter</i> ³⁵ (z.B. World Online)	Liefert den angeforderten Internet-Dienst Übermittelt Anfrage des Internet-Nutzers an <i>Proxy-Server</i> (Cache) Übermittelt Anfrage des Internet-Nutzers an Website Übermittelt Antwort des <i>Proxy-Servers</i> an Internet-Nutzer Übermittelt Antwort der Website an Internet-Nutzer	Protokollierung der eintreffenden Anruferkennung (CLI) Zuweisung einer IP-Adresse zu einer "Sitzung" ("session") Möglichkeit der Speicherung von Verzeichnissen über besuchte Websites, nach IP-Adressen sortiert Datenaustausch mit angeforderten Websites Protokollierung der "Sitzungen" (Zeitpunkt der Anmeldung und Abmeldung und Menge der übertragenen Daten) Entnahme von Informationen aus dem Header und den Inhalten.	Telekommunikations-Richtlinie, insbesondere: Vertraulichkeit der Kommunikation, der Verkehrsdaten und der Daten für die Gebührenabrechnung
<i>Portal-Dienste</i> (z.B. Yahoo, AOL, Macropolis)	Auswahl aus Informationsangebot Angebot an Informationen (Inhalte-Anbieter) und zuweilen an Dienstleistungen oder Waren	Protokollierung der Anforderung von Websites hinter den <i>Portalen</i> Mögliche Protokollierung der Besuche der Websites Protokollierung der Referenzseiten und der eingegebenen Stichwörter (chattering data) Platzierung von <i>Cookies</i> auf der Festplatte des Internet-Nutzers Profilerstellung	Telekommunikations-Richtlinie (auf <i>ISP</i> anwendbar, die <i>Portale</i> anbieten)
Gewöhnliche Website/Homepage (z.B. www.coe.int)	Angebot an Informationen (Inhalte-Anbieter) und zuweilen an Dienstleistungen oder Waren	Mögliche Protokollierung der Besuche bei der Website Protokollierung der Referenzseiten und der eingegebenen Stichwörter (chattering data) Platzierung von <i>Cookies</i> auf der Festplatte des Internet-Nutzers Profilerstellung	
Anbieter zusätzlicher Dienste (z.B. Nedstat, DoubleClick, Banners)	Anpassung von Dokumentenseiten an Kundenwünsche	Profilerstellung (durch Zusammenstellung des <i>clickstream</i> verschiedener Websites)	Sind nicht in allen Fällen Telekommunikationsdienste. Deshalb gilt die Telekommunikations-Richtlinie nur für manche Fälle.

³⁵ Im Prinzip umfasst der Ausdruck *Internet-Diensteanbieter*, so wie er in diesem Arbeitsdokument verwendet wird, auch die Internet-Zugangsanbieter (siehe Definition im Glossar der Fachausdrücke). Hier ist von Internet-Zugangsanbietern nur dann die Rede, wenn Aspekte behandelt werden, die ausschließlich auf sie zutreffen.

Anbieter von <i>Routern</i> und Leitungen (häufig im Besitz der Telekommunikationsbetreiber)	Verknüpfung von <i>ISP</i> untereinander	Weiterleitung von Daten des Internet-Nutzers an die IP-Website Gefahr des unberechtigten Zugriffs	Telekommunikations-Richtlinie, insbesondere Sicherheit und Vertraulichkeit der Kommunikation
--	--	--	--

Ob beide Richtlinien Anwendung finden, hängt entscheidend davon ab, ob der fragliche Dienst als "Telekommunikationsdienst" betrachtet werden kann, wie er in Richtlinie 97/66/EG, Artikel 2 Buchstabe d) definiert ist: *Übertragung und Weiterleitung von Signalen über das Telekommunikationsnetz.*

Wenn die besondere Telekom-Richtlinie anwendbar ist, sind auch die in ihrer enthaltenen besonderen Vorschriften einzuhalten.

Telekommunikations-Anbieter

Ohne Zweifel handelt es sich bei der Herstellung von Verbindungen zwischen den Internet-Nutzern und den *ISP*, beim Angebot von Internet-Dienstleistungen an Internet-Nutzer und bei der Weiterleitung von Anfragen und Antworten der Internet-Nutzer an Website-Server und umgekehrt um Telekommunikationsdienste. Richtlinie 97/66/EG gilt also für Telekommunikations-Anbieter, Internet-Diensteanbieter und Anbieter von *Routern* und Leitungen für den Internet-Verkehr.

Internet-Diensteanbieter (einschließlich der Zugangsanbieter)

Dasselbe kann von den *Internet-Diensteanbietern* gesagt werden; es besteht kein Zweifel, dass für ihre Tätigkeiten die spezifische Telekommunikations-Richtlinie gilt.

Ein interessanter Fall sind die Einrichtungen oder Personen, die direkten Zugang zum Internet ohne Vermittlung eines *ISP* haben. Diese Gruppe operiert tatsächlich als Internet-Diensteanbieter, indem sie ihr eigenes privates Netzwerk mit dem Internet verbindet.

Der Geltungsbereich der Richtlinie 97/66/EG ist in Artikel 3 definiert und gilt für öffentlich zugängliche Telekommunikationsdienste in öffentlichen Telekommunikationsnetzen in der Gemeinschaft. In den vorgenannten Fällen besteht kein öffentlich zugängliches Netzwerk, sondern ein privates Netz für eine bestimmte Benutzergruppe. Es kann deshalb gefolgert werden, dass diese Dienste zwar unter die Definition der Telekommunikationsdienste fallen, aber nicht als öffentlich zugängliche Dienste zu betrachten sind und somit nicht unter die Richtlinie 97/66/EG fallen.

Allerdings ist darauf hinzuweisen, dass die Bestimmungen dieser besonderen Richtlinie wieder gelten, sobald Informationen an Adressaten außerhalb des privaten Netzwerks versandt werden.

Die Bestimmungen der allgemeinen Datenschutzrichtlinie gelten selbstverständlich ohne Abstriche auch für diese Fälle.

Gewöhnliche Websites

In der Regel werden Websites bei einem *ISP* aufbewahrt. Dies bedeutet, dass der für eine Website (etwa diejenige des Europäischen Rats) Zuständige bei einem *ISP* Speicherkapazitäten mietet, um dort die Website zu platzieren und zugänglich zu machen. Ferner bedeutet dies, dass der *ISP* im Auftrage des Europäischen Rats die Nachfrage von Internet-Nutzern nach Dokumentenseiten beantwortet.

Folglich entscheidet derjenige, der eine Website "betreibt" (in diesem Fall also der Europäische Rat) lediglich, welche Informationen auf einer Website zugänglich gemacht werden, führt aber selbst keinerlei Operationen aus, die mit der *Übertragung und Weiterleitung von Signalen über das Telekommunikationsnetz* zu tun haben.

Wenn über eine Website Waren oder Dienstleistungen geordert werden können, muss der für diese Seite Verantwortliche die Dienstleistungen/Waren liefern. Die reinen Telekommunikationsdienste werden in der Regel nicht von dem für die Website Verantwortlichen, sondern vom *ISP* bereitgestellt.

Es lässt sich also sagen, dass Websites Teilnehmer an den Telekommunikationsdiensten (Übertragung) des die Websites beherbergenden *ISP* sind, aber diese Dienste nicht selbst ausführen. Die besondere Richtlinie 97/66/EG gilt also für *ISP* als solche, nicht aber für die Websites, die der allgemeinen Richtlinie unterliegen.

Portal-Dienste

Portal-Websites bieten in geordneter Form einen Überblick über die Web-Verknüpfungen. Über das besuchte *Portal* im Internet kann der Nutzer leicht ausgewählte Websites anderer Anbieter von Inhalten besuchen.

Portal-Sites werden bei *ISP* geführt. In manchen Fällen gehören sie dem *ISP* (z.B. worldonline.nl), in anderen Fällen dagegen verwaltet der *ISP* die *Portal*-Website für Dritte, die die Inhalte liefern.

In beiden Fällen erbringt der *ISP* den Telekommunikationsdienst im Sinne von Artikel 2 der Richtlinie 97/66/EG, die für ihn, nicht für den Inhalte-Anbieter gilt.

Zusätzliche Dienste

Für Erbringer zusätzlicher Dienste gilt nicht in allen Fällen die Datenschutz- oder Telekommunikations-Richtlinie.

Manche dieser Diensteanbieter (etwa Nedstat) verarbeiten Daten, die sie auf Websites erheben, und verkaufen sie wieder an die Eigentümer der Websites. Die von ihnen verarbeiteten Daten stammen zwar aus dem Internet, aber ihre Tätigkeit besteht im Prinzip nicht aus der *Übertragung und Weiterleitung von Signalen über das Telekommunikationsnetz*. Sie spielen deshalb keine entscheidende Rolle im Kommunikationsprozess zwischen dem Internet-Nutzer und der Website. Wenn die von ihnen verarbeiteten Daten lediglich aus aggregierten, nicht identifizierbaren Daten bestehen, könnte sogar gesagt werden, dass sie nicht unter die allgemeine Richtlinie fallen, da keine personenbezogenen Daten im Spiel sind.

Unternehmen wie DoubleClick, Engage oder Globaltrash platzieren Werbeeinträge auf nachgefragten Seiten. In der Regel schließen solche Werbefirmen Verträge mit den *ISP*, die die Dokumentenseiten beherbergen, auf denen die Werbeeinblendungen platziert werden.

Zu diesem Zweck wird, technisch gesprochen, jedesmal, wenn eine Website angeklickt wird, der Kontakt zu einer Werbefirma (durch einen automatischen *Hyperlink*) hergestellt, so dass sie Werbeeinblendungen auf die abgefragten Seiten platzieren kann.

Zusätzlich kann sie *Cookie*-Dateien auf den Festplatten der Internet-Nutzer ablegen, um Profile der Besucher der Website zu erstellen, damit später auf den zugehörigen Dokumentenseiten kundenorientierte Werbeeinblendungen platziert werden können³⁶.

Es ist nicht klar, ob die Hauptaktivitäten von DoubleClick, Engage oder anderen Werbefirmen als Telekommunikationsdienst zu betrachten sind oder nicht. Anscheinend übertragen und leiten sie keine Signale gemäß Artikel 2 der Telekommunikations-Richtlinie weiter, sondern erbringen lediglich inhaltliche

³⁶ In "Net Worth" (op cit.) heißt es auf Seite 275: "Da *Cookies* auch verwendet werden können, um Surf-Gewohnheiten und Einstellungen zusammen zu fügen, werden sie immer häufiger benutzt, um Werbebotschaften auf einzelne Personen auszurichten. Tatsächlich sind DoubleClick, Globaltrash und ADSmart Beispiele für Unternehmen, die *Cookies* verwenden, um auf den dafür eingerichteten Websites Werbung zielgerichtet auf Verbraucher auszurichten".

Informationen, die auf den abgefragten Dokumentenseiten platziert werden, und machen dabei von der vorhandenen Telekommunikationsinfrastruktur und den Netzwerken Gebrauch.

Jedenfalls ist dies ein gutes Beispiel für eine Situation, bei der sich die gegebene Definition für Telekommunikationsdienstleistungen nur schwierig auf Internet-bezogene Dienste anwenden lässt.

II. Die Überprüfung der Telekommunikations-Richtlinie: die Definition der "elektronischen Kommunikationsdienste"

Die Europäische Kommission gab 1999 in einer Mitteilung³⁷ ihre Absicht bekannt, eine allgemeine Überprüfung des bestehenden Rechtsrahmens für Telekommunikation in Europa vorzunehmen. Im Zusammenhang mit dieser geplanten Überprüfung wird auch die vorhandene Richtlinie über die Verarbeitung von personenbezogenen Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation überarbeitet und aktualisiert.

In ihrer Stellungnahme 2/2000, die von der Task Force 'Internet' vorgelegt und am 3. Februar 2000³⁸ angenommen wurde, hat die Datenschutzgruppe bereits einige Gedanken zu dieser Überarbeitung vorgetragen.

In der Mitteilung der Europäischen Kommission wird unterstrichen, dass in der geplanten Überprüfung besondere Aufmerksamkeit der in Richtlinie 97/66/EG verwendeten Terminologie zukommen soll, damit deutlich wird, dass die neuen Dienste und Technologien unter diese Richtlinie fallen, und um Unsicherheiten zu vermeiden und eine kohärente Anwendung der Grundsätze des Datenschutzes zu erleichtern. Die Arbeitsgruppe begrüßt in ihrer Stellungnahme 2/2000 eine solche Überarbeitung der Terminologie zu diesem Zweck.

Die Kommission legte den Vorschlag für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation am 12. Juli 2000³⁹ vor. In ihrer Pressemitteilung⁴⁰ betont die Europäische Kommission, dass eines der Ziele dieses neuen Pakets die Gewährleistung des Schutzes der Privatsphäre im Internet sei.

In diesem Vorschlag wird nicht mehr von "Telekommunikationsdiensten", sondern von "elektronischen Kommunikationsdiensten" gesprochen. In der Begründung zu diesem Vorschlag wird erklärt, dass der Wechsel der Definition erforderlich sei, um die Terminologie mit der vorgeschlagenen Richtlinie für die Schaffung eines gemeinsamen Rahmens für elektronische Kommunikationsdienste und -netzwerke in Einklang zu bringen⁴¹.

Der Ausdruck "elektronische Kommunikationsdienste" wird nicht im Richtlinienvorschlag zum Thema Privatsphäre und Telekommunikation definiert, sondern in Artikel 2 Buchstabe b) der vorgeschlagenen Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste.

Darin heißt es wie folgt: *"Elektronische Kommunikationsdienste": gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung und Leitweglenkung von Signalen über elektronische Kommunikationsnetze bestehen. Hierzu gehören Telekommunikations- und*

³⁷ Dokument KOM (1999) 539 endg.

³⁸ Stellungnahme 2/2000 zur allgemeinen Überarbeitung des rechtlichen Rahmens für den Bereich der Telekommunikation, vorgelegt von der Task Force 'Internet', angenommen am 3. Februar 2000, WP 29, 5009/00/EN/final.

³⁹ Dokument KOM (2000) 385 endg.

⁴⁰ Kommission schlägt überarbeitete Vorschriften für elektronische Kommunikation vor, Brüssel, den 12. Juli 2000, IP/00/749.

⁴¹ KOM (2000) 393 endg.

Übertragungsdienste in Rundfunknetzen, nicht aber Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben.

Die neue Definition beruht tatsächlich wie die vorangegangene auf demselben Kerngedanken (Übertragung und Leitweglenkung von Signalen über elektronische Kommunikationsnetze), aber die Ergänzung um Beispiele für Dienste, die unter die Definition fallen bzw. nicht, ist sehr hilfreich, da sie Licht auf die Erörterungen im vorangegangenen Abschnitt wirft.

Aus diesen Beispielen geht hervor, dass die Anbieter von Inhalten, die unter Nutzung elektronischer Kommunikationsnetze und -dienste übermittelt werden, nicht in den Geltungsbereich der überarbeiteten Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation fallen. Dies wird in der Präambel zum Vorschlag für eine Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste bekräftigt, wo es in Erwägungsgrund 7 heißt: *Die Regulierung der Übertragung ist von der Regulierung von Inhalten zu trennen.* Allerdings sind bei der Trennung dennoch die Verbindungen zwischen beiden zu berücksichtigen.

Die wichtigste Konsequenz dieser Trennung besteht darin, dass Zusatzdienste wie etwa DoubleClick oder solche, die Inhalte für *Portale* oder Websites bereitstellen (letztere aber nicht selbst führen) nicht unter diese Richtlinie, sondern lediglich unter die allgemeine Richtlinie fallen. Dies bedeutet ferner, dass für *Internet-Diensteanbieter* diese besondere Richtlinie gilt, sofern sie als Zugangsanbieter fungieren und Verbindungen zum Internet herstellen, aber unter die allgemeine Richtlinie fallen, wenn sie als Anbieter von Inhalten tätig sind⁴².

Der Vorteil einer klaren Trennung zwischen der Regulierung von Inhalten einerseits und der Übertragung andererseits liegt in der dadurch geschaffenen Eindeutigkeit. Aber in der Praxis ist es schwieriger, mit einer solchen Trennung zu arbeiten; man denke etwa an einen Internet-Diensteanbieter, der seine eigene *Portal-Site* mit Inhalten betreibt. Dieser *ISP* muss die allgemeine Richtlinie auf alle seine Aktivitäten anwenden und die besondere Richtlinie (die besondere Verpflichtungen enthält) auf diejenigen Aktivitäten, mit denen er die Funktion eines Zugangsanbieters ausübt.

Ein weiterer interessanter Aspekt der neuen Definition der "elektronischen Kommunikationsdienste" ist die Erwähnung, dass der Dienst gegen Entgelt erbracht wird. Weder in der Präambel noch in der Begründung wird auf diese Formulierung Bezug genommen oder irgendeine Anleitung zu ihrer Auslegung gegeben. Sie könnte so ausgelegt werden, dass freie Zugangsanbieter (FAP) nicht mehr in den Geltungsbereich der überarbeiteten Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation fallen, da sie keine (zumindest keine finanziellen) Entgelte von den Internet-Nutzern erhalten.

Eine solche Auslegung wäre allerdings nicht korrekt, da durch Rechtsprechung des Europäischen Gerichtshofs bezüglich der Behandlung von Dienstleistungen im Sinne von Artikel 50 (ex-Artikel 60) des EG Vertrags⁴³ nicht erforderlich ist, dass die Entgelte für den Dienst vom Empfänger stammen; sie können beispielsweise auch von werbenden Firmen stammen.

Im Falle der FAP sind es tatsächlich die Firmen, die Anzeigen oder *Werbepanner* auf den Dokumentenseiten im Internet platzieren, die Entgelte an die FAP leisten. Damit ist klar, dass diese Dienstleistungen unter die Definition für elektronische Kommunikationsdienste fallen und folglich auch unter die Richtlinie.

Es wäre jedoch wünschenswert, im Text der Richtlinie diese Problematik zu klären, da nicht jeder Leser des Textes die Auslegung dieser Formulierung durch den Europäischen Gerichtshof kennt. Dies könnte etwa in der Präambel der Richtlinie geschehen.

⁴² Dieser Aspekt wird in diesem Arbeitsdokument nicht behandelt.

⁴³ Rechtssache C-109/92 Wirth [1993] ECR I-6447, 15.

III. Sonstige anwendbare Rechtsvorschriften

Es gibt eine Reihe anderer Gemeinschaftsvorschriften, die ebenfalls den einen oder anderen Aspekt im Zusammenhang mit dem Internet behandeln. Darunter lassen sich folgende erwähnen: Richtlinie 1999/93/EG über gemeinsame Rahmenbedingungen für *elektronische Signaturen*⁴⁴, Richtlinie 97/7/EG über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz⁴⁵ und Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt⁴⁶.

Doch die meisten dieser Rechtsvorschriften stellen keine ausreichend konkreten Bestimmungen zum Datenschutz auf und überlassen in den meisten Fällen die Regelung dieser Frage den spezifischen Richtlinien. Beispielsweise heißt es in der Richtlinie zum elektronischen Geschäftsverkehr in Erwägungsgrund 14:

"Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ausschließlich Gegenstand der Richtlinie 95/46/EG (...) und der Richtlinie 97/66/EG (...); beide Richtlinien sind uneingeschränkt auf die Dienste der Informationsgesellschaft anwendbar (...) so dass diese Frage in der vorliegenden Richtlinie nicht geregelt werden muss". In Artikel 1 Absatz 5 Buchstabe b) heißt es: *"Diese Richtlinie findet keine Anwendung auf Fragen betreffend die Dienste der Informationsgesellschaft, die von den Richtlinien 95/46/EG und 97/66/EG erfasst werden".*

In Erwägungsgrund 14 dieser Richtlinie zum elektronischen Geschäftsverkehrs wird darauf hingewiesen, dass *"die Grundsätze des Schutzes personenbezogener Daten (...) bei der Umsetzung und Anwendung dieser Richtlinie uneingeschränkt zu beachten (sind), insbesondere in bezug auf nicht angeforderte kommerzielle Kommunikation und die Verantwortlichkeit von Vermittlern. Die anonyme Nutzung offener Netze wie des Internets kann diese Richtlinie nicht unterbinden".*

In der Richtlinie für elektronische Signaturen werden dagegen in Artikel 8 spezifische Datenschutzvorschriften für Zertifizierungsdiensteanbieter und die für die Akkreditierung und Aufsicht zuständigen nationalen Stellen erlassen. Darin werden die Mitgliedstaaten verpflichtet, dafür Sorge zu tragen, dass Zertifizierungsdiensteanbieter und die für Akkreditierung und Aufsicht zuständigen nationalen Stellen die Anforderungen der allgemeinen Datenschutz-Richtlinie erfüllen. Ferner heißt es in dieser Vorschrift, dass Zertifizierungsdiensteanbieter, die öffentlich Zertifikate ausstellen, personenbezogene Daten nur unmittelbar von der betroffenen Person oder mit ausdrücklicher Einwilligung der betroffenen Person und nur insoweit einholen können, als dies zur Ausstellung und Aufrechterhaltung des Zertifikats erforderlich ist. Die Daten dürfen ohne ausdrückliche Einwilligung der betroffenen Person nicht für anderweitige Zwecke erfasst oder verarbeitet werden.

Artikel 8 Absatz 3 dieser Richtlinie ist besonders wichtig, denn er legt fest, dass die Mitgliedstaaten unbeschadet der Rechtswirkungen, die Pseudonyme nach einzelstaatlichem Recht haben, die Zertifizierungsdiensteanbieter nicht daran hindern, im Zertifikat ein Pseudonym anstelle des Namens des Unterzeichners anzugeben.

In der Präambel zu dieser Richtlinie (Erwägungsgrund 24) wird betont, dass die Zertifizierungsdiensteanbieter die Vorschriften über den Datenschutz und den Schutz der Privatsphäre achten müssen,

⁴⁴ Richtlinie 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für *elektronische Signaturen*, Amtsblatt der Europäischen Gemeinschaften, 19 Januar 2000, L 13/12 bis 13/20.

⁴⁵ Richtlinie 1997/7/EG vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, Amtsblatt der Europäischen Gemeinschaften, 4. Juni 1997, L 144.

⁴⁶ Richtlinie 2000/31/EG vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), Amtsblatt der Europäischen Gemeinschaften, 17. Juli 2000, L 178/1 bis 178/16.

um das Vertrauen der Nutzer in die elektronische Kommunikation und den elektronischen Geschäftsverkehr zu stärken.

IV. Anwendung der einzelstaatlichen Datenschutzvorschriften und ihrer internationalen Auswirkungen

In Artikel 4 Absatz 1 Buchstabe a) und b) der Richtlinie wird der Geltungsbereich der innerstaatlichen Vorschriften der Mitgliedstaaten zur Umsetzung dieser Richtlinie festgelegt, indem es heißt:

"Jeder Mitgliedstaat wendet die Vorschriften auf alle Verarbeitungen personenbezogener Daten an,

– die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält;

– die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in seinem Hoheitsgebiet, aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet".

Der Begriff "Niederlassung" wird in der Richtlinie wie folgt definiert: *"Eine Niederlassung (...) setzt die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Die Rechtsform einer solchen Niederlassung, die eine Agentur oder eine Zweigstelle sein kann, ist in dieser Hinsicht nicht maßgeblich".*

Gemäß Artikel 4 Absatz 1 Buchstabe c) der Richtlinie unterliegt die automatisierte oder sonstige Verarbeitung von Daten auf dem Hoheitsgebiet der Gemeinschaft bzw. des Europäischen Wirtschaftsraums den Vorschriften des gemeinschaftlichen Datenschutzgesetzes.

In Erwägungsgrund 20 dieser Richtlinie wird dies näher erläutert: *"Die Niederlassung des für die Verarbeitung Verantwortlichen in einem Drittland darf dem Schutz der Personen gemäß dieser Richtlinie nicht entgegenstehen. In diesem Fall sind die Verarbeitungen dem Recht des Mitgliedstaats zu unterwerfen, in dem sich die für die betreffenden Verarbeitungen verwendeten Mittel befinden, und Vorkehrungen zu treffen, um sicherzustellen, dass die in dieser Richtlinie vorgesehenen Rechte und Pflichten tatsächlich eingehalten werden".*

Die Auslegung der Begriffe "Ausrüstungen" oder "Mittel" hat Anlass zu Debatten bezüglich ihrer Reichweite gegeben, aber manche Beispiele fallen zweifellos in den Geltungsbereich von Artikel 4.

Dies gilt etwa für eine Textdatei, die sich auf einer Festplatte eines Computers befindet und die Informationen empfängt, speichert und an einen Server zurücksendet, der sich in einem anderen Land befindet. Solche Textdateien, genannt *Cookies*, werden für die Erhebung von Daten für Dritte eingesetzt. Falls sich der Computer in einem EU-Mitgliedstaat und die Drittpartei außerhalb der EU befindet, muss jene die innerstaatlichen Rechtsvorschriften des entsprechenden Mitgliedstaates bezüglich der Datenerhebung mittels *Cookies* einhalten.

In einem solchen Fall muss gemäß Artikel 4 Absatz 2 der für die Verarbeitung Verantwortliche einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter benennen, unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst.

V. Zusammenfassung

– Im Internet werden große Mengen von personenbezogenen Daten verarbeitet, für welche die Datenschutz-Richtlinien gelten.

- Die allgemeine Richtlinie gilt für sämtliche Fälle, während die besondere Richtlinie für Telekommunikationsdienste gilt. Angesichts der in Richtlinie 97/66/EG verwendeten Terminologie ist es allerdings zuweilen schwierig, festzulegen, was eine Telekommunikationsdienstleistung ist.
- Die Überprüfung des rechtlichen Rahmens für den Telekommunikationsbereich hat etwas mehr Klarheit in bezug auf die Geltungsbereiche der Datenschutz- und der Telekommunikations-Richtlinie erbracht. Für einige Aspekte dürften allerdings weitere Erläuterungen erforderlich sein, insbesondere der Hinweis auf die Voraussetzung der Entgeltannahme für die Aufnahme unter die Definition der elektronischen Kommunikationsdienste. Die Auslegung des Europäischen Gerichtshofs sollte in den Erwägungsgründen für die Richtlinie erläutert werden, um jegliches Missverständnis bezüglich des Geltungsbereichs der Richtlinie zu vermeiden.
- Die europäischen Datenschutzvorschriften sind auf die automatisierte oder nicht automatisierte Erhebung von Daten auf dem Gebiet der EU/des EEA anzuwenden.

KAPITEL 4: ELEKTRONISCHE POST

I. Einleitung

Es ist nicht leicht, die technischen Grundlagen der elektronischen Post mit ein paar Worten zu beschreiben. Dies liegt hauptsächlich an folgenden Problemen:

- Es gibt ein paar offizielle *Protokolle*, aber die Gefahren für die Privatsphäre hängen, wie auch beim *HTTP-Protokoll*, von der Art und Weise ab, wie die *Protokolle* konkret implementiert werden. Es gibt Tausende von verschiedenen Client- oder Serverprogrammen für E-Mails, und es ist sehr schwierig, allgemeine Schlussfolgerungen zu ziehen, da keine zuverlässigen Daten über die Benutzung solcher Programme vorhanden sind.
- Die unsichtbaren Verarbeitungsprozesse, die von diesen Programmen durchgeführt werden, sind, wie das Wort "unsichtbar" bereits sagt, nicht leicht aufzuspüren, und solche Programme werden so groß und kompliziert, dass es fast unmöglich ist, sicher zu sein, dass alle Funktionsweisen, vor allem die am besten versteckten, aufgelistet werden können.

Deswegen also kann die folgende Darstellung nicht als vollständig betrachtet werden, und sie wird nicht immer repräsentativ dafür sein, was täglich auf mehreren zehnten Millionen an das Internet angeschlossenen Computern überall auf der Welt geschieht.

II. Beteiligte

An der Abwicklung der elektronischen Post sind mehrere Akteure beteiligt, die bei jedem Schritt der Übermittlung Datenschutzaspekte beachten müssen. Beteiligt sind⁴⁷:

- Der Absender einer Nachricht
- Der Empfänger einer Nachricht (Inhaber einer E-Mail-Adresse)
- Der E-Mail-Diensteanbieter (Mail-Server, der die an einen Nutzer versandten E-Mails speichert, bis dieser sie erhalten möchte)
- Der Software-Lieferant für das E-Mail-Client-Programm beim Absender
- Der Software-Lieferant für das E-Mail-Client-Programm beim Empfänger
- Der Software-Lieferant für das Mail-Server-Programm

III. Technische Beschreibung

Ein Teilnehmer, der sich der elektronischen Post bedienen will, benötigt dazu folgendes:

- Ein "E-Mail-Client-Programm", das auf dem PC des Nutzers installiert ist;
- Eine E-Mail-Adresse (ein E-Mail-Konto);

⁴⁷ Der Telekommunikationsbetreiber ist nicht ausdrücklich in den E-Mail-Vorgang eingebunden, spielt aber eine Schlüsselrolle bei der Übermittlung der Signale, die erst jede Form von elektronischem Postverkehr möglich machen. Diesem Beteiligten werden durch die Richtlinien spezifische Sicherheitsaufgaben zugewiesen.

- Eine Verbindung zum Internet.

Der Vorgang des Versendens einer E-Mail

Es gibt zahlreiche "E-Mail-Client"-Programme, aber alle müssen dem Internet-Standard entsprechen. Das Versenden einer E-Mail kann kurz wie folgt beschrieben werden:

- Der Nutzer schreibt eine Nachricht in sein "E-Mail-Client"-Programm und füllt das Adressfeld des Empfängers mit der entsprechenden E-Mail-Adresse aus.
- Beim Anklicken des "Versenden"-Knopfs ("Button") im E-Mail-Client wird die EMail an den Mail-Server des Empfängers geschickt (meistens eine Organisation) oder an die "Mailbox" (Postfach) beim E-Mail-Konto des Nutzers, das er bei einem *Internet-Diensteanbieter* führt.
- Falls die E-Mail an den Mail-Server einer Organisation geschickt wurde, wird dieser die E-Mail entweder unmittelbar an den Empfänger oder aber an einen Mail-Relais-Server ("outbound relaying") weiterleiten.
- Die E-Mail kann mehrere Mail-Relais-Server durchlaufen, bevor sie den Mail-Server des Empfängers erreicht.
- Der Empfänger ist entweder direkt mit dem Mail-Server verbunden (z.B. in einem lokalen Netzwerk), oder er muss eine Verbindung herstellen, um die Mail zu erhalten.

E-Mail-Adressen

Eine E-Mail-Adresse hat zwei Teile, die durch ein "@"-Zeichen getrennt sind, zum Beispiel john.smith@nowhere.com oder subs34219@nowhere.org

- Der rechte Teil identifiziert den Host, bei dem der Empfänger ein Konto hat. Es handelt sich um einen *DNS*-Namen, der auf die IP-Adresse des Mail-Servers verweist.
- Der linke Teil beschreibt die einmalige Kennung des Empfängers. Es handelt sich um denjenigen Namen, mit dem der Empfänger beim E-Mail-Service bekannt ist; dabei gibt es absolut keine technische Notwendigkeit dafür, dass dies der echte Name des Empfängers sein muss. Er kann ein vom Empfänger ausgesuchtes Pseudonym sein, oder aber ein Zufallscode, der dem Empfänger bei seiner Registrierung vom Mail-Server nach eigenem Gutdünken zugeteilt wurde.

Unter technischen Gesichtspunkten ist für das Versenden einer E-Mail keine Identitätsangabe erforderlich. Tatsächlich ist es also offensichtlich wie in der richtigen Welt, wo jeder einen Brief ohne seinen Namen verschicken kann. Beim Versand von unverlangten Werbesendungen ("*Spamming*") verwendet der Absender in der Regel kein E-Mail-Konto, sondern hat unmittelbaren Zugang zum *SMTP-Protokoll*, was ihm erlaubt, seine E-Mail-Adresse zu löschen oder zu ändern.

E-Mail-Protokolle

Neben dem TCP/IP-*Protokoll* werden für die elektronische Post zwei weitere *Protokolle* benutzt:

1. Das sogenannte Simple Mail Transport Protocol (SMTP) wird verwendet, um eine E-Mail von einem Client zum Mail-Server des Empfängers zu **versenden**. Die Mail wird nicht direkt zum Client-Computer des Empfängers geschickt, da dieser Computer unter Umständen nicht eingeschaltet oder korrekt mit dem Internet verbunden ist, wenn der Absender eine E-Mail versendet. Das heißt, dass Internet-Nutzer eine Mailbox (ein "Konto") auf einem Server führen müssen, um E-Mails empfangen zu können. Dies bedeutet auch, dass der Mailedienste-Anbieter die Nachricht so lange speichern muss, bis der Empfänger sie abholt.
2. Das zweite *Protokoll* wird POP-Protokoll genannt und vom Empfänger benutzt, um eine Verbindung mit dem Mail-Server herzustellen, damit er nachsehen kann, ob Post für ihn da ist. Zu diesem Zweck muss der Empfänger seinen Mailbox-Namen und sein Passwort eingeben, um zu verhindern, dass Fremde seine Post lesen.

In der Regel enthalten E-Mail-Client-Programme beide Protokolle, da Internet-Nutzer, die E-Mails versenden, wahrscheinlich auch Antwort erhalten möchten.

IV. Gefahren für die Privatsphäre

Einige Aspekte bergen spezifische Gefahren für die Privatsphäre.

Sammlung von E-Mail-Adressen

Wie weiter oben erwähnt, ist eine E-Mail-Adresse unerlässlich, um eine Verbindung herzustellen. Sie ist aber gleichzeitig eine wertvolle Informationsquelle, die personenbezogene Daten des Nutzers enthält. Daher ist es sinnvoll, sich etwas Klarheit über die verschiedenen Möglichkeiten des Sammelns von E-Mail-Adressen zu schaffen.

E-Mail-Adressen können auf verschiedene Weise erhoben werden:

- Der Anbieter der "E-Mail-Client"-Software, die gegen Entgelt oder gratis erworben wurde, kann den Nutzer zur Registrierung auffordern.
- Auch lässt sich in der Software des Clients ein Code eingeben, der die E-Mail-Adresse des Nutzers ohne dessen Wissen an den Software-Anbieter weiterleiten wird (unsichtbare Verarbeitung).
- In einigen Browsern wurden Sicherheitslücken entdeckt, die einer Website erlauben, die E-Mail-Adressen der Besucher zu erfahren. Dies kann durch vorsätzlich aktivierte Inhalte unter Verwendung etwa von *JavaScript* geschehen.
- Manche Browser können auch so konfiguriert werden, dass sie die EMail-Adressen als anonyme Passwörter versenden, wenn sie FTP-Verbindungen herstellen (dies ist allerdings nicht die Standard-Einstellung).
- E-Mail-Adressen können von verschiedenen Internet-Stellen in unterschiedlichen Situationen erfragt werden (z.B. auf kommerziellen Websites in einem Bestellformular, bei der Registrierung vor dem Zutritt zu einem Chatroom usw.).

- E-Mail-Adressen können auf verschiedene andere Weisen aus öffentlich zugänglichen Bereichen des Internets beschafft werden⁴⁸.
- E-Mail-Adressen können während der Übermittlung einer Nachricht abgefangen werden.

Verkehrsdaten

Es ist unerlässlich, zwischen dem Inhalt einer E-Mail und den Verkehrsdaten zu unterscheiden. Verkehrsdaten sind diejenigen Daten, die von den *Protokollen* benötigt werden, um eine korrekte Übermittlung vom Absender zum Empfänger durchzuführen.

Verkehrsdaten bestehen teilweise aus Informationen, die durch den Absender geliefert wurden (z.B. die E-Mail-Adresse des Empfängers) und teilweise aus technischen Informationen, die während der Bearbeitung der E-Mail automatisch erzeugt werden (z.B. Datum und Zeitpunkt des Versendens, Typ und Version des "E-Mail-Clientprogramms").

Alle Verkehrsdaten oder Teile davon werden in einen Vorspann ("Header") gesetzt, der dem Empfänger mit der Nachricht übermittelt wird. Die übermittelten Teile der Verkehrsdaten werden vom Mail-Server des Empfängers und dem "Mail-Client" benutzt, um die einkommende Post sachgerecht zu bearbeiten. Der Empfänger kann die übermittelten Verkehrsdaten (E-Mail-Eigenschaften) für Analysezwecke nutzen (z.B. um den Verlauf einer E-Mail durchs Internet zu verfolgen).

Unter die Definition der "Verkehrsdaten" wird üblicherweise folgendes gezählt:

- E-Mail-Adresse und IP-Adresse des Absenders
- Typ, Version und Sprache des Clientprogramms
- E-Mail-Adresse des Empfängers
- Datum und Zeitpunkt des Versands der E-Mail
- Größe der E-Mail
- Verwendete Zeichentabelle
- Thema des Schreibens (dieser Punkt informiert auch über den Inhalt der Mitteilung)
- Bezeichnung, Größe und Typ der eventuell beigefügten Dokumente
- Liste der SMTP-Relais, die für die Übermittlung verwendet wurden.

In der Praxis werden Verkehrsdaten üblicherweise auf den EMail-Servern des Absenders und des Empfängers gespeichert. Sie können auch auf den Relais-Servern in der Route im Internet gespeichert werden.

Da der Begriff "Verkehrsdaten" in der Richtlinie 97/66/EG nicht förmlich definiert ist, sollte beachtet werden, dass personenbezogene Daten, die nicht für die Herstellung einer Verbindung oder für Abrechnungszwecke benötigt, sondern während der Übermittlung erzeugt werden, von manchen Internet-Betreibern fälschlich als Verkehrsdaten betrachtet werden könnten, die sie speichern dürfen.

Die Datenschutzgruppe hat sich in ihrer Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch *Internet-Diensteanbieter* zum Zwecke der Strafverfolgung mit einigen Problemen bezüglich der

⁴⁸ Weitere Untersuchungen zu *Spam* und dem Sammeln von E-Mail-Adressen wurden von der Französischen Datenschutzbehörde CNIL durchgeführt. Siehe insbesondere den CNIL-Bericht über Elektronische Post und Datenschutz vom 14. Oktober 1999, abrufbar auf der CNIL-Internet-Seite: www.cnil.fr

Privatsphäre im Zusammenhang mit Verkehrsdaten befasst⁴⁹. Die Arbeitsgruppe ist der Auffassung, dass - bei Anerkennung der Erfordernisse einer wirksamen Strafverfolgung - die effektivste Maßnahme zur Verringerung nicht akzeptabler Bedrohungen der Privatsphäre darin besteht, dass Verkehrsdaten im Prinzip nicht lediglich aus Gründen der Strafverfolgung aufbewahrt werden sollten, und dass nationale Gesetze die Telekommunikationsbetreiber, Telekommunikationsdienste und *Internet-Diensteanbieter* nicht auferlegen sollten, Verkehrsdaten für einen längeren Zeitraum als für Abrechnungszwecke erforderlich aufzubewahren.

In der offiziellen Erklärung der Konferenz der Europäischen Datenschutzbeauftragten im Frühjahr 2000 in Stockholm wurde gefordert: "Wo Verkehrsdaten in besonderen Fällen aufbewahrt werden müssen, muss eine nachweisbare Notwendigkeit dafür vorliegen, muss die Aufbewahrungszeit so kurz wie möglich sein und muss diese Maßnahme gesetzlich eindeutig geregelt sein".

E-Mail Inhalte

Die Vertraulichkeit von Mitteilungen wird durch Artikel 5 der Richtlinie 97/66/EG geschützt. Dieser Bestimmung zufolge ist es Dritten nicht gestattet, die Inhalte von E-Mails zwischen zwei Partnern zu lesen. Falls der E-Mail-Inhalt während der Übermittlung auf Relais-Servern gespeichert wird, muss er, sobald er weitergeleitet wurde, gelöscht werden.

Falls ein Relais-Server die E-Mail nicht weiterleiten kann, darf diese für kurze und begrenzte Zeit auf dem Server gespeichert werden, bis sie dem Absender gemeinsam mit einer Fehlermeldung zurückgeschickt wird, aus der hervorgeht, dass die E-Mail dem Empfänger nicht zugestellt werden konnte.

Die Inhalte einer E-Mail werden so lange auf dem Mail-Server gespeichert, bis der "E-Mail-Client" des Nutzers ihre Zustellung anfordert. In manchen Fällen kann der Nutzer wählen, die elektronische Post im Mail-Server zu belassen, selbst wenn er bereits eine Kopie erhalten hat. Falls sich der Nutzer nicht dafür entschieden hat, ist die Mail zu löschen, sobald der Mail-Server sicher gehen kann, dass der Empfänger sie erhalten hat.

