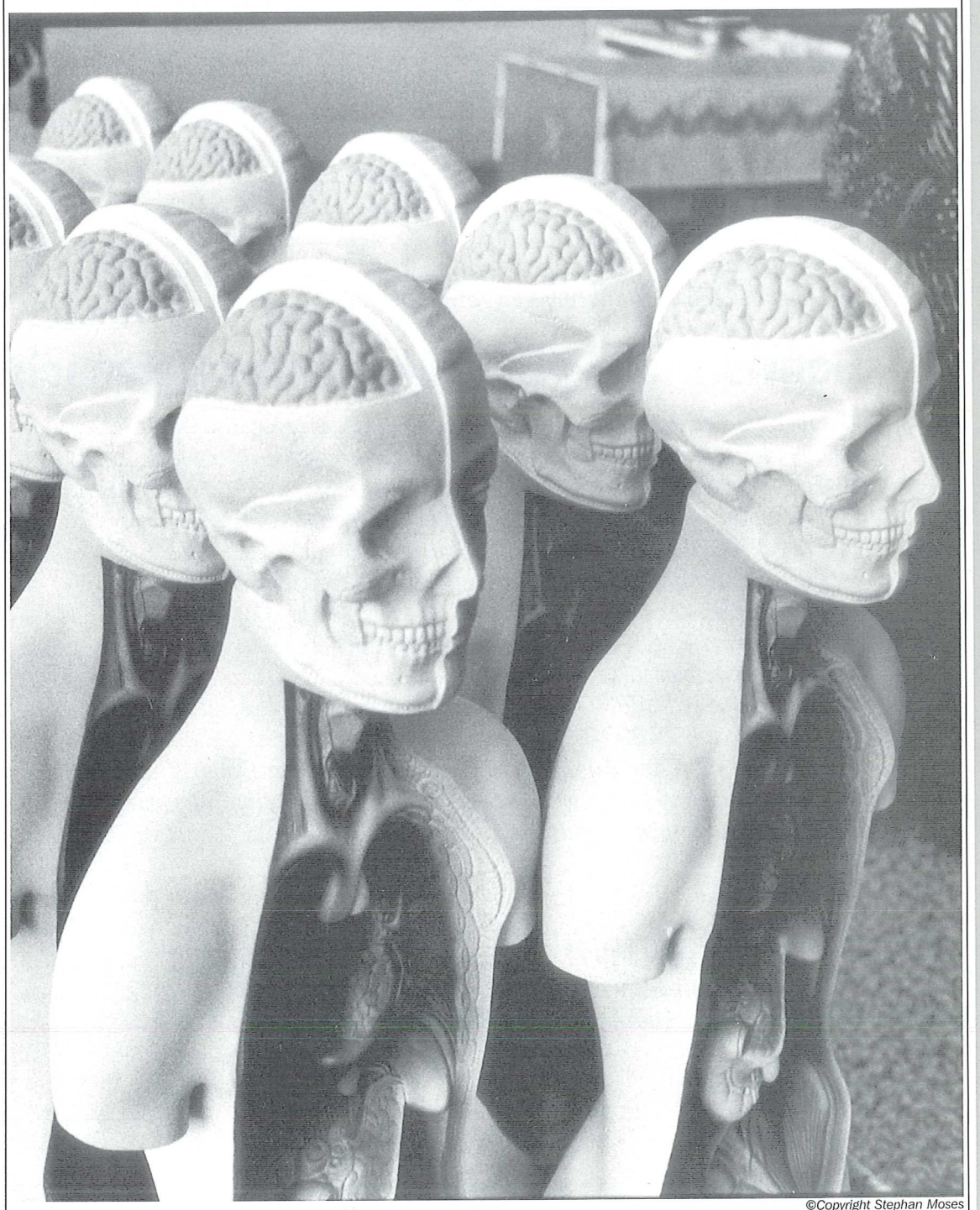
F.f.F.Kommunikation
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.
14. Jahrgang 1997 • Einzelpreis: 6 DM

Z 7625 F

DATENSPUREN
DATENSCHATTEN



©Copyright Stephan Moses

2/97 Juni 1997

ISSN 0938-3476

Inhalt

Editorial

- *Die Zukunft des Datenschutz* 3

Aktuell

- *Modernisierung der Demokratie durch Informationstechnik?* 4
- *Verschlüsselungsgesetze stellen Grundrechte auf den Kopf* 6
- *Deutsches Delphi, Mini-Delphi, FIfF-Delphi* 9
- *Internet auf dem Index* 12
- *Manöver in der Box* 14
- *Freiheit aushalten!* 15
- *Denkanstöße:Was läuft hier eigentlich ab?* 17

Schwerpunkt »Die Zukunft des Datenschutz«

- *Über die Autorinnen und Autoren* 21
- *Die Novellierungsvorschläge zum BDSG – ein gewaltiger Flop!* 22
- *Tele- und Mediendiensterecht* 24
- *Telekommunikations- und Medienrecht im Wandel* 27
- *Presseerklärung der Datenschutzbeauftragten* 30
- *FIFF-Stellungnahme zur Anhörung zum neuen Informations- und Kommunikationsdienste-Gesetz* 32
- *Multimedia-Regelungen – warum überhaupt?* 34
- *Voyeure im Netz* 35
- *Geheime „SIRENE": Garant für Ordnung und Staatssicherheit* 37
- *Brauchen wir EUROPOL?* 42
- *EUROPOL: Keine Aussicht auf Löschung sensitiver Daten* 46
- *Thesen zur Änderung der Staatsaufgaben in einer „civil information society"* 48
- *Datenschutz durch Technik?!* 53

FIFF e.V.

- *FIFF Jahrestagung 1997* 57
- *Einladung zur FIFF e.V. Mitgliederversammlung 1997* 58
- *FIFF e.V., Vorstand und Regionales* 59

Rubriken

- *Termine* 59
- *FIfF Bibliothek* 60
- *Vielzweck-Schnipsel* 61
- *Impressum* 62
- *Adressen* 63

Die Zukunft des Datenschutz

Vom Recht, von Jägern und Sammlern

Selten sind so viele Behauptungen in so kurzer Zeit in sich zusammengefallen, wie bei der publizitätsträchtigen Aufregung um den rechten Weg in die Informationsgesellschaft. Sie werde „der Gesellschaft Beine machen" verkündete des Kanzlers Innovationsrat, Deutschland werde durch das Internet nicht mehr dasselbe sein.

Das Gegenteil ist der Fall: Die Bundesrepublik ist unverändert, das Internet aber wird nicht mehr dasselbe sein, wenn sich Politiker aus Bund und Ländern durchsetzen, im August neue gesetzliche Regelungen für Angebote auf dem Internet in Kraft treten zu lassen. Mit dem Mediendienste-Staatsvertrag und dem Informations- und Kommunikationsdienste-Gesetz (IuKDG) treten neue Vorschriften in Kraft, die den AnbieterInnen und NutzerInnen überdies neue Unklarheiten in der Rechtslage bringen.

Auch wenn Politiker gern von Überregulierung reden, so war nicht ernsthaft zu erwarten, daß in einem für seine notorische Regelungswut bekannten Land wie diesem ein Bereich wie das Internet und andere elektronische Netze ausgespart bleiben. „Deutschlands mutiger Versuch, das Internet zu regulieren" so die internationale Presse, ist nicht der erste. Unter dem Mantel der Liberalisierung trat schon im letzten August mit dem Telekommunikationsgesetz (TKG) eine erste Neuregelung für Anbieter und Nutzer von elektronischen Netzen in Kraft. Werner Moritz stellt in seinem Beitrag die wichtigsten Aspekte zusammen.

Mit ihren Verfahren gegen CompuServe und die in der Internet Content Task Force (ICTF) verbandelten Internet-Provider haben bayerische und Bundes-Staatsanwälte seither versucht, ihre Vorstellung von Recht im Internet durchzusetzen. Bund und Länder belobigen sich und ihre neuen Regelungen nun damit, derartiges werde es in Zukunft nicht mehr geben, weil nun Rechtssicherheit herrsche. Daß davon nicht im mindesten die Rede sein kann, verdeutlichen mehrere Beiträge dieser Ausgabe. In seinem Beitrag analysiert Peter Schaar die entsprechenden Regelungen und zeigt Unklarheiten auf. Viele der geladenen Experten haben dies auch auf einer Anhörung des zuständigen Bundestagsausschusses klargemacht. Friedrich Holl nahm dabei für das FIfF teil, aus dessen Stellungnahme wir Teile dokumentieren.

Die Politik greift also massiv in das ein, was Grundlage elektronischer Interaktion ist – Netze und die darauf übertragenen Daten. Dabei lassen sich extreme Unterschiede beobachten. Auf der einen Seite wird versucht, nationale – im kulturellen verhaftete – Vorschriften zu Jugendschutz und politischer Meinungsfreiheit auf weltweite Netze anzuwenden. Ob dabei Politik, Recht und Kultur überhaupt zusammenpassen, ist oft unerheblich, wie die Beiträge von Michael Langer und Ingo Ruhmann zeigen. Nationales Recht wird hier zum Maßstab auf dem Internet. Auf der anderen Seite wird erstaunlich lax mit den sensiblesten persönlichen Daten umgegangen, wenn es der Arbeit von Polizei und Geheimdiensten dienen könnte. Ein besonderes Beispiel liefern dafür derzeit die EU-weiten Polizeikooperationen im Schengen-Verbund und die Planungen zu EUROPOL. In ihren Beiträgen verdeutlichen Thilo Weichert und Nicolas Busch, wie weit die bestehenden Schutznormen für die Sammlung von Daten über praktisch alle EU-BürgerInnen ausgehöhlt werden sollen und damit nationales Recht transnationalen Übereinkünften weichen soll. Stellungnahmen der Datenschützer weisen auf einige der gravierenden Probleme des heutigen Datenschutzrechts hin. Weichert zeigt außerdem, wie untauglich die derzeitigen Entwürfe zur Novellierung des Bundesdatenschutzgesetzes vor dem Hintergrund dieser und anderer Entwicklungen sind.

Wie könnte ein Schutz in der Informationsgesellschaft überhaupt aussehen, was sind dessen Voraussetzungen? Daß Datenschutz in einer immer stärker auf elektronischen Transaktionen aufbauenden Gesellschaft schon lange keine isolierte Frage mehr ist, sondern ein grundsätzlicher Schutz in einer demokratischen Gesellschaft, hat sich ja mittlerweile herumgesprochen. Das Problem heute ist jedoch, daß derartige Transaktionen international ablaufen und daher kaum noch durch nationale Regelungen geschützt sind. Beispiele derartiger Datensammlungen beschreibt Ute Bernhardt. In ihrem Beitrag beschreibt Marit Köhntopp die Möglichkeiten, Datenschutz in solchen Transaktionen durch technische Hilfsmittel selbst herzustellen.

Hier geht es also letztlich um eine Emanzipation des Individuums, die der Gesetzgeber offenbar nicht schätzt. Der in diesem Beitrag angesprochene Schutz durch Verschlüsselungstechnik wird nicht nur von Regierungsmitgliedern in diesem Lande für gefährlich erachtet – eine Sicht, die das FIfF in einer Stellungnahme entschieden zurückgewiesen hat. Ist aber Schutz in Netzen nur noch Sache des Individuums – wie weit reicht der Schutzschirm des Staates noch? Diese grundsätzlichen Fragen nach der Zukunft von Schutzstrategien stellt Alexander Roßnagel in seinem Beitrag.

Die Bedeutung des Datenschutzes nimmt zu, die Schutzwirkung nationalen Rechts ab. Gleichzeitig bedrohen staatliche Wünsche nach Verschlüsselungsverboten technische Lösungsansätze. Politisches Handeln und Nichthandeln bringt den Datenschutz von zwei Seiten unter Druck, statt endlich seine zentrale Bedeutung für die Zukunft einer vernetzten Welt zu akzeptieren. Eine solche rückwärtsgewandte Sicht gibt nicht nur dem Datenschutz keine Zukunft, sondern ebensowenig auch elektronischen Netzen.

Ingo Ruhmann, Ute Bernhardt

Aktuell

Modernisierung der Demokratie durch Informationstechnik?

Kommentar des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)

Anläßlich der Konferenz „Internet & Politik" der Burda Akademie zum Dritten Jahrtausend wurde eine „Münchner Erklärung" der Öffentlichkeit vorgestellt, die sich selbst als „Beitrag zu einer demokratischen Mediendebatte und Netz-Kultur" versteht.

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e.V.) begrüßt, daß wichtige Fragen der Ausgestaltung einer Informationsgesellschaft nun auch Gegenstand einer solchen Tagung waren. Die daraus entstandene Erklärung (http://www.akademie3000.de) stellt auf abstrakter Ebene einige dabei wichtige Probleme zusammen. Andere wesentliche Punkte werden jedoch in der Erklärung nicht oder nur unzureichend thematisiert.

So wird in der Münchener Erklärung unhinterfragt von der Prämisse ausgegangen, daß die Nutzung von Informations- und Kommunikationstechnik eine notwendige Voraussetzung für die „Modernisierung der Demokratie" darstellt. Viele Forderungen der Münchner Erklärung richten sich darauf, daß „Informationen elektronisch zur Verfügung gestellt" und „elektronische Beteiligungsverfahren" entwickelt werden sollen. Hierzu einige Anmerkungen:

1. Demokratie entsteht nicht durch Technik

Notwendige Voraussetzung für eine demokratische Gesellschaft, für politische Transparenz und Bürgerbeteiligung ist vor allem der politische Willen. Auch ohne Informations- und Kommunikationstechnik gäbe es vielfältige Möglichkeiten, BürgerInnen zu informieren und vor allem an politischen Diskursen und Entscheidungen zu beteiligen. Die Vorstellung, daß allein durch die Verfügbarkeit eines neuen Mediums quasi automatisch politisches Interesse und Aktivität auf allen Seiten entstehen würde, zeugt von einer unreflektierten technokratisch-deterministischen Weltsicht, die das erwünschte Ideal des autonom selbstbestimmten Bürgers konterkariert.

Erst wenn Politik und Verwaltung Prinzipien wie Bürgerfreundlichkeit, Offenheit und Partizipation tatsächlich praktizieren, kann Informationstechnik möglicherweise unterstützend wirken. Erforderlich wäre in einer solchen Erklärung die Formulierung konkreter Pflichten des Staates und Rechte der Bürger, die über die reine technische Versorgung (Grundversorgung, Zugang zu Dokumenten wie Gerichtsentscheide etc.) hinausgehen.

2. Gefahr einer Technokasten-Oligarchie

Die Bereitstellung von Informationen in elektronischer Form sowie die Implementierung elektronischer Diskussions- und Beteiligungsverfahren alleine ist unzureichend und undemokratisch. Zumindest für eine lange Übergangszeit kann nicht davon ausgegangen werden, daß derartige Medien von allen BürgerInnen genutzt werden (können). Dies ist nicht allein eine Frage des Zugangs zu öffentlichen Terminals, sondern vor allem auch eine Frage der Vertrautheit und des Umgangs mit dem Medium. Demokratie läßt sich nicht durch den Zwang zur Nutzung einer neuen Technik verwirklichen. Will man die Ausgrenzung weiter Teile der Bevölkerung vermeiden, so darf sich Information und Bürgerbeteiligung nicht auf elektronische Medien beschränken.

Auch darf die „Ausgestaltung von Pilot-Projekten" nicht allein den „Internet-Gemeinschaften" und damit genau jenen überlassen werden, die sich

ohnehin schon im Netz tummeln. Im Gegenteil käme es darauf an, die restlichen 95% der Bevölkerung, die dort noch nicht zu finden sind, in die Ausgestaltung dieser Projekte von Anfang an einzubeziehen.

3. Kompetenz und Verantwortung der InformatikerInnen

Berufsvereinigungen wie das FIfF, der Fachbereich „Informatik und Gesellschaft" in der Gesellschaft für Informatik und andere sind in der Diskussion zum Thema engagiert, doch leider nicht in die Tagung eingebunden worden. Damit sind solche Gruppen auch bei der Entwicklung dieser Erklärung außen vor gehalten worden, die sich zum Teil seit Jahrzehnten mit den gesellschaftlichen und politischen Folgen auseinandersetzen und einen umfangreichen Erfahrungsschatz mit der basisorientierten Gestaltung von Netzen gesammelt haben. Bei ihnen liegen Erfahrungen aus „Pilot-Projekten der Internet-Gemeinschaften" vor, die in der Erklärung erst noch gefordert werden.

Die AutorInnen der Erklärung ignorieren den Widerspruch, daß einerseits mit geringem Mitteleinsatz gemachte Erfahrungen mit wissenschaftlicher Begleitung vorliegen, an deren Umsetzung es jedoch hapert, andererseits aber nicht klar wird, woher Mittel für weitere Projekte kommen und welche Ziele damit überhaupt verfolgt werden sollen. Abstrakt ist die Forderung nach Pilotprojekten zwar richtig, ihre mangelnde Konkretisierung beraubt sie jedoch jeglicher Wirkung.