Falls ein Scannen nach Viren in Form einer Überprüfung der Inhalte erfolgt, muss sie automatisch lediglich für diesen Zweck eingestellt sein. Die Inhalte dürfen für keinen anderen Zweck analysiert und dürfen niemandem gezeigt werden, selbst wenn ein Virus gefunden wurde.

Eine weitere Gefahr für die Privatsphäre im Zusammenhang mit E-Mails liegt darin, dass die Nutzer E-Mail-Schreiben, die versandt oder empfangen wurden, nicht einfach und wirksam löschen können, da mit der Delete-Taste ein E-Mail nicht unbedingt auch wirklich aus dem System entfernt ist. In diesem Fall ist es für andere Benutzer desselben Computers oder - bei Netzwerken - einen Systemadministrator relativ leicht, Nachrichten wiederzufinden, die der ursprüngliche Nutzer löschen wollte und von denen er annimmt, dass sie aus dem System entfernt sind. Dieses Problem ist natürlich nicht nur auf E-Mails beschränkt, hat aber dort besondere Tragweite. Zur Behebung dieses Problems müssen Betriebssysteme so konzipiert werden, dass mit der Löschfunktion Informationen tatsächlich aus dem System entfernt werden.

Durch Hardware und Software kann der Verkehr in einem Netzwerk überwacht werden. Dies wird *Sniffing* genannt. *Sniffing*-Software ist in der Lage, alle Datenpakete in einem Netzwerk zu lesen und dadurch sämtliche Mitteilungen, die nicht verschlüsselt sind, in Klartext anzuzeigen. Die einfachste Form des *Sniffing* kann mit allgemein erhältlicher Software an einem gewöhnlichen PC durchgeführt werden, der an ein Netzwerk angeschlossen ist.

Wenn *Sniffing* an zentralen Knoten oder Verbindungsstellen im Internet ausgeführt wird, ermöglicht dies in großem Maßstab das Abfangen und Überwachen der Inhalte von E-Mails und/oder Verkehrsdaten nach

⁴⁹ Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch *Internet-Diensteanbieter* für Zwecke des Strafvollzugs, angenommen am 7. September 1999, 5085/99/EN/final, AG 25.

bestimmten Merkmalen, typischerweise nach dem Vorhandensein von Stichwörtern. *Sniffing* darf als allgemeine und sondierende Überwachung nur zugelassen werden, wenn es in Einklang mit den Bestimmungen von Artikel 8 der Europäischen Menschenrechtskonvention erfolgt, selbst wenn es von staatlichen Stellen betrieben wird.

Diesbezüglich ist die Erwähnung von Interesse, dass sich gegenwärtig weltweit Bedenken gegen mögliche internationale Kommunikationsüberwachungen und insbesondere das "Echelon"-Satellitenabhörsystem erheben. Globale Überwachung ist heutzutage ein aktuelles Thema auf der Tagesordnung des Europäischen Parlaments⁵⁰. In einem Bericht an den Generaldirektor für Forschung des Europäischen Parlaments⁵¹ über die Entwicklung der Überwachungstechnologie und die Gefahr des Missbrauchs ökonomischer Informationen heißt es, dass das Echelon-System seit mehr als zwanzig Jahren bestehe. Laut diesem Bericht macht Echelon umfassenden Gebrauch von globalen, Internet-ähnlichen Kommunikationsnetzwerken der NSA⁵² und des GCHQ⁵³, um entfernt arbeitenden Geheimdienstmitarbeitern zu ermöglichen, Computer an jeder Eingabestelle anzusprechen und Ergebnisse automatisch zu erhalten.

Ein anderes strittiges Überwachungssystem ist Carnivore, das nach den von EPIC⁵⁴ vorgelegten Informationen den Verkehr an den Einrichtungen von *Internet-Diensteanbietern* überwacht, um Informationen abzufangen, die sich in den E-Mails von Tatverdächtigen befinden. EPIC berichtet, dass Carnivore Millionen von E-Mails pro Sekunde überprüfen und Strafverfolgungsbehörden in die Lage versetzen kann, sämtliche digitalen Mitteilungen einzelner Kunden von Internet-Diensteanbietern abzufangen. Im US-amerikanischen Kongress, in den Medien und unter den Bürgern wurden dringliche Fragen bezüglich der Rechtmäßigkeit des Programms Carnivore und seines potentiellen Missbrauchs aufgeworfen. Als Reaktion auf die öffentliche Unruhe über Carnivore kündigte Justizministerin Janet Reno am 27. Juli 2000 an, dass einer "Gruppe von Experten" die technischen Spezifikationen des Systems offengelegt würden, um öffentliche Bedenken zu zerstreuen.

Im Europarat stehen Erörterungen über die globale Überwachung der Kommunikationsverbindungen ebenfalls auf der Tagesordnung. Der Sachverständigenausschuss zum Thema Kriminalität im Cyberspace legte am 27. April 2000 seinen "Entwurf für ein Übereinkommen zur Kriminalität im Internet" vor⁵⁵. Dieses Übereinkommen würde die Erhebung von Daten erleichtern, indem von Internet-Diensteanbietern verlangt würde, Informationen für Vollzugsbehörden zu sammeln und zu speichern. Es würde ferner den internationalen Austausch solcher Informationen zwischen Regierungsstellen verschiedener Staaten verlangen, selbst mit solchen, die nicht die Europäische Menschenrechtskonvention oder sonstige Instrumente des Europarates oder der Union im Bereich des Datenschutzes mittragen. Bislang sind keine substantiellen Vorschriften zum Schutz des Grundrechts auf Privatsphäre und der personenbezogenen Daten in Drittstaaten vorgesehen, die personenbezogene Daten über EU-Bürger erhalten, noch wurden Grundsätze für die Einhaltung grundlegender Menschenrechte wie etwa der Grundsatz der Notwendigkeit oder der Grundsatz der Verhältnismäßigkeit aufgestellt.

Ohne bereits den Wortlaut des Entwurfs für das Übereinkommen zu diesem Zeitpunkt kommentieren zu wollen, möchte die Arbeitsgruppe jedoch den Standpunkt wiederholen, der von den Europäischen Datenschutzbeauftragten in einer EntschlieÙung zu ihrer Stockholmer Konferenz im April 2000 vertreten wurde. Darin heißt es:

⁵⁰ Zu weiteren Informationen siehe Europäischer Parlamentsausschuss für Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten <http://www.europarl.eu.int/committees/de/default.htm>
Siehe auch EPIC Alert 7.07, 20. April 2000.

⁵¹ Bericht über Abhörmöglichkeiten 2000, Mai 1999.

⁵² National Security Agency – Nationale Sicherheitsagentur, USA.

⁵³ Britisches Gegenstück der NSA.

⁵⁴ EPIC Alert 7.15, 3. August 2000.

⁵⁵ Der Text des Vertragsentwurfs ist abrufbar unter: <http://conventions.coe.int/treaty/en/projets/cybercrime.htm>

Die Konferenz der Europäischen Datenschutzbeauftragten vom Frühjahr 2000 nimmt mit Sorge Vorschläge zur Kenntnis, dass die ISP Verkehrsdaten routinemäßig aufbewahren sollen, und zwar über die für Abrechnungszwecke nötige Zeit hinaus, um Vollzugsbehörden einen Zugang zu ihnen zu ermöglichen.

Die Konferenz weist nachdrücklich darauf hin, dass eine solche Aufbewahrung ein unerhörter Eingriff in die grundlegenden Rechte ist, die Artikel 8 der Europäischen Konvention der Menschenrechte jeder Person garantiert. Wo Verkehrsdaten in besonderen Fällen aufbewahrt werden müssen, muss eine nachweisbare Notwendigkeit vorliegen, muss die Aufbewahrungszeit so kurz wie möglich sein und muss diese Maßnahme gesetzlich eindeutig geregelt sein.

Die Datenschutzgruppe hat sich in ihrer Empfehlung 2/99 mit den die Privatsphäre berührenden Aspekten des Abfangens von Mitteilungen befasst⁵⁶. In dieser Empfehlung weist die Arbeitsgruppe darauf hin, dass jedes Abfangen im Bereich der Telekommunikation, definiert als Erwerb von Kenntnissen durch Dritte über Inhalte und/oder Verkehrsdaten aus privaten Telekommunikationsverbindungen zwischen zwei oder mehr Teilnehmern, und insbesondere von Verkehrsdaten, die die Inanspruchnahme von Telekommunikationsdiensten betreffen, eine Verletzung des individuellen Rechts auf Privatsphäre und des Briefgeheimnisses sind. Folglich kann dieses Abfangen nicht hingenommen werden, außer wenn es gemäß Artikel 8 Absatz 2 der Europäischen Konvention für den Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950⁵⁷ und den Auslegungen dieser Bestimmungen durch den Europäischen Gerichtshof für Menschenrechte drei grundlegende Kriterien erfüllt: eine solche Maßnahme besitzt eine gesetzliche Grundlage, ist in einer demokratischen Gesellschaft notwendig und verfolgt einen der in der Konvention aufgeführten begründeten Zwecke⁵⁸.

V. Analyse spezifischer Aspekte

Webmail

E-Mail-Systeme, die Dokumentenseiten als Schnittstelle benutzen, werden insgesamt als "Webmail" bezeichnet (z.B. Yahoo, HotMail usw.). *Webmail* kann von überall aus abgerufen werden, und der Benutzer braucht keine Verbindung zu einem besonderen *ISP* herzustellen, wie dies bei der Verwendung eines gewöhnlichen E-Mail-Kontos der Fall ist.

Webmail ist gewöhnlich gratis, aber um ein kostenfreies Konto zu erhalten, muss der Verbraucher häufig seine persönlichen Daten angeben. Nach Untersuchungen von Datenschutzbehörden verkaufen anscheinend viele *Webmail*-Anbieter personenbezogene Daten für Marketing-Zwecke oder tauschen sie untereinander aus.

Webmail verwendet anstelle des POP- das *HTML*-Protokoll, um E-Mails abzurufen und zu lesen. Tatsächlich werden die E-Mails auf klassischen *HTML*-Seiten geliefert. Diese Eigenschaft ermöglicht es Anbietern von E-Mail-Diensten, den *HTML*-Seiten, auf denen die Nachrichten angezeigt werden,

⁵⁶ Empfehlung 2/99 über die Wahrung der Privatsphäre im Zusammenhang mit der Überwachung der Telekommunikationsverbindungen, angenommen am 3. Mai 1999, 5005/99/EN/final, WP 18.

⁵⁷ Es ist hervorzuheben, dass die vom Europarat anerkannten Grundrechte Auflagen für die Mitgliedstaaten im Hinblick auf die Überwachung der Telekommunikationsverbindungen bedeuten, ungeachtet der Unterscheidungen, die auf Ebene der Europäischen Union je nach dem gemeinschaftlichen oder zwischenstaatlichen Charakter der betreffenden Bereiche getroffen werden.

⁵⁸ Konvention Nr. 108 des Europarats besagt ebenfalls, dass eine Überwachung nur dann zugelassen werden kann, wenn sie eine in einer demokratischen Gesellschaft für den Schutz der nationalen Interessen gemäß Artikel 9 Absatz 2 dieser Konvention nötige Maßnahme darstellt und streng in Bezug auf diesen Zweck definiert ist.

personenbezogene Werbung hinzuzufügen (graphisch betrachtet außerhalb der Nachricht selbst). *Webmail* wird stark gesponsert, weshalb viele Werbeeinblendungen angezeigt werden.

Da *Webmail*-Systeme auf dem *HTTP-Protokoll* beruhen, sind sie durch sogenannte "Web Bugs" gefährdet; dies sind Versuche, die E-Mail-Identität einer Person durch eingebettete *HTML*-Markierungszeichen und *Cookies* aufzudecken.

Webmail-Anbieter dürfen keine unsichtbaren *Hyperlinks* in Dokumentenseiten einfügen, bei denen das E-Mail-Konto Teil der URL ist. Denn dadurch würden sie dazu beitragen, die E-Mail-Adresse des Absenders an die werbenden Firmen weiterzuleiten. Dies ist eine weitere Methode, durch unsichtbare Prozesse in die Privatsphäre der Nutzer einzubrechen.

Teilnehmerverzeichnisse

Verschiedene Dienste im Internet bieten Verzeichnisse von E-Mail-Adressen an. Diese öffentlich zugänglichen Verzeichnisse sind, wie in Kapitel 6 dargestellt wird, denselben Regeln wie Telefonbücher und sonstige öffentlich zugängliche Daten unterworfen. Im Rahmen der vorhandenen Rechtsvorschriften muss den Nutzern gemäß Richtlinie 95/46/EG (Artikel 14) und Richtlinie 97/66/EG (Artikel 11) zumindest das Recht eingeräumt werden, gegen die Verarbeitung ihrer Daten Einspruch zu erheben.

Es sei erwähnt, dass der Vorschlag für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation die diesbezüglichen Verpflichtungen der für die Datenverarbeitung Verantwortlichen harmonisiert und zugunsten der Nutzer den Anspruch auf eine Aufnahme in die Teilnehmerverzeichnisse vorsieht. Die Arbeitsgruppe hält dies für eine wichtige Verbesserung.

Spam

"*Spam*" kann als die Praxis des massenhaften und wiederholten Versendens von unverlangten E-Mails mit gewöhnlich kommerziellem Charakter an Personen definiert werden, mit denen der Absender zuvor keinen Kontakt hatte⁵⁹. Die Datenschutzgruppe hat sich in ihrer Stellungnahme 1/2000 zu bestimmten Aspekten des elektronischen Geschäftsverkehrs bereits mit dieser Frage beschäftigt⁶⁰.

Vom Standpunkt der Verbraucher aus ergibt sich aus "*Spam*" ein dreifaches Problem: erstens die Beschaffung von E-Mail-Adressen von Personen ohne deren Wissen und Einwilligung, zweitens der Erhalt großer Mengen unerwünschter Werbung und drittens die Kosten für die Dauer der Verbindung.

E-Mail-Adressen lassen sich aus öffentlich zugänglichen Teilnehmerverzeichnissen oder mit Hilfe anderer Techniken gewinnen. Zum Beispiel können die E-Mail-Adressen von den Teilnehmern selbst geliefert werden, wenn sie Güter oder Dienste über das Internet erwerben. In anderen Fällen können die von Teilnehmern an Lieferanten gelangten E-Mail-Adressen an Dritte weiterverkauft werden.

Aus der Sicht der Arbeitsgruppe geben die Bestimmungen der Datenschutz-Richtlinie eine klare Antwort auf die Fragen des Schutzes der Privatsphäre, die durch *Spam* aufgeworfen werden, und legen eindeutig die Rechte und Pflichten der Beteiligten fest. Es sind zwei Situationen zu unterscheiden:

- Wenn von einer Firma eine E-Mail-Adresse unmittelbar bei einer Person eingeholt wird, und zwar zum Zwecke des E-Mail-Versands durch diese Firma oder durch Dritte, an die die Daten weitergegeben werden, dann muss die erstere Firma die betroffene Person zum Zeitpunkt der Erhebung der Adresse über diese Zwecke informieren⁶¹. Dem Dateninhaber muss ferner als absolute Mindestbedingung das

⁵⁹ Siehe CNIL-Bericht über elektronische Post und Datenschutz, 14. Oktober 1999.

⁶⁰ Stellungnahme 1/2000 der Task Force 'Internet' zu bestimmten Datenschutzaspekten des elektronischen Geschäftsverkehrs, angenommen am 3. Februar 2000, 5007/00/EN/final, WP 28.

⁶¹ Richtlinie 95/46/EG, Artikel 10.

Recht eingeräumt werden, zum Zeitpunkt der Erhebung der Daten und jederzeit danach gegen den Gebrauch seiner Daten durch die ursprüngliche Firma und alle nachfolgenden Firmen, die Daten von der ursprünglichen Firma erhalten haben, durch einfache elektronische Mittel, wie zum Beispiel das Anklicken eines Feldes, das zu diesem Zwecke dient, Widerspruch einzulegen⁶². Manche einzelstaatlichen Rechtsvorschriften verlangen bei der Umsetzung der einschlägigen Richtlinien von den Firmen sogar die ausdrückliche Einwilligung der Dateninhaber. Die Vorschriften des Artikels über unerbetene kommerzielle Informationen in der Richtlinie zum elektronischen Geschäftsverkehr ergänzen diese Bestimmungen auf der technischen Ebene, indem sie die Diensteanbieter dazu verpflichten, "Opt-out"-Register (sogenannte Robinson-Listen) zu konsultieren, ohne die für die Datenverarbeitung Verantwortlichen in irgendeiner Weise von den allgemeinen Verpflichtungen zu entbinden.

- Wenn eine E-Mail-Adresse in einem öffentlich zugänglichen Raum im Internet erhoben wird, steht ihre Benutzung für unverlangte E-Mail-Zusendungen im Widerspruch zum einschlägigen Gemeinschaftsrecht, und zwar aus drei Gründen. Erstens kann dies als "rechtswidrige" Verarbeitung von personenbezogenen Daten gemäß Artikel 6 Absatz 1 Buchstabe a) der allgemeinen Richtlinie gelten. Zweitens steht dies im Widerspruch zum Grundsatz der Zweckentsprechung gemäß Artikel 6 Absatz 1 Buchstabe b) derselben Richtlinie, da hier der Dateninhaber seine E-Mail-Adresse für ganz andere Zwecke veröffentlicht hat, etwa um an einer Newsgroup teilzunehmen. Drittens kann von solchen Sendungen angesichts der einseitigen Kosten und der Störungen für den Empfänger nicht angenommen werden, dass sie das Kriterium des berechtigten Interesses gemäß Artikel 7 Buchstabe f) erfüllen⁶³.

Ein besonderer Aspekt elektronischer Werbesendungen ist der Umstand, dass zwar die Kosten des Absenders gegenüber den traditionellen Methoden des Direktmarketings extrem niedrig sind, für den Empfänger aber Kosten für die Verbindungsdauer entstehen. Diese Kostensituation ist also ein deutlicher Anreiz zur Nutzung dieses Marketing-Instruments auf breiter Basis und zur Vernachlässigung der Datenschutzbelange und der Probleme, die sich durch den E-Mail-Versand ergeben.

Die durch unverlangte E-Mails entstehenden Kosten gehen zu Lasten sowohl der Empfänger als auch der Internet-Mail-Anbieter der Empfänger (entweder der *Webmail*-Server oder der *ISP* der Empfänger).

Denn die Mail-Server müssen auch die unverlangten E-Mails eine Zeit lang speichern, und die Empfänger müssen für das Herunterladen der Mitteilungen, die sie gar nicht erhalten möchten, zahlen⁶⁴ und verlieren Zeit mit dem Sortieren der erhaltenen Mitteilungen und dem Löschen der unerbetenen elektronischen Post, vor allem, wenn *Spam*-Mitteilungen in der Betreffzeile nicht als solche ausgewiesen sind (normalerweise durch die Einfügung des Codes für Werbung, "ADV", als erste Buchstaben der Betreffzeile).

Schätzungsweise machen heutzutage *Spam*-Sendungen (auch bekannt als unverlangte 'Junk Mail') zehn Prozent aller weltweit versandten E-Mails aus⁶⁵.

⁶² Richtlinie 95/46/EG, Artikel 14.

⁶³ Diese Bestimmung (eine von mehreren möglichen rechtlichen Grundlagen für eine Verarbeitung) verlangt, dass Datenverarbeitung "erforderlich [ist] zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen [...] wahrgenommen wird, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person [...] überwiegen".

⁶⁴ Der Telekommunikations-Betreiber, sofern der Nutzer ein *Modem* benutzt. Falls der Nutzer eine Mietleitung benutzt, ist - selbst wenn sich die Kosten durch die *Spam*-Nachrichten nicht plötzlich erhöhen, da ja Pauschalen gezahlt werden - unter gesamtwirtschaftlichen Gesichtspunkten klar, dass im Zusammenhang mit den Massensendungen an *Spam* bei den ISP Betriebskosten anfallen, die folglich Auswirkungen auf die Preise der Mietleitungen haben.

⁶⁵ Siehe "Net Worth" (op cit), Seite 3.

VI. Vertraulichkeit, Sicherheitsaspekte

Die elektronische Post eröffnet dieselben Möglichkeiten der Kommunikation wie die herkömmliche Post. Deshalb gelten für E-Mail hinsichtlich des Briefgeheimnisses auch dieselben Vorschriften.

Jede Person hat das Recht, jemand anderem elektronische Post zu schicken, ohne dass sie von Dritten gelesen wird. Artikel 5 der Richtlinie 97/66/EG, die für Nachrichten und entsprechende Verkehrsdaten gilt, die etwa durch elektronische Post versandt werden, stellt Vorschriften bezüglich der Vertraulichkeit von Mitteilungen auf. Daneben verpflichtet Artikel 4 derselben Richtlinie die Anbieter von Telekommunikationsdiensten, angemessene technische und organisatorische Maßnahmen zu treffen, um die Sicherheit ihrer Dienste zu schützen, und bei besonderem Risiko der Verletzung der Netzsicherheit die Teilnehmer über dieses Risiko und über mögliche Abhilfen einschließlich deren Kosten zu informieren.

In der Welt außerhalb des Internets hat jeder die Möglichkeit, einen Brief anonym oder unter einem Pseudonym zu verschicken. Um anonyme E-Mails zu versenden, kann der Nutzer bei verschiedenen Anbietern solcher Dienste eine anonyme E-Mail-Adresse erhalten.

Je nach Art der E-Mail sind unter Nutzer-Gesichtspunkten eine Reihe von Punkten relevant:

- Vertraulichkeit, d.h. Schutz der übermittelten Daten vor Ausspähung. Eine Möglichkeit zur Sicherstellung von Vertraulichkeit ist die *Verschlüsselung* der abzuschickenden E-Mails.
- *Verschlüsselung* und Entschlüsselung beruhen auf Programmen, die herkömmliche E-Mail-Programme ergänzen (Plug-Ins) oder auf E-Mail-Programmen und Browsern, die diese Möglichkeiten bieten. Die Sicherheit der *Verschlüsselung* hängt von den verwendeten Algorithmen und der Länge des Schlüssels ab.
- *Datenintegrität* – sie gewährleistet, dass Informationen nicht zufällig oder absichtlich verändert werden. *Datenintegrität* lässt sich erzielen, indem auf der Grundlage des zu übermittelnden Textes ein spezieller Code errechnet und dieser gemeinsam mit dem Text verschlüsselt wird. Der Empfänger kann den Code entschlüsseln und durch erneutes Berechnen des Codes überprüfen, ob die Nachricht verändert wurde.
- *Authentisierung* – sie ist die Garantie dafür, dass der Nutzer tatsächlich derjenige ist, der er zu sein behauptet. Die *Authentisierung* kann durch das Austauschen von *digitalen Signaturen* auf der Grundlage *digitaler Zertifikate* erfolgen. Diese Zertifikate brauchen nicht die echten Namen der Nutzer zu erwähnen, sondern können gemäß Artikel 8 der Richtlinie über gemeinschaftliche Rahmenbedingungen für *elektronische Signaturen* Pseudonyme angeben⁶⁶.

VII. Maßnahmen zur besseren Absicherung der Privatsphäre⁶⁷

Zwei Arten von Tools sollen in diesem Abschnitt erörtert werden: E-Mail-Filter und anonyme E-Mail⁶⁸.

1) E-Mail-Filter sieben die beim Nutzer ankommenden E-Mails und lassen nur diejenigen durch, die er erhalten möchte. Diese Programme werden hauptsächlich benutzt, um Werbemüll (*Spam*) auszusortieren.

Heutzutage bieten mehrere Firmen Tools an, die Internet-Nutzer auf ihrem Computer installieren können, um unerbetene E-Mails auszusortieren. Ferner ermöglichen verschiedene E-Mail-Programmpakete den Nutzern, Nachrichten zu filtern, sobald sie am Desktop angekommen sind.

⁶⁶ Richtlinie 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt der Europäischen Gemeinschaften vom 19.01.2000, L 13/12–20.

⁶⁷ Mehr dazu siehe in Kapitel 9 über Maßnahmen zur besseren Absicherung der Privatsphäre.

⁶⁸ Siehe "Net Worth" (op. cit), Seite 275 ff.

Am wirksamsten sind zwar solche Filter, die nur bestimmte E-Mails hereinlassen; diese Systeme arbeiten für Nutzer mit gleichbleibenden Netzwerken von E-Mail-Partnern. Aber für den größten Teil der Bevölkerung wären sie hinderlich, da jeder neue E-Mail-Partner zunächst zugelassen werden müsste.

Die üblicheren Filtertechnologien lassen alle E-Mails außer solchen mit bestimmten Bereichsnamen, E-Mail-Adressen oder Stichwörtern in der Betreffzeile durch. Hartnäckige Absender wechseln jedoch häufig den Domänenamen oder die E-Mail-Adresse, um diese Filter zu umgehen, vor allem, weil E-Mail-Konten im Web häufig kostenlos und einfach zu erhalten sind und jederzeit aufgelöst werden können. Schließlich ist es auch schwierig, Filter mit Hilfe von Stichwörtern zu verwenden, da die Fehlerwahrscheinlichkeit recht hoch ist.

2) Anonyme E-Mails gestatten dem Nutzer, seine E-Mail-Adresse online anzugeben, ohne seine Identität preisgeben zu müssen⁶⁹. Dieser Dienst ist derzeit im Internet bei einer Reihe von Firmen, die "Remailer"-Dienste anbieten, gratis erhältlich.

Bei diesen Diensten entfernt der Weiterversender bei ausgelieferten E-Mails die Identität des Absenders. Antworten auf jene anonymen E-Mails gehen an den "Remailer", der dann die anonyme Adresse mit der eigentlichen E-Mail-Adresse wieder zusammen fügt und die E-Mail-Antwort sicher an die Kunden weiterleitet.

VIII. Zusammenfassung

Unter dem Gesichtspunkt des Datenschutzes sind bezüglich der elektronischen Post folgende Probleme zu lösen:

Unsichtbare Verarbeitung durch "Mail-Clients" und SMTP-Relais

Den Dateninhabern ist die Möglichkeit zu geben, so anonym wie möglich zu bleiben, insbesondere bei der Teilnahme an Diskussionsforen. Anscheinend werden E-Mail-Adressen von Teilnehmern an solchen Foren sehr oft gemeinsam mit dem Inhalt ihrer Mitteilung versandt⁷⁰. Dies steht nicht in Einklang mit Artikel 6 der Richtlinie 95/46/EG, der die Verarbeitung von Informationen auf das für die legitimen Zwecke erforderliche Maß beschränkt⁷¹.

Aufbewahrung von Verkehrsdaten durch Zwischenträger und E-Mail-Diensteanbieter

Gemäß Artikel 6 der Richtlinie 97/66/EG sind Verkehrsdaten zu löschen, sobald die Verbindung beendet ist. Die Richtlinie sieht einige Ausnahmen von diesem Prinzip vor, z.B. wenn eine Weiterverarbeitung für den Zweck der Gebührenabrechnung erforderlich ist⁷².

Überwachung

Die Überwachung der elektronischen Post (Nachrichten und entsprechende Verkehrsdaten) ist rechtswidrig, außer wenn sie in besonderen gesetzlich zugelassenen Fällen und gemäß der Europäischen

⁶⁹ Auf diese Art von Diensten wird auch in Kapitel 6 dieses Berichts (Veröffentlichungen und Foren) in Abschnitt V über Maßnahme zur besseren Absicherung der Privatsphäre eingegangen.

⁷⁰ Zu weiteren Details siehe weiter unten Kapitel V.

⁷¹ Dieser Grundsatz wird in der Empfehlung 1/99 zum Thema 'Unsichtbare und automatische Verarbeitung von personenbezogenen Daten im Internet durch Software und Hardware' weiterentwickelt, die von der Arbeitsgruppe am 23. Februar 1999 angenommen wurde. 5093/98/EN/final, WP 17.

⁷² Siehe auch Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Diensteanbieter für Zwecke des Strafvollzugs, von der Arbeitsgruppe am 7. September 1999 angenommen.

Konvention der Menschenrechte und der Richtlinie 97/66/EG durchgeführt wird. Jedenfalls sind groß angelegte Schnüffelaktionen verboten. Der Grundsatz der Zweckentsprechung, dessen Konsequenz das Verbot jeglicher ausforschenden oder generellen Überwachung ist, besagt, dass die staatlichen Behörden, soweit es sich um Verkehrsdaten handelt, zu diesen nur fallweise Zugang erhalten, aber niemals vorausgreifend und als allgemeiner Regelfall⁷³.

Speicherung und Überprüfung der Inhalte von E-Mails

Die Inhalte von E-Mails sind geheim zu halten und dürfen weder von Zwischenträgern noch von Maildienste-Anbietern gelesen werden, auch nicht aus sogenannten "Gründen der Netzwerksicherheit". Falls Antiviren-Software zum Überprüfen der beigefügten Dokumente benutzt wird, muss die installierte Software ausreichende Garantien bezüglich der Vertraulichkeit liefern. Werden Viren gefunden, müssen Diensteanbieter in der Lage sein, die Absender vor dem Vorhandensein von Viren zu warnen. Doch selbst in diesem Fall darf der E-Mail-Diensteanbieter die Inhalte der Nachrichten oder beigefügten Dokumente nicht lesen.

Die Datenschutzgruppe empfiehlt nachdrücklich, die Inhalte von E-Mails zu verschlüsseln. Dies ist besonders wichtig, wenn sie empfindliche personenbezogene Daten enthalten. Benutzerfreundliche Programme für die Verschlüsselung der Inhalte von E-Mails sind von den E-Mail-Diensteanbietern ohne zusätzliche Kosten zur Verfügung zu stellen. Zudem sollten die Diensteanbieter die Möglichkeit bieten, die elektronische Post aus ihren Mailservern über sichere Verbindungen auf die Computer der Nutzer herunter zu laden. Auch ist zu erwägen, ob nicht *Datenintegrität* und *Authentisierung* erforderlich sind.

Unerbetene E-Mails (*Spam*)

Wenn eine Firma eine E-Mail-Adresse unmittelbar bei einer Person erhebt, und zwar zum Zwecke des Versands von unerbetenen E-Mails durch diese Firma oder durch Dritte, an welche die Daten weitergegeben werden, muss die erstere Firma die betroffene Person zum Zeitpunkt der Erhebung der Adresse über diese Zwecke informieren. Dem Dateninhaber muss ferner das Recht eingeräumt werden, zum Zeitpunkt der Erhebung der Daten und jederzeit danach gegen den Gebrauch seiner Daten durch die ursprüngliche Firma und alle nachfolgenden Firmen, die Daten von der ursprünglichen Firma erhalten haben, durch einfache elektronische Mittel, wie zum Beispiel das Anklicken eines Feldes, das zu diesem Zwecke dient, Widerspruch einzulegen.

Eine Verwendung von E-Mail-Adressen, die in einem frei zugänglichen Bereich im Internet erhoben werden, für elektronischen Postversand steht im Widerspruch zum einschlägigen Gemeinschaftsrecht.

E-Mail-Verzeichnisse

Wie auch bei Telefonverzeichnissen muss der Dateninhaber gegenwärtig zumindest die Möglichkeit haben, gemäß den oben erwähnten Grundsätzen der Zweckentsprechung (Artikel 6 Absatz 1 Buchstabe b) der Richtlinie 95/46/EG) und dem Recht zur (nachträglichen) Entscheidung gegen eine Eintragung in Teilnehmerverzeichnissen ("Opt-out"-Regelung – Artikel 11 der Richtlinie 97/66/EG), zu beantragen, dass er in ein Verzeichnis nicht aufgenommen wird.

Ferner müssen Dateninhaber die Möglichkeit erhalten, sich in speziellen E-Mail-Adressenverzeichnissen eintragen zu lassen, die nicht für das Direktmarketing verwendet werden.

⁷³ Siehe diesbezüglich die Empfehlung der Arbeitsgruppe 2/99 über die Wahrung der Privatsphäre im Zusammenhang mit der Überwachung von Telekommunikationsverbindungen, angenommen am 3. Mai 1999, 5005/99/final, WP 18.

Es sei daran erinnert, dass dieses Recht im gegenwärtigen Richtlinienvorschlag zum Schutz der Privatsphäre im Telekommunikationsbereich dahingehend abgeändert werden soll, dass eine **vorherige** Einwilligung erforderlich ist ("Opt-in"-Regelung); dies wäre eine wichtige Verbesserung für die Dateninhaber.

KAPITEL 5: SURFEN AND SUCHEN

I. Einleitung

Die am meisten verbreitete Aktivität von Internet-Nutzern ist wohl der Besuch von Websites, um dort Informationen zu sammeln. Dies bedeutet, dass der Inhalt einer Dokumentenseite passiv betrachtet wird. Aber es lässt sich mit Websites auch in einer aktiveren Form Kontakt aufnehmen. Oft soll sich der Internet-Nutzer über einen *Hyperlink* weiterklicken, ein auf dem Bildschirm erscheinendes Werbefenster (Banner) öffnen oder zusätzliche Angaben in ein Formular eintragen. Alle diese Aktivitäten zusammen werden hier als 'Websurfen' bezeichnet. Zum Surfen wird dabei ein Web-Browser benutzt, der den Internet-Nutzer mit einem Webserver irgendwo im Internet verbindet.

Unter Datenschutzgesichtspunkten stellen sich dabei drei wichtige Fragen:

- Welche Angaben zu den Aktivitäten des Internet-Nutzers werden während des Websurfens erzeugt?
- Wo werden diese Angaben abgespeichert?
- Welche Angaben werden bei der Bereitstellung von Diensten durch Websites abgefragt?

Bei der letztgenannten Frage geht es um persönliche Daten, die ein Internet-Nutzer freiwillig preisgibt, und um die entsprechenden Bedingungen. Aber dieser Punkt soll hier nicht diskutiert werden, da es in diesem Kapitel um die personenbezogenen Daten geht, die im (technischen) Vorgang des Websurfens involviert sind. Die dabei aufeinander folgenden Schritte werden aufgezeichnet und eine Meldung der erzeugten personenbezogenen Daten ausgegeben.

II. Technischer Ablauf und beteiligte Akteure

Der Vorgang des Websurfens

- Telekommunikationsanbieter. Um ins Internet und damit zu einer bestimmten Website zu gelangen, nimmt der Internet-Nutzer in der Regel eine telefonische Verbindung mit einem *Internet-Diensteanbieter (ISP)* auf. Der Telekom-Anbieter protokolliert den Anruf beim *ISP*.
- Internet-Zugangsanbieter (IAP). Den Zugang zum *ISP* vermittelt ein Netzwerkszugangs-Server. Dieser Server zeichnet in der Regel die Anruferkennung der Verbindung auf. Die meisten IAP protokollieren den Benutzernamen, den Beginn und das Ende einer Verbindung und die dabei übermittelten Datenmengen. Es ist zu beachten, dass in einigen Fällen der Telekom-Anbieter auch die Rolle eines IAP übernimmt.
- Zuweisung der IP-Adresse. Sobald die Verbindung mit dem IAP hergestellt ist, weist dieser dem Internet-Nutzer für die Dauer der "Sitzung" eine dynamische IP-Adresse zu⁷⁴. Von diesem Zeitpunkt an werden alle Kommunikationsleistungen während einer Sitzung zu und von dieser IP-Adresse abgewickelt. Die IP-Nummer ist in allen Datenpaketen enthalten, die während der aufeinander folgenden Kommunikationsvorgänge übertragen werden. Zu beachten ist, dass die zugewiesene IP-Nummer immer aus einem bestimmten, dem IAP zugewiesenen Nummernvorrat stammt. Daher können Außenstehende

⁷⁴ Manchmal werden statische IP-Adressen verwendet, die über einen längeren Zeitraum auf den gleichen Benutzer verweisen. Statische IP-Adressen werden häufig dann benutzt, wenn alternative Zugangstechnologien (Breitbandtechnik, Standleitung, Mobiltelefon) verwendet werden. Da diese immer größere Verbreitung finden, nimmt der Anteil statischer IP-Adressen ständig zu.

ohne Schwierigkeiten den IAP ermitteln, von dem die IP-Datenpakete herkommen^{75 76}.

Im Anschluss daran wird der Internet-Verkehr beim *ISP* nach der sogenannten Port-Adresse sortiert, die den Dienst und das entsprechende *Protokoll* aufschlüsselt. Eine Anfrage zum Besuch einer Website erfolgt gewöhnlich mit einem HTTP-Protokoll. Beim *ISP* wird dieser Verkehr an der entsprechenden Port-Adresse erkannt. Er kann auch unmittelbar an einen *Router* übertragen werden, der den Internet-Nutzer mit den gewünschten externen Websites verbindet.

Oft wird die Anfrage an einen speziell dafür eingerichteten *Proxy-Server* übertragen. Dieser Server registriert die Anfrage nach einer bestimmten Website. Er enthält Kopien der Inhalte der am häufigsten besuchten Websites. Falls die vom Internet-Nutzer angefragte Website im *Proxy-Server* enthalten ist, braucht dieser lediglich die betreffende Website zu einer Aktualisierung der Änderungen aufzufordern, die seit dem Augenblick ihrer Speicherung im *Proxy-Server* vorgenommen wurden. Dieses Vorgehen sorgt für eine starke Verminderung des Datenflusses zwischen *ISP* und Website, da nur die Änderungen und nicht der volle Seiteninhalt weitergegeben werden. Der *Proxy-Server* kann eine detaillierte Liste der Besuche abspeichern, die während eines gegebenen Zeitraums bei den mit einer IP-Adresse verknüpften Websites stattgefunden haben. Diese Besuche können über die IP-Adresse und die Protokolle der Sitzungszeiten auf einen einzelnen Benutzer zurückgeführt werden.

- *Router*. Auf dem Pfad zwischen dem *ISP* und der besuchten Website passiert der Internet-Verkehr in der Regel verschiedene *Router*, die die Daten zwischen der IP-Adresse des Internet-Nutzers und der IP-Adresse der Website vermitteln. Im Hinblick auf die Speicherung von personenbezogenen Daten werden diese *Router* hier als neutrale Elemente betrachtet, obwohl spezielle Programme dazu benutzt werden könnten, um den Internet-Verkehr an diesen Punkten zu überwachen.
- Reguläre Websites. Sobald die Verbindung mit einer Website hergestellt ist, sammelt diese Angaben über den Besucher. Denn alle Anfragen sind mit der IP-Zieladresse (für die Antwort) ausgestattet. Die Website erfährt darüber hinaus, von welcher anderen Dokumentenseite aus der Internet-Nutzer weitergeleitet wurde (die vorangegangene Referenzseite bzw. deren URL ist bekannt). Die Angaben zu den Besuchen der Websites werden meist im 'Common Log File' gespeichert. Alle oben genannten Angaben können dazu genutzt werden, um mit Hilfe eines Protokoll-Analyseprogramms ein Informationspaket über den Verkehr zu und von einer Website und die Aktivitäten ihrer Besucher herzustellen.

Bei der Verbindung mit einer Website werden einige zusätzliche Angaben gesammelt, und zwar bei der Kommunikation zwischen der bei Internet-Nutzern am meisten verbreiteten Browser-Software und den besuchten Websites. Die daraus stammenden Daten werden häufig als 'chattering data' ("ausplaudernde Daten") bezeichnet. Dabei geht es in der Regel um Angaben zu folgenden Punkten⁷⁷:

- Betriebssystem
- Typ und Version des Browsers
- *Protokolle*, die beim Websurfen verwendet werden
- Website, über die der Nutzer weiterverwiesen wurde
- Wahl der Sprache
- *Cookies*

Eine Website verfügt über zusätzliche Möglichkeiten der Datenerhebung, wenn sie sogenannte *Cookies*⁷⁸ einsetzt. Dabei handelt es sich um Datensequenzen, die in Textdateien gespeichert und nach Wahl auf der

⁷⁵ In manchen Fällen können Dritte - z.B. Universitäten, Organisationen oder Unternehmen - selbst als *ISP* auftreten.

⁷⁶ In gewissem Umfang werden IP-Adressen auch nach geographischen Gesichtspunkten vergeben.

⁷⁷ Zu weiteren Details siehe Kapitel 2.

⁷⁸ Hier geht es um dauerhaft installierte, d.h. über die Dauer einer Sitzung hinaus verbleibende *Cookies*.

Festplatte des Internet-Nutzers abgelegt werden können, während eine Kopie bei der Website verbleibt. *Cookies* sind ein Standardelement des HTTP-Verkehrs und können als solche ungehindert im IP-Verkehr mitgeführt werden. Ein *Cookie* kann eine weltweit einmalige Zahlenkombination (GUI – Global Unique Identifier) enthalten, die eine bessere Zuordnung zu Personen als die dynamischen IP-Adressen ermöglicht. Solche *Cookies* erweitern die Fähigkeit von Websites, Angaben über ihre Besucher zu speichern und "personenbezogen" zu machen. Das *Cookie* kann regelmäßig von der Website abgefragt werden, um Internet-Nutzer zu identifizieren und sie bei einem erneuten Besuch wiederzuerkennen, aber auch um mögliche Passworte zu prüfen, den Kommunikationspfad während der Sitzung und innerhalb einer Website zu analysieren, Transaktionen, z.B. den Erwerb von Waren, aufzuzeichnen und um die Website besser an die Kunden anzupassen usw.

Cookies können unterschiedliche Eigenschaften haben: sie können dauerhaft oder nur auf begrenzte Dauer installiert werden; in diesem Fall werden sie als "*Session-Cookies*" bezeichnet. Manchmal können sie von Nutzen sein, wenn es um die Bereitstellung einer bestimmten Dienstleistung durch das Internet oder um die Erleichterung des Internet-Surfens geht. So benutzen zum Beispiel bestimmte gewerbliche Websites *Cookies*, um ihre Benutzer bei jeder Wiederholung des Kontakts zu identifizieren und ihnen damit zu ersparen, sich bei jeder Durchsicht des neu eingegangenen Materials bei der Website erneut anmelden zu müssen.

Die Folgen des Einsatzes von *Cookies* für die Privatsphäre sollten dennoch nicht unterschätzt werden. Diese Frage wird im Abschnitt über die rechtlichen Aspekte des Themas weiter unten in diesem Kapitel näher erörtert.

- *Portal-Websites*

Wegen der zunehmenden Komplexität des Internets stellen Internet-Nutzer häufig den Kontakt mit der von ihnen gewünschten Website über eine sogenannte *Portal-Site* her, die einen geordneten Überblick über Weblinks bietet.

Häufig enthalten solche *Portal-Sites* Verknüpfungen zu kommerziellen Websites und können daher mit einem Einkaufszentrum verglichen werden, unter dessen Dach eine Vielzahl von Geschäften versammelt ist. Solche *Portal-Websites* sammeln Angaben wie andere Websites auch, darüber hinaus aber können sie Angaben zu Besuchen bei allen Websites sammeln, die 'hinter' dem *Portal* liegen.

Portal-Websites werden stets von *Internet-Diensteanbietern* geführt, können zuweilen aber auch in deren Besitz sein. In diesen Fällen verfügt der *ISP* über die Möglichkeit, Daten über die Besuche der Internet-Nutzer bei Websites "hinter" diesem *Portal* zu sammeln und so ein umfassendes Benutzerprofil zu erstellen.

Die niederländische Datenschutzbehörde (Registratiekamer) kam in einem Bericht⁷⁹ über den Schutz der Privatsphäre im Internet, der auf Untersuchungen der Lage in 60 niederländischen *ISP* beruht, zum Schluß, dass es den Anbietern von Inhalten (in diesem Fall den *ISP*, die Inhaber von *Portalen* sind) möglich ist zu wissen, wie viele Anzeigen geschaltet wurden, wie oft bestimmte Nutzer einen E-Shop besucht haben, welche Produkte sie gekauft und wieviel sie dafür bezahlt haben.

- Anbieter zusätzlicher Dienstleistungen

Die von Websites gesammelten Daten werden manchmal (automatisch) an nicht unmittelbar an der Kommunikation beteiligte Dritte übermittelt (z.B. an Unternehmen wie Nedstat, die auf die Analyse von

⁷⁹ Siehe Bericht der Registratiekamer (ARTZ, M.J.T., und VAN EIJK, M.M.M.), *Klant in het web: Privacywaarborgen voor Internettoegang*, Achtergrondstudies en verkenningen, 17. Juni 2000, abrufbar unter: www.registratiekamer.nl

In diesem Bericht wird der Sachverhalt betont, dass in den Niederlanden fast jeder Zugangsanbieter eine eigene Homepage besitzt, die auch als *Portal* zum Einstieg in das Netz-Surfen benutzt wird.

Webstatistiken spezialisiert sind). Dies kann den Zweck haben, eine Erhebung statistischer Daten über die Besuche auf Websites zu schaffen, die den Inhabern der betreffenden Websites wieder verkauft werden. Werbefenster sammeln in der Regel mit Hilfe von *Cookies* Angaben über die von einer Person besuchten Websites. Dienstleistungsanbieter wie DoubleClick oder Globaltrash speichern Angaben über Besuche bei sämtlichen Websites, in denen sie Anzeigen schalten. Anhand dieser Daten können Profile der Vorlieben der einzelnen Internet-Nutzer entwickelt werden, die anschließend zur Anpassung der Websites an Kundenwünsche benutzt werden.

Das Surfen aus der Sicht des Internet-Nutzers

Ein PC, auf dem eine Browsersoftware installiert ist, lädt in vielen Fällen nach dem Start eine bestimmte Startseite aus dem Web. Diese Startseite kann *Hyperlinks* enthalten, die zum Besuch anderer Websites oder Suchmaschinen aktiviert werden können. Beim Durchblättern von Bildschirmseiten ("browsen") fordert das Browserprogramm eines Internet-Nutzers einen Server (der sich an einem beliebigen Standort auf der Erde befinden kann) auf, eine bestimmte Dokumentenseite (die durch ihre gleichbleibende Kennung - URL - gekennzeichnet ist) zu übermitteln, die sich auf diesem Webserver befindet. Durch das Anklicken eines *Hyperlinks* laden also Internet-Nutzer die angefragte Dokumentenseite auf ihren Computer herunter.

Nach der Herstellung der Verbindung zu ihrem *ISP* entscheiden sich die Internet-Nutzer beim Surfen in der Regel für eine der folgenden Vorgehensweisen:

- Sie wenden sich unmittelbar an die gewünschte Website durch die Eingabe der URL, z.B. www.amazon.com. Die URL enthält zugleich auch das *Protokoll*.
- Sie erreichen die Website über eine Referenzstelle (*Portal-Website*), die *Hyperlinks* zu anderen Seiten enthält. Solche *Portal*-Dienste werden zunehmend populärer, da die Zahl der Dokumentenseiten ständig steigt und die Internet-Nutzer immer stärker auf Hilfestellungen angewiesen sind, um das interessierende Material zu finden.
- Sie finden in Frage kommende Websites durch vorherige Anfrage bei einer Website, die eine Suchmaschine einsetzt. Suchmaschinen verwenden die Technik der Indexerstellung durch Stichwörter. Der Nutzer gibt ein oder mehrere Stichwörter ein und startet die Suche. Die Suchmaschine sucht dann in ihrer eigenen Indexdatenbank nach den Titeln der entsprechenden Websites und ihren URL-Adressen. Die Suchmaschine ist besonders gut in der Lage, Personenprofile zusammen zu stellen, da sie die vom Internet-Nutzer eingegebenen Suchbegriffe und die daraufhin besuchten Websites sammelt und speichert. Die Zuordnung zu Personen wird häufig mit Hilfe von *Cookies* hergestellt. Verschiedene Suchmaschinen bieten auch stärker auf den Einzelnen zugeschnittene Dienste an, bei denen die Internet-Nutzer zu näheren Angaben über persönliche Vorlieben aufgefordert werden, um dann etwa regelmäßige Aktualisierungen der Websites zu einem bestimmten Thema zu erhalten⁸⁰.

Überblick über die wichtigsten, in verschiedenen Abschnitten des Websurfens erzeugten und gespeicherten Daten

	Erzeugte und/oder gespeicherte Daten	Bemerkungen
1. Telekom-Anbieter	Verkehrsdaten der Verbindung zum <i>ISP</i>	Kann zugleich auch <i>ISP</i> sein

⁸⁰ In diesem Zusammenhang ist ein Hinweis auf den gemeinsamen Standpunkt der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation zum Thema Suchmaschinen relevant, den sie auf ihrer Sitzung in Hongkong am 15. April 1998 angenommen hat, und der abgerufen werden kann unter: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm

2. ISP: Netzwerk-zugangs-Server	Anrufkennung, IP-Adresse, Sitzungsdaten	
3. ISP: Proxy-Server	Von einer IP-Adresse aus besuchte Websites zu einer bestimmten Zeit	
4. Router	IP-Adresse	
5. Websites	IP-Adresse, URL der vorherigen Website, Sitzungsdaten (Zeitpunkt und Art der Transaktion), Bezeichnung und Umfang der übermittelten Dateien, Cookies	Im 'Extended Common Log File' zusammen gestellt
6. Portal-Sites	Sammelangaben über Besuche bei den von dort aus zu öffnenden Websites, Cookies	Möglichkeit der Erstellung vollständiger Nutzerprofile (Kommunikations- und Verhaltensdaten der Nutzer, die vom ISP aus erreichbar sind)
7. Diensteanbieter (auch Suchmaschinen)	Gesammelte Protokollanalysen aus den Websites, aus Websites über Cookies zusammen getragene Daten/Profile, Suchmaschinen: von Internet-Nutzern eingegebene Stichwörter	z.B. NedStat z.B. DoubleClick

III. Gefahren für die Privatsphäre

Millionen von Internet-Nutzer in der ganzen Welt surfen häufig im World Wide Web oder suchen Informationen im Internet. Diese Aktivitäten sind jedoch nicht frei von Risiken, was den Schutz der Privatsphäre angeht.

Bei der Nutzung des Internets werden etliche Angaben erfasst und in einer Weise bearbeitet, die dem Dateninhaber verborgen bleibt. Internet-Nutzer sind sich manchmal nicht darüber im Klaren, dass ihre personenbezogenen Daten erfasst und verarbeitet wurden und für ihnen unbekannt Zwecke verwendet werden können. Der Dateninhaber weiß nichts von dieser Verarbeitung und hat nicht die Entscheidungsfreiheit, über sie zu entscheiden⁸¹.

Weitere Risiken bestehen, wenn Daten, die bei den Surf-Aktivitäten des Internet-Nutzers erhoben wurden, mit anderen bereits vorhandenen Angaben über denselben Teilnehmer verknüpft werden können. Die Furcht vor solchen Verknüpfungen von personenbezogenen Daten über Internet-Nutzer war in der Diskussion über die Fusion der Internet-Werbeagentur DoubleClick mit dem Marktforschungsunternehmen Abacus Direct sehr gegenwärtig.

Es bestand die Befürchtung, dass im Falle einer Fusion beider Firmen die DoubleClick-Datenbank mit ihren Angaben zu Internet-Nutzergewohnheiten durch Querverweise mit der Abacus Direct-Datenbank

⁸¹ Die Arbeitsgruppe Datenschutz hat dieses Thema bereits in ihrer Empfehlung 1/99 zum Thema 'Unsichtbare und automatische Verarbeitung von personenbezogenen Daten im Internet durch Software und Hardware' behandelt, die am 23. Februar 1999 angenommen wurde; 5093/98/EN/final, WP 17.

verknüpft werden würde, in der konkrete Namen und Adressen mit detaillierten Angaben zu Kundenkaufgewohnheiten enthalten sind⁸².

Die Fusion fand im November 1999 statt. Nach den Angaben, die auf der DoubleClick-Website dazu gemacht wurden⁸³, werden die von Besuchern einer 'Abacus Alliance'-Website freiwillig gemachten Namens- und Adressenangaben von Abacus mittels eines "Matchcodes" und eines *Cookie* von DoubleClick mit weiteren Angaben über die betreffende Person in Verbindung gebracht.

Zu den Angaben, die in der Abacus-Online-Datenbank enthalten sind, gehören Name, Adresse, Daten zu Einzelhandels-, Katalog- und Online-Käufen in der Vergangenheit und demographische Daten der einzelnen Internet-Nutzer. Die Datenbank enthält außerdem die von Websites und anderen Geschäftspartnern von DoubleClick bei den Internet-Nutzern erhobenen Angaben, die diesen nicht unmittelbar zuzuordnen sind. nach Aussagen von DoubleClick wurden die Datenbanken von DoubleClick und Abacus bislang nicht miteinander verknüpft.

Neue Überwachungssoftware

Die neuen Überwachungstechnologien, die den *ISP* heute zur Verfügung stehen, werden wesentlich mehr Angaben über Verkehrsabläufe und inhaltliche Vorlieben erzeugen, als dies schon bisher in öffentlichen Telekom-Vermittlungsnetzwerken (PSTN) der Fall war. Solche Technologien versprechen im Internet das Äquivalent für PSTN-Einzelverbindungsnachweise zu liefern, und mehr.

Diese Art von Softwareprogrammen sind unter dem Spitznamen "E.T.-Anwendungen" bekannt, *"denn wenn sie sich einmal im Computer des Benutzers eingenistet und herausgefunden haben, was sie wissen wollen, tun sie das, was Steven Spielbergs Außerirdischer tat: sie rufen 'zu Hause' an"*⁸⁴.

Beispielsweise bietet Narus, ein privates Softwareunternehmen in Palo Alto, Kalifornien (USA), den *ISP* Software an, die den Datenfluss überwacht und jedes Datenpaket durchsucht, um dessen Header und Information zum Inhalt zu entnehmen⁸⁵. Narus gibt an, mit wichtigen Softwareanbietern wie Bull, Cisco und Sun Microsystems eng zusammen zu arbeiten. Diese Software kann zur Identifikation und Messung von Internet-Telefonie und anderen Anwendungen (z.B. Web, E-Mail oder IP-Fax) genutzt werden, zielt aber auch auf die Überwachung von potentiell kostenpflichtigen Inhalten des IP-Verkehrs (z.B. urheberrechtlich geschütztes Material, für das Lizenzgebühren gezahlt werden müssen, oder die Nutzung einer Anwendung auf Anforderung, oder Audioclips). Die Narus-Software erstattet den *ISP* in Echtzeit Bericht über die am häufigsten besuchten Websites und über die Art der betrachteten und heruntergeladenen Inhalte⁸⁶.

Alexa⁸⁷ ist ein Werkzeug, das einem Browser hinzugefügt werden kann, um den Nutzer beim Surfen zu begleiten und ihm zusätzliche Informationen über die besuchte Website (über den eingetragenen

⁸² Siehe EPIC Alert 6.10, 30. Juni 1999. Die gleichen Befürchtungen wurden bereits während der Verhandlungen zur Rechtssache Harriet M. Judnick versus DoubleClick beim Superior Court des Bundesstaates Kalifornien zur Sprache gebracht.

⁸³ www.doubleclick.net:8080/privacy_policy/ Diese Fusion wird in Kapitel 7, elektronischer Geschäftsverkehr im Internet, ausführlicher zur Sprache gebracht.

⁸⁴ Titelgeschichte im Time-Magazine vom 31. Juli 2000 von Adam COHEN, *How to protect your privacy: who's watching you? They're called E.T. programs. They spy on you and report back by "phoning home". Millions of people are unwittingly downloading them (Wie die eigene Privatsphäre schützen: Wer beobachtet Sie? Sie werden E.T.-Programme genannt. Sie spionieren bei Ihnen und erstatten Bericht, indem sie 'zu Hause' anrufen. Millionen Menschen laden sie herunter, ohne es zu wissen).*

⁸⁵ <http://www.narus.com>

⁸⁶ Siehe PALTRIDGE, Sam, *Mining and Mapping Web Content*, in: Info, The Journal of policy, regulation and strategy for telecommunications, information and media, Bd. 1, Nr. 4, August 1999, S. 327-342.

⁸⁷ <http://www.alexa.com>

Eigentümer der Website, ihre Beliebtheit und Beurteilung) und Vorschläge für den Besuch verwandter Websites zu liefern. Als Gegenleistung für die Bereitstellung dieses Benutzerdienstes hat sich Alexa eine der größten Datensammlungen über Nutzungsmuster im Web geschaffen. Amazon zahlte 250 Millionen US-Dollars in Aktien, um Alexa Anfang 1999 zu erwerben. In ihrer Datenschutzerklärung gibt Alexa an, dass es anonym bleibende Informationen über die Webnutzung erfasst, für die Webnutzungsprotokolle und *Cookie*-Daten ausgewertet werden.

Alexa stellt neben anderen Produkten das Programm zBubbles her, ein Werkzeug für Online-Einkäufe, das Surfdaten über die Nutzer erfasst, um ihnen Produktempfehlungen und vergleichende Kaufberatung usw. anbieten zu können. Laut den im Time Magazine veröffentlichten Angaben⁸⁸ sendet zBubbles auch dann Informationen zurück an Alexa, wenn Internet-Surfer nicht einkaufen. Dieses Produkt ist dazu bestimmt, während der gesamten Internet-Sitzung auf dem Bildschirm installiert zu sein, auch wenn die meisten Nutzer nicht die ganze Zeit mit Einkäufen befasst sind.

Ein weiteres interessantes Beispiel für Überwachungssoftware ist Radiate, früher bekannt unter dem Namen Aureate. Radiate ist ein Werbeunternehmen, das mit den Herstellern von *Shareware* zusammenarbeitet. Berichten zufolge⁸⁹ wurden Radiate-Anzeigen von E.T.-Software begleitet, die sich in den Computern von 18 Millionen Menschen einnistete und deren Internet-Verbindung nutzte, um Bericht darüber zu erstatten, welche Anzeigen von diesen angeklickt wurden. Die Urversion der Radiate-Software, die noch immer in unzähligen Computern vorhanden ist, wurde so geschrieben, dass sie auch dann noch Rückmeldungen erstattet, wenn die *Shareware* bereits gelöscht ist, die sie dorthin beförderte. Internet-Nutzer benötigten zum Löschen der Datei ein spezielles Tool, das später vom Hersteller auf seiner Website zur Verfügung gestellt wurde.

Zur Zeit gibt es Hunderte von E.T.-Anwendungen. Mehr als 22 Millionen Menschen sollen sie aus dem Netz heruntergeladen haben⁹⁰. E.T.-Überwachungsprogramme sind wiederum ein Beispiel für Technologien, die personenbezogene Daten der Nutzer ohne ihr Wissen verarbeiten (unsichtbare Verarbeitung): die meisten Computerbenutzer haben keine Ahnung, dass diese Softwareprogramme in ihren Computern platziert worden sind.

Häufig erklären die Hersteller dieser E.T.-Anwendungen, dass sie zwar in der Lage wären, Daten über Computerbenutzer zu erfassen, diese Daten aber dennoch nicht auf Individuen beziehen. Dies allein bietet aber keine hinreichende Garantie für die Nutzer, da angesichts des kommerziellen Wertes von individualisierten Daten die Unternehmen, die sie erfassen, jederzeit ihr Vorgehen ändern können. Das potentielle Risiko des Datenmissbrauchs bleibt bestehen⁹¹.

IV. Rechtliche Beurteilung

Die rechtliche Beurteilung des Surfens und Suchens im Internet geht von der Voraussetzung aus, dass beide Datenschutzrichtlinien (Richtlinien 95/46/EG und 97/66/EG) im Prinzip auf das Internet anzuwenden sind⁹².

⁸⁸ A. COHEN im Time-Magazine (op cit).

⁸⁹ A. COHEN im Time-Magazine (op cit).

⁹⁰ A. COHEN im Time-Magazine (op cit).

⁹¹ A. COHEN in Time- Magazine (op cit.).

⁹² Siehe Arbeitsdokument WP 16: *Verarbeitung personenbezogener Daten im Internet*, von der Arbeitsgruppe am 23. Februar 1999 angenommen, 5013/99/EN/final.

Hauptvorgaben der allgemeinen Richtlinie 95/46/EG: Grundsatz der Zweckentsprechung, der Verarbeitung nach Treu und Glauben und der Unterrichtung der Dateninhaber

Drei Aspekte der allgemeinen Richtlinie verdienen in diesem Kapitel besondere Aufmerksamkeit: der Grundsatz der Unterrichtung der Dateninhaber, der Grundsatz der Zweckentsprechung und der Grundsatz der Verarbeitung nach Treu und Glauben.

Unterrichtung der Dateninhaber

Im Internet verlaufen Datenströme sehr schnell, und die üblichen Spielregeln für die Unterrichtung der Dateninhaber über die Verarbeitung und Zwecke werden häufig ignoriert. In manchen Fällen geschieht die Verarbeitung der Daten durch Soft- oder Hardware, deren Existenz oder Wirkungsgrad Internet-Nutzern nicht in vollem Umfang bewusst ist (z.B. durch *Cookies* oder E.T.-Softwareanwendungen).

Die Arbeitsgruppe hat sich mit diesen Fällen in ihrer Empfehlung 1/99⁹³ auseinandergesetzt. Darin unterstrich sie, dass eine verbindliche Voraussetzung für die berechtigte Verarbeitung von personenbezogenen Daten die Unterrichtung der Dateninhaber ist, denen damit die betreffende Verarbeitung bewusst gemacht wird. Internet-Software- und Hardwareprodukte sollten die Internet-Nutzer darüber informieren, welche Daten sie erfassen, speichern oder weitergeben sollen, und zu welchem Zweck diese Daten benötigt werden.

Internet-Software- und Hardwareprodukte sollten ferner den Dateninhabern die Möglichkeit geben, auf alle über sie erfassten Daten zu einem beliebigen späteren Zeitpunkt leicht zuzugreifen.

Die Geschwindigkeit des Datenflusses im Internet kann nicht als Ausrede dafür herhalten, um die Vorschriften der allgemeinen Richtlinie nicht zu erfüllen. In Wirklichkeit ist gerade das Internet ein Medium, das eine rasche und einfache Unterrichtung der Dateninhaber ermöglicht. Sobald personenbezogene Daten erhoben werden, sind dem Dateninhaber substantielle Informationen⁹⁴ in der Weise zu übermitteln, dass eine faire Verarbeitung der personenbezogenen Daten gewährleistet ist, also je nach Situation entweder unmittelbar auf dem Bildschirm oder dem Formular, über das die Datenerhebung stattfindet, oder aber über einen Hinweis auf dem Bildschirm (etwa wenn *Cookies* versandt werden). Den Dateninhabern muss die Möglichkeit gegeben werden, ein entsprechendes Feld anzuklicken, wenn sie einer Verarbeitung ihrer Daten nicht zustimmen oder weitere Informationen erhalten möchten.

Manche Websites platzieren Datenschutzhinweise, in denen Angaben über die von ihnen verarbeiteten Daten und die Ziele ihrer Verarbeitung sowie zur Art und Weise enthalten sind, in der Dateninhaber ihre Rechte ausüben können. Dies ist jedoch nicht immer der Fall, und selbst dort, wo Datenschutzhinweise angezeigt werden, enthalten sie nicht immer alle erforderlichen Informationen.

Die Arbeitsgruppe steht der Veröffentlichung von sorgfältig erarbeiteten und vollständigen Datenschutzhinweisen sehr wohlwollend gegenüber, empfiehlt aber auch nachdrücklich die Unterrichtung der Dateninhaber unmittelbar auf dem Bildschirm in Form von Informationsflächen, die im Augenblick der Datenerfassung auf dem Bildschirm erscheinen, ohne dass die Dateninhaber Maßnahmen zum Erhalt dieser Informationen treffen müssen, da Internet-Nutzer nicht immer alle Datenschutzhinweise der von ihnen besuchten Websites lesen, wenn sie von einer Site zur nächsten weitersurfen.

Damit sie mit der gebotenen Sorgfalt unterrichten können, sollten Datenschutzhinweise nicht zu lang ausfallen und klar strukturiert sein und in eindeutiger und verständlicher Sprache zuverlässige Angaben

⁹³ Empfehlung 1/99 zum Thema "Unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet mit Hilfe von Software und Hardware", angenommen von der Arbeitsgruppe am 23. Februar 1999, 5093/98/EN/final, WP 17.

⁹⁴ Zu den Angaben, die diese Texteinblendungen enthalten müssen, gehören mindestens ausführliche Hinweise darauf, wer die Verarbeitung der Daten kontrolliert, welche Zwecke ihre Verarbeitung verfolgt und, wo möglich, auf das Recht, die Verarbeitung zu untersagen.

über die Datenschutzmaßnahmen der Website enthalten. Die Arbeit der OECD auf diesem Gebiet (Datenschutzgenerator oder Datenschutzassistent – "Privacy Wizard") könnten für die Erreichung dieser Ziele hilfreich sein, wenngleich der Einsatz eines Datenschutzassistenten allein keine Einhaltung der europäischen Richtlinien garantiert.

In der Praxis reichen die Datenschutzhinweise an sich nicht aus, da die veröffentlichten Datenschutzhinweise unter Datenschutzgesichtspunkten häufig nicht ausreichend Informationen enthalten. Eine kürzlich durch EPIC⁹⁵ in den USA durchgeführte Untersuchung über die Datenschutzpolitiken bei den 100 wichtigsten E-Commerce-Websites zeigte, dass nur wenige der am stärksten besuchten Websites ein angemessenes Maß an Datenschutz gewährten. Tatsächlich erfüllte keine dieser Websites wesentliche Bestandteile fairer Informationsgepflogenheiten, die in dieser Untersuchung geprüft wurden⁹⁶.

Grundsatz der Zweckentsprechung

Die dem Dateninhaber zugänglich gemachten Informationen sollten in jedem Fall ausreichende und klare Aussagen zu Ziel oder Zwecken der Verarbeitung von Daten enthalten. Artikel 6 der allgemeinen Richtlinie verbietet die Weiterverarbeitung von Daten für damit nicht zu vereinbarende Zwecke.

Dieser Grundsatz ist für solche Websites von besonderer Bedeutung, die Angaben von Internet-Nutzern über ihr Surfverhalten erfassen, ferner für Softwareprogramme, die vom Internet-Nutzer beauftragt werden, ihr Internet-Verhalten für einen bestimmten Zweck zu überwachen, aber nicht für andere (unbekannte) Zwecke, und ferner für *Internet-Diensteanbieter*.

Die Navigationsdaten über Internet-Nutzer dürfen von den *Internet-Diensteanbietern* prinzipiell nur insoweit erfasst werden, als sie benötigt werden, um den Nutzern einen bestimmten Dienst anzubieten, hier den Besuch der Websites, wenn sie dies wünschen. *Internet-Diensteanbieter* behaupten gelegentlich, sie müssten diese Daten aufbewahren, um die Leistungsfähigkeit ihrer Systeme zu überwachen. Für diese Zwecke sind aber keine identifizierbaren Daten erforderlich, da es möglich ist, die Leistungsfähigkeit eines Systems auf der Basis der zusammen gefassten Daten zu messen und zu überwachen.

Ein aktueller Bericht der Registratiekamer⁹⁷ kam zu dem Schluß, dass *ISP*, wenn sie individuelle Verkehrsdaten über Internet-Nutzer aufbewahren, dies nicht im Rahmen ihrer Aufgaben als Zugangsanbieter tun. Solche Daten sind in erster Linie für ihre Aktivitäten als Anbieter von Inhalten interessant. Man muss sich im klaren darüber sein, dass es sich dabei um eine vollkommen andere Zweckbestimmung handelt.

Nützlich wäre es, wenn der Grundsatz der Zweckentsprechung in die technischen Mittel eingebaut werden könnte. Dies wäre auch als eine Art Technologie zur besseren Absicherung der Privatsphäre anzusehen⁹⁸.

Verarbeitung nach Treu und Glauben

Artikel 6 der allgemeinen Richtlinie enthält eine Anzahl von Grundsätzen, die dazu dienen sollen, einen fairen Umgang mit personenbezogenen Daten zu gewährleisten. Einer davon ist der Grundsatz der Zweckentsprechung, der im vorangehenden Absatz behandelt wurde.

Artikel 6 besagt aber ferner, dass personenbezogene Daten nicht länger als für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die eine Identifizierung der betroffenen Personen ermöglicht. Dies bedeutet, dass die Daten,

⁹⁵ Untersuchung "Surfer Beware III: Privacy Policies Without Privacy Protection", EPIC Alert 7.01, 12. Januar 2000. Abrufbar unter: www.epic.org/reports/surfer-beware.html

⁹⁶ Die "American Fair Information Practices" dienen als Orientierungsrichtlinien für den Schutz von Personendaten in den USA.

⁹⁷ *Klant in het web: Privacywaarborgen voor Internettoegang* (op cit.)

⁹⁸ Siehe unten, Kapitel 9.

sobald sie in einer Art und Weise anonymisiert sind, die es unmöglich macht, sie mit den betroffenen Personen zu verknüpfen, für andere Zwecke verwendet werden können, z.B. zur Messung der Leistungsfähigkeit des von einem *ISP* angebotenen Dienstes oder zur Ermittlung der Besucherzahl einer Website.

Große Suchmaschinen führen Protokolle über Suchanfragen in Form von Verzeichnissen der Suchanfragen in Kombination mit anderen Angaben wie etwa den dabei verwendeten Suchbegriffen⁹⁹. Die verwendeten Stichwörter sind für Unternehmen interessant, die versuchen, *Meta-Tags* für Dokumentenseiten auszuwählen, und für die Messung der Online-Nachfrage nach Inhalten, die sich auf ein bestimmtes Produkt, ein Unternehmen oder einen Markennamen beziehen. Wenn keine Verknüpfung zwischen dem Suchanfragenprotokoll und der Identität der Internet-Nutzer besteht, die Stichwörter eingegeben haben, gibt es keine gesetzlichen Hindernisse für eine Aufbewahrung dieser zusammengefassten Daten.

Sofern sie nicht anonymisiert werden, dürfen Daten über das Suchen und Surfen im Internet nach Abschluss der Internet-Sitzung nicht länger aufbewahrt werden. Dieser Aspekt soll bei der Behandlung der Vorschriften der besonderen Richtlinie über den Schutz der Privatsphäre im Bereich der Telekommunikation hinsichtlich der Verkehrsdaten detaillierter erklärt werden.

Bei Überlegungen bezüglich der Rechtmäßigkeit von Datenverarbeitungszwecken muss auch Artikel 7 der Richtlinie einbezogen werden. Dieser Artikel stellt verschiedene Voraussetzungen für eine zulässige Verarbeitung auf, u.a. die Einwilligung der betroffenen Personen und ein ausgewogenes Verhältnis zwischen den berechtigten Interessen der für die Verarbeitung Verantwortlichen und den Grundrechten der Dateninhaber. An diese Interessenabwägung muss der für die Verarbeitung Verantwortliche stets denken, wenn er Daten eines Internet-Nutzers erfasst.

Zentrale Bestimmungen der besonderen Richtlinie über den Schutz der Privatsphäre im Bereich der Telekommunikation

Wie aus der Tabelle in Kapitel 3 ersichtlich, gibt es einige Bestimmungen der Telekommunikations-Richtlinie, die von besonderer Bedeutung sind, wenn vom Surfen und Suchen im Internet die Rede ist.

Auch wenn sich der Titel der Richtlinie 97/66/EG auf den Bereich der Telekommunikation im allgemeinen bezieht, ist doch klar, dass die in ihrem Wortlaut verwendete Terminologie unmittelbar auf der ISDN-Technologie beruht. In den meisten Bestimmungen dieser Richtlinie werden Begriffe wie etwa "Anrufe" verwendet, die auf die herkömmliche und die ISDN-Fernmeldetechnik zurückgehen und die Anwendung auf Internet-Dienste nicht ganz einfach machen. Dennoch lassen sich Internet-Dienste gewöhnlich in den Anwendungsrahmen der Richtlinie einbeziehen, wenngleich dabei einige Schwierigkeiten bestehen, wie aus den folgenden Abschnitten ersichtlich wird.

Viele terminologische Probleme werden allerdings durch den Wortlaut des Vorschlags vom 12. Juli 2000 für eine Neufassung der Richtlinie gelöst¹⁰⁰. In dieser Vorlage werden eine Reihe von Begriffsbestimmungen auf den neuesten Stand gebracht, so dass alle unterschiedlichen Typen von Vermittlungsdienstleistungen bei der elektronischen Kommunikation abgedeckt werden, unabhängig davon, welche Technologie Verwendung findet.

Die Verwendung des Begriffs "Anruf" etwa wird nunmehr auf solche Fälle eingeschränkt, in denen sich der Gesetzgeber eindeutig auf Telefonanrufe beziehen will; dies wird durch die Aufnahme der Definition

⁹⁹ Siehe PALTRIGDE, S., *Search engines and content demand*, in *Mining and Mapping Web Content*, in: Info, The Journal of policy, regulation and strategy for telecommunications, information and media, Bd. 1, Nr. 4, August 1999, S. 330-333.

¹⁰⁰ KOM (2000) 385 endg.

dieses Worts in Artikel 2 Buchstabe e) deutlich gemacht¹⁰¹. In allen anderen Fällen wird im Text der Begriff "Kommunikation" oder "Kommunikationsdienste" verwendet.

In den folgenden Abschnitten werden die wichtigsten Vorschriften der Richtlinie 97/66/EG kommentiert. Soweit dies zweckmäßig ist, werden dabei die Veränderungen herangezogen, die im neuen Vorschlag für eine neu gefasste Richtlinie enthalten sind.

Artikel 4: Sicherheit

Die Anbieter von Telekommunikationsdiensten müssen angemessene Sicherheitsvorkehrungen treffen, die den aktuellen Stand der Technik berücksichtigen. Diese Maßnahmen müssen den bestehenden Risiken angemessen sein.

Für die Anbieter von *Routern* und Anschlussverbindungen ist diese Vorschrift von besonderer Bedeutung, da diese Einrichtungen sehr große Informationsmengen befördern.

Im neuen Vorschlag bleibt dieser Artikel bis auf die Ersetzung des Ausdrucks "Telekommunikationsdienste" durch "elektronische Kommunikationsdienste" unverändert.

Artikel 5: Vertraulichkeit

Innerstaatliche Vorschriften müssen die Vertraulichkeit der Kommunikation sicherstellen. Sie verbieten insbesondere das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt.¹⁰²

Dieser Artikel ist auf verschiedene Akteure anwendbar, die an den Surf- und Suchaktivitäten im Internet beteiligt sind: Anbieter von *Routern* und Anschlussverbindungen, *Internet-Dienstanbieter* und generell Telekommunikationsanbieter.

Der Artikel bezieht sich im Prinzip auf den Inhalt der Übertragungen. Die Unterscheidung von Verkehrsdaten und Inhalten lässt sich jedoch im Internet-Kontext nicht ohne weiteres treffen, und schon gar nicht, wenn es um das Surfen geht. Surfdaten können im Prinzip als Verkehrsdaten betrachtet werden. Die Arbeitsgruppe ist allerdings der Meinung, dass das Surfen durch verschiedene Websites als eine Art Kommunikation zu betrachten ist und als solche in den Geltungsbereich von Artikel 5 fällt.

Das Surfverhalten eines Internet-Nutzers (dessen Navigationsdaten), der verschiedene Websites besucht, kann bereits viel über die stattgefundenene Kommunikation verraten. Die Kenntnis der Namen der besuchten Websites erlaubt in den meisten Fällen ziemlich genaue Rückschlüsse auf die stattgefundenene Kommunikation. Außerdem ist es für jeden, der mit den Verkehrsdaten ausgerüstet ist, einfach, die Websites zu besuchen und genau nachzusehen, welche Inhalte abgefragt wurden.

Die Arbeitsgruppe ist deshalb der Meinung, dass die Surfdaten eines Internet-Nutzers das gleiche Maß an Schutz erhalten sollten wie "Inhalte". Diese Form der Kommunikation sollte demnach vertraulich bleiben. In diesem Sinne können auch *Clickstreams* als Datenfolgen betrachtet werden, die in den Geltungsbereich dieses Artikels fallen.

Der neue Vorschlag für eine überarbeitete Richtlinie enthält in ihrem Artikel 2 Absatz 1 Buchstabe c) eine Definition des Ausdrucks "Verkehrsdaten": das sind "*jegliche Daten, die im Zuge oder zum Zwecke der*

¹⁰¹ "(Weiterhin bezeichnet im Sinne dieser Richtlinie der Ausdruck ...) 'Anruf' eine über einen öffentlich zugänglichen Telefondienst aufgebaute Verbindung, die eine zweigleisige Echtzeit-Kommunikation ermöglicht". (Artikel 2).

¹⁰² Siehe hierzu die Empfehlung der Arbeitsgruppe 2/99 zur Wahrung des Schutzes der Privatsphäre im Zusammenhang mit der Überwachung der Telekommunikationsverbindungen, angenommen am 3.5. 1999, 5005/99/final, WP 18.

Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz verarbeitet werden". Navigationsdaten würden daher unter diese Definition fallen und als Verkehrsdaten zu behandeln sein.

Die Neufassung dieser Richtlinie hat große Verbesserungen gebracht, da Artikel 5 nicht mehr nur für die Inhalte von Nachrichten gilt, sondern auch für die damit zusammen hängenden Verkehrsdaten. Indem den inhaltlichen Daten und den entsprechenden Verkehrsdaten gleicher Schutz gewährt wird, tritt die (manchmal schwierige) Unterscheidung zwischen diesen Konzepten in den Hintergrund. Die Arbeitsgruppe begrüßt diese Verbesserung.

Artikel 6: Verkehrs- und Abrechnungsdaten

Verkehrsdaten sind **nach Beendigung der Übertragung** zu löschen oder zu anonymisieren. Um diesen Artikel im Internet-Kontext auslegen zu können, muss definiert werden, was als Verkehrsdaten und was als Inhalt einer Übertragung zu betrachten ist.

Dieser Artikel bezieht sich anscheinend stark auf leitungsvermittelte Übertragungen, die zwei oder mehr Gesprächspartner miteinander verbinden. Verkehrsdaten aber werden erst beim Prozess der Herstellung und Aufrechterhaltung solcher Verbindungen erzeugt. Dies macht die Anwendung des Artikels im Internet-Kontext besonders schwierig.

Bezogen auf den Internet-Verkehr gilt folgendes: die übermittelten Datenpakete sind in verschiedene 'Protokoll'-Kopfzeilen gepackt (z.B. TCP-Header, IP-Header und Ethernet-Header). Dieser *Protokoll*-Vorspann wird an jedem Netzknoten (*Router*) gelesen, den ein Datenpaket durchläuft, damit festgelegt werden kann, in welche Richtung es weitergeleitet werden soll. Eine Notwendigkeit dafür, dass die zwischen Sender und Empfänger liegenden Knoten nach der Weiterleitung des Datenpakets überhaupt irgendwelche Informationen aus dem Vorspann speichern müssen, ist aber nicht ersichtlich.

Die Verarbeitung der Angaben in den Kopfzeilen (in denen auch Daten zum Inhalt der Datenpakete enthalten sein können) sind als Verkehrsdaten im Sinne von Artikel 6 der Richtlinie 97/66/EG zu behandeln und daher zu anonymisieren oder zu löschen, sobald diese Daten nicht länger zur Aufrechterhaltung einer Verbindung benötigt werden; mit anderen Worten, sobald der Internet-Nutzer Zugang zur betreffenden Website erhalten hat.

Zweifelsohne fallen solche Daten wie das Anmeldeprotokoll von "Sitzungen" (Zeitpunkt der An- und Abmeldung, übermittelte Datenmenge, Zeitpunkt des Beginns und Abschlusses einer Sitzung usw.) in den Geltungsbereich von Artikel 6.

Die Verzeichnisse der von Internet-Nutzern besuchten Websites (Surfverhalten) müssen auf jeden Fall als Verkehrsdaten betrachtet werden (und können möglicherweise den gleichen Schutz erhalten wie die Inhalte). Vor allem aber müssen diese Listen **nach Beendigung einer Internet-Sitzung** prinzipiell gelöscht werden.

In diesem Zusammenhang ist die Tatsache von Interesse, dass ein *Protokoll* der eigenen Surfaktivitäten im PC des Internet-Nutzers aufbewahrt wird. Dies kann vor allem dann ein Problem sein, wenn mehrere Personen am gleichen Computer arbeiten.

Die Arbeitsgruppe hat bereits früher ihren Standpunkt zur Frage der Aufbewahrung von Verkehrsdaten durch die *ISP* zum Zwecke der Strafverfolgung geäußert¹⁰³. In dieser Empfehlung heißt es, dass Verkehrsdaten, die nicht für Abrechnungszwecke benötigt werden, grundsätzlich nicht aufbewahrt werden sollten. Bei kostenlosen *ISP* gäbe es also keinen Grund zur längeren Aufbewahrung von Verkehrsdaten, als für deren normale Operationen erforderlich ist, da diese für Abrechnungszwecke nicht benötigt werden.