4. Informationstechnik als Feigenblatt

Die katastrophale Situation vieler öffentlicher Bibliotheken zeigt, daß derzeit weder der politische Willen noch die notwendigen Finanzmittel für eine echte „Informationsinitiative" gegeben sind. Für Bürgerinformation und -beteiligung sind nicht nur Vernetzung und einige öffentliche Terminals erforderlich, sondern vor allem transparente Ordnungsstrukturen und die regelmäßige Pflege der Datenbestände sowie die Betreuung und Unterstützung der Bürger bei der Informationssuche. Dies erfordert auf Dauer einen hohen personellen und materiellen Aufwand. Wird dies nicht berücksichtigt, haben elektronische Informationen gegenüber weiten Teilen der Bevölkerung nur noch eine Alibi-Funktion, da „im Prinzip" jeder darauf zugreifen hätte können.

5. Demokratie braucht den Schutz der Bürgerinnen und Bürger

Die Sicherstellung des Datenschutzes wird in der Erklärung an keiner Stelle gefordert, obgleich sie eine der wesentlichsten Voraussetzung für demokratische Netznutzung darstellt. Zur Demokratisierung gehört auch, allgemein anerkannte Schutzrechte in netzbasierte Interaktionsformen zu übertragen. Kryptierung und „technische Selbstschutzmöglichkeiten" sind zwar richtige, doch letztlich unzureichende Forderungen, die nur die Hilflosigkeit in einer Wahl ultimativer Mittel dokumentiert. Selbstschutz allein ist hilflos gegen die weitgehende Aushöhlung der Persönlichkeitsrechte durch bestimmte Nutzungsformen der Netze, die weder die Technik noch der Markt verhindern werden. Der Schutz der Persönlichkeitsrechte ist notwendige Voraussetzung einer demokratischen Netznutzung.

6. Gesellschaftlicher Diskurs ist notwendig

Das FIfF beschäftigt sich – ausgehend von der Fach- und Sachkompetenz seiner Mitglieder – seit langem mit dieser Thematik, und warnt vor einer Überschätzung der Möglichkeiten der Technik. Informationstechnik mag für eine demokratische Gesellschaft nützlich sein, doch eine „Informationsgesellschaft" muß nicht automatisch demokratischer sein. Es ist notwendig, einen breiten gesellschaftlichen Diskurs anzustoßen und fortzuführen, um einseitig ökonomisch ausgerichteten Konzepten der Industrie sowie zunehmenden Überwachungsversuchen durch Staat und Geheimdienste entgegenwirken zu können. ■

Weitere Informationen bei:

FIFF-Geschäftsstelle

Reuterstraße 44
53113 Bonn
Tel.: (0228) 219548
FAX: (0228) 214924

Ute Bernhardt, stellvertretende Vorsitzende des FIfF
Ingo Ruhmann, FIfF-Vorstandsmitglied
Ralf E. Streibl, FIfF-Regionalgruppe Bremen

Verschlüsselungsgesetze stellen Grundrechte auf den Kopf

Presseerklärung des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Bonn, im April 1997

Zu den in den letzten Tagen bekannt gewordenen Planungen und Vorhaben zur gesetzlichen Regelung von Verschlüsselungsverfahren auf internationaler und nationaler Ebene erklärt der Vorstand des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF):

Unübersehbar verdichten sich die Anstrengungen zur Regulierung der Kryptographie. Nach verschiedenen Anläufen wurde von der OECD Ende März eine Richtlinie zur Kryptierpolitik verabschiedet.[1] Fast gleichzeitig sind aus den USA[2] und Großbritannien[3] Planungen zu neuen nationalen Kryptoregelungen bekannt geworden. Auch haben sich die Hinweise verdichtet, daß die Bundesregierung konkrete Vorschläge erarbeitet hat, um Kryptierverfahren in der Bundesrepublik zu reglementieren.[4]

Dem derzeitigen Planungsstand zufolge erwägt die Bundesregierung drei Varianten einer Verschlüsselungsregulierung:[5]

1. Eine Key-Escrow-Lösung, bei der Anbieter von Verschlüsselungsdienstleistungen bei Bedarf den Sicherheitsbehörden die Schlüssel von Kunden zur Verfügung stellen müssen.
2. Eine Key-Escrow-Lösung, bei der jedoch ausschließlich staatlich lizensierte Anbieter von Verschlüsselungsdienstleistungen operieren dürfen.
3. Eine Key-Escrow-Lösung mit gleichzeitigem Verbot aller nicht amtlich zugelassenen Verfahren.

Das FIfF sieht darin eine ernsthafte Gefahr für die Weiterentwicklung einer immer stärker auf elektronischen Datenaustausch angewiesenen Gesellschaft. Staatlichen Überwachungswünschen wird damit nicht nur der Schutz der Privatsphäre untergeordnet, sondern zugleich der Schutz all jener Interaktions- und Transaktionsformen, die auf elektronischen Netzen abgewickelt werden. Diesen nicht hinnehmbaren Einschränkungen stehen aus technischen Gründen nicht einmal Gewinne für die Ermittler gegenüber.

Die Planungen einer Kryptoregelung verdeutlichen nicht nur die völlige Mißachtung von Bürgerrechten unserer Verfassung. Sie werden zu einem Symbol für die gravierenden Defizite bei dem Verständnis von Problemen, Möglichkeiten und den Herausforderungen an neue Denkansätze der politischen Entscheidungsträger, die bei der Umsetzung ihrer Pläne einer Informationsgesellschaft zutage treten.

Für das FIfF lassen sich in fünf Bereichen Argumente für die Schädlichkeit einer Kryptoregelung anführen

I. Kryptoregelung als letzter Baustein der Überwachung

Weshalb muß die Kryptierung gesetzlich geregelt werden? Von offizieller Seite wird eine Kryptoregelung in der Bundesrepublik damit begründet, sie sei das letzte noch fehlende Element zur Überwachung des Fernmeldeverkehrs. Durch die Fernmeldeverkehrs-Überwachungsverordnung (FUeV)[6] sind die Betreiber von Fernmeldeanlagen dazu verpflichtet, Sicherheitsbehörden den überwachten Fernmeldeverkehr im Klartext zu übermitteln. Dies kann durch die End-zu-End-Verschlüsselung einzelner Nutzer unterlaufen werden. Da bei Telefon und Fax kaum verschlüsselt wird, träfe eine Kryptoregelung vor allem die Nutzer elektronischer Netze, die darin das Briefgeheimnis nur durch Verschlüsselungsverfahren herstellen können.

Damit wird so getan, als sei verschlüsselter Datenverkehr von Verdächtigen in elektronischen Netze an der Tagesordnung und diese somit nicht zu überwachen. Dies ist unzutreffend.

Die geltenden Gesetze und Verordnungen verpflichten auch Anbieter elektronischer Netze, eine Überwachung durch Strafverfolgungsbehörden und Nachrichtendienste zu gewährleisten; derartiges findet bereits statt.[7] Bisher wurde kein Fall bekannt, bei dem die Aufklärung einer Straftat durch Kryptierverfahren verhindert wurde. Dennoch werden vage Bedrohungsszenarien bemüht, um eine Ausweitung der Überwachung des Fernmeldeverkehrs zu begründen.

In der Bundesrepublik läßt sich jedoch ernsthaft kein Rückstand in der Fernmeldeüberwachung ausmachen. Während 1995 in den USA bei 240 Millionen Bürgerinnen und Bürger 1229 Telefonüberwachungen angeordnet wurden, entfielen auf die 80 Millionen Bundesbürgerinnen und -bürger im selben Zeitraum 3667 Anordnungen[8] – pro Kopf also neunmal soviel Überwachungsmaßnahmen hier wie in den USA. 1996 stieg die Zahl der Anordnungen in der Bundesrepublik nochmals um 175% auf 6428 an.[9] Kein Ver-

1. Cryptography Policy Guidelines; Recommendation of the Council, http://www.oecd.org/dsti/iccp/crypto_e.html
2. http://www.cdt.org/crypto/admin_397_draft.html
3. Minister for Science and Technology: Licensing of Trusted Third Parties for the Provision of Encryption Services; http://www.cl.cam.ac.uk/users/rja14/dti.html
4. Presseerklärung des forschungspolitischen Sprechers von Bündnis 90/Die Grünen, Dr. Manuel Kiper: http://www.gruenebt.de/aktuell/pm/indizes/in970236.htm
5. am konkretesten: C. Schulzki-Haddouti: Kanthers Kurs auf das Kryptoverbot; in: http://www.heise.de/tp/te/1146/fhome.htm
6. vgl. die Stellungnahme des FIfF zur FUeV unter http://hyperg.uni-paderborn.de/0x83ea6001_0x0036ce9
7. Erste Fälle einer Überwachung von Internet-Accounts wurden bekannt in: 30.000 Telephonate mitgehört; in: Süddeutsche Zeitung, 2.12.96, S. 15
8. USA: Newsweek 20.5.96, Bundesrepublik: Bt-Drs 13/3618
9. Bt-Drs. 13/7341

gleich der Verbrechenshäufigkeit zwischen der Bundesrepublik und den USA kann diese Unterschiede in der Überwachungshäufigkeit erklären. In welcher Weise diese Mittel zur Verbrechensaufklärung beigetragen haben, läßt sich nicht ermitteln, weil hier eine Kontrolle der durchgeführten Maßnahmen – im Gegensatz zu den USA – nicht stattfindet.

Obwohl Defizite nicht erkennbar sind, sollen mit Großem Lauschangriff und Kryptogesetz weitere Anwendungsfelder der Überwachung erschlossen werden. Dabei werden immer mehr Grundrechte eingeschränkt.

II. Grundrechte stehen Kopf

Die Protagonisten eines Kryptogesetzes behaupten, eine solche Regelung sei nichts Neues, sondern lediglich eine Anpassung der Fernmeldeüberwachung an die technische Entwicklung. Diese Aussage ist falsch.

Ein Verbot nicht zugelassener Kryptoverfahren stellt bisherige Grundrechtsprinzipien auf den Kopf. Die Einschränkung des Briefgeheimnisses erlaubt allein die Kontrolle von Sendungen. Weder sind dadurch bestimmte Schreibformen vorgeschrieben, noch bestimmte Sprachen oder Ausdrucksformen verboten. Keine Strafnorm verbietet es, mit Geheimtinte zu schreiben oder andere Verfahren zu nutzen, um Nachrichten zu verheimlichen. Wer Briefe öffnet, hat alle nötigen Entschlüsselungsarbeiten selbst zu leisten – kein Absender muß ihm dabei auch noch durch einen Brief nach Vorschrift helfen. Ein Kryptoverbot würde entgegen aller bisheriger Rechtssystematik die gesetzeskonforme elektronische Kommunikation dem Diktat staatlich sanktionierter Syntax unterwerfen. Dies hat in Deutschland noch keine Diktatur gefordert.

III. Schließlich ist es Ihr Geld...

Elektronische Netze transportieren nicht nur Briefe, soviel haben auch die politisch Verantwortlichen begriffen. Bei der Nutzung von Verschlüsselungsverfahren geht es neben dem Brief- und Fernmeldegeheimnis auch um andere schutzwürdige Belange.

Wer Kryptogesetze erläßt, will damit zugleich auch die Kontrolle über die elektronischen Varianten von Transaktionsformen, für die heute noch besondere Verschwiegenheitsrechte gelten. Deutlich macht dies das Teledienstegesetz des IuKDG, das explizit auch Telebanking als Teledienst definiert. Für Nutzer von Telebanking, Telearbeit und Telemedizin werden das Bank-, Betriebsgeheimnis und die ärztliche Schweigepflicht reduziert auf das Fernmeldegeheimnis. Das Fernmeldegeheimnis wird damit zum strategischen Grundrecht. Ein Kryptogesetz höhlt nicht nur dieses Grundrecht aus, sondern zugleich eine Vielzahl anderer Schutzrechte. Ein solches Gesetz wäre ein trojanisches Pferd für den Rechtsstaat in der Informationsgesellschaft.

IV. Zusätzliche Probleme in der Praxis

Nehmen wir an, ein Kryptogesetz würde formuliert. Wie wäre es überhaupt rechtsfest zu machen und wäre es praktikabel? Dabei ist auch das Gesetz zur digitalen Signatur im IuKDG zu beachten, das einen Rahmen für asymmetrische Kryptierverfahren andeutet. Dies führt zu charakteristischen Problemen.

1. Eine Offenbarung eines hinterlegten Schlüssels an die Sicherheitsbehörden bedeutet bei bislang verfügbaren Systemen, daß so lange eine unbegrenzte Überwachung des Schlüsselinhabers möglich ist, wie er diesen Schlüssel unverändert behält. Dies ist selbst bei Überwachungsmaßnahmen ein bislang ungekanntes Maß eines Eingriffs in Bürgerrechte, dessen Unverhältnismäßigkeit auch Kryptoexperten und Befürwortern eines Gesetzes klar ist: Kein geringerer als Otto Leiberich, ehemaliger Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), publizierte, wie durch die Einführung einer Zeitvariable in Kryptoverfahren die technische Voraussetzung für rechtlich vorgeschriebene zeitliche Begrenzungen der Überwachungsmaßnahme realisiert werden müßte.[10] Können die Sicherheitsbehörden aber ein Interesse an einem rechtskonformen Verfahren haben, das sich nicht mehr entschlüsseln ließe, wenn Nutzer die Aufklärung schon durch ein verändertes Systemdatum des Computers behindern können?

2. Der offenbarte private Schlüssel eines Verdächtigen macht dessen eingehenden Datenverkehr lesbar, nicht aber seine Nachrichten an Dritte. Anhaltspunkte oder Beweise für eine Verabredung zu einer Straftat mit Dritten lassen sich aufgrund der Eigenschaften asymmetrischer Kryptierverfahren nur gewinnen, wenn auch die Schlüssel seiner Kommunikationspartner offengelegt werden, unter Umständen auch noch darüberhinaus deren Partner. Die Folge ist ein tendenziell exponentielles Wachstum der Verdächtigen, der Fernmeldeüberwachungen und des Arbeitsaufwandes der Ermittler. Hier kann weder von einer Verhältnismäßigkeit der Mittel noch von einer effektiven Ermittlungsarbeit die Rede sein.

3. Mangels kompetenter Institutionen wird die Bundesregierung kaum umhin kommen, bei der Kontrolle über die Kryptierschlüssel auf jene Infrastruktur zurückzugreifen, die sie derzeit für Einführung und Ausgabe der digitalen Signatur etabliert. Kein Gesetz wird den Vertrauensverlust aufwiegen können, wenn dieselbe Instanz einerseits private Kryptierschlüssel an staatliche Stellen weitergeben muß und andererseits für die Sicherheit der digitalen Signatur bürgt. Gerät nämlich die digitale Signatur in falsche Hände, ließe sich jedes Dokument rechtlich verbindlich unterzeichnen. Die Furcht der Bürgerinnen und Bürger wäre naheliegend, der Manipulation staatlicher Schlüsselgewaltiger ausgeliefert zu sein. Bei derartigem Vertrauensverlust können sich die Bundesregierung und die auf die digitale Signatur setzenden Unternehmen die Mühe sparen.

4. Ein nationales Kryptogesetz ist kaum tauglich, angemessen auf die Probleme des für elektronische Netze typischen internationalen Datenverkehrs zu reagieren. Um an die Kryptoschlüssel einer „Mafiaorganisation" zu

10. Otto Leiberich: Verschlüsselung und Kriminalität II, in: BSI-Forum der KES 1/95

kommen, müßten in der Regel die Behörden mehrerer Länder mobilisiert werden. Wollen uns die Protagonisten eines Kryptogesetzes nun allen Ernstes weismachen, daß eine internationale Kooperation bei der Herausgabe hinterlegter Schlüssel besser funktionieren wird als die bislang absolut mangelhafte Kooperation bei der Verfolgung von Straftaten, bei denen elektronische Netze genutzt werden?

5. Im Vergleich dazu ist es fast schon nebensächlich, wie ein Kryptogesetz der Softwarebranche das Leben schwer macht. Um eine kryptogesetzkonforme Zuordnung von persönlichem Kryptoschlüssel und Nutzer zu gewährleisten, müßten beispielsweise die Hersteller von Internet-Browsern, die heute oft Verfahren zur verschlüsselten Übermittlung sensitiver Daten beinhalten, in Deutschland auf die Distribution ihrer Software per Internet verzichten und stattdessen nur noch Softwarepakete persönlich gegen Vorlage des Personalausweises verkaufen. Ein solcher Aufwand lohnt sich nur für wenige, was die legale Nutzung sicherer Verfahren nicht gerade verstärken würde. Wenn darüberhinaus unterschiedliche und damit technisch inkompatible nationale Regelungen entstehen, bleibt der vielbeschworene globale Electronic Commerce eine Illusion.