¹⁰³ Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch *Internet-Diensteanbieter* für Zwecke des Strafvollzugs, angenommen am 7. September 1999, 5085/99/EN/final, WP 25.

In der neu gefassten Richtlinie wird die Formulierung "nach Beendigung der Verbindung" (*upon termination of the call*) durch "nach Beendigung der Übertragung" (*upon completion of the transmission*) ersetzt, was wesentlich eindeutiger ist. Daten zum Surfverhalten sind also sofort zu löschen, sobald die Internet-Übertragung beendet ist.

Der neue Text führt die Möglichkeit einer Weiterverarbeitung personenbezogener Daten für die Bereitstellung von Diensten mit Zusatznutzen oder für den Zweck der Vermarktung eigener elektronischer Kommunikationsdienstleistungen ein, wenn die Teilnehmer darin eingewilligt haben. Der Ausdruck "Dienste mit Zusatznutzen" wird in diesem Vorschlag aber nicht näher bestimmt; die Arbeitsgruppe hält es für notwendig klarzustellen, was in diese Begriffsbestimmung eingeschlossen werden soll, um zugleich die Reichweite dieses Verwendungszwecks und neue Risiken für den Schutz der Privatsphäre in Grenzen zu halten. In diesem Sinne empfiehlt die Arbeitsgruppe auch die Einführung einer "Bedarfsprüfung" für die Möglichkeit, Verkehrsdaten für die Vermarktungszwecke des Anbieters selbst zu verarbeiten¹⁰⁴.

Artikel 8: Anzeige der Rufnummer des Anrufers und des Angerufenen

Im Internet gibt es keine Anrufe, deren Identifikation möglich ist oder nicht. Es gibt keinen getrennten Leitweg, durch den die Identität des Anrufers angezeigt werden kann, ehe die Verbindung hergestellt ist.

Im Internet kann die IP-Adresse nicht von der Übermittlung (den Datenpaketen) getrennt werden, so dass der Begriff der Anruferkennung (*CLI*) nicht unmittelbar auf das Internet anwendbar ist.

Technisch ist es nicht möglich, internetbezogene Telekommunikationsdienste anzubieten, ohne die IP-Adresse zu übermitteln und zu verwenden, die der Internet-Nutzer während einer Sitzung benutzt.

Daraus kann geschlossen werden, dass Artikel 8 der Telekommunikations-Richtlinie nicht in gleicher Weise auf eine IP-Adresse angewendet werden kann wie auf Telefonnummern.

Der Vorschlag vom 12. Juli 2000 für eine überarbeitete Richtlinie folgt dieser Überlegung. Der Wortlaut des Artikels bleibt praktisch unverändert und bezieht sich auf "Anrufe", ein Begriff, der im neuen Text ausschließlich Telefondiensten vorbehalten ist.

V. Maßnahmen zur besseren Absicherung der Privatsphäre

Der Schutz der Privatsphäre kann beim Websurfen auf verschiedene Weise erfolgen. Hier sollen einige Möglichkeiten zur besseren Absicherung der Privatsphäre von Internet-Nutzern kurz vorgestellt werden¹⁰⁵.

Erstens beruhen viele Methoden zur Erfassung personenbezogener Daten auf dem Einsatz von *Cookies*. Die von Internet-Nutzern gewöhnlich verwendete Browsersoftware bietet die Möglichkeit, die Platzierung von *Cookies* auf ihren Festplatten entweder von Fall zu Fall oder per Voreinstellung zu verhindern. Anzumerken ist jedoch, dass immer mehr Websites ihre Dienste nur dann voll zur Verfügung stellen, wenn die *Cookie*-Funktion eingeschaltet ist.

Am 20. Juli 2000 gab die Firma Microsoft bekannt, dass sie dabei sei, die Beta-Version einer Korrektur ("patch") für die Sicherheit der nächsten Version ihres Browsers Internet Explorer einzuführen, um eine bessere Verwaltung von Web-*Cookies* zu gestatten¹⁰⁶. Die Testversion des Korrekturprogramms solle Ende August öffentlich erhältlich sein.

Nach vorläufigen Beschreibungen wird das Patch verschiedene Eigenschaften haben, die den Internet-Nutzern eine wirksamere Kontrolle der *Cookies* erlauben werden. Der Browser wird in der Lage sein, zwischen *Cookies* von erster Seite und von dritter Seite zu unterscheiden, und voreingestellt wird eine

¹⁰⁴ Siehe Stellungnahme 7/2000 der Arbeitsgruppe, angenommen am 2. November 2000, WP 36.

¹⁰⁵ Zu weiteren Details siehe Kapitel 9 über Maßnahmen zur besseren Absicherung der Privatsphäre.

¹⁰⁶ EPIC Alert 7.14, 27. Juli 2000.

Meldung den Internet-Nutzer warnen, wenn ein dauerhaftes *Cookie* von dritter Seite eingeschleust wird. Dauerhafte *Cookies* von dritter Seite werden von Internet-Werbefirmen wie DoubleClick oder Engage in großem Umfang eingesetzt, um die Aktivitäten von Computernutzern zu verfolgen. Zusätzlich wird die neue Funktion den Internet-Nutzern ermöglichen, alle *Cookies* mit einem einzigen Anklicken zu löschen und Informationen über Sicherheit und Privatsphäre leichter zugänglich machen. Dieses Korrekturprogramm erhöht jedoch nicht die Verbraucherkontrolle über den Einsatz von *Cookies* aus erster Seite, die auf kommerziellen Websites vorherrschen.

Diese neuen Möglichkeiten zur Verwaltung von *Cookies* schließen unmittelbar an andere kürzlich von Microsoft herausgebrachte Korrekturen zur Unterbindung von Daten"lecks" an. Im Mai 2000 brachte das Unternehmen ein Patch für das verbreitete Programm Outlook heraus, das *Cookies* in E-Mailbotschaften abwehren soll.

Bedauerlicherweise gestattet diese Technik noch nicht, dass die das *Cookie* versendende Website auch unmittelbar angibt, zu welchem Zweck das *Cookie* verwendet wird.

Zweitens können *ISP* einen positiven Beitrag zum Schutz der Privatsphäre der Internet-Nutzer leisten, wenn sie die Speicherung von personenbezogenen Daten auf das Minimum beschränken, das zur Herstellung einer Verbindung und zur Aufrechterhaltung der technischen Leistungsfähigkeit notwendig ist. Insbesondere ist es den *ISP* in vielen Fällen möglich, die IP-Nummer eines Internet-Nutzers vor der besuchten Website geheim zu halten, indem auf diese Website über einen speziellen *Proxy-Server* zugegriffen wird. In diesem Fall wird nur die vom *Proxy-Server* zugewiesene "maskierte" IP-Nummer übermittelt, während die Adresse des Internet-Nutzers beim *ISP* verbleibt. Solche Dienste werden jedoch selten als Standarddienstleistung angeboten.

Drittens können manche *Portal-Websites* als *neutrale Dritte* auftreten, die über die personenbezogenen Daten der Nutzer wachen. Solche 'Informationsmittler' können als Wächter fungieren, die personenbezogene Daten nur an solche Websites weitergeben, die die Privatsphäre der Internet-Nutzer respektieren, oder sie können die ihnen überlassenen personenbezogenen Daten nach vollständiger Unterrichtung und mit Einwilligung der Internet-Nutzer gegen bestimmte Vorteile 'eintauschen'¹⁰⁷. Diese letztere Möglichkeit ist allerdings mit Vorsicht zu behandeln.

Die rigoroseste Möglichkeit besteht darin, dass Internet-Nutzer Dienste auswählen, die deren IP-Adresse erklärtermaßen vor den besuchten Websites geheim halten. Es sind manche 'Anonymisierungs'-Websites und entsprechend eingerichtete Softwareprodukte vorhanden, die die IP-Adresse der Internet-Nutzer verbergen, indem sie die Mitteilung über dafür eingerichtete Server umleiten, die eine IP-Adresse durch eine andere ersetzen.

Das Vorhandensein neuer Software zur Überwachung von E.T.-Programmen wirft natürlich neue Fragen in bezug auf den möglichen Schutz gegen solche Programme auf. Eine - allerdings nicht ohne weiteres umsetzbare - Schutzvorkehrung¹⁰⁸ wäre die Aufteilung von Computerfestplatten in öffentliche und private Bereiche, damit bei Downloads kein Zugriff auf Informationen erfolgt, die Nutzer unter Verschluss halten möchten. Jedenfalls ist größte Sorgfalt zu empfehlen, wenn Anwendungen aus dem Internet oder aus E-Mails heruntergeladen werden.

VI. Zusammenfassung

- Nutzern muss zum Surfen und Suchen im Netz ein anonymer Zugang zum Internet geboten werden. Zu diesem Zweck sind *Proxy-Server* sehr zu empfehlen.

¹⁰⁷ Zu weiteren Details siehe "Net Worth" (op cit.).

¹⁰⁸ Wie vom leitenden Wissenschaftler von Lucent Technologies, Cheswick, im Artikel von A. COHEN im Time-Magazine (op cit.) vorgeschlagen.

- Die zunehmende Verwendung von Überwachungssoftware ist ein Trend, der beachtet und genau verfolgt werden muss, da er schwerwiegende Konsequenzen für die Privatsphäre der Internet-Nutzer haben kann.
- Einige Begriffe und Definitionen, die im gegenwärtigen Wortlaut der Telekommunikations-Richtlinie verwendet werden, lassen sich nicht ohne weiteres auf internetbezogene Dienste übertragen.
 - Die herkömmliche Trennung zwischen Inhalts- und Verkehrsdaten kann nicht einfach auf Internet-Aktivitäten übertragen werden, insbesondere nicht im Kontext des Surfens. Einerseits sollte der Begriff der Verkehrsdaten weit ausgelegt werden, um Vorspanndaten (*Header*) ebenso wie sämtliche Anmeldedaten mit umfassen zu können. Andererseits sollten Daten zum Surfverhalten das gleiche Maß an Schutz erhalten wie Inhaltsdaten.
 - Die Bestimmungen zur Anrufkennung (*CLI*) müssten ebenfalls im Internet-Kontext neu überdacht werden.
- Die Neufassung dieser Richtlinie hat hinsichtlich des ersten Punktes eine große Verbesserung erbracht, indem sich der Geltungsbereich von Artikel 5 nicht mehr nur auf den Inhalt der Mitteilungen, sondern auch auf die damit zusammen hängenden Verkehrsdaten erstreckt, und somit beiden Datenformen gleicher Schutz gewährt wird. Die Arbeitsgruppe begrüßt diese Verbesserung. Auch der zweite Punkt wurde gelöst, indem klargestellt wurde, dass diese Vorschrift nur für Telefonanrufe, nicht aber für das Internet gilt.

Tatsächlich hat die Neufassung dieser Richtlinie ein hohes Maß an Klarheit geschaffen, indem sie die vorhandene Terminologie dem gegenwärtigen weiteren Zusammenhang anpasst und dadurch die Auslegung der bestehenden Vorschriften erleichtert. Die Arbeitsgruppe möchte jedoch darauf hinweisen, dass der Begriff "Dienste mit Zusatznutzen" einer weiteren Eingrenzung bedarf, um zu weit gefasste Auslegungen zu vermeiden.

KAPITEL 6: VERÖFFENTLICHUNGEN UND FOREN

I. Einleitung

Im Internet zugängliche Veröffentlichungen und Foren haben beide die Eigenschaft, dass sie personenbezogene Daten öffentlich zugänglich machen, und zwar (z.B. in öffentlichen Diskussionsforen) mit oder ohne Beteiligung der betroffenen Person (z.B. in Verzeichnissen). Die Gründe für eine Veröffentlichung persönlicher Daten hängen vom jeweiligen Kontext ab. In einem Fall machen Internet-Nutzer bestimmte Angaben, weil sie dazu aufgefordert werden, etwa um Zugang zu einem Chatroom zu erhalten; in anderen Fällen kann die Information durch Dritte veröffentlicht werden, z.B. aus Verwaltungsgründen durch Behörden.

Das grundlegende Problem, das sich aus der Freigabe solcher Informationen ergibt, ist die Anwendung der Grundsätze des Datenschutzes auf Daten, die im Web öffentlich zugänglich sind. Entgegen einer weit verbreiteten Ansicht gelten die Datenschutzvorschriften auch für veröffentlichte Daten. Dieses Kapitel widmet sich besonders den Gründen und der Notwendigkeit für die einzelnen Offenlegungen von personenbezogenen Daten, ihren Zwecken und dem Risiko des Missbrauchs dieser Daten.

II. Technische Beschreibung

Öffentliche Diskussionsforen

Die technischen Aspekte der Verarbeitung von Daten zu öffentlichen Diskussionsforen hängen von der Art des Forums ab. Es lassen sich zwei Hauptgruppen von Foren unterscheiden: Newsgroups und Chats.

Newsgroups

Newsgroups sind nach Themen klassifizierte Foren, in denen alle von Internet-Nutzern eingesandten Daten für eine bestimmte Zeit gespeichert werden, um Beiträge oder Antworten anderer Nutzer zu einem bestimmten Thema zu ermöglichen.

Eine Frage oder ein Beitrag schließt eine "Überschrift" und einen "Textkörper" ein. Die Verknüpfung zwischen einem Beitrag und der Antwort darauf ist ein "Thread" ("Faden").

Mitteilungen werden an Newsgroup-Server unter Verwendung besonderer *Protokolle* weitergeleitet. Das übliche Verfahrens-*Protokoll* für News heißt NNTP (News Network Transfer Protocol), aber manche Newsgroups verwenden auch das *HTTP-Protokoll*. NNTP bearbeitet Dauerverbindungen zwischen Newsgroup-Servern und sorgt für die automatischen Aktualisierungen der Nachrichten. Diese werden von den Newsgroup-Servern auf Festplatten gespeichert, die von jeder angeschlossenen Person abgefragt werden können. Nachrichten werden im *HTML-Format* wiedergegeben.

Jeder Server vergleicht mit jedem anderen seine Liste von Beiträgen in jeder Diskussionsgruppe und tauscht neue Beiträge mit ihnen aus. Dieser Abgleich von Inhalten führt zu Millionen von Datenaustauschvorgängen im Internet.

Angesichts der großen Zahl an Gruppen speichern Internet-Nutzer nur eine Auswahlliste von Newsgroups, und die Abrufsoftware gibt nur die Titel der News-Themen wieder, so dass das Herunterladen des Textkörpers der Beiträge der Initiative der interessierten Nutzer überlassen bleibt.

Chats

Es gibt drei Hauptformen des Internet-Chats: Internet Relay Chat (IRC), Webpage(Java-)-Chat und ICQ (I seek you)-Chat.

1. IRC ist das ursprüngliche Chatmedium im Internet. Es nutzt ein *Protokoll*, das den Nutzern die Kommunikation in Echtzeit erlaubt, und zwar öffentlich in einem Forum mit einer nicht festgelegten Anzahl von Menschen oder privat mit lediglich einem Gegenüber. Chatrooms bilden sich wie Newsgroups über die in ihnen diskutierten Themen, aber anders als bei Newsgroups werden die Verbindungen am Ende der Diskussion gelöscht.

Wegen Wartezeiten bei der Informationsübermittlung über den Haupt-IRC sind unabhängige Netzwerke hinzugekommen. Die wichtigsten Netzwerke sind EfNet, UnderNet und DalNet.

2. Webpage-Chat erlaubt das Chatten ohne spezielles Programm: dazu ist lediglich ein moderner Internet-Webbrowser erforderlich. Es gibt zwei Arten des Webpage-Chats: der speziell dazu eingerichtete Webpage-Chat, der bei den meisten *Portal*-Such-Sites vorhanden ist, und der von einzelnen Nutzern auf ihrer eigenen Homepage eingerichtete Webpage-Chat. Zwar ist der Webpage-Chat ganz einfach zu bedienen, hat aber auch nur begrenzte Möglichkeiten: es lassen sich nur Texten austauschen, die Veränderung von Farben oder die Übermittlung von Tönen, das Senden und Empfangen von Dateien, der Einsatz von Scripts oder Eingriffe in das Chat-Interface sind - anders als bei IRC - nicht möglich.

3. ICQ ist ein Werkzeug, das den Nutzer darüber informiert, wer zu einer gegebenen Zeit online ist. Es teilt ihm mit, wenn sich vorher festgelegte (d.h. in einer persönlichen Kontaktliste eingetragene) Personen anmelden und erlaubt die Kontaktaufnahme mit ihnen; Chatten und Versenden von Nachrichten können - unter der Voraussetzung, dass alle Teilnehmer ICQ verwenden - während des Surfens im Netz weitergehen. Das Programm kann so instruiert werden, dass der Nutzer als unsichtbar, abwesend oder nicht erreichbar erscheint.

Veröffentlichungen und Verzeichnisse

Veröffentlichungen und Verzeichnisse sind im Internet in der Regel in der Form von Datenbanken verfügbar, die Suchkriterien anbieten, mit denen Informationen über eine oder mehrere Einzelpersonen ermittelt werden können.

Die Informationsquelle für Telefonteilnehmer ist üblicherweise das offizielle nationale Telefonverzeichnis, das je nach Land von der wichtigsten Telefongesellschaft oder einem für seine Herausgabe speziell gegründeten Unternehmen auf der Grundlage der Listen der Telefonteilnehmer veröffentlicht wird.

E-Mailverzeichnisse werden unter Nutzung verschiedener Möglichkeiten zusammen gestellt: sei es die freiwillige Eintragung der Internet-Nutzer in eine von einem *ISP* vorgelegten Liste bis hin zur unkontrollierten Erfassung von E-Mails auf Websites wie denjenigen von Newsgroups.

Andere Arten von Veröffentlichungen, etwa Verzeichnisse von öffentlichen Körperschaften, werden nach Thematik erstellt. Dabei kann es sich beispielsweise um die Rechtsprechung der Gerichte eines Landes handeln, mit Datum des Urteils und Angaben zu Art und Sitz des zuständigen Gerichtshofs bis hin zu den Namen der streitenden Parteien und des Richters sowie einer Kurzfassung der Rechtssache.

Die meisten Internet-Datenbanken bieten verschiedene Suchkriterien, die einen personenbezogenen Zugang zu Informationen und unterschiedlich strukturierte Ergebnisse erlauben. In einem Telefonverzeichnis etwa kann die Suche von einem Namen oder einer Telefonnummer ausgehen, bei einer Rechtsprechungs-Datenbank könnte das Datum eines Urteils, der Name einer Partei usw. ein Suchkriterium sein.

III. Gefahren für die Privatsphäre

Öffentliche Diskussionsforen

Das größte Risiko für die Privatsphäre¹⁰⁹ ergibt sich aus dem leichten Zugriff auf die personenbezogenen Daten, die von den Internet-Nutzern mitgeteilt werden. Die Zugänglichkeit dieser Daten kann zu einer weiteren Erfassung und Nutzung für Zwecke führen, die von den Teilnehmern an öffentlichen Foren nicht immer deutlich vorhergesehen werden. Auch sind sich die Teilnehmer nicht immer darüber im klaren, welche Detailinformationen mit dem im Forum geleisteten Beitrag in der Regel ebenfalls veröffentlicht werden.

Was Newsgroups angeht, so wird z.B. in der Regel die E-Mail-Adresse des Absenders einer Mitteilung gemeinsam mit seinem Namen oder Pseudonym veröffentlicht.¹¹⁰ Manche Chat-Foren zeigen neben dem Pseudonym des Teilnehmers auch die IP-Adresse seines Computers an. Manche *Internet-Diensteanbieter* sehen die Möglichkeit vor, an einem Forum teilzunehmen, ohne von den anderen Teilnehmern erkannt zu werden, andererseits aber auch die Möglichkeit, dass Nutzer an Foren teilnehmen und die anderen Teilnehmer ein von ihnen selbst verfasstes spezifisches Personenprofil lesen lassen.

Die online verfügbaren personenbezogenen Informationen variieren von Forum zu Forum. Als allgemeine Regel gilt, dass die Gewährung des Zugangs zu einem Chatroom von der Beantwortung einer Liste detaillierter Fragen zur Identität des Teilnehmers abhängig gemacht wird, die vom *Internet-Diensteanbieter* verlangt wird. Dabei müssen gewöhnlich die E-Mail-Adresse, Geburtsdatum, Land, Geschlecht und manchmal auch die Vorlieben einer Person angegeben werden.

Unter technischen Gesichtspunkten ist die Bereitstellung dermaßen detaillierter Informationen für ein reibungsloses Funktionieren des Newsgroup- oder Chatdienstes gemäß Artikel 6 der Richtlinie 95/46/EG aber nicht erforderlich.

Ferner könnten diese Anmeldeinformationen zu einer Weiternutzung der Daten durch die *ISP* führen und mit weiteren Details zur Person kombiniert werden, die in den Chatrooms online erfasst werden.

Für die Verwendung der erhobenen und/oder veröffentlichten Daten gibt es im wesentlichen zwei Gründe:

1. Überwachung der verbreiteten Inhalte. Eine solche Überwachung wird durchgeführt, um sicherzustellen, dass keine unpassenden Inhalte vorgelegt werden und/oder damit Urheber haftbar gemacht werden können, wenn sich irgendwelche Inhalte als rechtswidrig erweisen¹¹¹. Zu diesem Zweck und um das Datenmaterial identifizierbar zu halten, werden häufig ohne Vorauswahl die gesamten Verkehrsdaten aufbewahrt, wann immer Material beigesteuert wird, obwohl die E-Mail-Adresse und eventuell der Name des Teilnehmers bereits genügen würden.
2. Zusammenstellung von Listen mit personenbezogenen Daten. Solche Daten können im Web mit Hilfe von Softwareprogrammen erfasst werden, die das Netz durchsuchen und sämtliche verfügbaren Daten zu einer namentlich bekannten Person zusammentragen können. Die Arbeitsgruppe zitierte in ihrer

¹⁰⁹ Die spanische Datenschutzbehörde (Agencia de Protección de Datos) hat sich mit diesem Problem in ihrem Dokument "Recomendaciones a los usuarios de Internet" (Empfehlungen für Internet-Nutzer) auseinandergesetzt, das in spanischer und englischer Sprache auf ihrer Website abrufbar ist: www.agenciaprotecciondatos.org

¹¹⁰ Die E-Mail-Adresse schließt häufig den Namen des Internet-Nutzers als ihren ersten Teil ein, vor allem dann, wenn die Adresse von einem IAP automatisch bestimmt und dabei der eingetragene Name des Nutzers verwendet wird. Meistens hat der Nutzer dennoch die Möglichkeit, den Inhalt dieses Adressenbestandteils zu ändern und z.B. ein Pseudonym zu verwenden. Ferner ist es möglich, sich eine zweite Adresse zuteilen zu lassen, bei der die Namenswahl dem Nutzer überlassen bleibt.

¹¹¹ Beziehungsweise um zu vermeiden, dass der für die Foren verantwortliche Diensteanbieter für deren Inhalt haftbar gemacht wird.

Empfehlung 3/97¹¹² einen Zeitungsbericht, in dem erläutert wurde, **wie eine detaillierte Biographie einer zufällig ausgewählten Person zusammengestellt werden kann, wenn man solche Softwareprogramme verwendet und das Informationsmaterial aus allen Diskussionsgruppen auswertet, an denen diese Person teilgenommen hat**; darin unter anderem etwa deren Adresse, Telefonnummer, Geburtsort, Arbeitsplatz, Lieblingsferienziel und andere persönliche Interessen. Diese Daten können erfasst und für verschiedene Zwecke weiterverarbeitet werden, z.B. für die Direktvermarktung, aber auch zur Prüfung der Kreditwürdigkeit, für den Verkauf der Daten an Versicherungsgesellschaften oder Arbeitgeber. Manche Internet-Sites bieten bereits öffentlich erhältliche Suchwerkzeuge an, die es erlauben, alle in Newsgroups geleisteten Beiträge einer einzelnen Person auf der Grundlage ihres Namens und/oder ihrer E-Mail-Adresse herauszufinden¹¹³.

Veröffentlichungen und Verzeichnisse

Der Online-Zugriff auf personenbezogene Angaben, die aus öffentlichen Personenverzeichnissen oder anderen öffentlich zugänglichen Quellen wie z.B. (Telefon-)Verzeichnissen stammen, wirft ähnliche Fragen wie weiter oben auf. Sie beziehen sich auf die mögliche Weiterverwendung von personenbezogenen Daten im weltweitem Maßstab für andere Zwecke als den, für den sie zunächst öffentlich zugänglich gemacht wurden¹¹⁴.

Wie bereits betont wurde, schafft die elektronische Datenverarbeitung und die mögliche Durchführung einer Volltextsuche grenzenlose Möglichkeiten zur Abfrage und Sortierung von Informationen, wobei ihre Verbreitung im Internet das Risiko der Erfassung für missbräuchliche Zwecke vergrößert. Darüber hinaus hat die elektronische Datenverarbeitung es viel einfacher gemacht, öffentlich zugängliche Daten aus unterschiedlichen Quellen miteinander zu kombinieren, aus denen Profile zur sozialen Stellung oder zum Verhalten von Einzelpersonen erstellt werden können. Besondere Aufmerksamkeit sollte darüber hinaus dem Sachverhalt gelten, dass die öffentliche Bereitstellung personenbezogener Daten dazu beiträgt, den neuen Techniken der Erstellung von Datenlagern (*datawarehouse*) und der Datenerschließung (*datamining*) zusätzlichen Auftrieb zu verleihen¹¹⁵. Unter Verwendung dieser Techniken können Daten ohne vorherige Festlegung des Verwendungszwecks erfasst werden; die verschiedenen Verwendungszwecke werden erst im Moment ihrer tatsächlichen Verwendung bestimmt¹¹⁶.

Mehrere besondere Fälle können hier erwähnt werden, die diesen Problembereich illustrieren:

- Zwar sind Rechtsprechungs-Datenbanken öffentlich-rechtliche Dokumentationsmittel, doch könnte ihre Veröffentlichung in elektronischer Form im Internet, die weit gefasste Suchkriterien für Gerichtsfälle

¹¹² Empfehlung 3/97 zur Anonymität im Internet, von der Arbeitsgruppe am 3. Dezember 1997 angenommen.

¹¹³ Siehe z.B. die Internetsite von Deja: "http://www.deja.com/home_ps.shtml?", die ein "Powersearch-Tool" bereithält, zu dessen verschiedenen Suchkriterien auch "Autor von Newsgroup-Beiträgen" gehört. Die Website gibt an, die größte Datenmenge zu Newsgroup-Beiträgen im Web zu sammeln.

¹¹⁴ Siehe diesbezüglich den Beitrag von Marcel PINET, Mitglied der Datenschutzbehörde CNIL, zur Internationalen Konferenz der Datenschutzbeauftragten in Santiago de Compostela, Spanien, im September 1998; abrufbar unter www.cnil.fr, Rubrik 'Internet', "Initiatives".

¹¹⁵ *Datenerschließung (Data mining)* und das Anlegen von *Datenlagern (data warehousing)* beinhalten "das Durchwühlen von Unmengen von Daten", um Muster und Beziehungen zu entdecken, die z.B. aus dem Geschäftsbetrieb und -verlauf von Organisationen hervorgehen; die Datenlager sollen Entscheidungsfindungen unterstützen. Die Verarbeitung riesiger Informationsmengen wird mit Hilfe von Softwareprogrammen geleistet, die eine leichte Verknüpfung zwischen verwandten Informationsbestandteilen der Datenbank erlauben. Siehe Bericht der Registratiekamer (BORKING, J., ARTZ, M., und VAN ALMELO, L.), *Gouden bergen van gegevens: over datawarehousing, datamining en privacy*, Achtergrondstudies en verkenningen 10, September 1998, abrufbar unter: www.registratiekamer.nl

¹¹⁶ Stellungnahme Nr. 3/99 zum Thema 'Informationen im öffentlichen Sektor und Schutz personenbezogener Daten', von der Arbeitsgruppe am 3. Mai 1999 angenommen.

eröffnet, zur Schaffung von personenbezogenen Informationsdateien führen. Dies wäre der Fall, wenn Datenbanken abgefragt würden, um eine Liste von Gerichtsurteilen zu einer bestimmten Person zu finden und nicht die Urteile zu bestimmten Fällen.

- Spezifische Angaben zu einzelnen Personen lassen sich auch dadurch erhalten, dass in getrennten Datenbanken enthaltene Daten miteinander verbunden werden. Personen ohne Wahlrecht können so durch die Abgleichung von Melderegistern und Wählerverzeichnissen ausgefiltert werden.
- Adressenverzeichnisse, die ins Internet gestellt werden, stellen in der Regel die Möglichkeit der Suche nach Einzelpersonen nicht nur über den Namen, sondern auch über die Adresse und Telefonnummer bereit. Die betroffenen Personen sind sich bei der Einwilligung zur Veröffentlichung ihrer Adresse im gedruckten Telefonbuch über die Möglichkeiten einer solchen Rückwärtssuche nicht im klaren. Das Vorhandensein von Daten in elektronischer Form ermöglicht ihre Nutzung für verschiedene Zwecke, z.B. für die Direktvermarktung mittels der Auswahl von Personen nach ihrer Wohngegend (etwa für den Verkauf von Alarmanlagen in Wohnvierteln), oder zur Identifizierung und Eintragung einer Person, die bei einer Firma anruft, um dort eine einfache und aus ihrer Sicht anonyme Auskunft einzuholen.

Veröffentlichungen im Internet können zu neuen Formen der Erfassung personenbezogener Angaben führen, die nicht nur personenbezogene Informationen betreffen, die in "Chatrooms", in öffentlichen Personenregistern oder in Teilnehmerverzeichnissen enthalten sind, sondern auch unmittelbar auf persönlichen Dokumentenseiten. Die automatische Indexierung solcher Seiten durch Suchroboter kann zur Zusammenstellung von Informationsdateien mit personenbezogenen Angaben aus diesen Seiten und zu Marketing-Attacken auf den Autor dieser Seiten oder auf diejenigen führen, die zu diesen Seiten beitragen, das heißt, zur Zustellung von unerwünschten E-Mails (*Spamming*).

IV. Rechtliche Beurteilung

Öffentliche Foren

Es gibt Pläne, *Internet-Diensteanbietern* Verpflichtungen aufzuerlegen, um das Risiko der rechtswidrigen Erfassung personenbezogener Daten zu vermindern, die in Chatrooms oder Newsgroups bekannt gemacht werden.

Die Empfehlung Nr. R (99) 5 des Europarates zum Schutz der Privatsphäre im Internet¹¹⁷ bietet *Internet-Diensteanbietern* einen Leitfaden, wonach sie ihre Kunden vor Vertragsabschluss oder Inanspruchnahme der Dienste über Risiken der Internet-Nutzung aufklären. Solche Risiken können die *Datenintegrität*, die Vertraulichkeit, die Netzwerksicherheit oder andere Gefahren für die Privatsphäre wie etwa die unsichtbare Erfassung oder Aufzeichnung von Daten betreffen.

Das von jedem einzelnen Teilnehmer auszufüllende Anmeldeformular für den Zugang zu einem öffentlichen Forum muss den Vorschriften von Artikel 6 der Richtlinie 95/46/EG bezüglich der Verarbeitung von personenbezogenen Daten nach Treu und Glauben entsprechen, in dem es heißt, dass personenbezogene Daten nur für rechtmäßige Zwecke erhoben und keine Daten erfasst werden dürfen, die für diesen Zweck nicht benötigt werden oder irrelevant sind.

Die Rechtmäßigkeit des Verwendungszwecks kann mit Bezug auf Artikel 7 der Richtlinie 95/46/EG festgestellt werden, der insbesondere die ausdrückliche Einwilligung der betroffenen Personen zur Verarbeitung ihrer personenbezogenen Daten und ein ausgewogenes Verhältnis zwischen den berechtigten Interessen der für die Datenverarbeitung Verantwortlichen und den Grundrechten der Betroffenen vorsieht (Artikel 7 Buchstabe a) und f)).

¹¹⁷ Empfehlung des Ministerausschusses an die Mitgliedstaaten, angenommen am 23. Februar 1999. Abrufbar unter: www.coe.int/dataprotection/

Die Betroffenen müssen klar und deutlich über den Verwendungszweck informiert werden, über die Art der erfassten Daten und die mögliche Dauer der Datenspeicherung. Wenn die Nutzer keine klaren Hinweise auf die Bedingungen für die Datenverarbeitung erhalten, darf aus einer fehlenden Stellungnahme des Nutzers nicht auf dessen implizite Einwilligung zur Weiterverarbeitung seiner Daten (z.B. für Vermarktungszwecke) durch die für die Datenverarbeitung Verantwortlichen geschlossen werden.

Es ist zu betonen, dass Diensteanbieter nicht notwendigerweise jederzeit die wirkliche Identität eines Nutzers kennen müssen. Ehe sie Verträge mit ihnen eingehen und sie mit dem Internet verbinden, müssen sie die Nutzer über die Möglichkeiten des anonymen Internet-Zugangs oder der Verwendung eines Pseudonyms und der Nutzung ihrer Dienste in anonymer Form unterrichten¹¹⁸.

Diesen Grundsatz hat die Arbeitsgruppe in ihrer Empfehlung 3/97 zur Anonymität im Internet anerkannt¹¹⁹. So duldet es zwar ohnehin keinen Zweifel, dass in bestimmten Situationen die Anonymität von Mitteilungen völlig legitim ist, wenn es z.B. um persönliche Erfahrungen (Opfer sexuellen Missbrauchs oder Alkoholabhängige) oder politische Meinungen geht; doch hat die Arbeitsgruppe betont, dass der Bedarf an Anonymität im Internet wesentlich über diese besonderen Fälle hinausgeht. **Denn identifizierbare Daten über Transaktionen im Netz schaffen durch ihre bloße Existenz ein Mittel, um Verhaltensweisen von Einzelnen zu beobachten und in einem Maß zu überwachen, wie es nie zuvor möglich war.**

Die Überwachung von Newsgroups und Chats mit dem Ziel, unpassende Inhalte auszuschneiden, sollte im Einklang mit dem Prinzip der Verhältnismäßigkeit gemäß Artikel 6 der Richtlinie 95/46/EG geschehen. Insofern ist die Feststellung und Erfassung aller zu einem öffentlichen Forum beigetragenen personenbezogenen Daten ein Vorgehen, das im Vergleich zu anderen vorhandenen Mitteln der Überwachung als nicht verhältnismäßig gelten kann. Zu den sonstigen Möglichkeiten, die vorgeschlagen wurden, gehören vertragliche Lösungen, die "inhaltliche Qualität" vorsehen, oder aber die Einbeziehung eines Moderators, der die eingehenden Beiträge auf gesetzwidrige oder schädliche Inhalte überprüft.

Neben diesen Grundprinzipien gilt im übrigen, dass die Aufbewahrung von Verkehrsdaten durch *Internet-Diensteanbieter* ebenso wie bei Telekommunikationsbetreibern sehr streng geregelt ist. Im Allgemeinen gilt die Regel, dass Verkehrsdaten gelöscht oder anonymisiert werden müssen, sobald die Verbindung beendet ist (Artikel 6 Absatz 1 der Richtlinie 97/66/EG). Telekommunikationsbetreibern und *Internet-Diensteanbietern* ist es verboten, Daten lediglich für Zwecke der Strafverfolgung zu erfassen und zu speichern, wenn sie dazu nicht aus spezifischen Gründen und unter ganz bestimmten Bedingungen gesetzlich verpflichtet sind¹²⁰.

Veröffentlichungen und Verzeichnisse

Die Arbeitsgruppe hat noch einmal daran erinnert¹²¹, dass die europäischen Datenschutzvorschriften auch für öffentlich zugängliche personenbezogene Daten gelten, und dass diese Daten noch stärker geschützt werden müssen.

Das entscheidende Prinzip, das für öffentlich zugängliche Personendaten gilt, ist der Grundsatz der Zweckentsprechung oder Zweckbegrenzung, demzufolge personenbezogene Daten zu besonderen, ausdrücklich genannten und legitimen Zwecken erfasst werden und anschließend nicht in einer Art verarbeitet werden dürfen, die mit diesen Zwecken nicht in Einklang steht (Artikel 6 Absatz 1 Buchstabe b) der Richtlinie 95/46/EG).

¹¹⁸ Siehe LOUVEAUX, A. SALAÜN, Y. POULLET, *User protection in the cyberspace: some recommendations*, CRID, S. 12. Abrufbar unter: <http://www.droit.fundp.ac.be/crid/>

¹¹⁹ Empfehlung 3/97, von der Arbeitsgruppe am 3. Dezember 1997 angenommen.

¹²⁰ Empfehlung Nr. 3/99 zur Aufbewahrung von Verkehrsdaten durch *Internet-Diensteanbieter* für Zwecke des Strafvollzugs, angenommen am 7. September 1999, 5085/99/EN/final, WP 25.

¹²¹ Stellungnahme Nr. 3/99 zum Thema 'Informationen im öffentlichen Sektor und Schutz personenbezogener Daten', von der Arbeitsgruppe am 3. Mai 1999 angenommen.

Die Arbeitsgruppe hat ferner unterstrichen, dass öffentlich zugängliche personenbezogene Daten keine homogene Kategorie darstellen, die unter dem Gesichtspunkt des Datenschutzes einheitlich behandelt werden kann: zwar sind bestimmte Daten möglicherweise öffentlich zugänglich, der Zugang kann aber gewissen Bedingungen (z.B. Nachweis eines berechtigten Interesses) und Einschränkungen bei ihrer weiteren Verwendung (z.B. der Nutzung für Vermarktungszwecke) unterworfen sein.

Die Veröffentlichung personenbezogener Daten im Internet kann zu einer Weiterverarbeitung dieser Daten führen, die Dateninhaber möglicherweise nicht erwarten. Die Artikel 10, 11 und 14 der Richtlinie 95/46/EG legen fest, dass Dateninhaber ein Recht auf die Unterrichtung über die Nutzung ihrer personenbezogenen Daten haben. Die betroffenen Personen sind ferner auf ihr Recht hinzuweisen, dass sie gegen eine Verarbeitung ihrer personenbezogenen Daten für Vermarktungszwecke auf einfachem und wirksamem Wege Widerspruch einlegen können.

Die Idee einer zentralen Anlaufstelle für Einsprüche gegen die Verarbeitung personenbezogener Daten könnte eine interessante Möglichkeit darstellen, um den Nutzern angesichts der Verbreitung der Datenverarbeitung auf nationaler und internationaler Ebene die Schwierigkeit zu ersparen, gegen jeden einzelnen Fall von Verarbeitung ihrer Daten Widerspruch einzulegen¹²².

Wenn der beabsichtigte Zweck der Datenverarbeitung mit dem ursprünglichen Zweck nicht vereinbar ist, ist das ausgewogene Verhältnis zwischen dem Recht auf Schutz der Privatsphäre und den Interessen der für die Datenverarbeitung Verantwortlichen durch strengere Auflagen für letztere herzustellen. Diese müssen die Einwilligung der Dateninhaber einholen oder eine rechtliche oder gesetzlich vorgeschriebene Grundlage für die Verarbeitung nachweisen.

Es ist allerdings nicht immer klar, ob die für die Datenverarbeitung Verantwortlichen lediglich das Widerspruchsrecht der Dateninhaber achten müssen oder ob sie deren Einwilligung einholen müssen, wenn sie Daten verarbeiten wollen.

Die Vorschriften über Internet-Verzeichnisse in verschiedenen Ländern sind ein Beispiel für solche unterschiedlichen Ansätze. Die Frage ist, ob eine Einwilligung erforderlich ist, bevor ein Verzeichnis in einer elektronischen Form zugänglich gemacht wird, die andere Suchkriterien aufweist als die des ursprünglichen, gedruckten Verzeichnisses.

Manche Länder (wie Spanien und Belgien) gehen davon aus, dass erweiterte Suchkriterien die Verarbeitung personenbezogener Daten für Zwecke ermöglichen, die mit dem ursprünglichen Zweck nicht vereinbar sind, und dass deshalb eine solche Verarbeitung ohne vorausgehende Unterrichtung und ausdrückliche Einwilligung der Dateninhaber nicht zulässig ist. In anderen Ländern (z.B. im Vereinigten Königreich) wird die Einräumung des in der Richtlinie vorgesehenen Widerspruchsrechts offenbar im Prinzip als ausreichend betrachtet, hängt aber davon ab, ob eine Rechtsvorschrift zur Veröffentlichung der Information im betreffenden Verzeichnis besteht oder nicht.

Diese Auslegungen der Rechtsvorschriften führen zu unterschiedlichen Schutzniveaus in den EU-Mitgliedstaaten und zu Konflikten in der Praxis, wenn etwa von einem Land mit weniger strengen Schutzvorschriften aus ein Verzeichnis ins Internet gestellt wird, das Personendaten von Bürgern eines Landes mit strengeren Vorschriften enthält.

¹²² Eine solche Lösung könnte vor allem im Hinblick auf die Verbreitung von Verzeichnissen im Internet von Nutzen sein. Beschwerden, die von Datenschutzbehörden bearbeitet werden, beziehen sich häufig auf die Veröffentlichung von Daten aus einem bestimmten Land, wenn die betroffene Person zwar in einer Einspruchsliste eingetragen wurde, aber nur in ihrem eigenen Land.

Solche Konflikte wurden auf europäischer Ebene erörtert, und eine gemeinsame Auslegung der Texte durch die Arbeitsgruppe hat zu einer offiziellen Stellungnahme geführt, die eine Harmonisierung der Anwendung des Grundsatzes der Zweckentsprechung durch die EU-Mitgliedsstaaten empfiehlt¹²³.

Der Vorschlag zur Neufassung der Richtlinie 97/66/EG¹²⁴ sieht in Artikel 12 das Recht der Teilnehmer vor, gebührenfrei darüber zu entscheiden, ob ihre personenbezogenen Daten - und ggf. welche - und zu welchem Zweck und in welchem Umfang in öffentliche Verzeichnisse aufgenommen werden. Dies ist ein Schritt in die richtige Richtung, der von der Arbeitsgruppe voll unterstützt wird.

V. Maßnahmen zur besseren Absicherung der Privatsphäre

Neben den oben genannten Rechtsvorschriften gibt es auch technische Lösungen, die auf verschiedenen Ebenen den Schutz von Personendaten verbessern können.

Die Arbeitsgruppe weist darauf hin, dass Browsersoftware grundsätzlich so voreingestellt sein sollte, dass nur das zur Herstellung einer Internet-Verbindung notwendige Minimum von Angaben verarbeitet wird¹²⁵.

Anonymität in öffentlichen Foren

Was das Problem der Anonymität im Internet und insbesondere in öffentlichen Foren angeht, so könnte der Begriff der "Pseudo-Identität" die Frage des ausgewogenen Verhältnisses zwischen einer berechtigten Kontrolle von Missbräuchen und dem Schutz personenbezogener Daten lösen. Eine solche Identität würde dem einzelnen Teilnehmer durch einen spezialisierten Diensteanbieter verliehen. Die Anonymität würde damit im Prinzip respektiert, doch könnte in bestimmten Fällen eine Verbindung zur wirklichen Identität des Einzelnen durch den spezialisierten Diensteanbieter wieder hergestellt werden, z.B. bei Verdacht auf Straftaten. Was E-Mails betrifft, so teilen Remailer (in diesem Zusammenhang ist zuweilen von Pseudonym-Servern die Rede) dem Nutzer entweder eine anonyme Adresse zu, an die Dritte ihre E-Mails schicken können, die dann an die wirkliche Adresse des Nutzers weitergeleitet werden, oder sie verschicken oder "mailen" die Nachricht des Absenders ohne jeden Hinweis auf dessen Namen oder Adresse¹²⁶.

Systematische Indexierung von Daten

Es gibt auch Tools, die verhindern könnten, dass die Verfasser privater Dokumentenseiten einer systematischen Indexierung ihrer Seiten und der Erfassung ihrer personenbezogenen Daten ohne ihr Wissen unterworfen werden. Ein "Roboter-Ausschlussprotokoll" hat den Zweck, die automatische Indexierung des Inhalts aller oder bestimmter Seiten einer Website durch eine Suchmaschine zu verhindern¹²⁷. Dieses *Protokoll* wird von den meisten Suchmaschinen im Web erkannt. Die in die

¹²³ Siehe Stellungnahme 5/2000 zur Verwendung von öffentlich zugänglichen Verzeichnissen für Dienste, die Rückwärtssuche oder Suche anhand vieler Kriterien (multi-criteria search) anbieten. Angenommen am 13. Juli 2000.

¹²⁴ In ihrer offiziellen Fassung vom 12. Juli 2000, KOM (2000) 385 endg.

¹²⁵ Empfehlung Nr. 1/99 der Arbeitsgruppe zur unsichtbaren und automatischen Verarbeitung persönlicher Daten im Internet unter Einsatz von Software und Hardware, angenommen am 23. Februar 1999.

¹²⁶ Diese Remailer heißen Cypherpunk (in der ersten Generation) oder Mixmaster (in der zweiten, fortschrittlichere Techniken verwendenden Generation). Bekannte Anonymisierungs-Server im Web waren "anon.penet.fi" oder "alpha.c2.org". Offenbar haben beide jedoch ihren Betrieb eingestellt. Ein neuer Server dieser Art ist "Nym.alias.net". Anonyme Mitteilungen können auch mit Hilfe eines HTML-Dokuments versandt werden. Die Mitteilung selbst und der schließliche Empfänger werden dann unverschlüsselt an den benutzten WWW-Server übermittelt.

¹²⁷ Stellungnahme Nr. 3/99, s. oben.

Internet-Adresse eingefügte Datei "robots.txt" enthält Anweisungen, die für die Suchroboter bestimmt sind und in denen z.B. bestimmten Robotern der Zugang verwehrt wird oder nur bestimmte Seiten einer Website zum Lesen und zur Indexierung freigegeben werden.

Da nur ein Diensteanbieter in der Lage ist, ein sogenanntes "Roboter-Ausschlussprotokoll" in die Adresse einer Website einzufügen, können die Inhaber privater Websites, die bei einem Diensteanbieter untergebracht sind, ein automatisches *Meta-tag* auf jeder Seite installieren, deren Indexierung sie unterbinden wollen, wenn sie den Diensteanbieter nicht veranlassen können, der Einfügung eines solchen Protokolls zuzustimmen. Der Nachteil solcher *Meta-tags* ist, dass sie noch nicht von jeder Suchmaschine im Internet erkannt werden.

Onlinezugang zu öffentlichen Informationsangeboten

Das letzte Thema, um das es in diesem Kapitel geht, ist der Onlinezugang zu öffentlichen Informationsangeboten, die gleichwohl ebenfalls den Datenschutzrichtlinien unterliegt.

Technische Lösungen für solche Datenbanken können dazu beigetragen, den gesetzwidrigen Missbrauch der in ihnen enthaltenen Informationen zu verhindern:

- Suchkriterien müssen so definiert werden, dass Daten nur in Einklang mit ihrem ursprünglichen Zweck genutzt werden können. In ihrer Stellungnahme vom 13. Juli 2000 über Rückwärtssuche bestand die Arbeitsgruppe darauf, dass *"die für die Datenverarbeitung Verantwortlichen (...) technische und organisatorische Vorkehrungen treffen müssen, die den Risiken entsprechen, die mit der Verarbeitung und der Art der geschützten Daten verbunden sind"* (siehe Artikel 17 der Richtlinie 95/46/EG). Dies heißt z.B., dass Datenbanken so aufgebaut sein müssen, dass etwaige missbräuchliche Anwendungen vermieden werden, etwa die rechtswidrige Veränderung von Suchkriterien oder die Möglichkeit, die gesamte Datenbank für eine Weiterverarbeitung zu kopieren oder in sie einzudringen. Die Suchkriterien müssen beispielsweise ausreichend genau sein, damit nur eine begrenzte Anzahl von Ergebnissen pro Seite angezeigt wird. Im Ergebnis sollte der Zweck, dem der Teilnehmer zugestimmt hat, auch durch technische Mittel gewährleistet sein¹²⁸.

- Die Onlinebenutzung von Datenbanken kann etwa durch eine Begrenzung des Suchfragenspektrums oder der Suchfragenkriterien eingeschränkt werden. Es sollte z.B. nicht möglich sein, Datenmengen zu erfassen, indem eine weite Suchfrage wie etwa nach den ersten Buchstaben eines Namens gestellt wird. Auch könnte es technisch unmöglich gemacht werden, beispielsweise Anfragen nach Gerichtsurteilen mit dem Suchkriterium "Namen von Einzelpersonen" oder die Anfrage nach dem Namen einer Person auf der Grundlage ihrer Telefonnummer durchzuführen.

Zu diesem Zweck sollten technische Tools in Einklang mit den in diesem Kapitel dargestellten Rechtsgrundsätzen konfiguriert und benutzt werden.

¹²⁸ Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation legte in ihrer Sitzung am 15. April 1998 eine vergleichbare Empfehlung zu Rückwärtsverzeichnissen vor: *Wenn Rückwärtsverzeichnisse nicht gänzlich gesetzlich verboten sind, sind sie doch Dienste, die eine ausdrückliche Zustimmung aus freien Stücken voraussetzen. Es ist zumindest das durch die vorhandenen einzelstaatlichen und internationalen Vorschriften zum Schutz personenbezogener Daten allgemein anerkannte Recht auf Einspruch und das Recht auf Zugang zu gewährleisten. Jedenfalls ist jeder Person das Recht zu gewähren, von ihrem Fernmelde- oder Mailedienste-Anbieter zum Zeitpunkt der Erhebung der ihn betreffenden Daten, oder falls sie bereits Teilnehmer ist, über eine gesonderte Mitteilung unterrichtet zu werden, und zwar vom Vorhandensein von rückwärts suchenden Diensten, und – sofern keine ausdrückliche Zustimmung dazu vorgeschrieben ist – von ihrem Recht, gegen eine solche Rückwärtssuche kostenlos Einspruch zu erheben.* Der gesamte Text der Empfehlung ist abrufbar unter: http://www.datenschutz-berlin.de/doc/int/jwgdpt/pr_en.htm

VI. Zusammenfassung

Die vorhandenen gesetzlichen Vorschriften und technischen Mittel bieten den Dateninhabern theoretisch einen wertvollen Schutz vor dem öffentlichen Zugang zu ihren personenbezogenen Daten im Internet.

Der Grundsatz der Zweckentsprechung, wonach personenbezogene Daten nicht für Zwecke verarbeitet werden dürfen, die mit dem ursprünglich festgelegten Zweck nicht vereinbar sind, ist von großer Bedeutung für Daten, die unter bestimmten Umständen öffentlich zugänglich gemacht werden.

Besondere Aufmerksamkeit ist auch dem Grundsatz der begrenzten Speicherdauer von personenbezogenen Daten zu schenken. Solche Daten müssen nach einer angemessenen Zeit wieder gelöscht werden, um die Erstellung von Profilen etwa aus den Mitteilungen zu verhindern, die von Nutzern über mehrere Jahre hinweg an Newsgroups versandt werden.

Die Betroffenen müssen von der vorgesehenen Speicherdauer und den Online-Zugriffsmöglichkeiten auf solche öffentlich zugänglichen Daten unterrichtet werden.

Derzeit ergeben sich Probleme vor allem daraus, dass sowohl den Dateninhabern als auch den für die Datenverarbeitung Verantwortlichen die notwendigen Informationen über die zu erfüllenden gesetzlichen Auflagen fehlen.

Der Hauptansatzpunkt für eine Verbesserung dieser Situation ist eine stärkere Transparenz im Internet und die Harmonisierung der Auslegung der Grundsätze bezüglich der Kontrolle des Dateninhabers über seine eigenen Daten.

Der Vorschlag vom 12. Juli 2000 zu einer Neufassung der Richtlinie 97/66/EG bietet eine willkommene Gelegenheit, einige dieser Fragen zu harmonisieren.

KAPITEL 7: ELEKTRONISCHER GESCHÄFTSVERKEHR IM INTERNET

I. Einleitung

Elektronischer Handel kann definiert werden als "jede Form von Geschäftsverkehr, in denen die Beteiligten anstelle des materiellen Austauschs oder unmittelbaren körperlichen Kontakts elektronisch miteinander interagieren".¹²⁹ Diese Definition deckt sowohl solchen Geschäftsverkehr, bei dem ein Erwerb von Gütern oder Dienstleistungen stattfindet, als auch solchen, der einer Verbesserung der Qualität von Dienstleistungen oder der Bereitstellung von neuen Diensten durch private und öffentliche Einrichtungen dient.

Angesichts dieser Definition und unter Berücksichtigung, dass das Hauptziel dieses Kapitels die Untersuchung von Fragen im Zusammenhang mit dem Internet ist, wird sein Themenbereich auf solchen Geschäftsverkehr beschränkt, der sich im Internet abspielt; alle anderen Formen der Interaktion in privaten oder öffentlichen Netzwerken werden ausgeklammert.

Der elektronische Geschäftsverkehr wird sich voraussichtlich weltweit spürbar machen, da der elektronische Handel per Definition global ist und jedes Unternehmen (unabhängig von seiner Größe oder seinem Umsatz) in die Lage versetzt, überall auf der Welt Produkte anzubieten oder zu erwerben.

Elektronischer Geschäftsverkehr versetzt Unternehmen in die Lage, effizienter und flexibler zu operieren, enger mit Lieferanten zusammen zu arbeiten und auf die Bedürfnisse und Erwartungen ihrer Kunden in einer neuen, bislang nicht gekannten Weise einzugehen.

Aber um alle diese Ziele zu erreichen, sind Informationsmengen erforderlich und dies könnte das Eindringen in wesentliche Teile der Privatsphäre der natürlichen Personen nach sich ziehen.

II. Akteure

Die wichtigsten Akteure im elektronischen Geschäftsverkehr sind:

- die Nutzer, das sind im Kontext der Richtlinie 95/46/EG natürliche Personen, die ein Produkt erwerben oder eine Dienstleistung anfordern möchten¹³⁰;
- die Telekommunikationsbetreiber, die nicht eigentlich am Geschäftsverkehr teilnehmen, aber die entscheidende Rolle bei der Weiterleitung der Signale spielen, die erst jegliche Form von elektronischer Datenübertragung möglich machen. Diesen Akteuren werden von den Richtlinien besondere Sicherheitsverpflichtungen auferlegt;
- die Internet-Diensteanbieter (*ISP*), die den Zugang zum Internet vermitteln;
- die elektronischen Händler – Firmen, die im Internet Produkte oder Dienste anbieten;
- die Finanzplattform, die in den meisten Fällen erforderlich ist und sowohl die Banken der Händler und Verbraucher umfasst als auch eine Zahlstelle (*payment gateway*), die die erforderlichen technischen

¹²⁹ Europäische Kommission, ISPO, *Electronic Commerce - An Introduction*
(<http://www.ispo.cec.be/ecommerce/answers/introduction.html>)

¹³⁰ Der größte Teil des elektronischen Geschäftsverkehrs (ca. 90%) wird heutzutage zwischen Unternehmen abgewickelt, also juristischen Personen, für welche die Richtlinie 95/46/EG nicht gilt (siehe Artikel 2 Buchstabe a) und Artikel 3 Absatz 1).

Aspekte für die Beglaubigung der Finanzoperationen und der Zahlungen behandelt. Diese Zahlstelle befasst sich mit allen Verbindungen zwischen Finanzeinrichtungen und macht elektronischen Geldwechsel dadurch möglich, dass sie gewährleistet, dass alle Beteiligten die erforderlichen Voraussetzungen zur Durchführung des geschäftlichen Vorgangs erfüllen;

- *Vertrauenssichernde neutrale Dritte (Trusted Third Parties)*. Für sehr komplexe und sicherheitsrelevante Fälle sind Stellen erforderlich, von denen die Geschäftspartner "authentisiert" werden und die eine möglichst wirksame Verschlüsselung bieten, um die Vertraulichkeit der Geschäftsvorgänge zu gewährleisten.

Nach Art der Geschäftsvorgänge und der beteiligten Akteure oder Betreiber lassen sich drei verschiedene Modelle für elektronischen Geschäftsverkehr aufstellen¹³¹.

1) Online-Lieferungen von immateriellen Waren und Dienstleistungen. Dieser Weg wird vorwiegend von Softwarehäusern und Kommunikationsdienstleistern genutzt, für welche die Internet-Infrastruktur eine ideale Form des Fernabsatzes in Echtzeit und des Verkaufs ihrer Produkte ist, die von Software über Videofilme, Spiele und Online-Musik bis zu Abonnements von Online-Zeitungen und -zeitschriften und Programmen für technische Unterstützung reicht.

In diesen Fällen ergeben sich, abgesehen von den deutlichen Einsparungen für den direkten Zugang zu den Verbrauchern unter Vermeidung der Abhängigkeit von Zwischenhändlern, große Vorteile für Unternehmen, die sich in dieser Form des Handels engagieren. Sie können präzise und genaue Informationen über den Endverbraucher, seine Hobbys, Interessen und Kaufmuster erhalten.

In dieser Kategorie finden sich auch die meisten Dienstleistungen öffentlicher Einrichtungen wie etwa Online-Steuerzahlungen oder Rückzahlungen, elektronisch übermittelte Anfragen oder Anträge auf Sozialleistungen und Folgemaßnahmen.

2) Elektronische Bestellungen materieller Güter. Diese Kategorie umfasst viele verschiedene Arten von Unternehmen; vor allem Grossunternehmen, die das Internet als Möglichkeit des direkten Zugangs zum Verbraucher nutzen. IT-Hardwarehersteller oder -einzelhändler waren die ersten Unternehmen, die diese Absatzwege nutzten; dies lässt sich wegen der Art der Internet-Nutzer leicht nachvollziehen. Aber nunmehr wächst die Zahl der Firmen, die Kleidung, Parfüms, Bücher, CDs, Flugtickets usw. verkaufen. Das Internet bietet kleineren und mittleren Unternehmen die Möglichkeit, neue Geschäftsaktivitäten in einer Größenordnung zu entwickeln, die mit ihren herkömmlichen Ressourcen nicht erreichbar war. Tatsächlich besteht, wie manche Beobachter feststellen, ein großer Unterschied zwischen einer Anfangsinvestition, die erforderlich ist, um 100.000 Musik-CDs in einem elektronischen Laden im Internet zu verkaufen und einer solchen, die für die Eröffnung eines ebenso umfangreichen Geschäfts in einer Innenstadt erforderlich wäre.

Der gesamte elektronische Handel mit materiellen Gütern hängt letzten Endes von einer logistischen Organisation für die Auslieferung der Waren an den Endverbraucher bei seiner Adresse ab. Diese logistischen Organisationen investieren derzeit in Internet-Technologien für die elektronische Bestellung und Verfolgung der Frachten zwischen Partnerunternehmen untereinander und zwischen den Logistikunternehmen und den Endverbrauchern, durch die alle Beteiligten in Echtzeit erfahren können, wo sich die bestellten Waren befinden und für wann ihre Ankunft zu erwarten ist. Diesbezüglich ist es durchaus möglich, dass in nächster Zeit Großhändler und Logistikexperten fusionieren, um die Schlüsselinformationen über Verteilungsvorgänge zu nutzen, die sich in der Hand der Logistikunternehmen befinden (vor allem Sammlungen der Anlieferadressen).

¹³¹ Die nachfolgende Klassifizierung wurde der Studie der Kommission der Europäischen Gemeinschaft entnommen: GAUTHRONET, S. und NATHAN, F., "On-line services and data protection and the protection of privacy". 1998, 150 S. Sie lässt sich abrufen unter:

http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serve.pdf

3) Händlernetze und Einkaufszentren. Online-Handel schließt nicht die traditionellen Verteiler aus, die keine weitgehenden Kenntnisse der neuen Technologien besitzen. Sie haben die Möglichkeit, an Strukturen teilzunehmen, die Internet-Mall genannt werden und ihnen die Option bieten, ihre Ware in den Schaufenstern eines elektronischen Einkaufszentrums darzubieten. In solchen Malls sind die Läden nach Kategorien geordnet und die Besucher benutzen ein internes Suchsystem mit einem Verzeichnis der Stellen, die das gewünschte Produkt anbieten. Werbebanner können je nach eingegebenen Stichwörtern oder besuchten Läden zielgerichtet eingesetzt werden, und das Internet-Einkaufszentrum bietet seinen Mitgliedern eine sichere Zahlungsinfrastruktur.

Aufgrund ihrer Rolle sammeln die Internet-Einkaufszentren häufig sehr ausführliche und präzise Informationen über die Besucher und Käufer (besuchte Läden, Interessen, Kaufgewohnheiten, Adressen, personenbezogene Details und Zahlungsinformationen), die von großem Interesse für die Erstellung von Kundenprofilen bei der Entwicklung von Werbe- oder Marketing-Strategien sein können¹³².

Die Rolle dieser Einkaufszentren kann sich in Zukunft ändern, wenn sie in umfassendere Bereiche integriert werden, nämlich die sogenannten *Portale*, die sozusagen Oberzentren im Web bilden, die eine Vielzahl von Diensten anbieten; dazu gehört die Suche im Netz, das Angebot an Nachrichten und an weißen und gelben Seiten, kostenlose E-Mail-Fächer, Diskussionsgruppen, Online-Einkauf und Verknüpfungen zu anderen Sites.

Diese modernen *Portale* bieten über klassifizierte Werbung und Suchmaschinen zunehmend mehr Einkaufsmöglichkeiten in weltweitem Maßstab. Und nichts hält diese *Portale* davon ab, in naher Zukunft ihrer eigenen sicheren Zahlungsplattformen und intelligenten "user-agents" anzubieten, die im Web suchen, Preise aushandeln (ja sogar die vertraulichen Bedingungen eines Geschäftsvertrags)¹³³ und Vereinbarungen im Auftrag des Verbrauchers schließen können.

III. Sichere Zahlungssysteme

Die wachsende Bedeutung des elektronischen Handels macht elektronische Zahlungssysteme für den Verkauf von Waren und Dienstleistungen erforderlich. Die Sorge bezüglich der Sicherheitsrisiken bei der Übermittlung von Details einer Kreditkarte im Internet und bezüglich der Möglichkeit, dass vertrauliche personenbezogene Informationen von unbefugten Dritten abgefangen werden, sind zwei Faktoren, die eine Ausweitung des elektronischen Handels hemmen.

Um diesen Bedenken zu begegnen, wurden und werden weiterhin verschiedene Methoden entwickelt. Derzeit am meisten verbreitet ist diejenige des Secure Sockets Layer (SSL)¹³⁴, die in den am häufigsten benutzten Browsern integriert ist und gestattet, eine sichere Verbindung zwischen dem Computer des Verbrauchers und dem des Händlers einzurichten. Sie wird mit Hilfe von *Verschlüsselungen* und *digitalen Zertifikaten* hergestellt.

¹³² Wie solche Informationen erhoben werden, wird ausführlicher in Kapitel 5 (Surfen und Suchen) erläutert.

¹³³ Stellungnahme 1/98: 'Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)', von der Arbeitsgruppe 'Schutz natürlicher Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten' am 16. Juni 1998 angenommen. (<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm>). Siehe auch HAGEL III, J. und SINGER, M., *Net Worth: the emerging role of the infomediary in the race for customer information*, Harvard Business School Press, 1999, und Bericht *Intelligent software agents and privacy* von J. BORKING, B.M.A. VAN ECK und P. SIEPEL, Registratorkammer in Zusammenarbeit mit dem Informations- und Datenschutzbeauftragten von Ontario, Achtergrundstudies and verkenningen, Januar 1999, abrufbar unter: www.registratiekamer.nl

¹³⁴ Eine vollständige Darstellung des SSL-Systems kann abgerufen werden unter: <http://www.netscape.com/tech/security/ssl/howitworks.html> und <http://www.netscape.com/tech/security/ssl/index.html>

Das grundlegende Verfahren bei SSL besteht in folgendem: Bevor der Computer (Server) des Händlers eine gesicherte Verbindung mit dem Computer (Client) des Verbrauchers herstellen kann, muss der Client sicher sein, dass er mit einem sicheren Server verbunden ist. Zur Feststellung der Identität des Servers wird dessen digitales Zertifikat herangezogen. Wenn der Server "authentisiert" ist, können Client und Server wechselseitig ihre Daten verschlüsseln und die *Integrität* dieser Daten einschließlich der Nummer der bei diesem Geschäftsvorgang verwendeten Kreditkarte sowie aller übrigen personenbezogenen Details gewährleisten.

Es ist zu beachten, dass SSL dem Verbraucher keine Kontrolle über die anschließende Verwendung oder Verarbeitung seiner personenbezogenen Daten durch den Händler ermöglicht und dass die Authentisierung des Computers des Verbrauchers (Client) nicht obligatorisch ist, was Betrügereien durch Missbrauch der Identität anderer möglich macht.

Um solche Schwierigkeiten aus dem Weg zu räumen und einen vollkommen zuverlässigen Rahmen für elektronische Geschäftsvorgänge zu schaffen, haben manche Kreditkarten-Gesellschaften gemeinsam mit den wichtigsten Softwareentwicklern ein neues *Protokoll* entwickelt. Dieses *Protokoll* wird 'Sichere elektronische Geschäftsvorgänge' (Secure Electronic Transactions – SET) genannt und bietet vertraulichen Geschäftsverkehr (durch *Verschlüsselung*), *Authentisierung* der Beteiligten (der Karteninhaber, Kartenaussteller, Händler, Käufer und Zahlungsstellen durch *digitale Zertifikate*) und schließlich *Datenintegrität* und Nichtwiderrufbarkeit von Zahlungsanweisungen für Waren und Dienstleistungen (durch *digitale Signaturen*)¹³⁵.

Dieses System ist allerdings nicht gut geeignet, wenn es um zahlreiche Vorgänge von geringfügigen Wertübertragungen geht; deshalb wird derzeit eine alternative Methode namens "Elektronisches Bargeld" oder "e-cash" entwickelt. Das allgemeine Prinzip besteht darin, Geld auf die Festplatte eines Computers (oder in Kürze auf einer Chipkarte) zu laden. Bei jeder Online-Zahlung übermittelt der Nutzer Geldeinheiten (tokens) von seinem Computer oder seiner Chipkarte auf das Konto des Händlers oder Diensteanbieters. In diesem Bereich konkurrieren verschiedene Technologien miteinander. Unter dem Gesichtspunkt des Schutzes der personenbezogenen Informationen sind am interessantesten vollständig anonyme Zahlungssysteme, die auf dem Verfahren der Blindsignatur beruhen¹³⁶. Mit diesen Verfahren wird die Verfolgung der Spur der Geschäftsvorgänge verhindert, da die Bank, die das "elektronische Bargeld" "signiert", keine Verknüpfung zwischen dem Verbraucher und einem besonderen Geschäftsvorgang herstellt.

¹³⁵ Bei der Verwendung von SET kommunizieren die Beteiligten während des Geschäftsvorgangs mit Hilfe zweier Paare von einmaligen und asymmetrischen Verschlüsselungen miteinander: mit den öffentlich zugänglichen Verschlüsselungen für die Unterzeichnung von Dokumenten bezüglich des Geschäftsvorgangs, zum Beispiel einer Kaufofferte, und mit privaten Verschlüsselungen, die die digitale Signatur für den tatsächlichen Geschäftsvorgang (zum Beispiel Zahlungsanweisung) enthalten, die Integrität der Übertragung gewährleisten und sicherstellen, dass die Bestellung nicht zurückgezogen wird. Das System wirkt wie doppelte Unterschriften: Beide Schlüssel sind so aufeinander bezogen, dass eine Zahlung solange nicht gültig ist, bis das Kaufangebot vom Händler akzeptiert wurde, während die konkrete Bestellung solange nicht ausgeführt wird, bis der Eingang der Zahlung von der Finanzinstitution bestätigt ist. Der Händler hat keine Kenntnisse von den Zahlungsanweisungen, während die Bank keinen Einblick in den Inhalt einer Bestellung hat. Zu einer ausführlichen Darstellung der Funktionsweise des komplexen SET- Protokolls siehe SET Secure Electronic Transaction Specification Book 1: Business Description, abrufbar unter:

<http://www.setco.org/download.html>

Siehe auch: GARFINKEL, S., *Web security and commerce*, O'Reilly associates, Juni 1997, Kapitel 12: Understanding SSL and TLS.

¹³⁶ Für eine theoretische Erörterung der Funktionsweise dieses Systems siehe CHAUM, David, "A Cryptographic Invention Known as a Blind Signature Permits Numbers to Serve as Electronic Cash or to Replace Conventional Identification. The Author Hopes It May Return Control of Personal Information to the Individual" unter:

http://www.eff.org/pub/Privacy/chaum_privacy_id_article; der Artikel erschien im August 1992 in *Scientific American*.

IV. Gefahren für die Privatsphäre

Unabhängig von der Art der durchgeführten Geschäftsvorgänge oder der verwendeten Zahlungssysteme besteht der entscheidende Unterschied zwischen der materiellen Welt und der elektronischen Welt darin, dass in Ersterer eine Reihe von Aktivitäten anonym bleiben können (Schaufenster betrachten, durch verschiedene Geschäfte schlendern, verschiedene Produkte prüfen und, sofern in bar bezahlt wird, auch der Kauf von Waren); in letzter hingegen kann jeder Vorgang registriert, zu früheren oder neu erzeugten Informationen hinzugefügt und fast ohne Kosten weiter verarbeitet werden, um ertragreichere Informationen über jeden Nutzer zu erzeugen. Vor allem aber kann dies ohne Einwilligung, ja sogar ohne Kenntnis der Betroffenen geschehen. Darüber hinaus können mit den derzeitigen *datawarehouse*- und *datamining*¹³⁷-Technologien enorme Informationsmengen verarbeitet werden, um nicht nur Einzelpersonen auszuwählen, die bestimmten Merkmalen oder Kriterien entsprechen, sondern auch versteckte Beziehungen zwischen scheinbar unverknüpften Daten aufzudecken, wodurch mancherlei Verhaltensmuster sichtbar gemacht werden, die kommerziellen oder behördlichen Entscheidungen, bestimmte Personen betreffend, zugrunde gelegt werden können.

Wenn jemand einen Einkauf tätigt oder eine Dienstleistung wie etwa ein Abonnement in Anspruch nimmt, ist es in den meisten Fällen unerlässlich, dem Händler oder Diensteanbieter personenbezogene Daten zu liefern, mit denen der Käufer authentisiert werden kann, um eine Garantie für die Bezahlung oder eine materielle oder elektronische Adresse für die Auslieferung der Waren oder Dienstleistungen zu erhalten. Gegenwärtig ist also im Web die Möglichkeit der Anonymität gering, es sei denn, es wird mit elektronischem Bargeld bezahlt, eine die Privatsphäre schützende Technologie verwendet, die die IP-Adresse unsichtbar macht, und immaterielle Ware gekauft.

In diesem Kapitel wird deshalb vor allem auf die Gefahren einer nicht autorisierten sekundären Verwendung von personenbezogenen Daten und auf die Risiken im Zusammenhang mit dem "Personalisieren" oder dem Bruch der Vertraulichkeit eingegangen.

1. Eine der gebräuchlichsten sekundären Verwendungen von personenbezogenen Daten gilt der Werbung. Wenn ein Nutzer identifiziert ist, weil er selbst die Informationen beim Einloggen in einen Server geliefert hat, oder aber mit Hilfe anderer technischer Kniffe wie etwa *Cookies*, werden frühere Informationen über ihn herangezogen, um Werbeanzeigen entsprechend seinen Gewohnheiten, Interessen, Anklicksequenzen oder Kaufmustern an ihn anzupassen. Dabei verweist die Werbung nicht nur auf den Träger der Website, der darin Dienstleistungen oder andere Angebote präsentiert, sondern auch auf solche von Dritten, die Vereinbarungen getroffen haben, gegen Kostenbeteiligung für den Betrieb des Servers Werbebanner zu platzieren.

Modell für die Internet-Werbung sind die Techniken, die von der Werbeagenturen wie etwa DoubleClick verwendet werden. Die Tätigkeit von DoubleClick besteht darin, Werbeflächen im Netz bereit zu stellen und es den Werbekunden leicht zu machen, denjenigen Raum zu finden, der eine geeignete Unterstützung für ihre Mitteilungen bietet. Ein weiteres Schlüsselement für den Erfolg von DoubleClick ist die IT-Technologie, die es ermöglicht, Identifikationskriterien zu isolieren und den Werbekunden Instrumente an die Hand zu geben, mit denen sie Nutzer zielgerichtet ansprechen können. Diese Technologie greift auf eine Datenbank zu, die Daten von mehreren Millionen Internet-Nutzern enthält und gewährleistet, dass mit Werbekampagnen nur die jeweils gewünschte Zielgruppe angesprochen wird.

Zu diesem Zweck sammelt und verarbeitet DoubleClick personenbezogene Daten, die eine Identifizierung der Nutzer gestatten und deren Gewohnheiten beschreiben und gleichzeitig in Echtzeit diejenigen Elemente der Bevölkerungsgruppe festlegen, die die Zielkriterien für die jeweilige Werbekampagne erfüllen dürfte. DoubleClick weist jedem Nutzer, der eine Website im Netzwerk von DoubleClick besucht und *Cookies*

¹³⁷ Siehe Bericht der Registratiekamer (BORKING, J., ARTZ, M. and VAN ALMELO, L.), *Gouden bergen van gegevens: over datawarehousing, datamining en privacy*, Achtergrondstudies en verkenningen 10, September 1998, abrufbar unter: www.registratiekamer.nl

akzeptiert, eine einmalige Identifikationsnummer zu, die später wieder verwendet wird, wenn der Nutzer eine andere Site von DoubleClick besucht, um entsprechend seinen Daten die passendste Werbung auf ihn auszurichten. Doch selbst wenn ein Besucher keine *Cookies* akzeptiert, kann sein Profil erstellt werden, insbesondere, wenn er eine statische IP-Adresse hat.

DoubleClick sammelt in seiner Datenbank folgende personenbezogenen Daten: Den konstanten Teil der IP-Adresse, also Netzadresse, Domain und Land sowie Bundesstaat (USA), Postleitzahl, SIC-Code (*Standard Industrial Classification* - USA), Größe und Umsatz des Unternehmens (nach Wahl), Betriebssystem, Versionsnummer, Diensteanbieter, Identifikations-Nummer (wird von DoubleClick zugewiesen) und Informationen über die Suche im Netz (Sammlung und Analyse der vom Nutzer besuchten Sites)¹³⁸.

DoubleClick hat am 23. November 1999 mit Abacus Direct Corporation fusioniert. Abacus betreibt weiterhin - nunmehr als eine Abteilung von DoubleClick - Abacus Direct, den Postversand-Zweig von Abacus Alliance. Ferner wurde bekannt gegeben, dass Abacus damit begonnen habe, Abacus-Online aufzubauen, den Internet-Zweig von Abacus Alliance.

Nach den Informationen auf der Website von DoubleClick soll der Online-Zweig von Abacus Alliance die US-amerikanischen Verbraucher im Internet in die Lage versetzen, Werbebotschaften zu erhalten, die auf ihre individuellen Interessen zugeschnitten sind¹³⁹.

Was übrigens die vorgenannte Fusion betrifft, hat ein kalifornischer Bürger beim Obersten Gerichtshof des Bundesstaates Kalifornien gegen die Firma DoubleClick eine Klage auf Unterlassung wegen rechtswidrigen, irreführenden und betrügerischen Geschäftsgebarens im Internet eingereicht, durch das das Recht der Öffentlichkeit auf Privatsphäre verletzt werde. In der Klageschrift heißt es, dass DoubleClick die Öffentlichkeit irre geführt habe und weiterhin führe "(...), indem diese Firma falsche Vorstellungen vom Schutz der Privatsphäre und Sicherheit bezüglich der Internet-Nutzung vermittelt, während sie in täuschender Absicht die privaten und persönlichsten Informationen von Millionen von Internet-Nutzern mit Gewinnabsicht erwirbt, speichert und verkauft. (...) Wenn ein Internet-Nutzer eine mit DoubleClick verknüpfte Website besucht, wird auf seinem Computer ein eindeutig identifizierbares Cookie platziert. Besucht dieser Nutzer nun eine weitere Website, die Informationen über die Identität des Nutzers enthält, (...) wird dessen Identität mit dem identifizierenden Cookie verknüpft. Somit sind die Beklagten durch Verwendung der Abacus-Datenbank in der Lage, gegebenenfalls umfangreiche personenbezogene Informationen über den Nutzer zu erhalten. Zusätzlich werden seine Kaufgewohnheiten und Reaktionen auf Werbespots sowie die besuchten Websites verfolgt und aufgezeichnet"¹⁴⁰.

DoubleClick erklärte, dass nach den Reaktionen der Öffentlichkeit auf das Vorhaben, ihre eigene Datenbank mit derjenigen der Firma Abacus zu verknüpfen, bisher keine konkreten Schritte zu einer solchen Zusammenlegung erfolgt seien.

Als weiteres Beispiel dafür, wie personenbezogene Daten auf eine Weise verarbeitet werden können, die der gewöhnliche Internet-Nutzer nicht erwartet, kann die Tätigkeit von SurfAid genannt werden, einem kleinen Unternehmen, das Teil der globalen Dienstleistungsabteilung von IBM ist und seinen Sitz in Somers (New York) hat¹⁴¹. Dieses Unternehmen erhält von seinen Kunden täglich die Protokolle über die Netzzugriffe und verarbeitet diese Dateien, um die Wege der Besucher der Websites seiner Kunden zu

¹³⁸ Dies wird erwähnt in der Studie von GAUTHRONET, S. und NATHAN, F., *On-line services and data protection and privacy*, herausgegeben von der Kommission der Europäischen Gemeinschaften, abrufbar unter: http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serve.pdf

¹³⁹ www.doubleclick.net:8080/privacy_policy/

¹⁴⁰ Harriet M. Judnick versus DoubleClick, Inc.

¹⁴¹ WATTERSON, Karen, *La minería de datos ya es una tendencia dominante*. DATAMATION (Spanische Ausgabe), Februar 2000.

verfolgen. Sodann setzt es höchst effektive *datamining*-Programme ein, um die elektronischen Karteien der Kunden auszuwerten, die in manchen Fällen mehr als 150 Millionen Klicks (hits) verzeichnen, und verfasst tägliche Berichte für die Kunden. Diese können die Daten anschließend mit Hilfe von *OLAP*-Programmen weiter aufschlüsseln und die Informationen analysieren.

2. Eine weitere Gefahr, der Privatpersonen ausgesetzt sind, wenn sie elektronische Geschäfte abwickeln, ist der Bruch der Vertraulichkeit der übermittelten Informationen. Da das Internet ein öffentlich zugängliches Netzwerk mit allseits bekannten *Protokollen* ist, das stärker auf den Austausch von Informationen als auf den Schutz der Vertraulichkeit oder auf die Sicherheit ausgerichtet ist, ist es für jemanden mit einigen technischen Kenntnissen nicht sehr schwierig, genügend Softwareprogramme zu finden, mit denen die im Internet übermittelten Daten abgefangen und entschlüsselt werden können. Auch Unternehmen oder Einrichtungen lassen sich "personalisieren", um über sie Informationen zu erhalten, die später für Betrügereien oder andere Straftaten verwendet werden können.

3. Es zeichnet sich eine neue Form der Geschäftsabwicklung ab: Mobiler elektronischer Handel, der auf der Entwicklung der dritten Generation der Handys und anderer handlicher Geräte beruht, die bei Verwendung eines neuen Protokolls¹⁴² einen sicheren Zugang zu E-Mails und Websites gestatten. Folglich können Standort- und Verkehrsdaten wie auch Reismuster zu den Daten über die Transaktionen und die Suchvorgänge hinzugefügt werden, um ein noch präziseres Profil des Verbrauchers zu erstellen. Berücksichtigt man ferner, dass Fusionen und Konzentrationen unter Telekommunikationsbetreibern, Diensteanbietern, *Portal*- und Inhalte-Unternehmen stattfinden, wächst die Möglichkeit der Aggregation von Daten und ihrer gemeinsamen Verarbeitung in exponentialer Form.

Als einfaches Beispiel, wie dies in naher Zukunft funktionieren könnte, lässt sich voraussagen, dass Werbespots Personen über ihre Handys oder PDA (Persönliche Digital-Assistenten) überall hin nachfolgen können. "Es handelt sich um eine Art Zielsuche mit Hilfe des globalen Positionierungssystems, die schon bald in Reichweite ist", erklärte ein Sprecher von DoubleClick¹⁴³.

Ein weiteres Beispiel ist das gemeinsame Projekt von Yahoo und CellPoint Systems AB, mit Hilfe der Mobiltelefone einen "Standortermittler" (Locator) von Person zu Person gemeinsam zu vermarkten. Mit dem System "Yahoo! Find-A-Friend" können unter Verwendung des GSM-Mobiltelefon-Netzwerks Informationen folgender Art erhalten werden: "John befindet sich in der Nähe des Piccadilly Circus, ca. 3,2 km nordwestlich von Ihnen". Selbst wenn eine Einwilligung zur Teilnahme an diesem System verlangt wird, zeigt das Beispiel doch die neuartigen Möglichkeiten der aktuellsten Telekommunikationstechnologien, die gestatten, Personen mit Hilfe mobiler Geräte aufzuspüren¹⁴⁴.