V. Ein Kryptogesetz macht die Strafverfolger auch nicht schlauer

Mittlerweile macht sich niemand mehr etwas vor: Ein Kryptogesetz ist leicht zu umgehen. Ein legales Kryptierverfahren läßt sich mehrmals auf eine Botschaft anwenden, eine mit einem illegalen Kryptierverfahren verschlüsselte Botschaft läßt sich mit einem legalen Verfahren „verpacken". Ein Kryptogesetz ist sogar so zu umgehen, daß niemand dies nachweisen kann: Die Steganographie und andere Verfahren zur Nutzung verdeckter Kanäle verstecken Botschaften z.B. in Klartext-Dateien und verschleiern schon die Existenz einer verschlüsselten Botschaft.

Von der Umgehung des Gesetzes erhoffen sich Experten der Inneren Sicherheit sogar schon Vorteile, ließen sich doch aus dem Nutzerkreis illegaler Kryptoverfahren ermittlungstechnisch wertvolle Rückschlüsse auf die Organisationsstruktur des verdächtigten Personenkreises gewinnen.

Bei steganographischen Verfahren ist dieser Personenkreis niemals zu ermitteln. Was ist aber gewonnen, wenn denn eine Gruppe von Personen gefunden wäre, die dasselbe nicht zugelassene Kryptoverfahren nutzen? Ihre Kommunikation ist nicht zu entschlüsseln, also muß auf andere Weise ermittelt werden. So, wie sich heute schon Beamte durch meterhohe Papierstapel mit den Protokollen von Telefonüberwachungen quälen, werden sie in Zukunft Personenkreise aufwendig ausforschen müssen, die sich nichts haben zuschulden kommen lassen, als nicht zugelassene Kryptierverfahren zu nutzen und zufällig mit Personen zu kommunizieren, die unter irgendeinem Verdacht stehen. Dieser Aufwand läßt sich nicht einmal mit arbeitsmarktpolitischen Gründen rechtfertigen. Die Nutzer nicht zugelassener Kryptierverfahren automatisch zu Verdächtigen zu stempeln, wäre also schon unter ermittlungstaktischen Aspekten nichts als Unfug.

Aus technischer und praktischer Sicht stellt sich ein Kryptogesetz als unsinnig und undurchführbar dar. Juristen vertreten dagegen den Standpunkt, unerheblich von der Durchsetzung sei dem Recht in jedem Fall Folge zu leisten. Eine solche dogmatische Auffassung ist jedoch mit einem demokratischen Rechtsstaat nur schwer vereinbar.

VI. Fazit

Nach Auffassung des FIfF trägt ein Kryptogesetz zur Forcierung der nicht gerade zaghaften Überwachung des Fernmeldeverkehrs in der Bundesrepublik bei. Es stellt grundrechtliche Prinzipien auf den Kopf. Es bedroht in wesentlichem Umfang die grundgesetzlich geschützten Persönlichkeitsrechte in elektronisch gestützten Transaktions- und Interaktionsformen. Es führt in der Praxis zu gravierenden zusätzlichen Rechtsproblemen und führt keineswegs zu einer Erleichterung der Arbeit der Strafverfolger. Die Probleme, die eine solche Regelung zwangsläufig hervorrufen wird, lassen sich auch nicht mit Rechtsdogmatismus lösen. Dem schwerwiegenden Schaden für Bürgerrechte, Demokratie, aber auch für wirtschaftliche Interessen steht ein äußerst magerer Nutzen gegenüber. Jede rationale Bewertung müßte vor diesem Hintergrund zu dem Schluß kommen, auf eine Kryptoregelung zu verzichten.

Daß die Bundesregierung trotz jahrelanger Beratung mit ausgewiesenen Experten dennoch nicht von einer Kryptoregelung Abstand genommen hat, ist entweder ein Indiz für mangelnde Kenntnis oder die mutwillige Mißachtung der Konsequenzen.

Die einander in hohem Maße ähnlichen Regelungen der OECD, Großbritanniens, der USA und mit ihnen die bundesdeutschen Pläne lassen sich mit den Visionen einer globalen demokratischen Informationsgesellschaft nicht in Einklang bringen.

VII. Forderungen

Statt einer Einschränkung von Kryptierverfahren ist es nach Auffassung des FIfF notwendig:

1. Die Verbreitung und Nutzung von Kryptiersystemen zu erhöhen,
2. die Nutzung von Kryptiersystemen nicht durch Einschränkung oder Verbot zu behindern,
3. die freie Wahl von Kryptosystemen zu ermöglichen,
4. die Entwicklung sicherer Kryptosysteme zu unterstützen,
5. den Schutz elektronischer Transaktions- und Interaktionsverfahren zu verstärken und
6. den Nutzen staatlicher Überwachung von Kommunikation einer regelmäßigen, unabhängigen und umfassenden Bewertung zu unterziehen. ■

Ralf Klischewski

Deutsches Delphi, Mini-Delphi, FIfF-Delphi

Fragen über Fragen zur Informationsgesellschaft

Das Instrument der Delphi-Umfrage hat mittlerweile seinen festen Platz in der Zukunftsschau der Forschungspolitik. Nach einer ersten Umfrage 1993 und einem Mini-Delphi 1995 wird derzeit wieder im Auftrag des Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie (BMBF) eine Delphi-Umfrage zur Entwicklung von Wissenschaft und Technik durchgeführt.

Diese Umfragen sind auf die wirtschaftliche Verwertbarkeit ausgerichtet: In Zeiten wirtschaftlicher Verunsicherung ist es noch wichtiger, nach den Schlüsseltechnologien der Zukunft zu fragen (Vorwort Umfrage 1993). Gefragt wird für die nächsten Jahrzehnte, wann welche wichtigen Entdeckungen gemacht oder im Prinzip bekannte technologische Innovationen unter wirtschaftlichen Gesichtspunkten eingeführt bzw. breit verwendet werden könnten (Blind 1996, S. 167). Dabei interessieren nicht nur die wissenschaftlichen und technischen Möglichkeiten, sondern auch die Hemmnisse, die die erhoffte wirtschaftliche Nutzung behindern (z.B. technische Probleme, gesetzliche Vorschriften, soziale und politische Faktoren, Kapitalmangel bzw. zu hohe Kosten, Ausbildung u.a.).

Diese Delphi-Umfragen sind Teil der strategischen Ausrichtung von Forschung und Entwicklung auf die Stärkung der Wettbewerbsfähigkeit der deutschen Wirtschaft. Andere strategische Ziele werden damit nicht verfolgt, beispielsweise der Versuch einer vorausschauenden Technikfolgenabschätzung, um die Sozial- und Ökologieorientierung von Forschung und Entwicklung zu verbessern. Denn obwohl dort hinter vielen knapp gefaßten Einzelfragen eine nicht näher ausgeführte Vision von gesellschaftlichem Rang steht, sind die Ergebnisse wenig hilfreich, weil nur die technologischen Leitbilder und Produktvisionen benannt sind.

Diese Einseitigkeit war Anlaß für das FIfF, 1995/96 selbst eine Delphi-Umfrage durchzuführen. Die Umfrage ist Teil der FIfF-Initiative „Informationstechnik für eine lebenswerte Welt" und ist im gleichnamigen Rundbrief #3 dokumentiert (siehe Literatur). Im folgenden werden Motivation und Verlauf der Umfrage vorgestellt sowie die Ergebnisse kritisch kommentiert. Die richtigen Fragen stellen ist jedenfalls nicht einfach: Es fragt sich vielmehr, ob und wie InformatikerInnen gemeinsam mit anderen im FIfF oder anderswo über ganzheitliche Aspekte von gesellschaftlicher Entwicklung ins Gespräch kommen und Perspektiven entwickeln können.

Warum die FIfF-Umfrage „Informationstechnik für eine lebenswerte Welt"?

Mittlerweile reden viele davon, die Informationsgesellschaft müsse sozial gestaltet werden. Wie immer wir die Gesellschaft auch nennen – bewußte Einmischung ist notwendig, damit nicht nur Standortfragen und Weltmarktzwänge die Entwicklung und Anwendung von Informationstechnik bestimmen. Das FIfF vertritt die Auffassung, daß eine sozialorientierte Gestaltung (Informations-) Technik und Gesellschaft immer im Zusammenhang betrachten muß, orientiert an der Frage „Wie wollen wir zusammen leben?" Die Umfrage sollte zu diesem Thema ein Meinungsbild erheben, Anregungen sammeln und die Diskussion im FIfF und in der Öffentlichkeit zu folgenden Fragen anregen:

- Was bedeutet sozialorientierte Gestaltung?
- Woran sollten sich Politik, Wirtschaft und Wissenschaft orientieren?
- Welche Visionen von Informationstechnik für eine lebenswerte Welt sollten im Zentrum stehen?

In bewußter Analogie zum Vorgehen des BMBF wurde auf die Delphi-Methode zurückgegriffen: ein Verfahren der Gruppeninteraktion, in dem wiederholt Fragebögen an einen bestimmten Kreis von Menschen verschickt werden, wobei ab der zweiten Runde auch Informationen über das Ausmaß an Gruppenkonsens übermittelt werden.

Während das BMBF (damals noch BMFT) z.B. für die erste Umfrage ihre Experten bewußt zu 75% aus Hochschulen und Wirtschaft rekrutierte, sollte die FIfF-Umfrage zu „Informationstechnik für eine lebenswerte Welt" vorab keine Einschränkung dieser Art vornehmen. Stattdessen wurde von den Teilnehmenden eine Selbsteinschätzung erbeten nach der Art ihrer Perspektive (einer/s Technikentwicklenden, einer/s Technikanwendenden, einer/s Wissenschaftlerin/s, als allgemein Interessierte/r o.a.). Als Experten zu diesem Thema wurden für die 1. Runde die ca. 120 Teilnehmenden der FIfF Jahrestagung im November 1995 in Mühlheim angesprochen, sowie die Mitglieder des FIfF-Rat und

des FIfF-Arbeitskreises ökologische Orientierungen in der Informatik angeschrieben.

Wie war die FIfF-Umfrage aufgebaut?

Die FIfF-Umfrage konnte nur mit geringem Aufwand und ohne jede finanzielle Unterstützung vorbereitet und durchgeführt werden – angesichts der komplexen Thematik ein gewagter Versuch mit entsprechenden Auswirkungen auf die Qualität der Ergebnisse (s.u.).

Der Aufbau des Fragebogens war ein Kompromiß zwischen standardisiertem und offenem Interview. Die einzelnen Themen wurden mit vorgegebenen, schnell zu beantwortenden Fragen eingeleitet. Daneben blieb genügend Raum, eigene Fragen, Perspektiven und sonstige Kommentare zu formulieren.

Der Fragebogen der 1. Runde gliederte sich in acht Einzelfragen zu wünschenswerter bzw. zu erwartender Nachfrage nach informationstechnischen Lösungen (zu den Themen Arbeitsqualität, ökologischer Strukturwandel, kulturelle Vielfalt, Demokratie/soziale Autonomie) sowie in vier Einzelfragen zu Perspektiven von Forschung und Entwicklung (Orientierung an dieser Nachfrage). Jede Einzelfrage bestand aus einer Vision über zukünftige soziale Praxis (Art des Technik- bzw. Methodeneinsatzes), die anhand vorgegebener Kategorien zu bewerten war:

- Wann vermuten Sie das Eintreten der Vision (Zeitraum der Verwirklichung in Deutschland)?
- Mit welchen Akteuren sollten WissenschaftlerInnen (z.B. aus der Informatik) bei der sozialen Gestaltung dieser Praxis zusammenarbeiten?
- Ist die angesprochene Praxis wünschenswert und förderungswürdig (oder nicht)?
- In welcher Phase der Technikentwicklung sehen Sie im Hinblick auf die angesprochene Anwendung den größten Bedarf für Diskurs und soziale Kooperation? (nur bei 1.-4.)
- Wo sehen Sie die wichtigsten Hemmnisse bzw. Ansatzpunkte zur Problemlösung auf dem Weg zu einer angemessenen sozialen Gestaltung?

Der Fragebogen war als Tabelle zum Ankreuzen angelegt – soweit sinnvoll, waren immer auch mehrere Antworten pro Kategorie möglich. Zu jeder Einzelfrage, aber auch zu jedem Themengebiet insgesamt, waren auch freie Antworten möglich bzw. erwünscht. Diese konnten z.B. die vorhandenen Thesen kommentieren oder eigene formulieren. Im Sinne der Umfrage waren alle Anmerkungen von Interesse, die Prioritäten und konkrete Perspektiven für eine sozialorientierte Informationstechnikgestaltung aufzeigen.

In der zweiten Runde wurden dieselben Fragen gestellt – doch beim Ankreuzen war (durch Balkendiagramme) unmittelbar sichtbar, wie sich die Antworten der ersten Runde verteilen. Dies gab den Befragten Gelegenheit, ihre Antworten nochmal neu zu überdenken. Zusätzlich wurden alle eingegangenen Kommentare und Visionen der 1. Runde in Kurzfassung wiedergegeben, um in der 2. Runde darauf reagieren zu können.

Die Auswertung

Bis Anfang Februar 1996 gingen 40 ausgefüllte Fragebögen ein, das bedeutet einen Rücklauf von etwa 30%.Die Auswertung der 1. Runde fand im März 1996 statt. Im April wurden die Fragebögen der 2. Runde an die Adressen verschickt, die den Fragebögen der 1. Runde beigefügt waren. Bis Ende Juni gingen 17 Fragebögen ein, das bedeutet einen Rücklauf von über 40% in der zweiten Runde (über beide Runden insgesamt etwa 12%).

Die Antworten aus beiden Runden sind vollständig dokumentiert (siehe Literatur), aber die Auswertung ließ in mancher Hinsicht zu wünschen übrig:

1. Mit statistischen Methoden waren keine sinnvollen Aussagen zu erhalten, dafür war die Zahl der abgegebenen Antwortbögen zu gering.
2. Die Antworten enthielten insgesamt eine Vielzahl von Anregungen und Kontroversen, konvergierten aber nur selten zu einem deutlich sichtbaren Konsens. Eine politikfähige Vorlage für einen forschungspolitischen Diskurs brachte die Umfrage daher nicht hervor.
3. Für den weiteren Diskurs zum Thema „Informationstechnik für eine lebenswerte Welt" bietet die Umfrage eine Fülle von Material für weitere Auswertungen hinsichtlich sowohl der Visionen in den einzelnen Themenbereichen als auch der Art und Weise der Annäherung an die Frage nach einer sozialorientierten Gestaltung der Informationsgesellschaft. Das Potential konnte aber mangels Arbeitskapazität (bisher) nicht genutzt werden.

Zwischenfazit: Klare Aussagen und unmittelbar weiterverwertbare Ergebnisse zum Thema „Informationstechnik für ein lebenswerte Welt" hat die Umfrage nicht zutage gefördert. Doch die FIfF-Delphi-Studie sollte „ein Meinungsbild erheben, Anregungen sammeln und die Diskussion im FIfF und in der Öffentlichkeit anregen". In dieser Hinsicht sind die hier dokumentierten Ergebnisse wertvoll – aber es bleibt jeder und jedem selbst überlassen, sich davon anregen zu lassen, eine Meinung zu bilden und sich an der Diskussion zu beteiligen.

Fragen über Fragen

Der FIfF-Vorsitzende Reinhard Keil-Slawik hat Verlauf und Ergebnisse der FIfF-Umfrage hinsichtlich ihrer Zielsetzung als enttäuschend bewertet (Keil-Slawik 1996). Im Zentrum der Kritik stand allerdings nicht die mangelnde Repräsentativität: Denn bei Fragen, die die quali-

tative Beziehung Technik und Gesellschaft in den Vordergrund stellen, ist es auch weniger die statistische Signifikanz von Einzelaspekten, die interessiert, als vielmehr die inhaltlichen Bemerkungen der Orakelisten. Doch gerade diese Anmerkungen ließen sich nicht zu qualifizierten Meinungen und Einschätzungen verdichten. Jeder Versuch, diese aus der Studie herauszudestillieren, offenbart, daß es eher Ratlosigkeit und unterschiedliche Interpretationen der Fragen waren, die zu dieser diffusen Vielfalt an Äußerungen geführt haben.

Die Ursachen für die relativ geringe Beteiligung, für die teilweise Ratlosigkeit bei der Beantwortung und für die oft wenig präzisen Äußerungen sieht Reinhard Keil-Slawik vor allem in der Art der Fragen: Wo es keine klaren Fragen oder Aussagen gibt, darf man auch keine klaren Antworten erwarten. Bedauerlich aber ist, daß es bestimmt viele Aussagen und Fragen gibt, die man hätte etwas präziser formulieren können. Vielleicht wäre es nützlicher gewesen, stärker darauf zu achten, daß Fragen und Aussagen halbwegs eindeutig, beantwortbar bzw. bewertbar sind, statt die Komplexität der Zusammenhänge und Wechselwirkungen so ausschließlich zum Thema zu machen.