V. Rechtliche Beurteilung

Zunächst muss daran erinnert werden, wie bereits ausführlich in Kapitel 3 erläutert wurde, dass die Datenschutzvorschriften der Richtlinien 95/46/EG und 97/66/EG für das Internet und die personenbezogenen Daten gelten, die beim elektronischen Geschäftsverkehr verarbeitet werden¹⁴⁵. In den folgenden Abschnitten werden diejenigen Aspekte dieser Rechtstexte im Mittelpunkt stehen, die für den Bereich des elektronischen Geschäftsverkehrs besonders relevant sind.

¹⁴² Wireless Application Protocol (WAP).

¹⁴³ Jane Weaver, MS NBC, 16.04.2000.

¹⁴⁴ Zu weiteren Informationen siehe: <http://www.cellpt.com/v2/000504.htm>

¹⁴⁵ *Verarbeitung personenbezogener Daten im Internet*. Arbeitsdokument der Arbeitsgruppe 'Schutz natürlicher Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten', angenommen am 23. Februar 1999. (<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm>).

Rechtmäßigkeit der Verarbeitung: Grundsatz der Zweckentsprechung (Artikel 5 bis 7 der Richtlinie 95/46/EG)

Zunächst einmal ist die rechtmäßige Erhebung und Verarbeitung von Daten nach Treu und Glauben nach den Grundsätzen der Zweckentsprechung und der Verhältnismäßigkeit zu betrachten. Im Zusammenhang mit dem elektronischen Geschäftsverkehr muss beachtet werden, dass die personenbezogenen Daten in einer Weise erhoben werden können, die dem Nutzer verborgen bleibt. Die Arbeitsgruppe hat wiederholt ihre Sorge über alle Formen von Verarbeitung zum Ausdruck gebracht, die derzeit durch Software und Hardware im Internet ohne Wissen der betroffenen Personen durchgeführt werden und für sie folglich "unsichtbar" bleiben¹⁴⁶.

Wenn personenbezogene Daten über Internet-Nutzer erhoben werden, sind ihnen klare Auskünfte über den Zweck der Verarbeitung und über die Empfänger oder Kategorien von Empfängern dieser Informationen zu erteilen, damit sie entscheiden können, ob sie unter den gegebenen Bedingungen den geschäftlichen Vorgang ausführen möchten.

Auch die sekundäre Verwendung der personenbezogenen Daten muss explizit gemacht und dafür die Einwilligung eingeholt werden, vorausgesetzt, dass die sekundäre Verwendung als nicht mit dem Hauptzweck vereinbar zu betrachten ist. Beispiele für nicht vereinbare sekundäre Verwendungen sind die Übermittlung von Daten aus dem Geschäftsverkehr an Dritte, mit denen jene für ihre Werbekampagnen Käuferprofile erstellen können¹⁴⁷, oder aber die Verwendung von *datamining*-Programmen, mit denen aus Listen von besuchten Websites Verhaltensmuster der Internet-Nutzer abgeleitet werden können.

Es ist darauf hinzuweisen, dass für die Verarbeitung von personenbezogenen Daten im Rahmen eines kommerziellen elektronischen Vorgangs keine Einwilligung des Betroffenen erforderlich ist, wenn die Erhebung der erforderlichen Daten für die Durchführung des Geschäftsvorgangs notwendig ist. Dies ist gemäß Artikel 7 Buchstabe b) der Richtlinie ein legitimer Grund für die Verarbeitung der personenbezogenen Daten des Nutzers an sich. Alle sonstigen damit zusammen hängenden Daten, vor allem auch unsichtbare Daten, die für die Durchführung des Vorgangs in keiner Weise erforderlich sind, können nur auf der Grundlage anderer rechtmäßiger Gründe, wie sie in Artikel 7 der Richtlinie aufgeführt sind, verarbeitet werden, also: Einwilligung ohne jeden Zweifel, Erfüllung einer rechtlichen Verpflichtung, Wahrung lebenswichtiger Interessen der betroffenen Person oder Verwirklichung eines berechtigten Interesses des für die Verarbeitung Verantwortlichen, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Dies gilt auch für staatliche Geschäftsvorgänge, da sich die Rechtmäßigkeit der Erhebung und Verarbeitung von personenbezogenen Daten durch öffentliche Stellen aus Rechtsvorschriften ableitet¹⁴⁸.

Eine sekundäre Verwendung, die häufig von den für die Datenverarbeitung Verantwortlichen genannt wird, ist die technische Wartung und Dimensionierung der IT-Ausrüstungen. Dies ist zweifellos ein legitimes Anliegen, um den Kunden einen guten Service zu bieten, kann aber problemlos mit nicht identifizierbaren Daten erfolgen, da für die Dimensionierung der Computer und Telefonleitungen lediglich aggregierte Zahlen erforderlich sind. Die für die Verarbeitung Verantwortlichen dürfen personenbezogene Daten nur dann aus technischen Gründen speichern, wenn es für diesen Zweck absolut unerlässlich ist und ein berechtigter Grund für die Verarbeitung dieser Daten vorhanden ist.

¹⁴⁶ Empfehlung 1/99 zum Thema "Unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet mit Hilfe von Software und Hardware", von der Arbeitsgruppe 'Schutz natürlicher Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten' am 23. Februar 1999 angenommen.
(<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm>).

¹⁴⁷ Richtlinie 95/46/EG, Artikel 14 Buchstabe b).

¹⁴⁸ Zur Erörterung des Grundsatzes der Zweckentsprechung bei öffentlich zugänglichen Daten siehe auch Kapitel 6.

Unterrichtung der betroffenen Personen (Artikel 10 der Richtlinie 95/46/EG)

Darüber hinaus müssen die für die Datenverarbeitung Verantwortlichen den betroffenen Personen eindeutige Informationen liefern, nämlich über die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung und die Empfänger der Daten sowie eine Erklärung, ob die Beantwortung von Fragen obligatorisch oder freiwillig ist und welche möglichen Folgen eine Nichtbeantwortung haben kann und schließlich Hinweise auf das Recht auf Auskunft und auf Berichtigung der sie betreffenden Daten. Sofern Dateninhaber berechtigt sind, eine Verarbeitung abzulehnen, müssen sie darauf hingewiesen werden.

Die entsprechenden Hinweise sind den Datenträgern entweder unmittelbar an dem Bildschirm zu liefern, an dem die Informationen erhoben werden, oder aber durch einen Hinweis, wie in Kapitel 5 erläutert wurde.

Bei Websites ist es sehr einfach, den Datennutzern diese Informationen zu liefern und sicher zu erfahren, ob die Betroffenen die Möglichkeit hatten, sie zumindest zu lesen, indem ein entsprechender Hinweis als obligatorischer Teil eines Geschäftsvorgangs eingeblendet wird, bevor vom Verbraucher irgendeine Entscheidung getroffen wird. Um vollständig sicher zu sein, dass die angezeigten Geschäftsbedingungen später nicht geändert werden, können sie mit dem privaten Schlüssel des Händlers elektronisch signiert werden. Auf diese Weise hat der Nutzer einen Nachweis darüber, welchen Bedingungen er zugestimmt hat. Dieses Konzept ist eine korrekte Umsetzung von Artikel 10 Absatz 3 der Richtlinie über den elektronischen Geschäftsverkehr, in der es heißt:

*"Die Vertragsbestimmungen und die allgemeinen Geschäftsbedingungen müssen dem Nutzer so zur Verfügung gestellt werden, dass er sie speichern und reproduzieren kann".*¹⁴⁹

Aufbewahrung von personenbezogenen Daten bzw. von Verkehrsdaten (Artikel 6 der Richtlinie 95/46/EG bzw. Artikel 6 der Richtlinie 97/66/EG)

Artikel 6 Absatz 1 Buchstabe e) der Richtlinie 95/46/EG enthält die Vorschrift, identifizierbare Daten nicht länger aufzubewahren, als für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

Bezüglich der Verkehrsdaten müssen die durch Artikel 6 der Richtlinie 97/66/EG auferlegten engen Beschränkungen eingehalten werden: Verkehrsdaten sind nach Beendigung der Verbindung (in diesem Fall des elektronischen Geschäftsverkehrs) zu löschen oder zu anonymisieren.

Die Arbeitsgruppe hat die besondere Thematik der Aufbewahrung von Verkehrsdaten durch die *Internet-Diensteanbieter* zum Zwecke der Strafverfolgung in ihrer Empfehlung 3/99 behandelt¹⁵⁰. In dieser Empfehlung wird betont, dass Verkehrsdaten im Prinzip nicht allein zum Zweck der Strafverfolgung aufbewahrt werden sollten, und dass die einzelstaatlichen Rechtsvorschriften den Telekommunikationsbetreibern, Telekommunikationsdiensten und Internet-Diensteanbietern nicht vorschreiben sollten, Verkehrsdaten für einen längeren Zeitraum aufzubewahren, als für Zwecke der Gebührenabrechnung erforderlich ist¹⁵¹.

¹⁴⁹ Richtlinie 2000/31/EG vom 8. Juni 2000.

¹⁵⁰ Siehe <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm>

¹⁵¹ Siehe hierzu auch die weiter oben erwähnte offizielle Erklärung der Europäischen Datenschutzbeauftragten auf ihrer Sitzung von Stockholm: *Wo Verkehrsdaten in besonderen Fällen aufbewahrt werden müssen, muss eine nachweisbare Notwendigkeit vorliegen, muss die Aufbewahrungszeit so kurz wie möglich sein und muss diese Maßnahme gesetzlich eindeutig geregelt sein.*

Automatisierte Einzelentscheidungen (Artikel 15 der Richtlinie 95/46/EG)

Wie bereits gesagt, dürfen Daten im Zusammenhang mit Geschäftsvorgängen nicht unbegrenzt aufbewahrt werden. Dies gilt insbesondere in den Fällen, in denen Daten für automatisierte Entscheidungen betreffend Einzelpersonen auf der Grundlage von früher gespeicherten Daten verwendet werden sollen (etwa die Ablehnung eines Antrags oder einer Kaufabsicht).

In solchen Fällen müssen den betroffenen Personen geeignete Garantien gewährt werden¹⁵². Dazu gehört erstens das Recht jeder Person, keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten ergeht, es sei denn, sie ergeht im Rahmen eines Vertrags oder ist durch ein Gesetz zugelassen, und zweitens das Recht auf Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten.

Rechte der betroffenen Personen (Artikel 12 der Richtlinie 95/46/EG)

Auch sind eindeutige und wirksame Verfahren gesetzlich vorgeschrieben, die eine Ausübung des Rechts der Betroffenen auf Zugang, Berichtigung, Streichung oder Blockierung ihrer Daten gestatten. Wenn die Betroffenen ihre Rechte wahrnehmen, müssen ihnen die für die Verarbeitung Verantwortlichen transparente Auskünfte darüber erteilen, ob in ihren Dateien entsprechende personenbezogene Daten registriert sind und falls ja, welche Daten verarbeitet werden, woher sie stammen, wozu sie verarbeitet werden, welche Kategorien von Daten betroffen sind und wer die Empfänger oder Gruppen von Empfängern sind, an die die Daten weitergegeben werden sollen. Diese Mitteilungen müssen in verständlicher Form erfolgen und es wird - im Zusammenhang mit dem elektronischen Geschäftsverkehr - empfohlen, diese Informationen über die hergestellte Online-Verbindung zu übermitteln, sofern die betroffenen Personen sie nicht auf irgend einem anderen üblichen Weg angefordert haben.

Ein sehr wichtiger Aspekt bezüglich des Zugangs zu Daten aus dem elektronischen Geschäftsverkehr ist das Recht der Betroffenen, Informationen nicht nur bezüglich der Grunddaten zu erhalten, sondern auch hinsichtlich der abgeleiteten oder zusammengefassten Informationen. Das heißt, wenn irgend eine Form von Profilerstellung, Klassifizierung, Einteilung in Kategorien oder auch Ergänzung mit Daten von Dritten erfolgt, müssen diese verarbeiteten Informationen ebenfalls den einzelnen Nutzern gemäß Artikel 12 Buchstabe a) der Richtlinie 97/66/EG mitgeteilt werden.

Verpflichtungen der für die Verarbeitung Verantwortlichen: Vertraulichkeit und Sicherheit (Artikel 16 und 17 der Richtlinie 95/46/EG bzw. 4 und 5 der Richtlinie 97/66/EG)

Im Hinblick auf die Vertraulichkeit und Sicherheit müssen die für die Verarbeitung Verantwortlichen geeignete Maßnahmen treffen, um die von ihren Kunden gelieferten Informationen gegen unberechtigten Zugang oder unberechtigte Weitergabe zu schützen, insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden, wie dies bei elektronischen Transaktionen im Internet der Fall ist. Diese Maßnahmen müssen die Risiken für Sicherheit und Vertraulichkeit, die Art der zu schützenden Daten und den Stand der Technik berücksichtigen.

Anwendbares einzelstaatliches Recht (Artikel 4 der Richtlinie 95/46/EG)

Ein weiterer Punkt, der beim elektronischen Handel im Internet beachtet werden muss, ist das Recht, das für die Verarbeitung von personenbezogenen Daten gilt, die aus Websites außerhalb der EU/EEA stammen. Hier stellen sich einer Reihe von Fragen, die nicht immer leicht beantwortet werden können und von Fall zu Fall zu analysieren sind. Dabei ist allerdings zu berücksichtigen, dass die Bestimmungen der Richtlinie 95/46/EG für Verarbeitungsvorgänge gelten, die vollständig oder teilweise mit Geräten auf dem

¹⁵² Siehe auch Artikel 12 Buchstabe a) Dritter Spiegelstrich der Richtlinie 95/49/EG.

Hoheitsgebiet der EU durchgeführt werden, selbst wenn sich die für die Verarbeitung Verantwortlichen außerhalb des Gemeinschaftsgebiets befinden¹⁵³.

VI. Zusammenfassung

- Zur vollständigen Einhaltung der Auskunftspflicht sind den betroffenen Personen eindeutige und verständliche Informationen zu liefern. Vor allem müssen die Datenschutzinformationen, die eng mit der Durchführung der elektronischen Transaktion zusammen hängen, als obligatorischer Schritt bei der elektronischen Transaktion sichtbar dargestellt werden, um zu gewährleisten, dass diese Hinweise den Nutzern zugestellt wurden. Dies gilt unbeschadet der Auskünfte für Websites-Besucher, die nicht einkaufen. Als ergänzende Maßnahme sind dem Nutzer die mit einer digitalen Signatur versehenen Bedingungen der Verarbeitung von personenbezogenen Daten zu überlassen, damit er später nachprüfen kann, dass die Klauseln nicht geändert wurden.
- Der Grundsatz der Verhältnismäßigkeit muss ohne Abstriche eingehalten werden. Es dürfen nur solche Daten erhoben werden, die für die Durchführung der elektronischen Transaktion unerlässlich sind. Zudem muss die Verarbeitung aller Daten (insbesondere solcher, die für den Nutzer nicht sichtbar verarbeitet werden) auf der Grundlage einer der in Artikel 7 der Richtlinie 95/46/EG angegebenen Bedingungen gerechtfertigt sein.
- Für den Fall, dass Nutzer entscheiden, nicht mehr personenbezogene Daten bekannt zu geben, als für die Durchführung der elektronischen Transaktion erforderlich sind, darf in den Geschäftsbedingungen für die Transaktion keine diskriminierende Klausel gegen sie enthalten sein.
- Ohne Wissen der betroffenen Personen darf keine sekundäre Verarbeitung stattfinden, und den Nutzern sind bereits beim Versuch des Zugangs vollständige Informationen über den logischen Aufbau der Verarbeitung ihrer Daten zu bieten. Ferner muss eine unzweideutige Einwilligung oder ein sonstiges Legitimierungskriterium gemäß Richtlinie 95/46/EG vorliegen, damit die Datenverarbeitung rechtmäßig ist.
- Es sind *Verschlüsselungs*-Technologien zu verwenden, die den gesetzlichen Bestimmungen entsprechen, um so weit wie möglich die Vertraulichkeit elektronischer Transaktionen sicherzustellen und mit Hilfe der *elektronischen Signatur* die *Datenintegrität* der Mitteilungen zu gewährleisten.
- Für sichere elektronische Transaktionen ist es gegebenenfalls ratsam, *digitale Zertifikate* zu verwenden und, falls höhere Sicherheiten erforderlich sind, diese *digitalen Zertifikate* auf Chipkarten zu speichern.
- Unter dem Gesichtspunkt des Datenschutzes ist die Möglichkeit zur Verwendung von sicheren und anonymen Zahlungsverfahren ein entscheidender Bestandteil für den Schutz der Privatsphäre im Internet.
- Die Erhebung und Verarbeitung von personenbezogenen Daten mit Hilfe von automatischen oder sonstigen Geräten, die sich im Hoheitsgebiet der EU bzw. des EEA befinden, unterliegt den Bestimmungen des gemeinschaftlichen Datenschutzrechts.
- Bei Verkehrsdaten müssen die strengen Auflagen von Artikel 6 der Richtlinie 97/66/EG beachtet werden und sollte die Empfehlung 3/99 über die Aufbewahrung von Verkehrsdaten durch *Internet-Diansteanbieter* zum Zwecke der Strafverfolgung Berücksichtigung finden.

¹⁵³ Zu weiteren Einzelheiten siehe Kapitel 3.

KAPITEL 8: CYBERMARKETING

I. Einleitung

Das Internet ist nicht nur eine weltweite Informationsplattform, sondern auch ein weltweiter Marktplatz, auf dem miteinander im Wettbewerb stehende Unternehmen potentielle Kunden anwerben wollen. Der Erfolg ist davon abhängig, dass möglichst viele Nutzer erreicht werden, und insbesondere solche, bei denen ein wirkliches Interesse an von Unternehmen angebotenen Produkten oder Dienstleistungen besteht. Um diese zu erreichen, werden Nutzerprofile und zielgerichtete Anzeigen verwendet, die durch Werbefenster auf Websites verbreitet werden.

Ein anderer Weg, Nutzer zu erreichen, ist der Versand von E-Mails; der wiederholte Versand nicht angeforderter E-Mails an E-Mail-Adressen (d.h. an Einzelpersonen), die in den öffentlichen Bereichen des Internets gefunden wurden, wird dabei häufig als der effizienteste Weg betrachtet. Dieser unbeliebte Typus des E-Mail-Versands wird als "*Spamming*" bezeichnet¹⁵⁴.

In beiden Fällen werden personenbezogene Verbraucherdaten benötigt. Diese Daten lassen sich häufig leicht im Internet erheben. Viele Internet-Nutzer merken nicht, dass sie beim Surfen eine große Menge von Daten zurücklassen, die Rückschlüsse auf ihre Interessengebiete, Vorlieben und ihr Verhalten ermöglichen¹⁵⁵.

Zielorientierte Werbung kann in gewissem Umfang akzeptiert werden, sofern sie im Verbraucherinteresse liegt. Wenn jedoch die Nutzer nicht wissen, welche Daten über sie von wem und für welchen Zweck erfasst werden, dann verlieren sie die Kontrolle über ihre personenbezogenen Daten. Daher ist es nicht korrekt, diese Daten ohne Zustimmung der Nutzer oder gar ohne ihr Wissen zu erfassen.

II. Technische Beschreibung

Online-Erstellung von Datenprofilen und Werbung¹⁵⁶

Die Online-Erstellung von Datenprofilen kann in verschiedener Form geschehen:

- Eine Website erzeugt Profile, indem sie Nutzerdaten erfasst, die bei der Interaktion zwischen Websites und ihren Besuchern entstehen. Dies geschieht mit Hilfe von *Cookies*, die die Bewegungen der Nutzer im Web aufzeichnen. Je nachdem, wie der Browser der Nutzer konfiguriert ist, sind diese nicht darüber im Bilde, dass die Website ein *Cookie* auf ihrer Festplatte platziert. Aufgrund des Nutzerprofils bietet die Website dem Kunden Produkte (z.B. Bücher) oder Verweise auf andere Websites an, die für den Nutzer von Interesse sein könnten.
- Beim "Cybermarketing mit Anreizen" können Personen an Spielen oder Wettbewerben teilnehmen, sofern sie personenbezogene Daten als Grundlage für Kundenprofile beisteuern. In diesem Fall wird die

¹⁵⁴ Siehe Kapitel 4: Elektronische Post, Abschnitt V. Analyse spezifischer Aspekte: *Spam*.

¹⁵⁵ Zu weiteren Details über die beim Surfen erzeugten Daten siehe Kapitel 5: Surfen und Suchen.

¹⁵⁶ In diesem Zusammenhang muss der gemeinsame Standpunkt der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation zum Thema Online-Erstellung von Datenprofilen erwähnt werden, den sie auf ihrer 27. Sitzung am 4./5. Mai 2000 in Rethymnon/Kreta angenommen hat. Der Text der Empfehlung ist abrufbar unter: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm

Datenerfassung in der Regel mit Wissen der betroffenen Personen und mit ihrer Zustimmung durchgeführt¹⁵⁷.

- Internet-Werbefirmen (z.B. DoubleClick, Engage¹⁵⁸) verwalten und liefern auf Vertragsbasis an zahlreiche Websites Werbe-Banner¹⁵⁹. Diese werden über unsichtbare *Hyperlinks* mit den Werbefirmen auf der gewünschten Website platziert.

Um die Nutzer mit den jeweils "passendsten" Werbe-Bannern zu versorgen, erstellen die Internet-Werbefirmen Profile, indem sie über unsichtbare *Hyperlinks Cookies* einsetzen. Je nach Browserkonfiguration erkennen die Nutzer, dass *Cookies* platziert werden und können dazu ihre Einwilligung geben. Das Nutzerprofil ist mit der Kennung der *Cookies* der Werbefirmen verknüpft, so dass sich dessen Inhalt jedes Mal erweitern lässt, wenn der Kunde eine mit der Werbefirma vertraglich verbundene Website besucht.

Nach ihrer Analyse können die erfassten Daten durch demographische Daten (Alter, Geschlecht usw.) ergänzt und mit anderen Daten in Zusammenhang gebracht werden, die die Gruppe kennzeichnen, zu der ein Nutzer offensichtlich - d.h. wegen seines Online-Verhaltens - gehört (z.B. Interessen, Einstellungen). Solche Analyse- und Ergänzungsarbeiten können von speziellen auf dem Markt erhältlichen Programmen ausgeführt werden (insbesondere *datamining*-Tools).

Das Ergebnis dieser Verfahren sind sehr detaillierte Profile, die den Web-Unternehmen oder Internet-Werbefirmen die Prognose der Vorlieben, Bedürfnisse und Kaufgewohnheiten einzelner Verbraucher und auf der Grundlage dieser Einschätzungen die Lieferung von Werbe-Bannern ermöglichen, die den Interessen des Verbrauchers am ehesten entsprechen.

Wenn die erfassten Daten, die über die Kennnummer der von den Werbefirmen platzierten *Cookies* gesammelt werden, nicht mit den identifizierenden Daten¹⁶⁰ einer bestimmten Person verknüpft werden, können sie als anonym gelten. Doch häufig - etwa wenn Nutzer Bestellformulare auf einer Website ausfüllen, auf der eine Werbefirma ihre *Banner* platziert hat -, können identifizierende Daten mit in *Cookies* bereits enthaltenen Daten verknüpft oder zusammengelegt werden und ein die betreffende Person kennzeichnendes Profil abgeben.¹⁶¹

Elektronische Post

Für kommerzielle E-Mail-Werbekampagnen müssen Unternehmen umfangreiche und für ihre Zwecke brauchbare Listen von E-Mail-Adressen potentieller Kunden erwerben. Wie oben bereits dargestellt, ist es häufig recht einfach, die im Internet vorhandenen Quellen zu nutzen.

Es gibt drei verschiedene Möglichkeiten, um E-Mail-Adressen im Internet zu sammeln¹⁶²: unmittelbare Erhebung bei Kunden oder Besuchern von Websites, Erwerb oder Ausleihe von Listen, die von Dritten zur

¹⁵⁷ Dies wird jedoch nur dann der Fall sein, wenn die Website dem Nutzer ausreichend Informationen bezüglich der verarbeiteten Daten, des Zwecks ihrer Verarbeitung und der Identität des für die Datenverarbeitung Verantwortlichen usw. bietet. Siehe Artikel 10 der Richtlinie.

¹⁵⁸ Zu weiteren Details über die von DoubleClick verwendeten Techniken siehe *Gefahren für die Privatsphäre* in Kapitel 5, Surfen und Suchen, und in Kapitel 7, Elektronischer Geschäftsverkehr im Internet.

¹⁵⁹ Werbebanner sind kleine graphische Kästchen, die oberhalb oder als Teil des Website-Inhalts erscheinen.

¹⁶⁰ Es ist zu berücksichtigen, dass die Definition der identifizierenden Daten gemäß Artikel 2 Buchstabe a) der Richtlinie 95/46/EG sehr weit ist: "Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind".

¹⁶¹ Siehe Kapitel 3: Anwendung der Datenschutzvorschriften; Abschnitt I, Allgemeine rechtliche Überlegungen: personenbezogene Daten im Internet.

¹⁶² Zu weiteren Details über die Erfassung von E-Mail-Adressen siehe Kapitel 4, Elektronische Post.

Verfügung gestellt werden¹⁶³, und Erfassung aus öffentlich zugänglichen Bereichen des Internets¹⁶⁴ wie etwa öffentlichen E-Mail-Verzeichnissen oder E-Mail-Versandlisten, Newsgroups oder Chatrooms.

Manche Tools, die bei der Erfassung von E-Mail-Adressen helfen, sind im Internet erhältlich. Solche Programme durchsuchen Websites oder Teile des Usenets (Newsgroups), die im Vorfeld durch eine Liste von URL oder Stichwörtern (z.B. Sport, Reisen) festgelegt werden, die sich auf ein vorher festgelegtes Interessengebiet beziehen; anschließend stellen sie alle in den betreffenden Websites/Dokumentenseiten oder Foren gefundenen E-Mail-Adressen zur Verfügung. Zahlreiche Dienste arbeiten als Makler von Adressenlisten, indem sie E-Mail-Adressen erfassen und E-Mail-Verzeichnisse zu sehr günstigen Preisen verkaufen oder verleihen.

Andere Tools sind darauf spezialisiert, E-Mails wie „Maidienste-Anbieter“ zu versenden, d.h. ohne Rückgriff auf einen *ISP* oder sonstige Anbieter, die E-Mail-Dienste anbieten. Solche Programme stellen einerseits sicher, dass alle von diesen Anbietern installierten E-Mail-Spamfilter umgangen werden und dass andererseits der Versand schnell und automatisch abläuft. Wenn vom Absender gewünscht, kann er E-Mail-Massenversanddienste als Host nutzen, wobei Dritte - ebenfalls für wenig Geld - das *Spamming* durchführen.

III. Rechtliche Beurteilung

Für die Online-Erstellung von Datenprofilen und für E-Mail-Werbeaktionen gelten verschiedene Richtlinien.

Datenschutzrichtlinie

In der allgemeinen Datenschutzrichtlinie 95/46/EG heißt es, dass personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet, für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nur in einer mit diesen Zweckbestimmungen zu vereinbarenden Weise weiterverarbeitet werden dürfen¹⁶⁵.

Die Verarbeitung darf lediglich aus rechtmäßigen Gründen wie Einwilligung, Erfüllung eines Vertrags oder einer rechtlichen Verpflichtung oder unter Interessenabwägung erfolgen.¹⁶⁶ Ferner muss die betroffene Person über die beabsichtigte Verarbeitung ihrer Daten - dazu gehört auch die Überlassung an Dritte - vor der Übermittlung informiert werden¹⁶⁷, und sie muss zusätzlich ein Widerspruchsrecht gegen die Verarbeitung ihrer personenbezogenen Daten zu Zwecken der Direktwerbung erhalten.¹⁶⁸ Der Dateninhaber muss also das Recht auf Zugang zu den ihn betreffenden Daten haben, und das Recht, diese zu berichtigen, zu löschen oder zu sperren¹⁶⁹.

¹⁶³ Diese Listen können auch E-Mail-Adressen enthalten, die in öffentlich zugänglichen Bereichen des Internets gesammelt wurden.

¹⁶⁴ Siehe Kapitel 6, Veröffentlichungen und Foren.

¹⁶⁵ Richtlinie 95/46/EG, Artikel 6.

¹⁶⁶ Richtlinie 95/46/EG, Artikel 7.

¹⁶⁷ Richtlinie 95/46/EG, Artikel 10.

¹⁶⁸ Richtlinie 95/46/EG, Artikel 14.

¹⁶⁹ Richtlinie 95/46/EG, Artikel 12.

Richtlinie zum Fernabsatz

Die Richtlinie zum Fernabsatz¹⁷⁰ verlangt von den Mitgliedstaaten, dafür Sorge zu tragen, dass Fernkommunikationen unter Verwendung von Fernkopierern oder mit Automaten als Gesprächspartnern nur dann verwendet werden dürfen, wenn der Verbraucher seine vorherige Zustimmung dazu gibt. Bei anderen Fernkommunikationsmitteln wie elektronische Post ist dem Verbraucher zumindest das Recht auf Widerspruch einzuräumen¹⁷¹.

Besondere Richtlinie zum Schutz der Privatsphäre im Bereich der Telekommunikation

Die Richtlinie 97/66/EG lässt den einzelstaatlichen Gesetzgebern die Wahl, ob sie eine „Opt-in“- (vorherige Einwilligung) oder eine „Opt-out“-Regelung (nachträglicher Widerspruch) für unerbetene kommerzielle Mitteilungen mit anderen Mitteln als Fernkopierer und Automaten als Gesprächspartner (Voice-Mail-System) treffen wollen¹⁷². Die Verwendung von ‘Automaten als Gesprächspartner’ oder Faxgeräten zu Marketing-Zwecken unterliegt in jedem Fall der vorherigen Einwilligung des Verbrauchers¹⁷³. Der Begriff ‘Automaten als Gesprächspartner’, der sehr allgemein gehalten ist, kann leicht auf die elektronische Post übertragen werden.

Am 12. Juli 2000 nahm die Europäische Kommission einen Vorschlag für eine neue Richtlinie für die Verarbeitung personenbezogener Daten und zum Schutz der Privatsphäre im Bereich der Telekommunikation an, der die Richtlinie 97/66/EG ersetzen soll.

In diesem Vorschlag schließt der Artikel über unerbetene kommerzielle Mitteilungen ausdrücklich auch die elektronische Post ein; dies bedeutet, dass auch die Verwendung von elektronischer Post für kommerzielle Mitteilungen nur bei vorheriger Einwilligung der Teilnehmer gestattet ist.

Die Richtlinie über den elektronischen Geschäftsverkehr

In der Richtlinie über den elektronischen Geschäftsverkehr¹⁷⁴ heißt es, dass elektronische Mitteilungen in denjenigen Mitgliedstaaten, die nicht angeforderte kommerzielle Kommunikation mittels elektronischer Post zulassen, klar und unzweideutig als solche erkennbar sein müssen¹⁷⁵, und dass sogenannte Robinson-Listen, in die sich natürliche Personen eintragen lassen können, die keine derartigen kommerziellen Kommunikationen zu erhalten wünschen, von den Diensteanbietern regelmäßig konsultiert und beachtet werden müssen¹⁷⁶.

Obwohl sich weder die allgemeine Richtlinie noch die Telekommunikationsrichtlinie auf den elektronischen Handel beziehen, sind sie auf diesen Bereich anzuwenden: in den Erwägungsgründen und in Artikel 1 Absatz 5 Buchstabe b) der Richtlinie zum elektronischen Geschäftsverkehr wird klar zum Ausdruck gebracht, dass mit dieser Richtlinie keineswegs beabsichtigt ist, die Rechtsgrundsätze und Vorschriften des geltenden Rechtsrahmens zu ändern. Daraus folgt, dass die Umsetzung der Richtlinie zum elektronischen Geschäftsverkehr vollständig mit den Datenschutzgrundsätzen in den entsprechenden Rechtsvorschriften in

¹⁷⁰ Richtlinie 97/7/EG des Europäischen Parlamentes und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, Amtsblatt L 144 vom 04.06.1997, S. 19–27.

¹⁷¹ Richtlinie 97/7/EG, Artikel 10.

¹⁷² Richtlinie 97/66/EG, Artikel 12, Absatz 2.

¹⁷³ Richtlinie 97/66/EG, Artikel 12, Absatz 1.

¹⁷⁴ Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), Amtsblatt der Europäischen Gemeinschaften, 17. Juli 2000, L 178/1 bis 178/16.

¹⁷⁵ Richtlinie 2000/31/EG, Artikel 7.

¹⁷⁶ Richtlinie 2000/31/EG, Artikel 7.

Einklang stehen muss. Daher gelten weiterhin die einzelstaatlichen Datenschutzvorschriften für Unternehmen, die für die Verarbeitung von personenbezogenen Daten verantwortlich sind¹⁷⁷. Außerdem können die Mitgliedsstaaten Vorschriften erlassen, die sich im Rahmen der Telekommunikationsrichtlinie halten, aber über die Vorschriften der Richtlinie zum elektronischen Geschäftsverkehr hinausgehen, das heißt, kommerzielle Mitteilungen können der vorherigen Zustimmung der Empfänger unterliegen¹⁷⁸.

IV. Zusammenfassung

Die in der allgemeinen Richtlinie, der Richtlinie zum elektronischen Geschäftsverkehr, der Richtlinie zum Fernabsatz und der Telekommunikationsrichtlinie festgelegten Vorschriften lassen sich auch auf die Nutzung der elektronischen Post für Cybermarketing-Zwecke anwenden.

Nur die allgemeine Richtlinie gilt für die Online-Erstellung von Profilen. Obwohl diese Bestandteil des elektronischen Geschäftsverkehrs sind, werden sie in der Richtlinie zum elektronischen Geschäftsverkehr nicht behandelt. Von der geänderten Telekommunikationsrichtlinie wird ebenfalls nicht die Werbung im Netz erfasst, da Anbieter solcher Dienstleistungen aus dem Geltungsbereich dieser Richtlinie ausdrücklich ausgeschlossen sind.

Es lässt sich also wie folgt zusammenfassen:

Online-Erstellung von Datenprofilen und Werbung¹⁷⁹

- Internet-Diensteanbieter müssen ihre Nutzer über die beabsichtigte Verarbeitung ihrer Daten informieren, ehe diese erfasst werden¹⁸⁰. Dazu gehören Art, Umfang und Dauer der Datenspeicherung sowie der Zweck ihrer Verarbeitung, d.h. die Verwendung für die Erstellung von Datenprofilen¹⁸¹. Wenn die Daten an Dritte weitergegeben werden, muss auch dies ausdrücklich angegeben werden.

Diese Angaben müssen auch in den Fällen gemacht werden, in denen Daten unter Verwendung von Pseudonymen oder nicht personenbezogenen Kennungen erfasst werden. Insbesondere müssen die Nutzer informiert werden, ehe *Cookies* für die Erstellung von Profilen eingesetzt werden. Dies muss durch eine besondere grafische Hinweisfläche geschehen, die auch dann aktiviert wird, wenn der Browser den Nutzer **nicht** über die Platzierung von *Cookies* informiert.

- Neben den rechtmäßigen Gründen, die als Voraussetzung für eine Verarbeitung vorhanden sein müssen (siehe Artikel 7 der Richtlinie 95/46/EG), ist den Nutzern das Recht einzuräumen, jederzeit der Verarbeitung ihrer Daten zu widersprechen¹⁸². Infolgedessen dürfen Daten, die bei künftigen Besuchen im Internet erfasst werden, nicht zur Erweiterung eines vorhandenen, personenbezogenen Profils verwendet werden. Dies gilt auch in solchen Fällen, in denen die Verarbeitung eine vorherige Einwilligung der Nutzer voraussetzt.

¹⁷⁷ Richtlinie 95/46/EG, Artikel 4.

¹⁷⁸ Richtlinie 97/66/EG, Artikel 12. – Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [KOM (2000) 385 endg.], Artikel 13, *Unerbetene Nachrichten*.

¹⁷⁹ Diese Schlussfolgerungen lehnen sich an einen Beschluss der deutschen Datenschützer an, der sich auf einen bestimmten Internet-Anzeigendienst bezieht. Die *Internationale Arbeitsgruppe zum Datenschutz im Telekommunikationsbereich* nahm einen *Gemeinsamen Standpunkt* an, der ebenfalls auf diesen Beschluss zurückgeht. Siehe dazu: http://www.datenschutz-berlin.de/doc/int/iwgdp/pt_en.htm

¹⁸⁰ Richtlinie 95/46/EG, Artikel 10.

¹⁸¹ Richtlinie 95/46/EG, Artikel 6.

¹⁸² Richtlinie 95/46/EG, Artikel 14.

- Das "Personalisieren" von Datenprofilen setzt die vorherige Einwilligung bei Kenntnis aller Details der betroffenen Personen voraus. Sie müssen das Recht haben, ihre Zustimmung jederzeit und mit sofortiger Wirkung zu entziehen.
- Die Nutzer müssen jederzeit Gelegenheit haben, ihre Datenprofile zu überprüfen. Sie müssen auch das Recht haben, die gespeicherten Daten zu berichtigen oder zu löschen¹⁸³.

Elektronische Post

- Unternehmen, die E-Mail-Adressen **unmittelbar bei den Nutzern** erfassen, um sie für den eigenen Versand von E-Mails oder für den E-Mail-Versand durch Dritte zu nutzen, an welche die E-Mail-Adressen weitergegeben werden, muss die Nutzer durch geeignete technische Mittel zum Zeitpunkt der Erfassung über diese Zwecke informieren¹⁸⁴.
- Solange den Mitgliedstaaten freigestellt ist, ob sie die Opt-in- oder die Opt-out-Regelung wählen, müssen Unternehmen, die kommerzielle E-Mails versenden, durch geeignete technische Mittel sicherstellen, dass diese E-Mails vom Empfänger als solche erkannt werden können¹⁸⁵.
- Solange den Mitgliedstaaten freigestellt ist, ob sie die Opt-in- oder die Opt-out-Regelung wählen, müssen die Unternehmen vor dem Versand kommerzieller E-Mails Robinson-Listen konsultieren, bei denen die Nutzer eingetragen sind, die keine kommerzielle E-Mails erhalten wollen. Diese Einträge sind in jedem Fall zu beachten¹⁸⁶. Das Vorhandensein internationaler Robinson-Listen wäre sehr vorteilhaft.
- Die Sammlung von E-Mail-Adressen **in öffentlich zugänglichen Bereichen des Internets** und ihre Verwendung für kommerzielle Zwecke widerspricht dem einschlägigen Gemeinschaftsrecht, d.i. der allgemeinen Richtlinie¹⁸⁷. Erstens stellt diese Praxis eine unlautere Form der Verarbeitung personenbezogener Daten dar¹⁸⁸. Zweitens wird damit gegen den Grundsatz der Zweckentsprechung verstoßen¹⁸⁹, da die Nutzer ihre E-Mail-Adressen für bestimmte Zwecke veröffentlichen, z.B. um an einer Newsgroup teilnehmen zu können; dieser Zweck ist ein ganz anderer als der des kommerziellen Versands von E-Mails. Drittens erfüllt diese Praxis nicht das Kriterium des ausgewogenen Verhältnisses der Interessen¹⁹⁰, da die Empfänger solcher E-Mails Nachteile durch Zeitverlust, Kosten und unzumutbare Störungen erleiden.
- In fünf Mitgliedstaaten (Deutschland, Österreich, Italien, Finnland und Dänemark) sind nicht angeforderte kommerzielle Kommunikation bereits verboten. In den übrigen Mitgliedstaaten gibt es entweder Regelungen, die Einsprüche gegen solche Sendungen zulassen, oder die Lage ist nicht ganz klar. Unternehmen in Staaten mit solchen Regelungen dürfen E-Mail-Adressen nicht nur im eigenen Land anschreiben, sondern auch an Verbrauchern in Mitgliedstaaten mit "Opt-in"-Regelungen. Da E-Mail-Adressen häufig keinen Hinweis auf den Wohnsitz des Empfängers enthalten, bietet ein System mit unterschiedlichen Regelungen innerhalb des Binnenmarktes keine gemeinsame Lösung zugunsten des Schutzes der Privatsphäre der Nutzer. Opt-in-Regelungen sind somit eine ausgewogene und

¹⁸³ Richtlinie 95/46/EG, Artikel 12.