Trotz aller Kritik wurde dennoch entschieden, die FIfF-Umfrage zu veröffentlichen. Denn die hierbei gemachten Erfahrungen sind geeignet, weitere Fragen anzustoßen und daraus zu lernen:

- Lassen sich komplexe Zusammenhänge überhaupt mit der Delphi-Methode erheben, und welche Form müßte sie dann haben (vgl. z.B. auch Hoppé/Nake 1995)?
- Zeigt die Vielfalt der teils widersprüchlichen Anmerkungen nicht, daß es in bezug auf Technikentwicklung und -gestaltung keine einfachen Rezepte gibt?
- Und schließlich: Ist das Ergebnis der Studie nicht die beruhigende Versicherung, daß es ohne die tägliche und professionelle Arbeit einer Berufsorganisation wie dem FIfF und ohne unsere aktuellen und ausführlich begründeten fachkundigen Stellungnahmen nicht geht?

Das Fazit von Reinhard Keil-Slawik möchte ich an dieser Stelle ungekürzt wiedergeben: „Wie dem auch sei, die Studie hat wieder einmal deutlich gemacht, daß es nicht reicht, allein das Gute zu wollen; man muß es auch können. Dabei kann es auch einmal von Vorteil sein, etwas weniger ganzheitlich vorzugehen oder sich auch an die alte Weisheit zu erinnern, daß der Fortschritt in der Wissenschaft nicht davon abhängig ist, wie ehrgeizig die Problemstellung ist, sondern wieweit es gelingt, diejenigen Fragen zu finden, die sich mit den gegebenen Mitteln in hinreichend kurzer Zeit lösen lassen. Kritik kann sehr umfassend sein; das ist auch gut und richtig so. Konstruktive Kritik muß aber, damit sie wirken kann, immer punktuell sein. Wenn wir als Fifferlinge einen konstruktiven Beitrag zur Gestaltung der Informationstechnik für eine lebenswerte Welt leisten wollen, dann müssen wir gelegentlich auch etwas bescheidener werden und unsere Ansprüche reduzieren. Mit der vorliegenden FIfF-Studie haben wir – und das wäre mein Fazit – zu viel gewollt. Die Frage, zu der die FIfF-Studie Anregungen und Visionen liefern sollte, nämlich Wie wollen wir zusammen leben?, ist wohl ein Hauch zu grundsätzlich, zu allumfassend gewählt, als daß man sich wirklich durch Ankreuzen einzelner Rubriken ernsthaft damit auseinandersetzen könnte. Nicht die Frage ist verkehrt, sondern sie auf diese Weise zu stellen".

Diesem Fazit kann ich in Bezug auf die Delphi-Umfrage zustimmen, obwohl (oder gerade weil) ich sie selbst durchgeführt habe. Nur in die angedeutete Bescheidenheit mag ich mich nicht fügen: Angesichts der Probleme, mit denen wir uns in der heutigen Welt konfrontiert sehen, müssen wir lernen, auch über ganzheitliche Fragen zu kommunizieren und Perspektiven zu entwickeln, die über punktuelle Maßnahmen hinausgehen. Als InformatikerInnen sind wir maßgeblich daran beteiligt, die Bedingungen für gesellschaftliche Entwicklung zu verändern. Nach meinem Verständnis bedeutet professionelle Verantwortung daher auch, die gesellschaftliche Entwicklung ganzheitlich in den Blick zu nehmen und nach Kräften für eine bewußte Gestaltung durch demokratische Prozesse zu öffnen.

Die FIfF-Initiative Informationstechnik für eine lebenswerte Welt ist ein Versuch, der einseitigen Ausrichtung von Forschung und Entwicklung im Bereich Informationstechnik eine (fach-)öffentliche Diskussion über sozial- und ökologieorientierte Perspektiven entgegenzusetzen. Die FIfF-Delphi-Umfrage hat dabei kaum Ergebnisse gebracht, dafür aber um so mehr Fragen aufgeworfen. In aller Unbescheidenheit werde ich auch weiterhin versuchen, das Thema auf die Tagesordnung zu setzen und mich dabei über alle ganzheitlich-konstruktiven (aber auch -kritischen!) Beiträge freuen. ■

Literatur

Blind, K.: Technikvorausschau als Mittel der Technikbewertung und der Entwikkung von Innovationsstrategien: Delphi-Studien im Vergleich. In: Büllingen, F. (Hg.): Technikfolgenabschätzung und Gestaltung in der Telekommunikation. Proceedings. Bad Honnef: Wissenschaftliches Institut für Kommunikationsdienste GmbH, 1996, S. 159-182

Bundesministerium für Forschung und Technologie: Deutscher Delphi-Bericht zur Entwicklung von Wissenschaft und Technik. Bonn 1993

Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie: Delphi-Bericht 1995 zur Entwicklung von Wissenschaft und Technik, Mini-Delphi. Bonn 1996

FIfF-Delphi-Umfrage 95/96 Informationstechnik für eine lebenswerte Welt. In: FIfF-Rundbrief Informationstechnik für eine lebenswerte Welt #3, Bonn 1996, S. 3-27

Hoppé, A., Nake, F.: Das allmähliche Auftauchen des Computers als Medium. Ergebnisse einer Delphi-Studie. Universität Bremen, Fachbereich Informatik, Bericht Nr. 3/1995

Keil-Slawik, R.: Die Orakel des DELFIfF. Kritische Anmerkungen zur Delphi-Studie des FIfF. In: FIfF-Rundbrief Informationstechnik für eine lebenswerte Welt #3, Bonn 1996, S. 28-30

Ingo Ruhmann

Internet auf dem Index

Wie lange wird das Internet noch Freiraum grenzenloser Meinungsfreiheit sein?

Kaum eine der letzten Wochen verging, ohne daß sich irgendwer öffentlich über neue Scheußlichkeiten im Internet erregte. Vom Symbol für eine Zukunftstechnologie ist das Internet zu einem Gefahrenherd mutiert.

Titel über das Internet als Gefahr für Kinder (Focus) oder über „erotische Bilder von TV-Stars im Netz" (TV-Movie) waren Anfang des Jahres noch Mittel der Auflagensteigerung. Um das Interesse der Kundschaft zu erhalten, berichten in jüngster Zeit mehrere TV- und Printmagazinen zunehmend über Kinderpornographie im Internet. Auch mit der Sperrung des elektronischen Zugangs zur etwa ein Jahr alten Ausgabe der linken Untergrundzeitschrift „radikal" ließ sich immer noch Publicitywirkung erzielen. Währenddessen ist das WWW-Angebot des rechtsradikalen Thule-Netzes der Presse zwar fast völlig entgangen, wird aber immerhin im aktuellen Verfassungsschutzbericht erwähnt.

Neben Pornographen und Extremisten werden auch Waffenschieber, Drogenhändler und Geldwäscher im Internet geortet: Ein TV-Magazin berichtete über die Ersteigerung von Kriegswaffen per Internet, der Ärztebund warnte vor verschreibungspflichtigen Medikamenten, die sich per Internet von jedermann bestellen lassen und die Financial Actions Task Force der OECD wandte sich offiziell der Aufgabe zu, die Nutzung des Internets zur Geldwäsche zu verhindern.

Durchschnittsnutzer des mittlerweile 56 Millionen TeilnehmerInnen in aller Welt umfassenden Internets werden da oft nur staunen. Obgleich im Telefonnetz die größeren Verbrechen verabredet wurden, hat sich das ebenfalls als Vermittlungsnetz ausgelegte Internet in der öffentlichen Debatte mittlerweile zum Hort des Bösen gewandelt. Kaum eine Rede konservativer Politiker, die das Thema Neue Medien und Technologie auch nur streift, läßt heute die Forderung nach verschärfter Kontrolle über das Internet aus. Der Schluß des bayerischen Ministerpräsidenten Stoiber: „Der Schutz der Kinder ist höher einzustufen als eine schrankenlose Meinungsfreiheit."

Während sonst Konservative die Informationstechnik besonders durch linke Technikfeindlichkeit behindert sehen, beklagen sie nun selbst lautstark fehlende Grenzen dieser Technologie. Gerade jene, die im Umgang mit dem Internet wenig Erfahrung haben, überbieten sich mit Vorschlägen. Ohne Kenntnis technischer Möglichkeiten für polizeiliche Arbeit im Netz wird vor unkontrollierbaren Gefahren gewarnt, die immer noch gut funktionierende Kultur der Selbstkontrolle des Internets als Anarchie diffamiert. Konservativen gelten jene Teile der SPD und vor allem Grüne, die das Internet für sich entdeckt haben, als gefährlich, weil sie sich nicht der Aufregung um grenzenlosen Datenaustausch im Internet anschließen.

Fakten sind dabei oft unerheblich. Offenbar fällt es auch der Bundesanwaltschaft schwer, über die genannten Beispiele hinaus auch nur annähernd gerichtsverwertbare extremistische Publikationen im Internet zu finden, weswegen den Fall „radikal" ein ums andere Mal aufwärmt. Die Kriegswaffen entpuppen sich als vom Pentagon per Internet versteigertes ausgemustertes Gerät, das – sofern überhaupt noch nutzbar – legal nicht exportierbar ist. Das für Geldwäsche im Internet nötige elektronische Zahlungssystem existiert noch gar nicht. Der Ärztebund schließlich warnt nicht nur vor Arzneimittelimporten per Internet, sondern auch vor Reimporten der Apotheken aus der EU, obwohl dies zur Kostendämpfung im Arzneimittelrecht vorgesehen ist. Selbst die Bundesregierung erklärt, daß nach deutschem Recht Illegales – einschließlich Pornographie und Extremismus – auf dem Internet „deutlich weniger als 1%" ausmacht.

Verwirrung prägt die Debatte. Stoiber ist beispielgebend, wenn er strafbare Kinderpornographie mit Meinungsfreiheit vermengt und so fälschlicherweise suggeriert, das Internet sei ein rechtsfreier Raum. Kinderpornographie ist jedoch unter Nutzung des Internets ebenso strafbar wie ohne. Gleiches gilt für die meisten der anderen Tatbestände. Die EU-Kommission trennt deshalb nun zwischen illegalen und gefährdenden Inhalten.

Illegales, also Straftaten per Internet, sind ein Problem der Strafverfolgung. Bei der Frage, welche Polizeidienststelle denn über die Kompetenz und technische Ausstattung verfügt, um dies im Internet zu verfolgen, zeigt sich, wie hohl Stoibers markige Worte sind. Die vom forschungspolitischen Sprecher der Bündnisgrünen im Bundestag, Manuel Kiper, erfragten Daten sind ernüchternd. Das BKA nutzt zwar das Internet, kann aber nicht angeben, wie oft dies zum Ermittlungserfolg beitrug. Das Zollkriminalamt hat gar keinen Internet-Anschluß, die Bundesprüfstelle für jugendgefährdende Schriften immerhin einen. Wenn es so überhaupt zu Ermittlungen kommt, sorgen fehlende Amtshilfeabkommen dafür, daß polizeiliche Kooperation nicht stattfindet. Selbst bei der Verfolgung von Kinderpornographie konnte die Bundesregierung kein einziges Beispiel für eine Zusammenarbeit mit den USA nennen. Der Beitrag des Münchener TV-Magazins Report machte daher vor allem deutlich, daß die Polizei ohne Unterstützung von Internet-Nutzern mangels Personal und technischer Ausstattung ohnmächtig ist. Kiper sieht daher „hilflose Fahnder im Internet", die sich auf „wichtige Kriminalitätsbereiche" konzentrieren sollten, statt auch noch „übernormierte Tatbestände der Meinungsäußerung" zu verfolgen.

Denn wie zum Trotz wollen Politiker und Strafverfolger vor allem die Unterdrückung von gefährdenden

Inhalten im Internet, all das, was die Jugend politisch oder sittlich gefährden könnte oder bei dem das zulässige Maß an Meinungsfreiheit unterschiedlich gesehen wird. Deshalb ist gerade bei Meinungstatbeständen oft hier verboten, was anderswo erlaubt ist. Das Internet nimmt keine Rücksicht auf Landesgrenzen. Hier Verbotenes ist dort im Internet abrufbar und die Staatsgewalt machtlos.

Der Jugendschutz ist oft genannter Grund für Sperrungswünsche. Surfen kann man als Student oder Arbeitnehmer – private Nutzung ermöglichen nur Provider, die für Zahlungen Bankkonto oder Kreditkarte verlangen. Provider schließen daher kaum Verträge mit Minderjährigen. Deren größerer Spieltrieb aber ist im kindersicheren Internet nützlich, um mehr kostenpflichtige Onlinezeit und höhere Telefonrechnungen zu verursachen. Lehrgeld dafür, daß auch Sperrungen im Internet nicht die Probleme elterlicher Aufsichtspflicht lösen.

Doch Jugendschutz ist nur ein kleiner Teil. Je rigider das politische System, desto intensiver scheint der Wille, ungehinderten Datenaustausch per Internet zu unterbinden. China und Singapur erlauben ihren Bürgern nur den Zugriff auf die von den Zensurbehörden genehmigten Internet-Inhalte. Europäische Staaten setzen derzeit mangels rechtlicher Befugnisse auf eine Sperrung von Inhalten durch die Internet-Provider. Deren Einverständnis wurde mehrfach durch die Drohung mit einem Ermittlungsverfahren hergestellt. Die erste Sperrung des Amsterdamer Providers XS4ALL und der dort legalen Zeitschrift „radikal" ging mit einer Androhung eines Ermittlungsverfahrens einher, das auch eingeleitet wurde, als die deutschen Provider ihre Sperrung wieder aufhoben. Die zweite Sperrungsaufforderung gegen das DFN folgte diesem Muster. Die britische Polizei droht Providern mit Beschlagnahmen wegen Internet-Newsgruppen mit legalen pornographischen Inhalten. Programmierer sind dabei, die für Unternehmen verfügbaren Firewall-Systeme zur selektiven Unterdrückung einzelner Internet-Inhalte so zu modifizieren, daß sich diese bald auch für ganze Länder sperren lassen könnten.

Wie zum Hohn auf diejenigen, die sich per Internet mehr Demokratie und Meinungsfreiheit versprechen, geht es in allen Fällen nicht um das Belangen von Urhebern, sondern um das Unterbinden des freien Zugangs zu Daten. Hier zeigt sich einmal mehr, daß Technik nicht politische und soziale Unterschiede ausgleicht. Klar wird: Das Internet eint nicht die Welt, es beleuchtet ihre politische und kulturelle Differenz. Es macht die Unvereinbarkeit unserer Rechtsordnungen sichtbar und damit schon eine Einigung auf ein einheitliches Weltrecht unwahrscheinlich, vollends unvorstellbar aber den kleinsten gemeinsamen Nenner verschiedenster Moralvorstellungen. Nicht die Kontrolle des Internets sollte daher die Frage sein, sondern, wie wir mit unseren kulturellen Unterschieden umgehen.

Soll das Internet vom globalen Transporteur von Daten und Meinung auf einen Flickenteppich nationalen Maßes gestutzt werden? Wer im Internet Sperrungen verlangt, kann nicht mehr gegen die Internet-Zensur Chinas protestieren, das auch nur nationalem Recht Geltung verschafft. Wo wären die Grenzen nationalen Rechts? Die Sperrung von Internet-Newsgruppen durch Münchener Staatsanwälte zwang allen Kunden eines globalen Diensteanbieters bayerisches Rechtsverständnis auf. Mit welchem Recht sollte China gleiches verwehrt werden?

Meinung im Internet in seiner heutigen Form national regeln zu wollen, bleibt so illusionär wie die Einigung auf eine weltweite Moral. Globalisierung ist eben auch die größere Vielfalt von Gedanken. Da gibt es Nachholbedarf. Während wir uns über China entrüsten, halten es US-Bürger für ungeheuerlich, daß die Bundesrepublik in Kanada angebotenes rechtsextremes Material verbietet. Das Internet zeigt einen anderen Weg: Dutzende Angebote liefern Argumente gegen die Lügen der Rechten.

Die Alternative zu Verbot und Index ist lange schon die Aufklärung. Die Welt am Internet vertritt eine weit größere Meinungspluralität als viele bislang gewohnt sind. Meinungsfreiheit ist die Voraussetzung des Miteinanders. Es wäre an der Zeit, Meinungsfreiheit auch hierzulande zu stärken und den Nutzen historisch gewachsener Gesetze zu prüfen. Das – kaum noch verfolgte – Verbot des Zeigens von Hakenkreuzen ist ebenso überflüssig wie Spezialgesetze aus der Zeit der Terroristenjagd. Denn eines geht nicht: Globale Meinungsfreiheit zu fordern, aber die Durchsetzung unserer Rechtsordnung zu meinen. ■

CyberLex.TXT (Stand: 2.4.97)

Diese Übersicht bietet in alphabetischer Form mit ca. 60 Stichwörtern einen Überblick über Informationsangebote im Internet und anderen Netzen. Der inhaltliche Schwerpunkt des Textes liegt in den Bereichen Bildung, Datenbanken, Medien und Internet. Für Hinweise, Kritik und Verbesserungsvorschläge ist der Bearbeiter immer zu haben. Adresse steht ganz am Ende. Copyright-Vermerk auch!

Per E-Mail kann dieser Text bei der LINK-CR bestellt werden! E-Mail an:

MARVIN@LINK-CR.BAWUE.CL.SUB.DE.

Betreff: beliebig,Text: SEND POOL:CyberLex.TXT nouu

Per FTP ist der Text ebenfalls verfügbar:

ftp://ftp.free.de/pub/netze/diverse/cyberlex.txt

Anmerkung: Falls der Stand mehr als zwei Monate hinter dem aktuellen Datum zurückliegt, sollten Sie sich eine aktuellere Version von CyberLex.TXT bestellen!! Hinter den Stichwörtern steht das Datum der letzten Aktualisierung.

Copyright-Vermerk

Copyright © 1996,1997 für den Text „CyberLex.TXT" Karl Dietz, Stuttgart – Alle Rechte vorbehalten.

Es ist ausdrücklich erlaubt, Kopien der jeweils aktuellen Fassung dieses Dokuments für den persönlichen Gebrauch zu erstellen! Weitere Verwendung gerne nach Rücksprache mit dem Verfasser.

Ralf E. Streibl

Manöver in der Box

Im bayerischen Hohenfels – auf dem mit rund 16.000 Hektar größten Manöver-Stützpunkt der US-Armee in Europa, auf dem seit 1960 auch die Bundeswehr trainiert[1] – ist ebenso wie im „National Training Center" der US-Armee in Fort Irwin (USA) seit längerem das „Multiple Integrated Laser Engagement System" (MILES) im Einsatz: Alle im Manöver eingesetzten Waffen simulieren den Schuß mit einem Laserimpuls. Die mit Sensoren überzogenen Fahrzeuge erkennen Treffer und schalten ggf. das Fahrzeug als „zerstört" ab. Über Satellit sind die Einheiten mit Computern in der Kommandozentrale des „Combat Maneuver Training Center" verbunden, wo die Schlacht auf Bildschirmen dargestellt wird. Ein vergleichbares System ist auch für das geplante, über 680 Mio. DM teure Gefechtsübungszentrum der Bundeswehr auf dem Truppenübungplatz Altmark bei Magdeburg vorgesehen.

Der nächste Schritt ist auch schon Realität: In Schweinfurt fahren keine echten Panzer durchs Gelände – die Panzerbesatzungen trainieren in langen Reihen von Trainingsboxen. Die einzelnen Simulatoren sind über Datenleitung miteinander verknüpft, was das gemeinsame Training ganzer Einheiten ermöglicht. Das SIMNET erlaubt die Vernetzung von hunderten solcher Simulationsboxen auch über Kontinente hinweg. Das Innere der Simulatoren ist dem Orginalpanzer realgetreu nachempfunden. SIMNET-Training wird nicht als Ersatz für echtes Feldtraining gesehen und weist auch noch Defizite z.B. im Hinblick auf die Simulation der Umgebungsbedingungen auf. Dem soll durch das Nachfolgesystem „Close Combat Tactical Trainer" (CCTT) abgeholfen werden, dessen Einführung von 1996 bis 1999 geplant ist.[2] Von solcher Detailtreue erhofft man sich zum einen bessere Lerneffekte, zum anderen wird der Mensch – oder wie es im Jargon heißt: das „menschliche Teilsystem im Gesamtsystem von Mensch und Maschine" – auf seine Zuverlässigkeit und Belastbarkeit getestet.

In dem 1982 entstandenen „Warrior Preparation Center" (WPC) in Ramstein[3] werden verteilte interaktive Computersimulationen entwickelt und durchgeführt. Nachdem 1989 erstmalig eine NATO-weite Übung im Rahmen des „Distributed Wargaming System" stattfand, begannen ab 1992 Übungen mit weltweit verteilten Teilnehmern: Unter dem Namen „Ulchi Focus Lens" werden seither jährliche „Wargaming"-Übungen durchgeführt, um Verhalten und Entscheidungsfindung unter realitätsnahen Streßbedingungen zu testen und zu trainieren. 1996 fand in diesem Rahmen eine gemeinsame interaktive Echtzeit-Simulation des „Warrior Preparation Center" in Deutschland, dem „Korean Air Simulation Center" in Süd-Korea, der 7. Flotte der US Navy, dem „Air Force's Theater Battle Arena" im Pentagon und weiterer Einrichtungen statt.[4] Bis zum Jahr 2000 sollen im Rahmen des „Synthetic Theater of War"-Programms (STOW)[5] des amerikanischen Verteidigungsministeriums mehr als 100.000 verschiedene Waffenplattformen in ein simuliertes Gefechtsfeld integriert werden. Im Oktober 1997 soll ein erster großer Einsatz des Prototypen im Zusammenhang mit „Unified Endeavor 98-1" stattfinden.

Ein Hauptaspekt des Trainings am Simulator ist die scheinbare Gefahrlosigkeit des Handelns: egal welche „Fehler" sich im Verhalten oder in den Entscheidungen ereignen – das Szenario kann erneut begonnen werden. Daneben besteht die Gefahr, daß bestimmte Aspekte des Simulationsmodells vom Soldaten als normal angesehen werden. Das kann dazu führen, daß er im wirklichen Einsatz die so gelernten Verhaltensweisen anwendet, obwohl die Situation möglicherweise anders ist. Im Simulator wird die Wirklichkeit vereinfacht dargestellt. Solch eine Reduzierung der Komplexität einer Situation kann zur Erreichung spezifischer Trainingsziele hilfreich sein. Sie kann jedoch auch gezielt für eine systematische subtile Einflußnahme auf den Soldaten im Simulator genutzt werden, wenn bestimmte Aspekte weggelassen werden oder absichtlich weniger realistisch dargestellt werden als andere (z.B. keine blutigen, schreienden Opfer, sondern nur Qualmwölkchen über einem zerstörten Fahrzeug). Auch die Palette der im Simulationsmodell vorgesehenen Handlungsmöglichkeiten beeinflußt das Erleben der Situation: militärische Simulationen sind zumeist auf die Handhabung militärischen Geräts oder die strategische Ebene beschränkt. Die Optimierung des Kampfverhaltens ist das zentrale Ziel.[6] Politisch-vermittelnde Aktionen jeglicher Art bleiben ebenso außen vor wie die Erarbeitung neuer Konfliktvermeidungs- und Deeskalationsstrategien – erst recht in einer Zeit, in der die Bundeswehr im Eilschritt von humanitären out-of-area-Missionen zu ihren ersten Kampfeinsätzen eilt und Friedensmissionen der Vereinten Nationen ohne schlagkräftige „Schnelle Eingreiftruppen" kaum denkbar scheinen. ■

1. vgl. http://www.militarycity.com/ins/site1645.rlc.html
2. vgl. http://www.atsc-army.org/atdl/docs/tc/71-5/c2.htm
3. http://www.wpc.af.mil/index.html
4. vgl. http://www.af.mil/news/Sep96/an092396_23sep96_960963.html
5. http://www.stow.com
6. vgl. Götz Neuneck: Computersimulation und moderne Kriegführung. In: H.-J. Kreowski, T. Risse, A. Spillner, R.E. Streibl & K. Vosseberg (Hrsg.): Realität und Utopien der Informatik. Münster: agenda 1995, S.95-103.

Michael Langer

Freiheit aushalten!

Das Internet, die Zensur und die Meinungfreiheit[1]

Als vor gut einer Woche der Entwurf des neuen Informations- und Kommunikationsdienstegesetzes in erster Lesung im Deutschen Bundestag behandelt wurde, waren sich Regierungskoalition und Opposition einig, wirksame Maßnahmen gegen die Verbreitung von Pornographie und Nazi-Propaganda zu fordern. Gleichzeitig warnte man aber auch vor Hysterie. Allenfalls ein Prozent der Inhalte im Internet sei krimineller Art – eine Erkenntnis, zu der unsere Bundesregierung auch schon vor geraumer Zeit gelangte und die sie öffentlich kundtat.

Die Warnung aber vor hysterischen Reaktionen bleibt offenbar wirkungslos. Nichts geht so gut wie die Meldungen über Schmutz und Schund im Internet – das bringt Quote, steigert die Auflage und versetzt die deutschen Bundesbürger, von denen ohnehin nur ungefähr 5% online sind, in Angst und Schrecken, zumal dann, wenn das Reizwort „Kinderporno" fällt. Es entsteht der Eindruck, man wäre mit den Datennetzen vollkommen hilflos einer Flut von Gewaltdarstellungen und Sex & Crime ausgesetzt. Wer allerdings einmal versucht, etwa im populären World Wide Web des Internets entsprechende Angebote einzuholen, wird feststellen, daß das ohne massive Anstrengungen technischer und finanzieller Art sich kaum machen läßt, und daß sich „frei" zugängliches Material nicht vom üblichen Zeitschriftenangebot am Kiosk unterscheidet bzw. davon, was uns (und also unseren Kindern) die Boulevardblätter tagtäglich „zumuten" (ohne daß ein Aufschrei durch die Nation geht): nackte Brüste also.

Es ist ein gerüttelt Maß an Pharisäertum in der Diskussion, und bedenklich ist, daß sich dies gut instrumentalisieren läßt, wenn der Ruf nach Zensur noch lauter werden sollte.

Wer ist verantwortlich für die Inhalte? Wie soll man sie kontrollieren? Die Post, um ein gerne zitiertes Beispiel zu nehmen, wird auch nicht verfolgt, wenn in von ihr transportierten Briefen kriminelle Inhalte stecken. Gegen den Chef des deutschen on-line-Dienstes Compuserve aber erhob die Staatsanwaltschaft München Anklage wegen des Verdachts der Beihilfe zur Verbreitung harter Pornographie und gewaltverherrlichender Computerspiele – da Compuserve einen Zugang zum letztlich nicht kontrollierbaren Internet bietet. Keine Rolle spielt dabei, daß Compuserve in den von ihm kontrollierbaren Bereichen ohnehin peinlichst genau darauf achtet, suspekte Angebote zu tilgen.

Wenn aber on-line-Dienste weiterhin mit einem Bein im Gefängnis stehen, dann ist es Essig mit dem digitalen Wirtschaftsstandort Deutschland, und schon vernimmt man die ersten Abwanderungsgerüchte aus der Branche.

Wie verzwickt die Lage ist, zeigt noch ein anderer aktueller Fall, der sich in den vergangen zwei Wochen in Deutschland zutrug. Beteiligt waren die Generalbundesanwaltschaft und das „Deutsche Forschungsnetz". Unter dem Dach dieses Vereins versammeln sich die deutschen Akademiker: die Universitäten des Landes, die Max-Planck-Institute etwa und die Fraunhofer-Gesellschaft, aber auch viele Bibliotheken und Museen.

Das „Deutsche Forschungsnetz" hatte auf „Hinweis" des Bundeskriminalamtes den Zugang zum niederländischen Internetanbieter XS4all gesperrt, da dort wieder eine on-line-Ausgabe der mißliebigen linksradikalen Zeitschrift „radikal" zu lesen ist, deren Verbreitung hierzulande verboten ist. Der Geschäftsführer des Deutschen Forschungsnetzes Dr. Klaus-Eckart Maass hatte den Schritt damit begründet, daß nach gängiger Rechtsprechnung und nach dem Entwurf des neuen Multimedia-Gesetzes (welches wie gesagt gerade einmal in erster Lesung im Bundestag beraten wurde) für einen Internet-Dienste-Anbieter die Verpflichtung zur Sperrung der Nutzung rechtswidriger Inhalte bestehe, wenn er von diesen Inhalten unter der Wahrung des Fernmeldegeheimnisses Kenntnis erlange und eine Sperrung technisch möglich und zumutbar sei.

So weit, so ungut! Denn eine Sperrung der einen sogenannten Homepage bei XS4all, welche die „radikal"-Seite zugänglich macht, war und ist nicht möglich, sondern eben nur die Sperrung des ganzen Providers XS4all und also des gesamten Angebots; dazu zählen über 6000 Homepages: Projekte von Künstlergruppen, Dienstleistungsunternehmen, Informationsseiten humanitärer Organisationen, Angebote, die auch nach deutschem Recht nicht zu beanstanden sind; im Übrigen hat sich XS4all (was übrigens übersetzt: „Zugang für alle" heißt) nach niederländischem Recht auch in Sachen „Radikal" nicht strafbar gemacht.

Gar nicht zumutbar fanden nun viele Intersurfer, also auch surfende Akademiker in Deutschland, das Vorgehen des Deutschen Forschungsnetzes, das, im Sinne des Generalbundesanwalts Kay Nehm, man kann es nicht anders sagen: mit Kanonen auf Spatzen schoss. Denn unversehens war man auch ausgeschlossen von solchen Informationsangeboten, welche die Freiheit der Forschung und Lehre betreffen.

Desweiteren bedeutete der vorauseilende Gehorsam des DFN einen Akt der Zensur: denn von der Sperrung

1. BR Kulturkritik: Der Kulturkommentar, vom 27.April 1997; Redaktion: Dieter Heß

war z.B. auch der serbische Radiosender B 92 betroffen, der (internationale) Berühmtheit erlangte durch seine Berichterstattung von den Massendemonstrationen in Belgrad, und dem sogenannten Operettendiktator Milosevics ein Dorn im Auge war und ist. B 92 sendet nämlich sein 24-Stunden-Internetradio-programm vom holländischen Anbieter XS4all. Schon im Dezember 1996, als B 92 kurzzeitig Sendeverbot erhalten hatte, waren die oppositionellen Stimmen übers Netz weltweit zu vernehmen. Was einem Milosevics nicht gelingt, nämlich B 92 zum Schweigen zu bringen, das besorgte nun das DFN hierzulande. Wahrlich kein Ruhmesblatt, das man sich da an die Brust heften konnte: höchstens der Beifall von Dikatoren aus China oder Singapur wäre einem sicher gewesen.

Als schließlich klar war (was zuvor auch nichts Geheimes war), daß die inkriminierte Ausgabe der „radikal" seit Monaten auf mindestens 40 anderen WWW-Seiten abrufbar ist (und eben nicht bloß bei XS4all), und nach harschen internationalen Protesten, vor allem aus der akademischen Welt, hob das „Deutsche Forschungsnetz" die Sperrung wieder auf. Man hätte ansonsten z.B. auch die Verbindungen zu amerikanischen Universitätsnetzen kappen müssen...

Im Grunde genommen gibt es in solchen Fällen nur eine Lösung: Deutschland goes off-line! Aber das ist ja auch keine Lösung: das Licht mit dem Holzhammer auszumachen. Stichwort: Verhältnismäßigkeit der Mittel. Man muß sich diesen Fall aus der digitalen Welt einmal folgendermaßen in unsere physische übersetzen: Verbietet man uns die Reise nach Amsterdam, weil wir dort einen Spitzbuben kennenlernen *könnten*? Oder verbieten wir umgekehrt *allen* Amsterdamern die Einreise, damit nicht der eine Bösewicht ins Land gelangt?

Im Zeitalter des Internets kann es die Freiheit der Forschung und Lehre nur dann geben, wenn auch ansonsten die Freiheit des Wortes garantiert ist – was die Verfolgung von strafbaren Handlungen im Netz übrigens nicht unmöglich macht. Die deutsche Generalbundesanwaltschaft wurde aber in besagtem Fall nicht vorstellig bei den niederländischen Behörden und auch an den Anbieter XS4all war man, so die Auskunft der Amsterdamer, nicht herangetreten.

Das Internet, so weltumspannend wie es ist, ist beileibe kein rechtsfreier Raum, sondern es verbindet verschiedene Kulturen, Nationen und die unterschiedlichen Rechtssysteme miteinander: In einigen Südstaaten der USA etwa ist on-line-gambling, also Glückspiel im Netz verboten; bei uns veranstaltet das „Rote Kreuz" eine Internet-Lotterie, was als mildtätig gilt. Was wäre von einem entsprechenden Rechtshilfeersuchen aus den Staaten an die deutschen Behörden zu halten? Oder nähme man ein Internetangebot von Amnesty International bei uns vom Netz, weil die chinesischen Machthaber es wünschten?

Das sind die Fragen im Zeitalter des Internet, die eigentlich schon jahrhundertealt sind und mit dem Zeitalter der Aufklärung zu tun haben: Das Problem ist nämlich nicht bloß informationstechnischer, sondern prinzipieller Natur, ganz im Sinne des Voltaire'schen Satzes: „Ihre Meinung ist das genaue Gegenteil der meinigen, aber ich werde mein Leben daran setzen, daß Sie sie sagen dürfen."

„Die Auschwitzlüge muß verboten bleiben", sagte Forschungsminister Rüttgers im Bundestag, „egal ob sie in schwarz oder weiß, in bit oder byte verbreitet wird".