¹⁸⁴ Richtlinie 95/46/EG, Artikel 10.

¹⁸⁵ Richtlinie 2000/31/EG, Artikel 7.

¹⁸⁶ Richtlinie 2000/31/EG, Artikel 7.

¹⁸⁷ Siehe *Stellungnahme 1/2000 zu bestimmten Datenschutzaspekten des elektronischen Handels*, vorgelegt von der Task Force 'Internet' (WP 28).

¹⁸⁸ Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe a).

¹⁸⁹ Richtlinie 95/46/EG, Artikel 6 Absatz 1 Buchstabe b).

¹⁹⁰ Richtlinie 95/46/EG, Artikel 7 Buchstabe f).

effiziente Lösung zur Beseitigung von Hindernissen für kommerzielle Mitteilungen, die gleichzeitig das Grundrecht der Verbraucher auf ihre Privatsphäre schützt. Die Arbeitsgruppe begrüßt und unterstützt infolgedessen den Vorschlag, unerbetene elektronische Mitteilungen wie Voice-Mail-Systeme und Faxgeräte zu behandeln. In allen diesen Situationen hat der Teilnehmer kein menschliches Gegenüber und trägt insgesamt oder teilweise die Kosten für die Kommunikation. Der Umfang des Eindringens in die Privatsphäre und der wirtschaftlichen Belastung sind also vergleichbar.¹⁹¹

¹⁹¹ Siehe dazu Stellungnahme 7/2000 vom 2. November 2000 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000, KOM (2000) 385 endg. WP 36.

KAPITEL 9: MASSNAHMEN ZUR BESSEREN ABSICHERUNG DER PRIVATSPHÄRE

I. Einleitung

Die EG-Datenschutzrichtlinie enthält zwei Grundsätze, die unmittelbare Folgen für Entwurf und Nutzung neuer Technologien haben:

- der Grundsatz der **Zweckentsprechung** besagt, dass personenbezogene Daten nur benutzt werden dürfen, wenn dies für festgelegte eindeutige und rechtmäßige Zwecke notwendig ist; mit anderen Worten, personenbezogene Daten dürfen nicht ohne berechtigten Grund benutzt werden, und der einzelne Nutzer bleibt anonym (Artikel 6 Absatz 1 Buchstabe b) und Artikel 7);
- der Grundsatz der **Datensicherheit** besagt, dass die für die Datenverarbeitung Verantwortlichen den Risiken entsprechende Sicherheitsmaßnahmen für die Speicherung oder Übermittlung personenbezogener Daten treffen müssen, durch die ihr Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang sichergestellt ist, insbesondere dann, wenn ihre Verarbeitung mit einer Datenübermittlung in einem Netzwerk einhergeht, kurz, dass diese Daten gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten geschützt werden (Artikel 17).

Der vorgenannte Grundsatz der Zweckentsprechung liegt dem Konzept der Technologien zur besseren Absicherung der Privatsphäre (PET) zugrunde. Dieses Konzept bezieht sich auf eine Anzahl ganz verschiedener Technologien, die dem Schutz der Privatsphäre dienen, indem sie insbesondere die Erfassung oder Weiterverarbeitung identifizierender Daten auf ein Mindestmaß beschränken oder unterbinden¹⁹².

Technologien zur besseren Absicherung der Privatsphäre haben das Ziel, jede rechtswidrige Form der Datenverarbeitung dadurch zu verhindern, dass sie es z.B. nicht autorisierten Personen technisch unmöglich machen, Zugang zu personenbezogenen Daten zu gewinnen, um deren mögliche Zerstörung, Veränderung oder Offenlegung zu verhindern.

Die praktische Umsetzung dieses Konzepts verlangt organisatorische und technische Lösungen.

Diese Technologien beruhen häufig auf dem Einsatz eines sogenannten Identitätsschutzes¹⁹³. Ein Identitätsschutz kann als Systembestandteil betrachtet werden, der die Freigabe der wahren Identität des Nutzers an verschiedene Prozesse innerhalb des Informationssystems regelt. Seine Wirkung besteht in der Abschirmung bestimmter Systemabschnitte, die keinen Zugang zur wahren Identität benötigen. Eine der wichtigsten Funktionen des Identitätsschutzes ist die Umwandlung der tatsächlichen Identität des Nutzers in eine Pseudoidentität, also eine stellvertretende (digitale) Identität, die der Teilnehmer annimmt, wenn er das System benutzt.

Um einen Identitätsschutz in ein Informationssystem einzubauen, können mehrere Techniken verwendet werden, unter anderem *Verschlüsselungs*-Techniken, bei denen *digitale Signaturen*, *Blindsignaturen*, *digitale Pseudonyme* und *vertrauenssichernde Dritte* eine Rolle spielen.

¹⁹² Siehe Bericht von HES, R. und BORKING, J. (Hg.), *Privacy-enhancing technologies: the path to anonymity (revised edition)*, Registratiekamer in Zusammenarbeit mit dem Informations- und Datenschutzbeauftragten von Ontario, Achtergrundstudien en Verkenningen 11, Den Haag, November 1998. Abrufbar unter: www.registratiekamer.nl

¹⁹³ Zu weiteren Details siehe PET-Bericht der Registratiekamer (op. cit.), vor allem S. 7ff.

II. Technologien zur besseren Absicherung der Privatsphäre

In diesem Abschnitt werden verschiedene Technologien zur besseren Absicherung der Privatsphäre beschrieben und untersucht¹⁹⁴.

Cookie-Killer

Nachfolgend werden zwei Lösungsmöglichkeiten für die Probleme näher untersucht, die sich für Schutz der Privatsphäre durch *Cookies* ergeben. Die erste stammt aus der Internet-Wirtschaft selbst und wurde in die wichtigsten marktgängigen Browser eingebaut. Die zweite Lösung stammt von verschiedenen Vorkämpfern für den Schutz der Privatsphäre oder von Softwareherstellern. Sie besteht aus Tools, die eine Löschung aller oder einiger *Cookies* ermöglichen.

Cookie-Abwehrverfahren der Softwarehersteller

Der einzige sichtbare Versuch, das Problem mit den *Cookies* zu lösen, ist ein Abwehrverfahren, das in den marktgängigen Browsern ab Version 3 eingesetzt wird. Es gestattet informierten Internet-Nutzern, ihre Browser auf folgende Alternativen einzustellen:

- alle *Cookies* akzeptieren;
- alle *Cookies* zurückweisen oder festlegen, dass sie keine Daten an ihren Herkunftsserver zurückschicken (Netscape);
- jedesmal neu anfragen, welche Maßnahme getroffen werden soll.

Solche *Cookie*-Abwehrverfahren bleiben aus vielerlei Gründen unzureichend:

1. Normalerweise sind die Browser so voreingestellt, dass sie die Privatsphäre am weitesten öffnen (nämlich: "alle *Cookies* akzeptieren"), und der durchschnittliche Internet-Nutzer weiß nicht, dass *Cookies* vielfach - z.B. von Cybermarketing-Unternehmen - dazu benutzt werden, in Suchmaschinen eingegebene Suchbegriffe mit Hilfe unsichtbarer Verarbeitungsverfahren zurückzuverfolgen.
2. Die Abweisung aller *Cookies* verhindert zwar den Erhalt neuer *Cookies*, nicht aber das systematische und unsichtbare Absenden bereits empfangener *Cookies*.
3. *Cookies* können sehr verschiedene Eigenschaften aufweisen: Manche *Cookies* sind nützlich und haben keinen Identitätsbezug (z.B. Ermittlung der Sprachpräferenzen). Andere verweisen zwar auf eine Identität, werden aber in Einklang mit den Datenschutzvorschriften verwendet. Die Abwehr **aller** *Cookies* muss also nicht im Interesse des Internet-Nutzers sein. Allgemein lässt sich sagen, dass *Sitzungs-Cookies*¹⁹⁵ wesentlich weniger in die Privatsphäre eindringen als dauerhafte *Cookies*.
4. Verschiedene Websites verweigern Nutzern den Zugang, die keine *Cookies* akzeptieren wollen.
5. Manche Websites (auch solche, die über unsichtbare *Hyperlinks* angeschlossen sind) senden massenweise *Cookies* aus und zwingen die Internet-Nutzer, eines nach dem anderen abzulehnen, was zu einer sogenannten "Anklickmüdigkeit" führt und die Nutzer veranlasst, *Cookies* ein für alle Mal zu akzeptieren, um ihre Ruhe zu haben.
6. In manchen Fällen kann eine unvollständige Formulierung der *Cookie*-Warnung¹⁹⁶ anscheinend

¹⁹⁴ Siehe auch EPIC-Onlineführer zu praktischen Werkzeugen zur Absicherung der Privatsphäre, abrufbar unter: www.epic.org/privacy/tools.html

¹⁹⁵ Solche *Cookies* ohne festgelegte Verweildauer werden nicht auf der Festplatte, sondern nur im RAM gespeichert und somit beim Abschalten des Computers gelöscht.

¹⁹⁶ Im britischen Programm des Microsoft-Internet-Explorers (MSIE 4.0) lautet die Cookiewarnung folgendermaßen: "Gestatten Sie dieser Website, Ihrem Computer zum Zwecke einer besser auf Sie zugeschnittenen Nutzung des Internets Informationen zur Verfügung zu stellen? Wenn Sie die Taste Ja betätigen, wird die Website eine Datei auf Ihrem Computer speichern. Wenn Sie die Taste Nein betätigen, kann es sein, dass die aufgerufene

missverständlich sein.

7. Bei der Installation eines neuen Browsers kann die erste besuchte Website (voreingestellt ist diejenige des Browserherstellers) ein *Cookie* aussenden, ehe der Nutzer Gelegenheit hatte, den *Cookie*-Empfang zu deaktivieren.

Im Juli 2000 kündigte Microsoft für die nächste Version des Internet-Explorers die Einführung der Beta-Version einer Programmkorrektur ("Patch") für die Datensicherheit an, die eine bessere Verwaltung der *Cookies* ermöglichen soll¹⁹⁷. Der Voraufklärung zufolge wird das Patch verschiedene Eigenschaften haben, die den Nutzern eine wirksamere Kontrolle der *Cookies* ermöglichen. Der Browser wird zwischen *Cookies* von erster und von dritter Seite unterscheiden können, und er wird so voreingestellt sein, dass er den Nutzer warnt, wenn ein *Cookie* von dritter Seite zur dauerhaften Installation eingeschleust werden soll. Außerdem erlaubt die neue Funktion der Programmkorrektur, dass die Internet-Nutzer sämtliche *Cookies* mit einem einzigen Tastendruck löschen und Informationen zu Sicherheit und Datenschutz leichter erhalten. Das Sicherheitspatch verbessert jedoch nicht die Kontrolle der Verbraucher über die Verwendung der *Cookies* von erster Seite, die auf kommerziellen Websites die Regel sind.

Unabhängige Programme

"*Cookie*-Wäscher", "*Cookie*-Zerkleinerer", "*Cookie*-Meister" oder "*Cookie*-Zermalmer" sind einige der Freeware- oder *Shareware*-Programme, die jeder Internet-Nutzer herunterladen und im Netz benutzen kann.¹⁹⁸ Auch hier gelten ähnliche Einwände wie oben:

1. Die Internet-Nutzer müssen über die *Cookies* wegen ihrer unterschiedlichen Art jedes Mal von Fall zu Fall entscheiden.
2. Bei *Shareware*-Programmen müssen die Internet-Nutzer manchmal für ihren Schutz bezahlen.
3. Die Programme zur Behandlung der *Cookies* sind nicht immer benutzerfreundlich oder für einen durchschnittlichen Internet-Nutzer leicht verständlich.

Proxy-Server

Proxy-Server vermitteln zwischen Internet-Nutzern und dem Netz. Sie wirken als *Web-Zwischenspeicher* ("Cache") und verbessern die Leistungsfähigkeit des Internets drastisch. Viele Organisationen oder Internet-Zugangsanbieter setzen diese Lösung bereits ein. Jede Seite, jedes Bild oder Logo, das von einem Mitarbeiter einer Organisation von außen heruntergeladen wird, ist in einem "Cache" gespeichert und steht damit augenblicklich auch anderen Mitarbeitern der Organisation zur Verfügung.

In diesem Fall benötigen die einzelnen Mitarbeiter einer Organisation, die dem *Proxy-Server* vorgeschaltet ist, keine eigene IP-Adresse, da sie nicht unmittelbar Zugang zum Internet erhalten. Außerdem übermittelt der *Proxy-Server* in der Regel¹⁹⁹ die IP-Adresse des Internet-Nutzers nicht an die Website und kann darüber hinaus die "Browser-Mitteilungen" herausfiltern. Da der *Proxy-Server* auch das *HTTP-Protokoll* verwaltet, können die dort eingefügten *Cookies* vom *Proxy-Server* leicht entfernt, verändert oder gespeichert werden.

Dokumentenseite nicht richtig wiedergegeben wird. Die Internet-Nutzer müssen anschließend ein weiteres Feld anklicken, um die Domain (nicht den Absender!) des *Cookies* und seine Speicherdauer zu erfahren.

¹⁹⁷ EPIC Alert 7.14 vom 27. Juli 2000.

¹⁹⁸ Einige dieser Programme finden sich unter <http://tucows.belgium.eu.net/cookie95.html>

¹⁹⁹ Leider fügen einige *Proxy-Server* die IP-Adresse des PCs, für den sie arbeiten, der *HTTP*-Kopfzeile hinzu.

Anonymisierungs-Software

Anonymisierungs-Software erlaubt es Nutzern, beim Besuch von Websites anonym zu interagieren, indem sie zunächst eine Anonymisierungs-Website aufsuchen, die ihre Identität kaschiert²⁰⁰.

Wenn sie bei einer Anonymisierungs-Website einen Zwischenstopp einlegen, ehe sie sich im Internet anderswohin wenden, können die Nutzer dafür sorgen, dass von dieser Website die personenbezogenen Daten, z.B. ihre IP-Adresse, zurückgehalten werden. Anonymisierungs-Websites unterbinden auch den Versand von Systemdaten (etwa über die verwendeten Betriebssysteme und Browser) an Websites, sie verhindern das Einfügen von *Cookies* in Browser und sie wehren *Java* und *JavaScript* ab, die Zugang zu personenbezogenen Daten in Browsern haben können.

Gute Beispiele für Anonymisierungs-Software sind "anonymizer"²⁰¹ oder das "zeroknowledge"-System²⁰².

Anonymisierer versprechen:

- als Vermittler zwischen Nutzern und besuchten Websites die Nutzeridentität vor eindringenden Spürprogrammen zu schützen,
- in Dokumentenseiten eingebettete Internet-Programme (*Java* und *JavaScript*) abzuwehren, die den Computer des Nutzers beschädigen oder sensible personenbezogene Daten erfassen können.

Anonymisierer bieten zwei Dienste, nämlich anonymes Surfen und anonymen EMail-Versand, und ein Produkt, nämlich den Anonymisierungs-Server. Dieser erlaubt es allen Nutzern, ihre eigene Anonymisierungs-Website herzustellen.

Internet-Nutzer müssen manchmal ein Entgelt entrichten, um Anonymisierungsdienste ohne Abstriche in Anspruch nehmen zu können. Ferner müssen sie jedes Mal eine Verbindung zur Anonymisierungswebsite herstellen, um Anonymisierungsdienste nutzen zu können, was bedeutet, dass dieser Dienst gegen eine Überwachung durch Dritte doch sehr anfällig ist. Anonymisierer bieten Dienste wie anonymes Surfen, Mailen oder Übermitteln von Dateien.

Technisch betrachtet funktioniert der Anonymisierer wie ein *Proxy-Server* und unterdrückt die Browser-Mitteilungen im *HTTP-Protokoll* und die IP-Adresse des Surfers.

Das Hauptproblem bei der Nutzung dieses Dienstes liegt darin, dass der Internet-Nutzer einem bestimmten Unternehmen vertrauen muss, und dass dieses Unternehmen über alles informiert ist, was der Nutzer im Web treibt.

Das **Zero Knowledge-System** bietet eine Software namens "Freedom". Diese Lösung beruht auf mindestens drei TCP/IP-Relais in Kombination mit starker *Verschlüsselung* (mindestens 128-Bit-Länge). Damit werden sämtliche Dienste verschlüsselt und anonymisiert, da das *TCP/IP-Protokoll* von jedem Netzdienst benutzt wird. Jede der drei TCP/IP-Zwischenstationen kennt jeweils nur die IP-Adresse ihres Vorgängers. Es wird kein Logbuch geführt, so dass selbst zwei Relais gemeinsam nicht in der Lage sind, eine angefragte oder eingeholte Information zurückzuverfolgen. Selbstverständlich wird der Leitweg der Mitteilungen dynamisch festgelegt und ändert sich selbst bei sehr kurzen Mitteilungen mit einiger Wahrscheinlichkeit. Ein System zur *Cookie*-Verwaltung ist in Freedom anscheinend integriert.

Ein anderes Beispiel für diese Art von Diensten bietet privada.com. Dieses Unternehmen bietet Dienste zur Unterstützung aller Arten von Transaktionen im Internet, darunter Suchen, elektronische Post, Nachrichtenübermittlung und in Kürze auch Handel. Die Infrastruktur von Privada beruht auf einem System der Abschottung und Verschlüsselung. Die Nutzer erhalten eine CD-ROM mit einem Computerprogramm namens PrivadaControl oder laden es von ihrem *ISP* herunter. Dieses Programm stellt

²⁰⁰ Siehe "Net Worth" (op. cit), S. 273ff.

²⁰¹ <http://www.anonymizer.com/3.0/index.shtml>

²⁰² <http://www.zeroknowledge.com>

die Verbindung zu den Netzwerkservern von Privada her, die sich bei den ISP befinden, und dient als Schutzwall ("firewall") für die Privatsphäre der einzelnen Nutzer. PrivadaControl soll sämtliche Nutzerinformationen und Daten vom Ausgangspunkt der Transaktion durch das gesamte Netz schützen und die Privatsphäre der Nutzer vor allen Beteiligten, auch Privada und dem *ISP*, sichern.

Durch die Verwendung von PrivadaControl richten die Nutzer ein privates elektronisches Konto ein, das ihre Online-Aktivitäten repräsentiert, während sämtliche persönlichen Nutzerinformationen davon abgekoppelt werden. PrivadaControl ermöglicht also den Nutzern, elektronische Identitäten zu schaffen und wieder zu beseitigen, während der Online-Interaktionen zwischen ihnen zu wechseln und sich selbst Merkmale und Eigenschaften zuzuweisen.

Dieses System blockiert nicht sämtliche Java-Programmbausteine ("applets"), *Cookies* oder Active-X-Kontrollen, sondern gestattet, dass die Nutzer selbst entscheiden können, auf welchem Niveau die nutzerbezogenen Anpassungen und Webdienste stattfinden sollen. *Cookies* werden auf den zentralen Servern innerhalb des Privada-Netzwerks platziert, nicht auf den PC der Nutzer. Alle Protokolle oder Datenerschließungsversuche durch eine Website werden mit der Online-Identität der Nutzer assoziiert - nicht mit seiner wahren Identität. Privada erklärt, dass die Nutzer leicht einzelne oder auch sämtliche installierten *Cookies* entfernen können.

Das von der Firma iPrivacy vorgestellte System soll anonymen elektronischen Handel vom Surfen und Einkaufen bis zum Versand ermöglichen. Es gestattet den Verbrauchern, vertraulich im Internet zu blättern und zu suchen, vertraulich Käufe zu tätigen und sie angeliefert zu bekommen, ohne die Identität des Empfängers preiszugeben. Nach Aussagen des Unternehmens ist selbst ihm die wahre Identität des Verbrauchers nicht bekannt, der seine Dienste in Anspruch nimmt. Was den Geschäftsvorgang betrifft, haben lediglich der Käufer und der Inhaber der Kreditkarte alle personenbezogenen Informationen über den online getätigten Kauf²⁰³.

E-Mail-Filter und anonymer E-Mail-Versand²⁰⁴

Diese Systeme wurden in Kapitel 4, Elektronische Post, bereits beschrieben. Ihre wichtigsten Eigenschaften seien hier noch einmal zusammen gefasst:

- E-Mail-Filter überprüfen die beim Nutzer eingehenden E-Mails und sorgen dafür, dass nur solche E-Mails durchgelassen werden, die vom Nutzer für den Empfang freigegeben wurden. Solche Systeme werden weithin zum Aussortieren von Massensendungen benutzt.
- Anonymer E-Mail-Versand erlaubt den Nutzern, ihre E-Mail-Adresse online anzugeben, ohne ihre Identität preiszugeben²⁰⁵. Dieser Dienst ist derzeit kostenlos im Internet über eine Reihe von Unternehmen erhältlich, die "Remail"-Dienste anbieten. Bei diesen Diensten entfernt der Remailer bei den weiter zu versendenden E-Mails die Identität des Absenders.

Informationsmittler

Die Nutzer können sich auch dafür entscheiden, sogenannte Informationsmittler (*Infomediary*) in Anspruch zu nehmen²⁰⁶. Ihre Rolle wurde wie folgt beschrieben: "Ein Infomediary oder Informationsmittler ist eine Vertrauensperson oder eine webfähige Organisation, die auf Informations- und

²⁰³ <http://www.iprivacy.com>

²⁰⁴ Siehe "Net Worth" (op. cit), S. 275ff..

²⁰⁵ In diesem Arbeitsdokument wird auf solche Dienste auch in Kapitel 6 (Veröffentlichungen und Foren) im Abschnitt über *Maßnahmen zur besseren Absicherung der Privatsphäre* eingegangen.

²⁰⁶ <http://www.fourthwavegroup.com/Publicx/1635w.htm>

Wissensdienstleistungen für, über und im Auftrage einer Gemeinschaft im Netz spezialisiert ist. Der Informationsmittler erleichtert und fördert die intelligente Kommunikation und Interaktion zwischen den Mitgliedern der virtuellen Gemeinschaft. Er verwaltet und wartet eine eigene Wissensdatenbank mit Inhalten und *Hyperlinks* von besonderem Interesse für die Gemeinschaft. Im Einklang mit den Datenschutzaufgaben der virtuellen Gemeinschaft sammelt und organisiert der Informationsmittler Informationen über die Gemeinschaft und ihre Mitglieder und stellt sie nach Bedarf der virtuellen Gemeinschaft in Auswahl zur Verfügung..."

Informationsmittler sind ein neuer Typ von kommerziellen Maklern, die ihren Kunden helfen, den Wert ihrer personenbezogenen Daten zu erfassen, zu verwalten und zu maximieren²⁰⁷. Die Verbraucher haben gezeigt, dass sie zur Freigabe persönlicher Informationen bereit sind, wenn sie davon profitieren können, sie werden sich aber auch immer mehr der Tatsache bewusst, dass sie ihre Privatsphäre zu billig an Firmen verkaufen, die sie im eigenen Interesse verwenden. Der Gegenwert der Informationen, die sie weitergeben, ist einfach gesagt unbefriedigend²⁰⁸.

Informationsmittler können den Verbrauchern dabei helfen, mit den Adressenverkäufern den für sie besten Handel abzuschließen, indem sie deren Daten mit denen anderer Kunden zusammen legen und die gemeinsame Marktmacht nutzen, um in deren Namen mit den Verkäufern zu verhandeln. Sie übernehmen die Rolle von Verwaltern, Bevollmächtigten und Maklern der Kundeninformationen, die sie im Auftrag der Verbraucher an Unternehmen vermarkten (d.h. diesen zugänglich machen), während sie zugleich die personenbezogenen Daten gegen Missbrauch schützen.

Der positive Aspekt der Tätigkeit des Informationsmittlers besteht darin, dass er in vielen Fällen die gewünschten Güter oder Dienstleistungen erwerben und an die Endverbraucher bei Wahrung ihrer Anonymität liefern kann. Informationsmittler können auch intelligente Dienstprogramme zur Verfügung stellen, die ihren Teilnehmern bei der Durchführung dieser Aufgabe helfen.

Die Kunden von Informationsmittlern haben theoretisch die Möglichkeit, beim Websurfen und bei Online-Einkäufen immer anonym zu bleiben. Aber zugleich werden Anreize geschaffen, genau dies nicht zu tun, da ihnen von den Adressenverkäufern jedes Mal ein kleines Honorar gezahlt wird, wenn sie ihre Identität oder ihre E-Mail-Adresse preisgeben. Dieses Honorar kann aus einer Geldzahlung oder aus einem Rabatt auf den Preis des verkauften Produktes bestehen.

Die Kunden erhalten darüber hinaus Geldzahlungen auch als Gegenleistung dafür, dass sie ausgewählten Adressenverkäufern Zugang zu ihren Informationsprofilen gewähren. Der Umfang der Geldzahlungen hängt von den Ansprüchen der einzelnen Kunden an den Schutz ihrer Privatsphäre ab. Kunden, die vollkommen anonym bleiben wollen, verzichten auf Geldzahlungen, um so die Gewissheit zu haben, dass ihre Privatsphäre unangetastet bleibt. Kunden, die sich mit den Sperrern zufrieden geben, die der Informationsmittler gegen den Zugang zu ihren Informationen errichtet, und die in einer selektiven Freigabe ihrer Daten an Adressenverkäufer eine Einnahmequelle sehen, können so Bareinkünfte erzielen.

Zusammenfassend lässt sich sagen, dass Informationsmittler zwar eine positive Rolle beim Schutz der personenbezogenen Daten der Nutzer übernehmen **können**, mit denen sie eine auf Vertrauen beruhende Beziehung eingehen, dass aber die Grundlage ihres Geschäfts darin besteht, Gewinn zu erzielen, indem sie die personenbezogenen Daten ihrer Kunden weitergeben oder zugänglich machen.

Je nach Umständen und Eigenschaften der Informationsmittler können sie also sowohl zum Schutz wie zur Durchdringung der Privatsphäre beitragen.

²⁰⁷ Eine der vollständigsten Untersuchungen zu dieser neuen Art von Akteuren ist das Werk "Net Worth: the emerging role of the infomediary in the race for customer information"; HAGEL III, J. und SINGER, M., Harvard Business School Press. 1999.

²⁰⁸ HAGEL III, J. und SINGER, M, op. cit.

III. Weitere Maßnahmen zur besseren Absicherung der Privatsphäre

Auch andere Techniken können dazu genutzt werden, die Transparenz der Datenverarbeitung zu erhöhen oder den Dateninhabern die Ausübung ihrer Rechte zu erleichtern. Als Beispiele wären hier etwa zu nennen:

P3P

P3P steht für *Platform for Privacy Preferences*²⁰⁹. Das Ziel von P3P ist es, zu ermöglichen, dass auf den Websites die Datenschutzbedingungen angezeigt werden, und gleichzeitig die Nutzer in die Lage zu versetzen, selber zu entscheiden, wie sie mit dieser Praxis umgehen; die Nutzer können also begründete Entscheidungen über die Art ihres Umgangs mit dem Web treffen und die Kontrolle über die Verwendung ihrer personenbezogenen Daten ausüben. Alle, die mit Datenschutz befasst sind, haben die Entwicklung von P3P mit großem Interesse verfolgt.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation legte im April 1998 einen gemeinsamen Standpunkt zu den entscheidenden Elementen für Technologien zur besseren Absicherung der Privatsphäre (z.B. P3P) im World Wide Web²¹⁰ vor. Nachfolgend seien die wesentlichen Bedingungen genannt, die von jeder technischen Plattform für den Schutz der Privatsphäre im World Wide Web erfüllt werden müssen, wenn sie eine systematische Erfassung von personenbezogenen Daten verhindern soll:

1. Eine Technologie kann nicht an sich den Schutz der Privatsphäre im Web gewährleisten. Sie muss entsprechend einem ordnungspolitischen Rahmen eingesetzt werden.
2. Jeder Nutzer muss das Recht haben, sich anonym im Web zu bewegen. Dies gilt auch für das Herunterladen von Informationen aus dem öffentlich zugänglichen Bereich des Web (Public Domain).
3. Bevor personenbezogene Daten, insbesondere die von Nutzern selbst mitgeteilten, vom Anbieter einer Website verarbeitet werden, muss die Einwilligung des Nutzers bei Kenntnis aller Details eingeholt werden. Außerdem sind bestimmte unverzichtbare Grundregelungen in die voreingestellte Konfiguration der technischen Plattform einzubauen.

Zwei Monate später, im Juni 1998, gab die Arbeitsgruppe Datenschutz ebenfalls eine Stellungnahme ab²¹¹. Darin betont auch sie, dass eine technische Plattform für den Datenschutz allein nicht genügt, um den Schutz der Privatsphäre im Internet zu garantieren. Vielmehr muss eine solche Plattform im Zusammenhang eines Rahmenwerks von rechtlich durchsetzbaren Datenschutzvorschriften eingesetzt werden, das ein nicht weiter verhandelbares Mindestmaß an Privatsphäre für jeden Einzelnen gewährt. In dieser Stellungnahme wurde auch auf eine Anzahl spezifischer Probleme hingewiesen, die mit der Umsetzung eines solchen Systems in der Europäischen Union verbunden sind.

Um die Anwendung von P3P im Kontext der europäischen Datenschutzrichtlinie zu untersuchen und die Verständigung zwischen den EU-Datenschutzbeauftragten und den Software-Entwicklern zu fördern, fand im September 1999 ein gemeinsames Seminar statt. Eine hochrangige Delegation des World Wide Web-Konsortiums und Mitglieder der Task Force 'Internet' nahmen an diesem Seminar teil. Dabei zeigte sich, dass noch diverse Probleme zu klären sind.

²⁰⁹ Der letzte Entwurf des P3P-Protokolls ist auf der W3C-Website abrufbar unter: <http://www.w3.org/TR/1999/WD-P3P>

²¹⁰ Dieser Text ist abrufbar unter: http://www.datenschutz-berlin.de/doc/int/iwgdp/priv_en.htm

²¹¹ Stellungnahme 1/98 zum Protokoll 'Platform for Privacy Preferences' (P3P) und zum Open Profiling Standard (OPS), angenommen am 16. Juni 1998, WP 11, XV D/5032/98.

Wenn diese Probleme einmal gelöst sind, könnte P3P - in einem adäquaten Rahmen angewandt - eine positive Rolle spielen. P3P weist folgende wichtige Vorteile auf²¹²:

- P3P kann dazu beitragen, Datenschutzhinweise zu normen. Dies bietet zwar an sich noch keinen Schutz der Privatsphäre, könnte aber, einmal eingeführt, die Transparenz stark fördern und Maßnahmen zu einem besseren Schutz der Privatsphäre unterstützen.
- P3P kann die Wahlmöglichkeiten bezüglich der Privatsphäre erweitern, zu denen auch Anonymität und die Annahme von Pseudonymen gehören.

Es sind jedoch auch die Grenzen²¹³ von P3P zu beachten:

- P3P ist nicht in der Lage, die Privatsphäre der Nutzer in Ländern zu schützen, die über keine ausreichende Gesetzgebung zum Schutz der Privatsphäre verfügen: es kann keine staatliche Politik ersetzen noch beanspruchen, dass seine Spezifikationen auf dem Markt eingehalten werden.
- P3P kann nicht gewährleisten, dass Privatunternehmen Maßnahmen zum Schutze der Privatsphäre treffen. P3P kann also nicht garantieren, dass eine Website wirklich erfüllt, was sie verspricht. Sanktionen für die Nichterfüllung von Absichtserklärungen können nur gesetzlich oder durch Mitgliedschaft in Organen der Selbstkontrolle festgelegt werden.

Kennzeichen für den Schutz der Privatsphäre

Die Kennzeichnung besteht aus einem Gütesiegel auf einer Website. Im Laufe der Zeit sind eine ganze Reihe von Datenschutz-Gütesiegeln aufgetaucht; Beispiele für solche Kennzeichnungssysteme sind TRUSTe²¹⁴, Privaseek²¹⁵, Better Business Bureau²¹⁶ und WebTrust²¹⁷. Diese amerikanischen Organisationen zielen auf Unternehmenstätigkeiten auf internationaler Ebene, also auch in Europa, ab, was bei einigen bereits der Fall ist. Gleichzeitig gehen ähnliche Unternehmensinitiativen mit internationaler Perspektive von Europa aus, wie etwa L@belsite in Frankreich.

Ein Gütesiegel für den Schutz der Privatsphäre wird Unternehmen verliehen, die eine Reihe von Auflagen der Organisation erfüllen, die das Gütesiegel verleiht. Diese Organisation kann eine gewisse Kontrolle darüber ausüben, ob die ihr Gütesiegel führenden Unternehmen ihren deklarierten Regelungen zur Wahrung der Privatsphäre tatsächlich entsprechen, indem sie die Aktivitäten dieser Unternehmen regelmäßig überprüfen. In manchen Fällen geht die Organisation, die das Gütesiegel verleiht, auch den Beschwerden von Dateninhabern über Unternehmen nach, die ihr Gütesiegel auf ihren Websites führen.

Die Kennzeichnung des Schutzes der Privatsphäre wirft allerdings folgende Probleme auf:

1. Das erste Problem betrifft den Inhalt des Gütesiegels. Das Recht auf Information und Zugang, der Grundsatz der geringst möglichen Datenerfassung, das Widerspruchsrecht, der Grundsatz der Rechtmäßigkeit und Verhältnismäßigkeit und die Verpflichtung, die nationale Datenschutzbehörde zu unterrichten, sind einige Eckpunkte der europäischen Datenschutzgrundsätze. Das größte Risiko bestünde in einer Vielfalt von Datenschutz-Gütesiegeln in ganz Europa, was sowohl die Nutzer als auch die für die Datenverarbeitung Verantwortlichen verwirren würde. Auch wenn sie manchmal diesen Eindruck

²¹² Siehe Artikel von CAVOUKIAN, A. und GURSKI, M. (Informations- und Datenschutzbeauftragte von Ontario) und MULLIGAN, D. und SCHWARTZ, A. (Center for Democracy Technology), *P3P and privacy: an update for the Privacy Community*, abrufbar unter: [wysiwyg://16/http://www.cdt.org/privacy/pet/p3pprivacy](http://www.cdt.org/privacy/pet/p3pprivacy)

²¹³ Siehe vorangehende Fußnote.

²¹⁴ <http://www.truste.org>

²¹⁵ <http://www.privaseek.com>

²¹⁶ <http://www.bbbonline.org/businesses/privacy/index.html>

²¹⁷ <http://www.cpawebtrust.org/consumer/index.html>

erwecken, garantieren nicht alle Gütesiegel wirklich eine Übereinstimmung mit den vorgenannten Datenschutzgrundsätzen.

2. Das zweite Problem liegt in der Kontrolle der Website-Praktiken bezüglich der Wahrung der Privatsphäre. Viele Arten von Kontrolle lassen sich ins Auge fassen. Einige wichtige Fragen zu diesem Problem sind folgende:

- Wer übt die Kontrolle wie und mit welcher Art von Befugnis seitens der kontrollierten Firma aus? Schlimmstenfalls wird ein Dateninhaber selbst diese Kontrolle übernehmen, mit allen daraus herrührenden Problemen, was das Erkennen und den Nachweis von Fällen betrifft, in denen die deklarierten Regeln zur Wahrung der Privatsphäre missachtet wurden, wobei auch der Bericht an die Kontrollstelle für die Gütesiegel problematisch sein kann. Abgesehen davon können nicht alle Einrichtungen, die Gütesiegel verleihen, auch sicherstellen, dass sich die Unternehmen an die Spielregeln halten, zu denen sie sich bekennen.
- Wer wird zahlen? Angesichts der Tatsache, dass die Kennzeichnungen Privatinitiativen sind, die oft nicht auf die finanzielle Unterstützung einer Regierung zurückgreifen können, werden manche Kennzeichnungs-Einrichtungen unter dem Druck der Unternehmen stehen, die sie eigentlich kontrollieren sollen.
- Welche Sanktionen werden, wenn überhaupt, verhängt?

Die Wirkungen von Datenschutz-Gütesiegeln zugunsten eines besseren Schutzes der Privatsphäre sollten gleichwohl nicht unterschätzt werden, da diese Gütesiegel dazu beitragen, die Frage der Privatsphäre ins Bewusstsein der Internet-Nutzer zu rücken. Einige Vorschläge zur Lösung der vorgenannten Probleme sind immerhin möglich:

1. Zum Inhalt der Kennzeichen: Damit eine Übereinstimmung der Datenschutz-Gütesiegel mit den europäischen Datenschutzvorschriften gewährleistet werden kann, könnte von der Arbeitsgruppe eine europäische Norm für Kennzeichen für den Schutz der Privatsphäre vereinbart werden. Diese Norm müsste die Anforderungen festlegen, die ein solches Gütesiegel erfüllen muss²¹⁸.

Verschiedene Kennzeichen können auch nebeneinander bestehen, sofern für die Internet-Nutzer erkennbar bleibt, welche Gütesiegel europäischen Normen entsprechen.

2. Zur Kontrolle der Website-Praktiken bezüglich der Privatsphäre: Die Verlässlichkeit der Website-Praktiken könnte erheblich verbessert werden, wenn Websites mit Gütesiegel einer regelmäßigen Prüfung unterzogen werden müssten. Eine europäische Norm für Kennzeichen für den Schutz der Privatsphäre könnte diese Vorschrift enthalten und die verschiedenen Möglichkeiten festlegen, wie solche Pflichtkontrollen durchgeführt werden: Selbstprüfung anhand einer Normprüfliste, Prüfung durch Dritte usw.

IV. Zusammenfassung

- Es sollten Empfehlungen zur Entwicklung von Browsern ausgesprochen werden, die den Schutz der Privatsphäre gewährleisten und die dafür vorteilhaftesten Voreinstellungen aufweisen;
- anonymisierende *Proxy-Server* können die IP-Adresse kaschieren und könnten von jedem *ISP* als kostenlose Standardleistung des Internet-Abonnements angeboten werden;
- Websites dürfen Nutzern, die keine *Cookies* akzeptieren wollen, den Zugang nicht verwehren, es sei denn, solche Sitzungs-*Cookies* sind unbedingt erforderlich, um eine Verbindung zwischen den Nutzern

²¹⁸ Einige sehr interessante Arbeiten auf diesem Gebiet legte die französische Datenschutzbehörde (CNIL) vor. Diese Arbeiten können als Anregungen für eine europäische Norm dienen. Siehe www.cnil.fr

und ihren verschiedenen Online-Einkäufen herzustellen und die entsprechenden Abrechnungen zu ermöglichen;

- die Nutzung von Technologien mit verbessertem Datenschutz (PET) sollte gefördert werden, was insbesondere durch ihre Installation bei *ISP* oder anderen Netzbetreibern zu geschehen hätte;
- offenbar müssen die einzelnen Nutzer mehr Informationen über das Vorhandensein von Technologien zur besseren Absicherung der Privatsphäre erhalten. Der öffentliche Sektor sollte die notwendigen Schritte unternehmen, um die Bekanntheit und die Entwicklung solcher Lösungen zu unterstützen, abgesehen davon, dass er sie selber nutzen und fördern sollte;²¹⁹
- von der Arbeitsgruppe könnte eine europäische Norm für Kennzeichen für den Schutz der Privatsphäre vereinbart werden. Diese Norm sollte die Vorschrift für Websites enthalten, sich einer regelmäßigen Überprüfung zu unterziehen.

²¹⁹ In den Niederlanden wurde bei der parlamentarischen Beratung des neuen Datenschutzgesetzes in der Zweiten Kammer einem Antrag zugestimmt, mit dem die Regierung aufgefordert wurde, die Entwicklung und Nutzung von PET zu fördern und dabei insbesondere den öffentlichen Sektor zu veranlassen, bei der Verarbeitung der eigenen personenbezogenen Daten als Verfechter von PET die Initiative zu übernehmen. Antrag Nr. 31 zum Gesetz Nr. 25 892 (Regels inzake de bescherming van persoonsgegevens, Wet bescherming persoonsgegevens), vorgelegt von C.S. NICOLAÏ am 18. November 1999, Den Haag, Zweite Kammer, Sitzungsjahr 1999–2000, 25 892, Nr. 31.

KAPITEL 10: ZUSAMMENFASSUNG

Trends und Gefahren

In diesem Dokument wurden in einzelnen Kapiteln verschiedene Themen behandelt; jedes einzelne enthielt zusammenfassende Bemerkungen zu spezifischen Fragen. Gleichwohl gibt es gemeinsame Fragen zu allen in diesem Dokument dargestellten Internet-Diensten, die in allgemeinerer Form gemeinsam behandelt werden können. Nach einer Zusammenfassung der Trends und Gefahren für den Datenschutz, die bei allen unterschiedlichen Aspekten der Internet-Nutzung zu beobachten sind, wird versucht, einige Leitlinien und Empfehlungen aufzustellen und zu erörtern, welche Maßnahmen auf den verschiedenen Ebenen getroffen werden können.

Das Internet erlebt eine exponentielle Entwicklung. Den Internet-Nutzern steht eine wachsende Zahl an Diensten zur Verfügung, von Online-Einkäufen bis zur Teilnahme an Foren mit Personen aus der ganzen Welt. Wegen dieser Komplexität wird es immer schwerer, einen angemessenen Überblick über all die Möglichkeiten zu behalten, die den Nutzern geboten werden. Unternehmen trachten nach Möglichkeiten, die Nutzer anzulocken und sich selbst von anderen Konkurrenten zu unterscheiden, indem sie nutzerbezogene und/oder unentgeltliche Dienstleistungen anbieten.

Die Anpassung von Dienstleistungen an Nutzerbedürfnisse hängt von der Verwendung der personenbezogenen Daten der Nutzer ab, und die Unternehmen versuchen mit verschiedenen Mitteln, diese Daten zu erhalten, zum Beispiel, indem sie die Nutzer anregen, solche Daten selbst preiszugeben, etwa im Rahmen von sogenannten Loyalty-Programmen, kostenlosen Geschenken oder Dienstleistungen, durch Erhebungen an öffentlich zugänglichen Quellen usw.

Die erstellten Benutzerprofile sind nicht allein für die Unternehmen von Wert, die den Verbraucher im Auge haben, sondern haben auch einen kommerziellen Wert an sich, da sie häufig an Dritte verkauft oder vermietet werden.

Die Entwicklung neuer Technologien macht es heutzutage leichter, die Spur der Internet-Nutzer zu verfolgen. Wenn sich etwa Verbraucher per Handy in das Internet einloggen, können Daten erzeugt werden, die deren Standort anzeigen.

Wenn Nutzer eine Verbindung zum Internet über die neuen Techniken wie ADSL oder Festleitung herstellen, wird Ihnen eine statische IP-Adresse zugewiesen, die eine Verfolgung der Bewegungen von Sitzung zu Sitzung erlaubt. Neue Generationen von Softwareprogrammen und Hardware bieten neue Möglichkeiten zur erweiterten Überwachung der Aktivitäten der Nutzer in Echtzeit, häufig ohne ihr Wissen. Im vorliegenden Dokument wurden zahlreiche Beispiele für die unsichtbare Verarbeitung und für die sogenannten E.T.-Softwareprogramme genannt.

Vor diesem Hintergrund ist es für den Durchschnittsnutzer schwierig, bei seinen Internet-Aktivitäten anonym zu bleiben.

Die Kombination dieser noch zunehmenden Möglichkeiten bringt neue Gefahren für den Schutz der Privatsphäre der Internet-Nutzer mit sich, insbesondere, wenn die Daten in Händen eines einzigen Verantwortlichen für die Datenverarbeitung oder nur weniger solcher Personen konzentriert sind.

Wenn sie etwa von den Datenerschließungstechniken Gebrauch machen, haben sie technisch die Möglichkeit, nicht nur personenbezogene Daten zu verarbeiten und neu zusammenzustellen, sondern auch neue Verknüpfungen und Merkmale bezüglich der Dateninhaber zu erschließen, die von diesen Möglichkeiten gewöhnlich nichts wissen und von einer solchen Verarbeitung nichts ahnen.

Solche Gefahren ergeben sich aus dem Sachverhalt, dass manche Daten über lange Zeiträume hinweg online erhalten bleiben; etwa die Nachrichten an Newsgroups und Versandlisten werden häufig mehrere Jahre lang gespeichert und können mit Hilfe zurück verfolgender Programme abgefragt werden.

Eine solche Zugänglichkeit personenbezogener Daten ermöglicht ungeahnte sekundäre Verwendungen dieser Daten, die häufig keineswegs dem Zweck entsprechen, für den die Daten ursprünglich erhoben wurden.

Leitlinien und Empfehlungen

2.1 Bewusstseinsbildung bei den Internet-Nutzer

Angesichts der zunehmenden Gefahren für die Privatsphäre der Internet-Nutzer, wie sie oben dargestellt wurden, ist es besonders wichtig, zu gewährleisten, dass angemessene Mittel und Wege bereitgestellt werden, damit die Nutzer alle Informationen erhalten, die sie benötigen, um fundierte Entscheidungen zu treffen. An der Bereitstellung dieser Informationen an die Nutzer wirken verschiedene Akteure mit.

Zunächst einmal müssen alle für die Verarbeitung Verantwortlichen, die personenbezogene Daten online erheben, den Dateninhabern sämtliche erforderlichen Informationen zukommen lassen. Wie in Artikel 10 der Richtlinie 95/46/EG ausgeführt, müssen diese Informationen stets zum Zeitpunkt der Erhebung der Daten geliefert werden. Auch wenn ein Datenschutzhinweis auf Websites ein gutes Verfahren ist, um der Öffentlichkeit allgemeine Informationen zu liefern, sind auch die einzelnen Dateninhaber, von denen Daten erhoben werden, auf einfache und verständliche Weise zu unterrichten, und zwar jedesmal, wenn Daten erhoben werden, zum Beispiel über denselben Bildschirm, auf denen die Nutzer ihre Daten eintragen, oder aber über eine Texteinblendung.

Sofern ein Privatunternehmen für die Datenverarbeitung verantwortlich ist, ist die Einhaltung dieser Vorschriften nicht nur unter rechtlichen Aspekten wichtig, sondern auch im eigenen wirtschaftlichen Interesse, weil dadurch das Vertrauen der Nutzer wächst, was Konsequenzen für ihre Einstellung gegenüber dem Unternehmen hat. So ist etwa bei der Entwicklung des elektronischen Handels festzustellen, dass sich Nutzer scheuen, sich auf elektronische Geschäftsverbindungen einzulassen, wenn sie fürchten, dass ihre personenbezogenen Daten nicht korrekt geschützt und gesichert werden.

Wo für die Datenverarbeitung öffentliche Behörden verantwortlich sind, ist die Einhaltung der Datenschutzvorschriften von zentraler Bedeutung, da das Verhalten einer solchen Behörde als Vorbild für die Öffentlichkeit insgesamt dient. Wenn etwa staatliche Behörden ihre Tätigkeiten auf eine elektronische Abwicklung umstellen, muss der Schutz der Privatsphäre als ein Eckpfeiler des Systems des Datenaustauschs eingebaut werden. Aber auch wenn sie nicht selbst für die Verarbeitung verantwortlich sind, tragen solche Behörden Verantwortung für den Bereich der allgemeinen Bildung und Unterrichtung der Öffentlichkeit.

Vor allem den Datenschutzbehörden obliegt die Aufgabe der Aufklärung über die Gefahren im Zusammenhang mit der Internet-Nutzung, aber auch über die gesetzlichen Rechte und Pflichten. Dies kann auf verschiedene Weise erfolgen, etwa durch Broschüren, Berichte, Pressemitteilungen, praktische Empfehlungen auf den Anmeldeformularen, Veranstaltung von oder Mitwirkung an Konferenzen oder Seminaren zu diesen Fragen, die sich an verschiedene Akteure und Bereiche der Gesellschaft richten.

Traditionellerweise betreiben Datenschutzverbände und -anwälte diese Aufklärung der Öffentlichkeit in einer Form, die zuweilen zu beachtlichen Verbesserungen der Internet-Produkte im Hinblick auf den Datenschutz geführt hat.

In verschiedenen Staaten der Europäischen Union lässt sich feststellen, dass Verbraucherverbände ebenfalls zunehmend stärker an den Aspekten des Datenschutzes im Zusammenhang mit den Verbraucheraktivitäten interessiert sind und sich dabei engagieren. Dies kann besonders vorteilhaft sein, wenn man sich nicht allein auf das Angebot an Informationen beschränkt, sondern die Verbraucher in ihren Beziehungen zu den Unternehmen oder staatlichen Behörden vertritt. Solche Verbände können zum

Beispiel die Einhaltung der Rechtsvorschriften durch die *ISP* überwachen oder die Behörden über Klagen von Verbrauchern über eine bestimmte Website oder Internet-Firma unterrichten.

Berufsverbände können ebenfalls einen positiven Einfluß nehmen, indem sie neue Mitglieder über ihre gesetzlichen Pflichten unterrichten.

Alle genannten Beteiligten spielen eine wichtige Rolle bei der Übermittlung der Informationen, die der Verbraucher benötigt, um eine fundierte Entscheidung zu treffen. Es liegt dann am Einzelnen, die ihm zur Verfügung stehenden Mittel zu nutzen, um seine Rechte wahrzunehmen und gegebenenfalls auch deutlich zu machen, dass er keine Dienstleistungen oder Produkte akzeptiert, die mit dem vorhandenen Rechtsrahmen nicht in Einklang stehen.

2.2 Konsequente und koordinierte Anwendung der vorhandenen Rechtsvorschriften

Ein Online-Datenschutz kann nur dann ausreichend gewährleistet sein, wenn der vorhandene Rechtsrahmen auch tatsächlich eingehalten wird. In Anbetracht des internationalen Charakters des Internets ist es von größter Bedeutung, dass sich die für die Verarbeitung Verantwortlichen auf eine konsistente und koordinierte Auslegung und Anwendung der europäischen Datenschutzvorschriften stützen können. Dies ist nicht nur für sie und die Dateninhaber innerhalb der Europäischen Union wichtig, sondern auch für solche außerhalb der Union, die diesen Rechtsrahmen ebenfalls berücksichtigen müssen, vor allem, wenn sie personenbezogene Daten über Geräte erheben, die in der Union installiert sind. In diesem Zusammenhang erfüllt die Arbeitsgruppe eine wichtige Aufgabe.

Die Arbeitsgruppe hat bei verschiedenen Gelegenheiten Lücken und strittige Fragen in den vorhandenen Rechtsvorschriften festgestellt und Dokumente für gemeinschaftliche Auslegungen und mögliche Lösungen vorgelegt. Besondere Aufmerksamkeit galt der Überprüfung der Richtlinie 97/66/EG, die einige wichtige Verbesserungen bezüglich der verwendeten Terminologie erbrachte. Die Arbeitsgruppe begrüßt zwar, dass im Richtlinienentwurf neue Fragen berücksichtigt wurden, bemängelt aber einige Vorschläge zu spezifischen Punkten, die noch besser hätten gelöst werden können.

Die Arbeitsgruppe ist darüber besorgt, dass Änderungen der vorhandenen Rechtsvorschriften zuweilen zu strengeren Bestimmungen führen sollen, insbesondere, was die Möglichkeiten der Kontrolle im Internet und eine allgemeine Identifizierungspflicht der Nutzer angeht. Die Arbeitsgruppe hat daran erinnert, dass zwar auch andere legitime Interessen eine Rolle spielen können, aber stets ein ausgewogenes Verhältnis zwischen ihnen und dem Schutz der personenbezogenen Daten hergestellt werden muss.

Es sei darauf hingewiesen, dass die Auslegung und Anwendung der Rechtsvorschriften nicht nur Aufgabe der staatlichen Behörden ist, sondern dass auch der private Sektor einen fruchtbaren Beitrag dazu liefern kann, indem er sich für die Entwicklung von Selbstkontrollregelungen oder Verhaltenskodizes für die Lösung von spezifischeren Fragen engagiert, die in einzelnen Bereichen aufgetreten sind.

2.3 Entwicklung und Verwendung von Technologien, die den Datenschutz gewährleisten, fördern und verbessern

Die Verarbeitung von personenbezogenen Daten im Internet hängt in großem Maße von der technischen Konfiguration der Hardware und Software sowie von den Protokollen und technischen Normen ab, die für die Übertragung der Informationen verwendet werden.

Es ist deshalb extrem wichtig, die Datenschutzbelange in einem möglichst frühen Entwicklungsstadium all dieser Instrumente und Programme zu berücksichtigen. So sollten beispielsweise Browser nicht mehr Informationen übermitteln, als für eine Verbindung zu einer Website erforderlich sind. Programmierer und Entwickler solcher technischen Tools werden aufgefordert, sich bei den nationalen Datenschutzbehörden über die bestehenden Datenschutzvorschriften zu informieren.

Um darüber hinaus der breiten Öffentlichkeit deutlich zu machen, welche Produkte die Datenschutzvorgaben einhalten, wäre es zweckmäßig, ein Kennzeichnungssystem zu schaffen, das eine leichte Erkennung solcher Produkte gestattet, die die Datenschutzvorschriften erfüllen.

Während neue Technologien in der Regel als eine Bedrohung für den Datenschutz betrachtet werden, sollte betont werden, dass sie ebenso ein nützliches Instrument zum Schutz der Privatsphäre darstellen können.

Einige vorhandene Technologien können erstens dazu verwendet werden, die Transparenz und Benutzerfreundlichkeit der Informationen für die Dateninhaber zu verbessern, zum Beispiel, indem ihnen einfache und leicht verständliche Informationen in dem Augenblick geliefert werden, in dem personenbezogene Daten erhoben werden.

Zweitens können sie sinnvollerweise dazu dienen, dass Dateninhaber ihre Rechte leichter wahrnehmen können, etwa indem sie online leichten Zugang zu ihren personenbezogenen Daten erhalten oder gegen deren Verarbeitung Einspruch erheben können.

Berücksichtigt man, dass der durchschnittliche Nutzer nicht unbedingt mit den technischen Aspekten der Internet-Nutzung vertraut ist und nicht immer in der Lage ist, über die Konfiguration der verwendeten Hardware und Software zu entscheiden oder sie gar selbst zu verändern, ist es sehr wichtig, dass die Produkte auf den höchsten Grad an Datenschutz voreingestellt sind.

Mittlerweile wurden zahlreiche zusätzliche Instrumente entwickelt, besser bekannt als "Technologien zur Erweiterung des Datenschutzes", die den Nutzern zu einer Sicherung ihrer Privatsphäre verhelfen sollen, insbesondere, indem die Sammlung oder Weiterverarbeitung von Daten, die die Identität preisgeben, auf ein Mindestmaß beschränkt oder völlig ausgeschlossen und auf technischem Wege jegliche rechtswidrige Form der Verarbeitung verhindert wird. Zu solchen Instrumenten zählen etwa *Proxy-Server*, *Cookie-Killer*, Anonymisierungssoftware, Pseudonymisierungstools (die für die Erstellung von Profilen besonders geeignet sind) und E-Mail-Filter usw. Mögliche neue Produkte sind etwa eine Chipkarte, die einen "portablen Identitätsschützer" (portable identity protector - PIP) enthält und die von ihrem Eigentümer in jeden beliebigen Computer gesteckt werden kann, von dem aus er eine Internet-Verbindung herstellen will.

Unter allen in Absatz 2.1 genannten Akteuren sind die Wirtschaft und der öffentliche Sektor die ersten, die die Entwicklung und Einführung von Datenschutztechnologien betreiben und fördern sollten. Die Nutzer sollten auf das Vorhandensein solcher Möglichkeiten hingewiesen werden, die ohne übertriebene Kosten zur Verfügung stehen müssten.

2.4 Schaffung vertrauensbildender Verfahren für Kontrolle und Feedback

Online-Datenschutz kann nur dann wirksam sein, wenn angemessene Möglichkeiten zur Beaufsichtigung und Beurteilung der Einhaltung der Rechtsvorschriften und vorgenannten technischen Voraussetzungen vorliegen.

Selbst wenn die Kontrolle über die Einhaltung der Vorschriften in erster Linie Aufgabe der Datenschutzbehörden ist, unternehmen auch andere Akteure Schritte in Richtung auf eine Selbstkontrolle, da sie erkannt haben, welchen Einfluss ihre Datenschutzpolitik auf das Verhalten der Verbraucher ihnen gegenüber hat.

Die Datenschutzbehörden können die Entwicklung und das gute Funktionieren solcher Selbstkontrollregelungen fördern, etwa indem sie Leitfäden herausgeben, zum Beispiel in Form von Checklisten für die Selbstbewertung, die auf europäischer Ebene vereinbart werden.

Ferner könnten Label vergeben werden, um den Verbrauchern vertrauenswürdige Hinweise auf die Einhaltung der EU-Datenschutzrichtlinien bei der Verarbeitung ihrer Daten zu liefern. Die Arbeitsgruppe plant Maßnahmen in diesem Bereich, um vor allem sicherzustellen, dass Datenschutzkennzeichen an

Websites vergeben werden, die mit den europäischen Datenschutzvorschriften auch tatsächlich in Einklang stehen.

Die Arbeitsgruppe lädt alle an Internet-Aktivitäten beteiligten Akteure ein, das vorliegende Arbeitsdokument zu berücksichtigen und die erforderlichen Schritte zu unternehmen, um dessen Empfehlungen in die Praxis umzusetzen.

Die Arbeitsgruppe hofft, mit diesem Arbeitsdokument einen Beitrag zur Bewusstseinsbildung zu leisten und eine öffentliche Diskussion zu diesem Thema zu fördern, das sicherlich noch weitere Untersuchungen und Folgemaßnahmen erforderlich machen wird.

GLOSSAR DER FACHAUSDRÜCKE²²⁰

ADSL

ADSL (Asynchronous Digital Subscriber Line) ist ein Telekommunikationsprotokoll, das einfache Kupferleitungen nutzen kann, aber Transferraten bis zu 1 MB/sec gestattet, wobei die Leitungen gleichzeitig für herkömmliche Telefongespräche frei bleiben. ADSL erfordert dafür ausgelegte Modems an beiden Enden der Leitung.

Authentisierung (Authentication)

Beglaubigung der Identität eines Benutzers, der sich in ein Computersystem einloggt oder Beglaubigung der *Datenintegrität* einer übertragenen Nachricht.

Banner

Werbe-*Banner* sind kleine grafische Bildflächen, die oberhalb oder in den Inhalten von Websites erscheinen.

Anruferkennung (Calling Line Identification - CLI)

Bei einem Anruf kann der Angerufene den Anrufer anhand der angezeigten Telefonnummer erkennen.

Clickstreams (Klicksequenzen)

Clickstreams sind Informationen über das Verhalten einzelner Personen, über die von ihnen eingeschlagenen Wege oder über die getroffenen Entscheidungen beim Besuch einer Website. Sie enthalten die Links, denen ein Benutzer gefolgt ist und werden beim Webserver (bzw. bei denjenigen Nutzern, die keinen eigenen Webserver betreiben, beim *Internet-Diensteanbieter*) protokolliert.

Cookies

Cookies sind Daten, die von einem Webserver erzeugt, in Textdateien gespeichert und auf der Festplatte des Internet-Nutzers abgelegt werden können, wobei eine Kopie von der Website aufbewahrt werden kann. *Cookies* sind ein regulärer Bestandteil des HTTP-Verkehrs und können als solche ungehindert im IP-Verkehr mitgeführt werden. Ein *Cookie* kann eine einmalige Zahl enthalten (GUI, Global Unique Identifier), mit der eine bessere Verknüpfung zu Personen ("Personalisierung") als bei dynamischen IP-Adressen möglich ist, was einer Website die Möglichkeit bietet, die Verhaltensmuster und Präferenzen ihrer Besucher aufzuzeichnen.

Cookies enthalten einen Satz von URL-Adressen, für die sie Gültigkeit haben. Wenn ein Browser wieder auf solche URL stößt, schickt er diese spezifischen *Cookies* an den entsprechenden Webserver.

Es gibt verschiedene Arten von *Cookies*: Sie sind entweder dauerhaft oder von begrenzter Dauer wie etwa die sogenannten "*Session-Cookies*".

²²⁰ Einige dieser Definitionen wurden folgenden Quellen entnommen:

- <http://www.techweb.com/encyclopedia>

- <http://webopedia.Internet.com>

- *Personal Data Privacy and the Internet: a guide for data users*, Office of the Privacy Commissioner for Personal Data, Hong Kong, 1998.

Ein Browser kann so eingestellt werden, dass er entweder für *Cookies* gesperrt wird oder aber ein Warnzeichen gibt, bevor ein *Cookie* akzeptiert wird.

Datamining (Datenerschließung)

Hierbei handelt es sich darum, "Tonnen von Daten zu durchwühlen", um Muster und Beziehungen in Wirtschaftstätigkeiten und -abläufen zu entdecken. Dies erfolgt gewöhnlich mit Programmen, die Daten automatisch analysieren.

Datawarehouse (Datenlager)

Eine Datenbank, mit der die Entscheidungsfindung in einer Organisation unterstützt wird. Sie kann enorme Datenmengen enthalten. So können etwa große Einzelhandelsorganisationen 100 oder mehr Gigabyte an Geschäftsabläufen verzeichnen. Wenn eine Datenbank lediglich für eine Abteilung oder eine Funktion organisiert wird, spricht man häufig von einem Datenmarkt (data mart) anstatt von einem Datenlager.

Datenintegrität

Der Vorgang des Schutzes vor zufälligen Löschungen oder Abänderungen in einer Datenbank.

Digitale Signatur

Eine *digitale Signatur* ist eine Zeichenfolge, die einer Nachricht hinzugefügt wird und deren *Datenintegrität* gewährleistet, indem sie diese (oder ihre Zusammenfassung) mit dem privaten Schlüssel des Signaturinhabers verschlüsselt. Jeder, der eine signierte Nachricht erhält, kann einfach prüfen, ob sie geändert wurde, indem er die Signatur mit dem öffentlichen Schlüssel des Absender entschlüsselt und die verschlüsselte Zeichenfolge mit der Originalbotschaft oder ihre Zusammenfassung vergleicht.

Digitales Zertifikat

Ein *digitales Zertifikat* ist ein elektronisches Dokument, das zwei Gruppen von Informationen enthält und als Identitätsnachweis in der elektronischen Welt dienen soll. Die erste Information betrifft das Zertifikat selbst und umfasst den Namen oder ein Pseudonym der natürlichen oder juristischen Person, die das Zertifikat anfordert, ihren öffentlichen Schlüssel, die Gültigkeitsdaten des Zertifikats und den Namen der Zertifizierungsbehörde. Die zweite Information ist die digitale Signatur der Zertifizierungsbehörde. Die gesamte Nachricht wird von Zertifizierungsbehörden (eine besondere Art von *Trusted Third Parties*), die für viele Server zuständig sind, digital signiert und kann die Beziehung zwischen einer natürlichen oder juristischen Person und ihrem öffentlichen Schlüssel beglaubigen.

Domain Name System (DNS)

Das DNS (*Domain Name System* – Bereichsnamensystem) ist ein Verfahren, mit dem Computern, die durch eine IP-Adresse identifiziert wurden, ein Name verliehen werden kann. Solche Namen haben die Form <Name>.übergeordneter Bereich, wobei <Name> eine Zeichenfolge ist, die von einer oder mehreren, durch Punkte voneinander getrennten Unterzeichenfolgen gebildet wird.

Dynamic Host Configuration Protocol (DHCP)

Das *Dynamic Host Configuration Protocol* (DHCP) ist ein *Internet-Protokoll* für die automatische Konfiguration der Computer, die TCP/IP verwenden. DHCP kann benutzt werden, um IP-Adressen automatisch zu vergeben. (<http://www.dhcp.org>)

Elektronische Signatur

Daten in elektronischer Form, die an andere elektronische Daten angehängt oder mit ihnen logisch verknüpft sind und als *Beglaubigungsverfahren* dienen (Artikel 2.1 der Richtlinie über *Elektronische Signaturen*).

Firewall (Schutzwall)

Methode zur Aufrechterhaltung der Sicherheit des Netzes. Der Schutzwall kann in einzelne *Router* installiert werden, die unerwünschte Pakete herausfiltern, oder als Kombination von Verfahren in *Routern* und in Hosts verwendet werden. *Firewalls* werden in großer Masse verwendet, um Nutzern einen sicheren Zugang zum Internet zu bieten, aber auch, um die öffentlichen Webserver von Unternehmen von deren internem Netz zu trennen. Darüber hinaus werden sie verwendet, um interne Netzsegmente zu schützen. Beispielsweise könnte ein Netzsegment für Forschung oder Buchhaltung für Schnüffeleien aus den übrigen Netzsegmenten anfällig sein.

HTML

Hypertext Markup Language, Sprache zur Darstellung von Seiten im Internet-Dienst World Wide Web. Sie legt die Anordnung von Text, Grafik und Bildern auf einer Web-Seite fest.

Hyperlinks

Eine festgelegte Verknüpfung zwischen zwei Objekten. Die Verknüpfung wird entweder als Text oder als Piktogramm (Icon) dargestellt. Auf Dokumentenseiten im World Wide Web wird ein textförmiger *Hyperlink* typischerweise als unterstrichener Text in blauen Buchstaben dargestellt, während ein graphischer *Hyperlink* ein kleines graphisches Bild ist.

Internet-Diensteanbieter (Internet Service Provider - ISP)

Ein Unternehmen, das der Öffentlichkeit und anderen Unternehmen den Zugang und die Verbindung zum Internet ermöglicht.

Kleine *Internet-Diensteanbieter (ISP)* bieten ihre Dienste über *Modem* und ISDN an, während die größeren auch private Leitungen anbieten. Den Kunden wird im allgemeinen eine feste Monatspauschale in Rechnung gestellt, aber es können auch andere Abrechnungsformen erfolgen. Gegen eine Gebühr kann eine Website geschaffen und auf dem Server des Providers platziert werden, was kleineren Einrichtungen gestattet, mit einem eigenen Bereichsnamen im Netz präsent zu sein.

Große Internet-Dienste bieten neben dem Internet-Zugang auch eigene Datenbanken, Foren und Dienstleistungen an.

In diesem Bericht wird der Ausdruck *ISP* im allgemeinen unter Einbeziehung der IAP verwendet. Der Terminus IAP wird nur dann verwendet, wenn deutlich ist, dass es sich lediglich um den Internet-Zugang handelt; in allen übrigen Fällen wird der Terminus *ISP* verwendet.

Java und JavaScript

Java ist eine ausgereifte Programmiersprache, die nicht für den Gelegenheitsprogrammierer und erst recht nicht für den Endnutzer konzipiert ist. *JavaScript* ist dagegen eine Script-Sprache, die eine ähnliche Syntax wie *Java* verwendet, aber nicht in einen Bytecode übersetzt ist. Sie bleibt im Quellcode erhalten, ist in ein *HTML*-Dokument eingebettet und muss mit Hilfe des *JavaScript*-Interpreters zeilenweise in einen Maschinencode übertragen werden. *JavaScript* ist sehr beliebt und wird von allen Web-Browsern unterstützt. *JavaScript* hat einen kleineren Befehlssatz als *Java* und bearbeitet in erster Linie die Elemente auf Dokumentenseiten.

Meta Tags

Meta Tags sind *HTML*-Markierungen, die Informationen über eine Webseite enthalten. Anders als normale *HTML*-Markierungen beeinflussen *Meta Tags* nicht die Darstellung der Seite, sondern liefern Informationen darüber, wer die Seite geschaffen hat, wie oft sie aktualisiert wurde, welchen Inhalt die Seite hat und welche Stichworte den Seiteninhalt darstellen. Viele Suchmaschinen benutzen diese Informationen bei der Erstellung ihrer Indexverzeichnisse.

Modem

(**MO**dulator-**DE**Modulator) Ein Gerät, das ein Terminal oder einen Computer mit einer analogen Telefonleitung verbindet und digitale Impulse in akustische Frequenzen verwandelt und umgekehrt. Unter diesem Begriff werden in der Regel 56Kbit/s-Modems (V.90 – die derzeitige Höchstgeschwindigkeit), oder ältere 28.8 Kbit/s-Modems (V.34) verstanden. Er kann sich aber auch auf die noch schnelleren Kabel- oder DSL-Modems oder auf ISDN-Terminaladapter beziehen, die digital arbeiten und technisch betrachtet keine Modems sind. Ein *Modem* ist ein Analog-Digital- und Digital-Analog-Umwandler. Es wählt ferner die Telefonnummer, beantwortet Anrufe und kontrolliert die Übertragungsgeschwindigkeit. Die Entwicklung der Modems verlief über 300, 1200, 2400, 9600, 14400, 28800, 33300 und 56000 bps. Unabhängig von der möglichen Höchstgeschwindigkeit werden von den Modems jeweils auch mehrere geringere Geschwindigkeiten unterstützt, damit sie mit älteren langsameren Modellen kommunizieren oder bei Störgeräuschen in den Telefonleitungen "herunterschalten" können.

OLAP

OnLine Analytical Processing. Hierbei handelt es sich um eine Software zur Unterstützung von Entscheidungen, die es Nutzern gestattet, Informationen rasch zu analysieren, die in multidimensionalen Ansichten und Hierarchien zusammen gefasst wurden. So werden etwa OLAP-Tools verwendet, um Trendanalysen von Verkäufen und Finanzinformationen durchzuführen. Sie ermöglichen es den Benutzern, in umfangreiche Verkaufsstatistiken einzudringen, um etwa diejenigen Erzeugnisse herauszukristallisieren, die sich am leichtesten verkaufen lassen. Herkömmliche OLAP-Programme, auch bekannt als multidimensionales OLAP oder MOLAP, fassen Geschäftsabläufe in multidimensionale Ansichten im Zeitverlauf zusammen. Bei diesen Datenbankarten werden Kundenabfragen extrem schnell bearbeitet, da die Konsolidierung bereits erfolgt ist. OLAP platziert die Daten in eine Würfelstruktur, die vom Nutzer gedreht werden kann, was sich für finanzielle Zusammenfassungen besonders eignet.

Portalseite

Eine *Portalseite* bietet in geordneter Form einen Überblick über die Web-Verknüpfungen. Über das besuchte *Portal* im Internet kann der Nutzer leicht ausgewählte Websites anderer Anbieter von Inhalten besuchen. Moderne Portale sind "übergeordnete Standorte" ("supersites"), die eine Vielzahl von Dienstleistungen bieten, etwa die Suche im Netz, Neuigkeiten, weiße und gelbe Telefonbücher (=Personen- und Branchenverzeichnisse), freie E-Mail-Adressen, Diskussionsgruppen, "Online-shopping" und Links zu anderen Standorten.

PPP

PPP (Point to Point Protocol) ist ein häufig genutztes Telekommunikationsprotokoll zur Verbindung von zwei Computern über ihre serielle Schnittstelle oder ein Modem. Es handelt sich um ein *Protokoll* der untersten Schicht (siehe *Protokoll*), das vorwiegend zwischen den PCs privater Nutzer und dem Internet-Zugangsserver eines Internet-Diensteanbieters bei TCP/IP-Verbindungen über herkömmliche Telefonleitungen verwendet wird.

Proxy-Server

Der *Proxy-Server* ist ein Zwischenserver zwischen dem Internet-Nutzer und dem Netz. Er funktioniert als Zwischenspeicher für das Netz, wodurch er die Leistung des Internets drastisch verbessert. Viele große Organisationen oder Internet-Anbieter haben diese Lösung bereits eingeführt. Jede Seite, jedes Bild oder Logo, das Beschäftigte einer Organisation von außerhalb heruntergeladen, wird in einem sogenannten Cache gespeichert und ist unmittelbar darauf für andere Mitarbeiter derselben Organisation zugänglich.

Es ist also nicht mehr erforderlich, dass jeder Mitarbeiter einer Organisation, die vor einem *Proxy-Server* platziert ist, seine eigene IP-Adresse hat, da er ja keinen direkten Zugang zum Internet hat.

Protokoll

In diesem Kontext ist ein *Protokoll* ein Bündel von technischen Regeln, die beim Austausch von Informationen von beiden Partnern eingehalten werden müssen. Die Protokolle sind in einer Hierarchie von sogenannten Schichten organisiert. Jede Schicht ist für die Behandlung eines bestimmten Aspekts des Telekommunikationsprozesses zuständig und stellt die Grundfunktionen bereit, die von der nächsthöheren Schicht genutzt werden. Im Internet wird das *TCP/IP-Protokoll* typischerweise immer als mittlere Schicht benutzt. Ethernet (für Lokale Netzwerke), ADSL (für Telefonleitungen), ATM (für Telekommunikationsbetreiber), X-75 (für ISDN-Leitungen), PPP (für die herkömmlichen Telefonleitungen) sind Beispiele von Protokollen, die als unterste Schicht verwendet werden. Protokolle der oberen Schicht sind dagegen HTTP (für das "Surfen" im Netz), SMTP und POP (für E-Mail-Versand), FTP (für die Übermittlung von Dateien). Dies bedeutet, dass jede eventuell im *TCP/IP-Protokoll* vorhandene Gefahr für die Privatsphäre auch ein Schwachpunkt für die höheren Protokolle ist. Schichten sind also Bündel von Unterprogrammen, die auf den Computern operieren, die mit dem Internet verbunden sind.

Router

Ein *Router* ist ein wichtiges Gerät, mit dem Kommunikationswege für *TCP/IP-Netzwerke* ermittelt werden. Dies bedeutet, dass die Routen beim TCP/IP dynamisch sind und je nach Ausfall oder Überlastung einiger Strecken oder Verbindungen verlaufen. Das Gerät kann auch als Schutzwall zwischen einer Organisation und dem Internet verwendet werden. Vor allem gewährleistet es, dass nur autorisierte IP-Adressen von einem bestimmten *ISP* ausgehen können.

Shareware

Software, die aus dem Internet heruntergeladen werden kann. Gewöhnlich darf sie zum Testen gratis heruntergeladen werden, aber um sie auf Dauer legal zu nutzen, muss den Softwareentwicklern ein geringer Betrag gezahlt werden. Darf eine Software völlig gratis heruntergeladen und genutzt werden, spricht man von *Freeware*.

Sniffing

Mit "Schnüffel"-Software können die Datenströme in einem Netzwerk überwacht und sämtliche Datenpakete gelesen werden, indem alle Mitteilungen, die nicht chiffriert sind, in Klartext dargestellt werden. Die einfachste Form des Schnüffels kann mit Hilfe überall erhältlicher Software mit einem gewöhnlichen PC durchgeführt werden, der an ein Netzwerk angeschlossen ist.

Spamming (oder Spam)

E-Mail-Massenversand von unerbetenen Werbeanzeigen.

TCP/IP-Netzwerk

Ein *TCP/IP-Protokoll* (Transport Control Protocol/Internet Protocol) beruht auf der Übertragung von kleinen Informationspaketen. Jedes Paket enthält die IP-Adresse des Absenders und des Empfängers. Dieses Netzwerk ist verbindungslos, d.h., im Gegensatz etwa zu einem Telefonnetz setzt der Beginn einer Kommunikation zwischen zwei Geräten nicht voraus, dass sie bereits miteinander verbunden sind. Ferner bedeutet dies, dass gleichzeitig viele Kommunikationen mit vielen Partnern möglich sind.

UMTS

UMTS (Universales Mobiles Telekommunikations-System) ist ein breitbandiges Protokoll der "dritten Generation" für die drahtlose und paketförmige Übertragung, die eine Übertragungsgeschwindigkeit von mehr als 2 MBit/s zulässt. Dieses neue Breitbandprotokoll wird digitale Videoübertragungen in TV-Qualität an mobile Geräte gestatten. Das derzeitige GSM-Netz gestattet Geschwindigkeiten von 11 Kbit/s, was für die Übertragung von Sprache, nicht aber von bewegten Bildern ausreicht.²²¹

Verschlüsselung

Die Chiffrierung von Informationen und Nachrichten erfolgt in einer Weise, dass sie im Prinzip nur von dem beabsichtigten Empfänger gelesen werden können, der Zugang zu einem Schlüssel oder Passwort hat. Es gibt zwei Hauptformen von Chiffriersystemen:

- Das symmetrische oder private Schlüsselsystem, das einen geheimen Schlüssel zwischen dem Absender und dem Empfänger einer Nachricht verwendet; sein wichtigster Vorteil ist die hohe Verarbeitungsgeschwindigkeit, sein größter Nachteil die Schwierigkeit, die Schlüssel in sicherer Form mit einer Großzahl von Benutzern zu teilen.
- Das asymmetrische oder öffentliche Schlüsselsystem, das ein Schlüsselpaar verwendet, das in der Weise erzeugt wird, dass es selbst bei Kenntnis des einen Schlüssels nahezu unmöglich ist, den anderen zu kennen. Nachrichten, die mit dem einen Schlüssel chiffriert werden, werden mit dem anderen dechiffriert. Einer der beiden Schlüssel ist öffentlich bekannt und wird zur Chiffrierung der Nachrichten verwendet, die jeder Empfänger mit seinem privaten Geheimschlüssel dechiffriert. Der private Geheimschlüssel wird auch dazu verwendet, Nachrichten digital zu unterzeichnen.

Vertrauenssichernde neutrale Dritte (Trusted Third Parties)²²²

Vertrauenssichernde neutrale Dritte (*TTP*) lassen sich als Organe beschreiben, die von anderen Körperschaften mit sicherheitsrelevanten Diensten und Tätigkeiten betraut werden.

TTP bieten Dienste mit Zusatznutzen für solche Nutzer, die stärkere Vertrauenswürdigkeit und geschäftliche Vertraulichkeit der Dienste beanspruchen, die sie erhalten; sie erleichtern eine sichere Kommunikation zwischen Geschäftspartnern. *TTP* müssen Zusatznutzen in bezug auf *Datenintegrität*, Vertraulichkeit und Gewissheit der Dienstleistungen und Informationen bieten, die in der Kommunikation zwischen geschäftlichen Anwendungen ausgetauscht werden. Ferner verlangen die Nutzer von *TTP*-Diensten, im Rahmen des vereinbarten Dienstleistungsvertrags, dass diese zur Verfügung stehen, wenn sie gebraucht werden.

Vertrauenssichernde neutrale Dritte sind in der Regel Einrichtungen, die Lizenz und Beglaubigung von einer Regulierungsbehörde erhalten und auf kommerzieller Basis einem breiten Spektrum von Körperschaften, einschließlich solcher in den Bereichen Telekommunikation, Finanzen und Einzelhandel, Sicherheitsdienstleistungen bieten.

²²¹ Siehe: <http://www.umts-forum.org/>

²²² Definition aus: "Requirements for *TTP* services", ETSI.

So können *TTP* etwa für die Bereitstellung von *digitalen Signaturen* zur Gewährleistung der *Datenintegrität* von Dokumenten herangezogen werden. Zusätzlich können sie Nutzern Rundum-Verschlüsselungen mit Schlüsseleratzfunktion liefern, damit diese wieder an die Daten gelangen können, falls ein Schlüssel verloren ging (typisch für Dokumente und Ordner, die von Beschäftigten erstellt wurden), oder sie unterstützen bei Bedarf einen rechtmäßigen Zugriff auf verschlüsselte Daten.

Der Nutzen der *TTP* hängt von der grundlegenden Voraussetzung ab, dass ihnen die Einrichtungen, denen sie dienen, Vertrauen entgegenbringen.

WAP

WAP (Wireless Application Protocol) ist ein Telekommunikationsprotokoll, das von zahlreichen Herstellern von Mobiltelefonen konzipiert wurde. Es gestattet den Zugang von dafür eingerichteten Handys zu Internet-Diensten wie E-Mails, Chat und Web-Surfen.²²³

Web cache

Ein Computersystem in einem Netzwerk, das Kopien der jüngst abgefragten Dokumentenseiten in einem Speicher oder auf einer Festplatte abspeichert, um ihr Wiederfinden zu beschleunigen. Wenn die folgende abgefragte Seite bereits im Cache gespeichert ist, wird sie nicht mehr aus dem Internet, sondern lokal abgerufen. Solche Speicherserver befinden sich innerhalb des *Schutzwalls* eines Unternehmens und gestatten es, dass vielgefragte Seiten, die von Nutzern aufgesucht werden, augenblicklich zur Verfügung stehen. Da sich der Inhalt von Dokumentenseiten ändern kann, sucht solche Speichersoftware ständig nach neueren Versionen der Seite und lädt sie herunter. Nach einer eingestellten Zeitspanne der Nichtaktivität werden Seiten wieder aus dem Cache entfernt.

Webmail

E-Mail-Systeme, die Dokumentenseiten als Schnittstelle verwenden (z.B. Yahoo, HotMail usw.). *Webmail* können von überall her erreicht werden und die Nutzer müssen keine Verbindung zu einem besonderen *ISP* aufnehmen, wie dies bei den gewöhnlichen E-Mail-Konten der Fall ist.

Geschehen zu Brüssel am 21. November 2000

Für die Arbeitsgruppe

Der Vorsitzende

Stefano RODOTA

²²³ Zu mehr Informationen siehe: <http://www.wapforum.org>