Die Auschwitzlüge bleibt auch weiterhin verboten – bei uns; nur leider fallen die widerlichen Pamphlete des Neonazis Ernst Zündel in den USA unter das verfassungsmäßig verbriefte Recht der Meinungsfreiheit, und von dort aus gehen Hetzschriften ins Internet. Eine Indizierung dieser Seiten kann aber nichts ausrichten. Wenn man also Sorge hat ums Bewußtsein anderer Leute, Sorge etwa, daß unsere Jugend anfällig sein könnte für diese Thesen, dann hieße das nichts Gutes für unser Bildungswesen, dann hätten sozusagen unsere Lehrer versagt. Anders gesagt: man muß schon wissen, wogegen man ist und vor allem warum! Wer hat die besseren Argumente?

Die Freiheit des Wortes aushalten! – lautet denn auch eine der vielen Botschaften der Netze. Wie schnell demokratische Prinzipien angesichts eines neuen Mediums, welches für viele noch immer ein Gerücht ist, ins Wanken geraten, ist schon erstaunlich. ■

Anzeige

Komitee für Grundrechte und Demokratie

Auf Anfragen senden wir Ihnen gerne nähere Informationen zur Komiteearbeit, unsere Publikationsliste sowie Hinweise zur Möglichkeit der Fördermitgliedschaft.

Komitee für Grundrechte und Demokratie
Bismarckstr. 40, 50672 Köln bzw.
An der Gasse 1, 64759 Sensbachtal
Postbank Frankfurt, Kto. 39 1881-600, BLZ 500 100 60

Die Gefährdung der Grund- und Menschenrechte hat viele Dimensionen.

Einige Schwerpunkte unserer derzeitigen Arbeit seien herausgegriffen:

- Demonstrationsbeobachtungen z.B. bei den Castor-Transporten ins Wendland
- FREIe HEIDe als Beispiel des Widerstands gegen die out-of-area- Politik
- Flucht und Migration
- Soziale Bürger- und Menschenrechte
- Strafrechtsfragen und Gefangenenhilfe
- neue Informationstechnologien
- Bioethik-Konvention
- humanitäre und friedenspolitische Hilfe im ehemaligen Jugoslawien

Jürgen Ditz Schroer

Was läuft hier eigentlich ab?

Philosophische Denkanstöße

Das Arbeitsumfeld für MitarbeiterInnen und Unternehmen im 21. Jahrhundert: „Inventing the Organisations of the 21st Century".[1]

Der Prozeß: Wir wollen Kenntnisse erwerben, mit denen wir begreifen können, was abläuft, um zu verstehen, was wir selbst tun. Es genügt nicht, die Welt zu verändern. Das tun wir ohnehin. Und weitgehend geschieht das sogar ohne unser Zutun. Wir haben diese Veränderungen auch zu interpretieren. Und zwar, um diese zu verändern. Damit sich die Welt nicht weiter ohne uns verändert. Und nicht schließlich in eine Welt ohne uns.

Der Betriebsrat, seine Rolle, seine inneren Umbrüche!

Warum arbeitet eine Person, die an der Spitze eines Unternehmens steht, mit vollem persönlichen und zeitlichem Einsatz – wo ihr doch niemand befehlen und sie autonom und selbstbestimmt entscheiden kann? Auf der Antwort zu dieser Frage fußen neue Unternehmensstrategien, die Beschäftigte als „unselbständige" zu Höchstleistungen bewegen.

Begreifen, was geschieht

Bislang war in der traditionellen Siemens-Nixdorf (SNI)-Unternehmensorganisation die Lage der Beschäftigten durch einen Mangel an Autonomie gekennzeichnet. Mit „Autonomie" ist dabei das Gegenteil einer Unterordnung unter einen fremden Willen gemeint: „tun, was man selbst will". Wenn man eine Menge autonom handelnder Menschen aus der Perspektive eines SNI-Unternehmerzwecks betrachtet, erscheinen sie nur als ein unorganisierter Haufen. Erst in dem Maße, indem die einzelnen auf ihre Autonomie verzichten, verwandelt sich diese Ansammlung von SNI-Beschäftigten in eine Organisation und damit in ein Unternehmen, das geführt werden kann. Die Organisation, die durch diesen Autonomieverzicht der Organisierten entstanden ist, hat die Form eines Kommandosystems, das auf der Basis von Zwang funktioniert.

Reden allein genügt nicht!

Die Grundlage von Befehl und Gehorsam ist die Angst vor Sanktionen. Darum ist Gehorchen nicht angenehm. Aber auch Befehlen ist nicht leicht. Einer muß die Tätigkeit von vielen steuern, und er muß gleichzeitig die Disziplin aufrechterhalten. Bei einer zunehmenden Anzahl von Untergebenen wächst ihm die Sache bald über den Kopf (disziplinarische Aufgaben wandeln sich).
Das Kommandosystem (des Vorgesetzten und seine Rolle in der Hierarchie) befreit sich aus dieser Verlegenheit, indem es eine spezielle Eigenschaft von Befehl und Gehorsam ausnutzt: SNI-ArbeitnehmerInnen, die gehorchen können, kann man das Befehlen befehlen. Dabei delegiert der Befehlende einen Teil seiner Befehlsgewalt per Befehl an Untergebene – das heißt, der Unternehmer delegiert Unternehmerfunktionen an abhängig Beschäftigte, und diese Untergebenen haben nun den Auftrag, Anweisungen zu geben. Sie gehorchen also genau dadurch, daß sie selbst (gegenüber anderen) Befehle z. B. in der Gruppen- und Projektarbeit erteilen; sie befehlen gehorchend. Durch den sogenannten Vorgesetzten verwandelt sich die einfache Gegenüberstellung von Befehlenden und Gehorchenden in eine ausdehnungsfähige Hierarchie von Befehlsgewalten.

Autonomie als Auftrag:

In der Hierarchie steht nun aber die Autonomie ihrem Gegenteil nicht mehr bloß gegenüber, sondern sie wird von ihm vereinnahmt. Die Form, die diese Vereinnahmung möglich macht, ist der eingeräumte Handlungs- und Entscheidungsspielraum. Seine Grenzen sind fremdbestimmt, aber innerhalb dieser Grenzen muß der Untergebene (der abhängige SNI-Beschäftigte) autonom entscheiden. Diese seine Autonomie gehört zu seinem Auftrag, und wenn er sie nicht im Sinne seines Auftrages benutzt, verschwindet sein Spielraum wieder, wie er gekommen ist; auf fremdbestimmten Wegen. Diese Art von fremdbestimmter Selbstbestimmung oder heteronom bedingter Autonomie dient dem Kommandosystem als universelles Schmiermittel, mit dem es sich immer dann weiterhilft, wenn es sich selbst im Weg steht. Dabei sind vor allem zwei Fälle von Bedeutung:

Erstens macht Gehorchen keinen Spaß; die mangelnde Motivation wird, wie wir gesehen haben, durch Zwang ersetzt, aber Zwang ist etwas anderes als Schwung. Zweitens kommt ein Kommandierender in Schwierigkeiten, wenn er darauf angewiesen ist, daß seinem Befehlsempfänger eine gute Idee einfällt oder eine Lösung für ein neuartiges und unerwartetes Problem.

Beide Male antwortet das Kommandosystem mit der Einräumung von Spielräumen. Dabei macht es Politik mit seiner eigenen Widersprüchlichkeit. Es ist den Menschen

1. Der Text ist eine Zusammenfassung aus Veröffentlichungen des Philosophen Dr. Klaus Peter in der Zeitschrift Mitbestimmung, Gedanken von Stefan Siemens und Wilfried Glismann zu „Business Reengineering, Culture Change" und Ergebnissen aus dem IG Metall Arbeitskreis: Status der ArbeitnehmerInnen im 21. Jahrhundert: Barbara Albrecht, Thomas Grashoff, Erich Jonas, Jürgen Laimer, Otto Müller, Jürgen Ditz Schroer, Franz Tolle und Martin Weis. Ansprechperson: Jürgen Ditz Schroer, SNI Betriebsrat Mch P, Telefon: 089/636 48967, Telefax: 089/636 44843, Internet:
100613.660@compuserve.com oder
jugen.schroer@s11.mch1.x400.sni.de

bekanntlich etwas wert, wenn sie sich zueinander verhalten, als ob das Verhältnis von Befehl und Gehorsam gar nicht da wäre. Um in den Genuß dieses Vorteils zu kommen, antizipieren die Weisungsgebundenen im eingeräumten Spielraum „freiwillig" die Absichten der Weisungsbefugten. Sie verinnerlichen die befehlende Instanz und können dadurch ein Gefühl von Selbständigkeit entwickeln, das sich, weil es angenehm und sogar schmeichelhaft ist, bis zu der Selbsttäuschung steigern kann, daß sie gar nicht in einem Kommandosystem arbeiten. Mit dieser Selbsttäuschung der Beschäftigten erreicht das Kommandosystem den Punkt seiner höchsten Perfektion.

Mehr Druck – weniger Zwang:

Bis hierher haben wir es mit der Form zu tun, in der die alte Unternehmensorganisation autonomes und selbständiges Handeln von abhängig Beschäftigten zuläßt (und fordert). Menschen, die unter solchen Bedingungen arbeiten, fällt es besonders schwer, das Neue an den neuen Managementformen zu erkennen. Sie gewinnen sehr leicht den Eindruck, daß es bei der gegenwärtigen Reorganisation in der SNI nur um einen weiteren Ausbau ihrer Spielräume geht – daß sich also die neuen Formen (die Zeit mit Schulmeyer) von den alten Formen (die Zeit vor Schulmeyer) nur graduell unterscheiden. Aber das ist falsch.

Mit Handlungs- und Entscheidungsspielräumen wird das Kommandosystem perfektioniert (der Machtzuwachs in der Zentrale war noch nie so groß wie in der Zeit mit Schulmeyer), aber die neuen Managementformen wollen es abschaffen und ersetzen. Ist das überhaupt möglich? Die Erfahrung im Kommandosystem zeigt ja, daß die Menschen sich nicht mehr anstrengen, wenn der Zwang fehlt – oder nur noch so anstrengen, wie sie sich heute schon beim Spielen anstrengen, aus Spaß an der Sache. Nun sind in der Tat einige Optimisten der Meinung, daß die Arbeit in Zukunft immer mehr Spaß machen werde, aber pessimistischere Gemüter können eine solche Tendenz selten oder gar nicht erkennen und schließen daraus, daß eine Alternative zum Kommandosystem unrealistisch sei. Ich möchte mich zwischen diese beiden Stühle setzen.

Die Logik des Kommadosystems führte beide – „Optimisten" wie „Pessimisten" – dazu, den Abbau von Zwang und Kommando ganz selbstverständlich als eine Entlastung der bei SNI abhängig Beschäftigten zu verstehen. Mir scheint es aber im Gegenteil um eine neuartige Steigerung ihrer Belastung zu gehen, nämlich um eine Erhöhung des Leistungsdruckes über dasjenige Maß hinaus, das mit Befehl und Gehorsam erreicht werden kann. Es handelt sich um das paradox klingende Programm, den Druck auf die Beschäftigten zu erhöhen, indem man den Zwang, dem sie ausgesetzt sind – wegnimmt.

Ein Mechanismus der Vereinzelung der Menschen

In dieser Situation wird es deutlich: Die Individuen stehen in der Dynamik als individuelle Anbieter ihres Skills, und diese Dynamik ist ein Mechanismus der Vereinzelung dieser Menschen, sie macht die Menschen in dieser Einheit zu Konkurrenten. Hoffnungsvoll sagt sich jeder: „Wer gut ist, der hat kein Problem." In diesem Satz bedeutet „gut sein" dieses:

- einen aktuellen Skill mit hohem Marktwert besitzen
- einen hohen Leistungsbeitrag erbringen
- unverzichtbar sein für den Unternehmenszweck der Einheit.

Die Dynamik trennt somit die Menschen (vor allem in krisenhaften Situationen): in „Unverzichtbare" und „Verzichtbare", in „Starke" und „Schwache" (z.B. Leistungsschwache). Wer zweifelsfrei zu den „Unverzichtbaren" gehört, der hat (vorläufig!) kein Problem. Die „Schwachen" und „Verzichtbaren" spüren die Bedrohung, und die Menschen „dazwischen" wollen natürlich nach Möglichkeit zu den „Starken" gezählt werden.

Um nicht mißverstanden zu werden: Trotz dieser Einschätzung bin ich der Meinung, daß man den Abbau von Kommandostrukturen unbedingt begrüßen muß – aber nicht, wie die Optimisten meinen, weil sich daraus eine Humanisierung der Arbeit bei SNI ergibt, sondern obwohl eher das Gegenteil der Fall ist. Aber wie sieht dieses Gegenteil aus?

Wenn man die Logik des Kommandosystems durchbrechen will, braucht man nicht lange zu suchen. Man muß sich dazu nur diejenige Position einer Befehlshierarchie näher anschauen, die selbst keinem Kommando unterworfen ist: die Spitze (leitende Angestellte, der Vorstand). Hier – und nicht bei Spaß und Spiel – finden die neuen Organisationsformen ihr Leitbild.

Wenn es richtig wäre, daß die Menschen weniger arbeiten, sobald von anderen kein Zwang auf sie ausgeübt wurde, dann dürfte es den selbständigen Unternehmer nicht geben, der ein neues Unternehmen gründet und aufbaut.

Niemand zwingt ihn! Und doch arbeitet er, wenn nötig, bis zum Umfallen – hochmotiviert und engagiert.

Diese Kombination von Freiwilligkeit und Anstrengung bis an die eigenen Grenzen (und darüber hinaus) ist es, die unsere SNI-Vorstände, Managementtheoretiker und Unternehmensberater nervös macht. Die Preisfrage heißt: Wie läßt sich dieses Phänomen bei den bei SNI abhängig Beschäftigten reproduzieren und zum Hauptmotor der Produktivitätssteigerung bei SNI machen?

Der „Gegenpart" ist nicht mehr der Kapitalist, sondern der Kapitalismus! Daraus folgt: Für die Arbeitenden gibt es nur noch „Sachzwänge":

„Macht was ihr wollt ..." ... dieses neue Prinzip setzt die Arbeitenden (auf dem doing-level) in eine neue und verwirrende Situation: Der Zwang ist weg, sie selbst sollen handeln (und erfolgreich am Markt sein). Verantwortlich für den Erfolg am Markt sind jetzt sie selbst – und niemand sonst.

„... aber ihr müßt profitabel sein!" Diese zweite Seite gehört untrennbar dazu, z.B. so: „Eine Einheit, die zwei Jahre hintereinander rote Zahlen schreibt, wird zugemacht!" Das ist jetzt das Problem der Arbeitenden auf dem doing-level (also nicht mehr das Problem des Unternehmers!).

Autonomie und Fremdbestimmung:

Die Antwort ist – wieder einmal – paradox. So wie das Kommandosystem aus Gehorchenden Befehlende gemacht hat – aber gehorchende Befehlende –, so zielen die neuen Organisationsformen auf eine Verwandlung von Unselbständigen in Selbständige ab – allerdings in unselbständige Selbständige. Um diese neue Figur verstehen zu können, müssen wir noch einmal einen Blick auf das Verhältnis von Autonomie und Fremdbestimmung werfen.

Der oberste Chef der SNI-Kommandohierachie ist autonom, er muß sich nicht nach anderen richten, sondern kann tun, was er selbst will (was mag dazu v. Pierer sagen?). Nun kann man mit einer leichten Akzentverschiebung nachfragen: Heißt das denn auch, daß er tun kann, was er will? Wohl nicht. Es gibt auch an der Spitze der Hierarchie eine Art von Fremdbestimmung, die sich allerdings von der Fremdbestimmung innerhalb der Hierarchie unterscheidet. Das Verständnis der Fremdbestimmtheit des Unternehmers ist der Schlüssel zum Verständnis der neuen Managementformen. Worin besteht sie?

Der Unternehmer muß zwar niemandem gehorchen, aber er ist, wie man so sagt, „Sachzwängen" ausgesetzt. Eine irreführende Redeweise! Eine Sache zwingt niemanden, weil sie von niemandem etwas will. Umgekehrt: Der Unternehmer will etwas von ihr, und das verlangt allerdings ein sachgemäßes Tun seinerseits, nämlich ein Tun, das sich nach den in der Sache liegenden Gesetzmäßigkeiten und Notwendigkeiten richtet. Und das ist etwas anderes als die Unterordnung unter einen Zwang.

Niederlage statt Strafe:

Nehmen wir zum Beispiel das Verhältnis des Unternehmers zum Markt. Der Markt wird zwar von Menschen gemacht und ist überhaupt nichts anderes als eine Form des wechselseitigen Verhaltens von Menschen zueinander, aber trotzdem kann er vom Unternehmer nicht so beherrscht und kontrolliert werden wie die Abteilung eines kommandomäßig organisierten Unternehmens. Der Markt hört nicht auf Kommandos. Er entwickelt sich den Menschen gegenüber – und jetzt fällt das entscheidende Wort – autonom.

Damit haben wir nun den Begriff der Autonomie in einer völlig neuen Gestalt vor uns. Er hat die Fronten gewechselt und bedeutet ungefähr das Gegenteil von dem, was vorher damit gemeint war. Wenn er vorher auf die Selbstbestimmung von Individuen zielte, zielt er jetzt auf die Eigendynamik der Bedingungen, die die Individuen in ihrem Verhalten bestimmen, ob sie es wollen oder nicht – also auf ihre Fremdbestimmtheit. Der Unternehmer ist Gegenstück und Resultat der Autonomie der gesellschaftlichen Zusammenhänge, der Gesetze der Kapitalverwertung, des Marktes usw. ihm gegenüber.

Und daraus ergibt sich die Auflösung der Paradoxie: Weil die Autonomie des Unternehmers bereits mit dieser Art von Fremdbestimmung verbunden ist, kann sie ohne Aufhebung der Macht- und Eigentumsverhältnisse auf das Innenverhältnis eines Unternehmens übertragen werden. Die Abhängigkeitsform des Kommandosystems wird dabei nicht ersatzlos gestrichen, sondern sie wird in diejenige Form der Abhängigkeit verwandelt, in der sich der Unternehmer gegenüber den ökonomischen Rahmenbedingungen seines Handelns befindet. Zu diesem Zweck werden die Anweisungs- und Kontrollverhältnisse zwischen den Mitarbeitern der SNI durch marktförmige Verhältnisse ersetzt, die aus Vorgesetzten und Untergebenen Konkurrenten am Markt – innerhalb und außerhalb der SNI – machen, und an die Stelle der Strafe tritt der „eigene" unternehmerische Mißerfolg, die Niederlage in der Konkurrenz.

Vereinzelung und Solidarität

Die alte Vereinzelung: Vereinzelung von Arbeitnehmern ist natürlich nichts neues. Zur Zeit der Erfindung/Entdekkung von Manufakturen und Fabriken waren die (damit zugleich entdeckten und erfundenen) Arbeitnehmer vereinzelt:

- Sie waren individuelle Anbieter ihrer Fähigkeiten
- Sie waren untereinander Konkurrenten um den Arbeitsplatz.

Hinsichtlich der historischen Überwindung der Vereinzelung war folgendes wichtig: Die Arbeitnehmer wurden in der Arbeit vom Unternehmer organisiert (durch Fremd-Organisation [=Kommandosystem] der Arbeit und auch durch die organisierende Wirkung der Maschinerie). Unter dieser Voraussetzung erlebten sich die Arbeitnehmer in Konflikten als gleichermaßen Abhängige (abhängig vom Unternehmer).

Die Erfindung der alten Solidarität

Diese beiden Sachverhalte haben die Erfindung solidarischer Bewegungsformen (z.B. die Erfindung von Gewerkschaften) erleichtert – obwohl das immer noch schwer genug war und viele Jahrzehnte erfordert hat. Die alte Solidarität hatte diese Grundlage – sie war die Solidarität der Abhängigen (abhängig Beschäftigten).

Die neue Vereinzelung

Die neue Vereinzelung erscheint dagegen in einer anderen, paradoxen Gestalt: Die Vereinzelung unter den Menschen eines Unternehmens-Segments geschieht gerade dadurch, daß diese Menschen gemeinsam um das Überleben an ihrem Marktsegment kämpfen. Jeder fordert von jedem seinen Beitrag zu diesem Prozeß und jeder kontrolliert jeden, ob er den Beitrag bringt, ob er „seine Kosten reinbringt". D.h.: Das Gemeinsame der Menschen einer Einheit wird somit ihre Existenz als Konkurrenten untereinander (Konkurrenten um die Möglichkeit der weiteren Teilnahme an diesem Prozeß).

Die neue Solidarität

Die neue Solidarität kann nicht mehr die Solidarität der Abhängigen sein. Denn die Instrumentalisierung der Individuen für den Unternehmenszweck erfolgt nicht mehr durch Abhängigkeit von Weisungen (Abhängigkeit von Menschen), sondern durch eine Form von Selbständigkeit (die in Wahrheit eine Abhängigkeit von Prozessen und Rahmenbedingungen ist). Diese neue Form der Unterord-

nung von Individuen unter den Unternehmenszweck funktioniert mit Hilfe einer Selbsttäuschung der Individuen. Die Durchbrechung dieser Selbsttäuschung (d.h.: die Entwicklung der Individualität der Individuen durch zunehmendes Erlernen einer tatsächlichen Fähigkeit der Selbstbestimmung) wird zur notwendigen Voraussetzung einer neuen Solidarität. Sie kann daher nur eine Solidarität selbständig sein wollender Individuen sein, die begreifen, daß gemeinsame Selbstverständigung und gemeinsames Handeln Voraussetzung dafür sind, daß sie die entscheidende Frage nach dem Unterschied zwischen dem Unternehmenszweck und ihren individuellen Zwecken beantworten können.

Das Ende der Interessenvertretung?

Wenn aus der dargestellten Veränderung für die SNI-Arbeitnehmer eine Steigerung des Leistungsdrucks durch eine Verminderung des Zwangs herauskommt, so geht es für die Unternehmer um einen Zuwachs von Macht durch einen Verzicht auf Kontrolle. Die „autonom" ablaufenden Prozesse in der reorganisierten SNI entziehen sich der direkten Steuerung nach Art des Kommandosystems, aber sie lassen sich indirekt steuern, indem man die Rahmenbedingungen manipuliert, auf die sie dann – autonom – reagieren. Die Rolle des Unternehmers verwandelt sich dabei aus derjenigen eines Kommandanten von Untergebenen in diejenige eines Biotechnikers des „Humankapitals" – ein realer Machtgewinn, der aber nur um den Preis realer Autonomie- und Selbständigkeitsgewinne auf Seiten der einzelnen SNI-Arbeitnehmer und SNI-Arbeitnehmerinnen zu haben ist.

Beschäftigte, Betriebsräte und Gewerkschaft haben damit nicht nur ein Problem völlig neuer Qualität und Größenordnung vor sich, sondern es verändern sich auch – gleichsam hinter ihren Augen – die Voraussetzungen für die Wahrnehmung von Arbeitnehmerinteressen überhaupt.

Die Reorganisation und der Betriebsrat

Der Umbruch in der SNI stellt sich in vielfacher Hinsicht „individuell gebrochen" dar. Weniger denn je sind die MitarbeiterInnen im Betrieb in einer gemeinsamen, allgemeinen Lage, die durch eine allgemeine Lösung (Regelung) des Betriebsrates beantwortet werden kann. Der einzelne Mitarbeiter, die einzelne Mitarbeiterin findet sich in Situationen, in denen er bzw. sie sich gezwungen sieht, für sich selbst individuelle Lösungen und individuelle Strategien zu entwickeln.

Ansätze des Kollektiven

Durch diese faktische Vereinzelung der Individuen in der neuen Organisation bekommen erste, unscheinbare Ansätze des Kollektiven eine ganz neue Bedeutung: Das Reden der Individuen miteinander darüber, wie sie die Situation sehen. Das Reden über ihre individuellen Strategien (und ihr Umgehen mit den Dilemmata), und (auf der Grundlage dieser wechselseitigen Verständigung und Reflexionen) das Erkennen von vorteilhaften Rahmenbedingungen für die Individuen, die dann durch den Betriebsrat durch betriebliche Regelungen vereinbart werden können.

In unser Arbeit als Betriebsrat müssen wir die große Bedeutung von „Selbstverständigungsgesprächen mit dem Perlacher Gespräch" erkennen.

Solidarität (wie wir sie bisher kannten) wird in der neuen Organisation der Arbeit zum Problem. Die Phänomene „Vereinzelung" und „Entsolidarisierung" haben in den neuen Prozessen eine objektive Grundlage. Eine „neue Solidarität" wird nicht von selbst entstehen.

Wie könnte das Neue gestaltet werden?

Es kommt darauf an, hilfreiche Rahmenbedingungen zu erarbeiten: Wie kann verhindert werden, daß die MitarbeiterInnen alles Risiko aufgebürdet bekommen? Wie können sie sich über diese Dynamik selbst verständigen und von sich her Grenzen ziehen? Wie müssen Vereinbarungen aussehen, auf die sich MitarbeiterInnen aus solchen Teams berufen können, wenn sie ihre Interessen durchsetzen wollen?

Dies erfordert aber, das neue Phänomen tief zu verstehen. Gemeinsam mit den Kollegen und Kolleginnen, die in solchen Arbeitsformen stehen, müssen wir als Betriebsrat versuchen, diese neue Dynamik zu begreifen.

Eins ist klar:

Gegen die negativen Folgen der neuen Managementformen kann man sich weder mit einer Verteidigung des alten Kommandosystems wehren noch mit Kampfformen, die speziell auf das Kommandosystem zugeschnitten waren.

In Zukunft wird alles davon abhängen, wieweit es gelingt, aus der zunehmenden individuellen Autonomie und Selbständigkeit der SNI-Beschäftigten am Arbeitsplatz Energien für die Entwicklung von Gegenmacht zu gewinnen. ■

Literatur

Günther Anders: Die Antiquiertheit des Menschen. 1. Band: Über die Seele im Zeitalter der zweiten industriellen Revolution. 2. Band: Über die Zerstörung des Lebens im Zeitalter der dritten industriellen Revolution. Verlag C.H.Beck

Humberto Maturana; Franciso Varela: Der Baum der Erkenntnis. Verlag Scherz

Hans Jonas: Erkenntnis und Verantwortung. ders.: Was für morgen lebenswichtig ist. ders.: Das Prinzip Verantwortung. Insel Verlag

Hermann Haken: Erfolgsgeheimnisse der Wahrnehmung, Verlag DVA

Fritjof Capra: Wendezeit. ders.: Das Tao der Physik. ders.: Lebensnetz. Verlag Scherz

Dietrich Dörner: Die Logik des Mißlingens.

Jiddu Krihnamurth; David Bohm: Vom Werden zum Sein. Verlag Barth

William Bridges: Ich & Co. Wie man sich auf dem neuen Arbeitsmarkt behauptet. Hoffmann und Campe Verlag

Ralf Reichwald: Die grenzenlose Unternehmung. Informationen, Organisationen ... Gabler Verlag

Große-Oetringhaus: Strategische Identität, Springer

Else Fricke: Betrieblicher Wandel und Autonomie von Ingenieuren, Heft 14, Friedrich Ebert Stiftung

Martin Schumann:Die Globalisierungsfalle. Rowolt

Leo Nefiodow: Der sechste Kondratieff. Rhein-Sieg Verlag

Wigang Picot: Die grenzenlose Unternehmung. Verlag Gabler

Christian Lutz: Leben und Arbeiten in der Zukunft. Edition Seminat Langen Müller Herbig Verlag

Hans-Joachim Schadeldoth: Zukunft ohne Arbeit? Neue Wege aus der Strukturkrise, Knaur Verlag

Peter M.Senge: Die fünfte Disziplin, Klett-Cotta

Lester C.Thurow: Die Zukunft des Kapitalismus, Verlag Metropolitan

Thea Bauriedl: Leben in Beziehungen. Von der Notwendigkeit, Grenzen zu finden

Jeremy Rifkin: Das Ende der Arbeit und ihre Zukunft. Campus Verlag

Schwerpunkt:

»Datenspuren Datenschatten«

Die Autorinnen und Autoren:

Ute Bernhardt ist Geschäftsführerin und stellvertretende Vorsitzende des FIFF.

Nicholas Busch ist Jurist und Publizist. Er gibt die Zeitschrift „Fortress Europe?" – Circular Letter mit den Themenschwerpunkten Justiz/Innenpolitik/Polizei/Einwanderung in Europa heraus.

Marit Köhntopp ist wissenschaftliche Mitarbeiterin beim Landesbeauftragten für den Datenschutz Schleswig-Holstein im Bereich „Neue Medien und Informationstechnologien".

Jan Mönikes ist wissenschaftlicher Mitarbeiter bei SPD-MdB Jörg Tauss.

Werner Moritz ist wissenschaftlicher Mitarbeiter beim Landesbeauftragen für den Datenschutz der Freien Hansestadt Bremen sowie Mitglied des FIfF-Vorstands.

Alexander Roßnagel ist Professor für Rechtswissenschaft an der Universität Kassel und Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" an der Universität Darmstadt sowie Mitglied des FIfF-Beirats.

Ingo Ruhmann ist wissenschaftlicher Mitarbeiter des forschungs- und postpolitischen Sprechers von Bündnis90/Die Grünen im Bundestag Dr. Manuel Kiper sowie Mitglied des FIFF-Vorstands.

Peter Schaar ist stellvertretender Landesbeauftragter für den Datenschutz der Freien und Hansestadt Hamburg.

Thilo Weichert ist stellvertretender Landesbeauftragter für den Datenschutz in Niedersachsen und Vorsitzender der Deutschen Vereinigung für den Datenschutz e.V.

Verantwortlich für diesen Schwerpunkt sind:

Ute Bernhardt und Ingo Ruhmann.

Thilo Weichert

Die Novellierungsvorschläge zum BDSG – ein gewaltiger Flop!

Am 24. Oktober 1995 wurde die „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" von den Präsidenten des Europäischen Parlamentes und des Rates unterzeichnet.[1] Diese unter dem kürzeren Namen „EU-Datenschutzrichtlinie" (EU-DSRL) diskutierte europäische Vorgabe muß jetzt von den nationalen Gesetzgebern umgesetzt werden. Damit kommt auch das Bundesdatenschutzgesetz (BDSG) von 1990 wieder auf den politischen Prüfstand. Innerhalb von drei Jahren, also bis zum Oktober 1998, muß das BDSG an die EU-DSRL angepaßt sein. Die Datenschutzbeauftragten des Bundes und der Länder (BDSG-Konferenz) setzten sich zusammen und formulierten für das federführende Bundesministerium des Innern (BMI) einen Katalog von notwendigen BDSG-Änderungen.[2] Ähnliche Empfehlungen gab auch der „Düsseldorfer Kreis" ab, in dem die obersten Aufsichtsbehörden für den Datenschutz im privaten Bereich, also vor allem die Landesinnenministerien, zusammengeschlossen sind. Die Datenschutzkontrolleure gingen davon aus, daß anläßlich der Anpassung an die EU-DSRL das BDSG umfassend überarbeitet werden muß. Das BDSG entspricht nicht mehr dem Stand der technischen und wirtschaftlichen Entwicklung. Der Vernetzungsgrad von Personalcomputern, insbesondere über das Internet, der Einsatz von modernen Überwachungstechniken (z.B. Video) und die Nutzung von neuen Speicher- und Übermittlungsmedien (z.B. CD-ROM oder Chipkarten) machten das BDSG, das noch von der Großrechnertechnologie der 70er Jahre geprägt ist, überarbeitungsbedürftig.

Tatsächlich machte sich das BMI auch alsbald an die Arbeit und führte allerlei Gespräche. Die Auswahl der Gesprächspartner vor allem aus der Wirtschaft ließ schon wenig Gutes erahnen. Diese Ahnungen wurden bestärkt durch vereinzelte Äußerungen aus dem BMI, aus denen hervorging, daß eine Minimalnovellierung angestrebt werde: nicht das, was technisch nötig ist, sondern nur das, was von der EU-DSRL unbedingt gefordert wird, sollte per Gesetz umgesetzt werden.[3] Waren also die Ziele des BMI nicht allzu hoch gesteckt, so benötigte die Umsetzung doch sehr viel Zeit: erst im Februar 1997 erblickte ein erster Referentenentwurf des BMI das Licht der Öffentlichkeit (Stand 14.1.1997). Was da präsentiert wurde, blieb nicht nur weit hinter den Notwendigkeiten, sondern selbst hinter den aufgrund der Ankündigungen reduzierten Erwartungen zurück.

Bei der Lektüre des Entwurfes kann man den Eindruck haben, als legten die AutorInnen es darauf an, den Text des BDSG so aufzublasen, daß selbst die bzw. der Gutwilligste nicht mehr durchsteigt. Die derzeitig schon komplizierte Struktur des BDSG wird durch noch mehr Komplexität und Text, hinter dem aber wenig Regelungsinhalt steckt, noch komplizierter gemacht. Statt überflüssige Regelungen aus dem Gesetz zu werfen, werden neue aufgenommen. Beispiel: Obwohl die EU-DSRL ebenso wie die meisten Landesdatenschutzgesetze (LDSG) einen umfassenden Verarbeitungsbegriff verwenden, differenziert § 3 Abs. 4-6 BDSG-E weiterhin zwischen „Verarbeiten", „Erheben" und „Nutzen". Die Datenübermittlung in sog. Drittländer ist in Art. 25 f. EU-DSRL schon unübersichtlich genug geregelt. Dieser Kompliziertheit wird in den §§ 4b f. BDSG-E noch eins draufgesetzt.

Art. 2 c) EU-DSRL definiert „Datei" als „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind". Damit wird auch die Datenverarbeitung in konventionellen Akten, soweit diese nach bestimmten Kriterien strukturiert sind, erfaßt. Diese Vorgabe meinte das BMI nicht umsetzen zu müssen. Nach § 3 Abs. 2 S. 2 BDSG-E werden nur Sammlungen erfaßt, die gleichartig aufgebaut sind und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden können. Die Konsequenzen sind fatal: Soweit Banken, Versicherungen, Arbeitgeber oder auch so problematische Stellen wie „Scientology" Daten in Personalakten führen, unterfallen sie, entgegen den Vorgaben der EU-DSRL, auch weiterhin nicht dem Datenschutz. Entgegen dem eindeutigen Erwägungsgrund Nr. 14 der EU-DSRL bleibt § 3 Abs. 3 Satz 1 2. HS dabei: Bild- und Tonträger sind Akten. Es drängt sich der Eindruck auf, daß die Damen und Herren vom BMI von Technik keine Ahnung haben. Schon heute ist trotz der BDSG-Regelung unbestritten, daß auswertbare digitale Bild- und Tonaufzeichnungen den Dateibegriff erfüllen.

Für die Presse und sonstige Meinungsmedien erlaubt Art. 9 EU-DSRL nur Privilegierungen insoweit, als dies sich im Rahmen einer Abwägung mit dem Recht auf Privatsphäre als notwendig erweist. Der bisher völlig verunglückte § 41 BDSG, dessen Wortlaut z.B. Adressen-, Telefon- und Branchenverzeichnisse zur Presse rechnet, wird nicht nach den Vorgaben der Richtlinie neu gefaßt. Dies wäre im übrigen nichts anderes als eine Umsetzung deutschen Verfassungsrechts. Vielmehr meint das BMI, mit redaktionellen

1. Amtsblatt EG v. 23.11.1995, L 281, 31 ff.
2. DSB-Konferenz, Beschluß v. 14./15.3.1996, abgedruckt in: XIII. TB LfD Nds. 1995/96, 201 ff.; vgl. auch Dammann, DSB 10/1996, 1 ff.
3. Weber, CR 1995, 297 ff.; Werthebach, RDV 1997, 1 ff.

Änderungen und der Klarstellung, daß auch die „Deutsche Welle" das Presseprivileg genießt, auszukommen.

Art. 8 EU-DSRL zwingt zu erhöhten materiellen Anforderungen bei der Verarbeitung besonders schutzwürdiger Daten, z.B. über rassische und ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, über Gesundheit und Sexualleben. Statt nun diese Regelung mit der über Berufs- und Amtsgeheimnisse (§ 39 BDSG) abzustimmen und insofern auszuweiten, scheint das BMI die europäische Vorgabe völlig übersehen zu haben. Aber nein! Private Stellen werden in § 28 Abs. 2 S. 2 BDSG-E bei solchen Daten einer verschärften Abwägungspflicht unterworfen. Für öffentliche Stellen soll es auch künftig keine sensiblen Daten geben.

Die DSB-Konferenz forderte wegen der Gefahr unkontrollierbarer Überwachung eine ausdrückliche Regelung zur Videoüberwachung. Im BDSG-E ist davon nichts zu finden. Sie forderte eine Regelung zu Chipkarten, um die datenschutzrechtliche Verantwortung der Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen. Wieder Fehlanzeige. Die Datenschutzbeauftragten forderten eine Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing. Selbst die Wirtschaft signalisierte hier die Bereitschaft, den Anforderungen der Datenschutzpraxis entgegenzukommen, z.B. durch die Verbindlicherklärung der Robinsonliste oder durch Erhöhung der Transparenz über Herkunft und Selektion von Daten. Im Entwurf erneut totaler Ausfall. Selbst die Kleinigkeit, Listbroker als mögliche Widerspruchsadressaten zu benennen, verkneift sich der Entwurf.

In einem einzigen Punkt versucht das BMI über die EU-DSRL hinauszugehen: bei der Zulassung elektronischer oder gedruckter Adreß-, Telefon- und Branchenverzeichnisse. Diese Regelung erfolgte aber nicht freiwillig; sie wurde durch Änderungen im Telekommunikationsrecht erzwungen. Statt aber nun eine praktikable und vor allem an die sonstigen BDSG-Regelungen angepaßte Norm zu schaffen, beschränkt sich § 29 Abs. 3 BDSG-E mit der Zulassung von solchen Verzeichnissen, Kennzeichnungen müßten übernommen werden. Und wieder gibt es Wasser statt Wein: Folgeregelungen (§§ 29 Abs. 2, 33 BDSG) hat das BMI offensichtlich übersehen. Noch schlimmer: Die Regelung ist so gefaßt, daß über eine Datenwaschstation, d.h. eine rechtlich nicht ganz korrekte Zwischenpublikation, jedes veröffentlichte Verzeichnis mit Personendaten elektronisch multifunktional auswertbar veröffentlicht werden kann.

Bezüglich der Technik hat sich in Sachen Datenschutz in den letzten sieben Jahren am meisten geändert. Genau in diesem Bereich meint das BMI überhaupt nichts ändern zu müssen. Es tut so, als lebten wir nicht in einer Zeit weltweit, z.B. über Internet vernetzter Personalcomputer und Rechner mit den vielfältigsten Möglichkeiten von Datenattacken. Die Erkenntnis, daß die Lizenzierung von Verfahren über ein Datenschutz-Audit einen höheren Sicherheitsstandard schaffen kann, ist wohl von den für die Multimedia-Gesetzgebung verantwortlichen Ministerien für Wirtschaft und für Forschung nicht bis zum BMI gedrungen. Verschlüsselung, Quittierungspflicht, Datensparsamkeit ... all dies sind Instrumente, von denen das BMI fahrlässigerweise bisher unbeleckt geblieben ist.

Tatsächlich gibt es nicht nur allgemeine Vorschläge der Datenschutzbeauftragten. Es liegen auch schon vorformulierte Vorschläge zu Einzelregelungen und umfassende Verbesserungsvorschläge vor, z.B. von der Deutschen Vereinigung für Datenschutz (DVD) in Bonn.[4] Darin werden noch weitere drängende Probleme geregelt, auf die das BDSG – anders als manche Landesdatenschutzgesetze – keine Antwort gibt: Klärung des Begriffs der Einwilligung, Regelung der externen Wartung, Durchführung eines Verfahrens der Technikfolgenabschätzung mit Einbeziehung von gemeinnützigen Verbänden wie z.B. FIfF oder DVD, Erprobungsklausel, Verbesserung der Kontrollstruktur und der Kontrollkompetenzen, materielle Einschränkung und verfahrensrechtliche Erleichterung bei der Verfolgung von Datenschutzverstößen.

Der Entwurf kapituliert offensichtlich vor den wirtschaftlichen Interessenverbänden und vor der Komplexität der Informationstechnik. Dies ist ein Armutszeugnis in einem Land, das nicht nur bei der Informationstechnik, sondern auch beim Grundrechtsschutz Spitze sein möchte. Es ist geplant, daß das Bundeskabinett im Schnellverfahren schon im Juni 1997 über den BMI-Referentenentwurf entscheidet. Dies muß verhindert werden. Würde dieser Entwurf, auch mit kleinen Änderungen, Gesetz, so würde der Datenschutz schon mittelfristig zum bürgerrechtlichen Akzeptanztrottel einer ungehemmten Expansion der Informationstechnik verkommen. Die dringende Modernisierung des Datenschutzrechtes würde auf den Sankt-Nimmerleinstag verschoben. Der Referentenentwurf muß zurückgezogen werden. Im Dialog mit den Datenschutzbeauftragten, der Wissenschaft und der (Fach-) Öffentlichkeit muß ein zweiter Versuch gestartet werden. Dieser Dialog muß öffentlich geführt werden und nicht, wie bisher, mit der Wirtschaftslobby hinter verschlossenen Ministeriumstüren. Die Deutsche Vereinigung für den Datenschutz, als besonders inhaltlich betroffene Organisation, steht für diesen Dialog bereit.[5]

4. Datenschutznachrichten (DANA) 1/1997, 4 ff., 7 ff.
5. DVD, Presseerklärung vom 10.4.1997: Novellierung des Datenschutzgesetzes? Klassenziel verfehlt!

Peter Schaar

Tele- und Mediendiensterecht

Neue Maßstäbe für die Verarbeitung personenbezogener Daten im Internet

Nach dem „Gesetzgebungsfahrplan" des Bundes und der Länder werden im August wesentliche Rechtsänderungen im Bereich des Mediendienste- und Teledienstesrechtes in Kraft treten. Sowohl das Informations- und Kommunikationsdienste-Gesetz (IuKDG) des Bundes als auch der Staatsvertrag der Länder über Mediendienste (Mediendienste-Staatsvertrag) haben den Anspruch, bestimmte Aspekte des Internet (aber auch anderer elektronischer Dienste) zu regulieren. Nur kurz erwähnt werden soll in diesem Zusammenhang, daß auch das bereits im letzten Jahr in Kraft getretene Telekommunikationsgesetz (TKG) diejenigen Dienste im Internet berührt, die als „Telekommunikationsdienstleistungen" anzusehen sind; hierzu gehört insbesondere die reine Übertragungs- und Vermittlungsfunktion.

Abgrenzung von Tele- und Mediendiensten

Gemäß § 2 IuKDG sind **Teledienste** elektronische Informations- und Kommunikationsdienste, die „für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne" bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt; hierzu gehören insbesondere

- Individualkommunikationsdienste (z.B. Telebanking, Datenaustausch),
- Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, z.B. Verkehrs-, Wetter-, Umwelt- und Börsendaten),
- die Nutzung des Internets oder weiterer Netze,
- Telespiele,

Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit.
Nicht ausdrücklich genannt wird e-mail, d.h. der individuelle Austausch elektronischer Briefe. Es ist davon auszugehen, daß dieser Dienst kein Teledienst, sondern ein Telekommunikationsdienst ist, für den das Telekommunikationsrecht Anwendung findet.

- § 2 Abs. 2 Mediendienste-Staatsvertrag definiert **Mediendienste** als „das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten in Text, Ton oder Bild, die unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters verbreitet werden."

Als wesentliches Unterscheidungsmerkmal zwischen Tele- und Mediendiensten ist dementsprechend anzusehen, inwieweit ein Dienst zur Abwicklung einer individuellen Geschäfts- bzw. Kommunikationsbeziehung erbracht wird bzw. ob ein elektronisches Angebot sich an eine mehr oder minder unbestimmte Allgemeinheit wendet, also eine Vielzahl von Nutzern gleichartige Informationen zugestellt bekommen oder diese abrufen können. Prototyp für einen derartigen Mediendienst sind elektronische Zeitschriften.

Klar ist dabei jedoch, daß es im Einzelfall durchaus schwierig bleiben kann, eine eindeutige Zuordnung vorzunehmen. Gerade im World Wide Web ist das Zusammenwachsen von Telekommunikationsdiensten, Tele- und Mediendiensten zu erkennen; ein technisch auf einem Server abgewickeltes Angebot kann insofern allen drei Sphären zugerechnet werden: So können etwa von einer Webseite aus e-mail-Funktionen angeboten werden; es können elektronische Bestellungen über Formulare abgewickelt, Fahrplanhinweise abgerufen oder elektronische Zeitschriften oder Audio-Dateien angeboten werden.

Abweichende rechtliche Vorgaben

Angesichts der technischen Konvergenz von Tele- und Mediendiensten hatten die Autoren der Regelungen ursprünglich angestrebt, die Vorschriften über die Zulässigkeit der Verarbeitung personenbezogener Daten im Mediendienste-Staatsvertrag und im Teledienstedatenschutzgesetz (TDDSG) gleich zu formulieren. Allerdings ist festzustellen, daß bereits der Entwurf des Mediendienste-Staatsvertrages (der inzwischen von allen Länderministerpräsidenten unterzeichnet wurde und damit inhaltlich faktisch abgeschlossen ist) und der Gesetzentwurf der Bundesregierung vom 20.12.1996 für ein TDDSG in einigen Punkten voneinander abweichen:

- § 5 Abs. 3 des Teledienstedatenschutzgesetzes verpflichtet Diensteanbieter dazu, auf Ersuchen Bestandsdaten ihrer Kunden an die für die Verfolgung von Straftaten und Ordnungswidrigkeiten zuständigen Stellen, an die Verfassungsschutzbehörden des Bundes und der Länder, den Bundesnachrichtendienst, den Militärischen Abschirmdienst sowie an das Zollkriminalamt zu übermitteln. Demgegenüber enthält § 14 des Mediendienste-Staatsvertrages eine abschließende Regelung zur Verarbeitung von Bestandsdaten, in der keine derartige Übermittlungsverpflichtung – ja sogar die Übermittlungsbefugnis – an die Sicherheitsbehörden vorgesehen ist. Wenn demnach ein Diensteanbieter Bestandsdaten eines kombinierten Tele- und Mediendienstes an die Sicher-

heitsbehörden übermittelt, würde er sich gemäß § 20 Abs. 1 Nr. 14 des Mediendienste-Staatsvertrages einer Ordnungswidrigkeit schuldig machen.

- § 17 des Mediendienste-Staatsvertrages enthält eine Vorschrift zum Datenschutz-Audit, wonach zur Verbesserung von Datenschutz und Datensicherheit Anbieter ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen können; die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter sollen durch ein besonderes Gesetz geregelt werden. Im Teledienstedatenschutzgesetz des Bundes fehlt eine entsprechende Vorschrift; es ist nicht deutlich, inwieweit die Länder überhaupt eine Regelungskompetenz bezüglich der Ausgestaltung des Datenschutz-Audit für sich beanspruchen können oder ob dies nur ein Bundesgesetz leisten kann.

Schon an diesen beiden Punkten wird deutlich, daß die Rechtsunsicherheiten für die Anbieter von Diensten im Internet mit dem neuen Recht nicht beseitigt werden.

Datenminimierungsgebote

Uneingeschränkt positiv zu bewerten ist, daß sowohl der Mediendienste-Staatsvertrag als auch das Teledienstedatenschutzgesetz den Grundsatz zur Datensparsamkeit enthalten. Die Diensteanbieter haben sich bei der Gestaltung und Auswahl technischer Einrichtungen an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.

Mit dieser Vorgabe wird – anders als im herkömmlichen Datenrecht – die Erforderlichkeitsprüfung verfahrensmäßig vor die technische Systementscheidung verlagert. Kein Anbieter wird sich in Zukunft darauf berufen können, er habe sich zunächst aus rein betriebswirtschaftlichen Gründen für ein bestimmtes System entschieden, in dem nun mal die Verarbeitung bestimmter personenbezogener Daten vorgesehen sei. Er muß der Frage nachgegangen sein, ob es technische Alternativen zu einer personenbezogenen Datenverarbeitung in dem vorgesehenen Umfang gibt. Dieser „Grundsatz der Datenvermeidung" kommt auch darin zum Ausdruck, daß Angebote und ihre Bezahlung dem Nutzer anonym oder unter Pseudonym zu ermöglichen sind, soweit dies technisch möglich und zumutbar ist.

Im Hinblick auf das Internet bedeutet dies, daß die Nutzung bestimmter im Internet angebotener Dienste – soweit dies der Sache nach möglich und vertretbar ist – auch in anonymer Form erfolgen können soll. Den Surfern ist also eine echte Alternative zu einer personenbezogenen Nutzung zu bieten.

Problematisch könnte an dieser Vorschrift sein, daß unter Berufung auf die Anonymität auch Daten unter falschem Namen im Internet in Umlauf gebracht werden, wie dies bereits heute in großem Umfang festzustellen ist. Es ist jedoch nicht Ziel der rechtlichen Vorgaben, diese Praxis zu legitimieren oder zu verstärken. Dementsprechend wird zwischen „Angebot" und „Nutzung" differenziert. Soweit Angebote im Internet veröffentlicht werden sollen, geschieht dies unter voller Verantwortlichkeit der jeweiligen Diensteanbieter. Soweit ein Anbieter nur den technischen Rahmen für die jeweilige Veröffentlichung bietet, hat er gleichwohl sicherzustellen, daß der Urheber einer entsprechenden Information, die z.B. auf einer Webseite verbreitet wird, im Nachhinein ausfindig gemacht werden kann.

Nutzungs- und Abrechnungsdaten

Besonders bedeutsam ist das Gebot zur Datenvermeidung beim Abruf einzelner Angebote. Anbieter dürfen personenbezogene Daten über die Inanspruchnahme von Diensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme zu ermöglichen (Nutzungsdaten) oder abzurechnen (Abrechnungsdaten). Die Nutzungsdaten sind frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen, soweit es sich nicht um Abrechnungsdaten handelt. Die Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind, wobei nutzerbezogene Abrechnungsdaten Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Dienste nicht erkennen lassen dürfen, es sei denn, der Nutzer beantragt eine Einzelabrechnung.

Diese restriktiven Vorgaben haben erhebliche Auswirkungen auf die Datenverarbeitung im Internet. So sehen praktisch sämtliche WWW-Server eine Speicherung von Benutzerdaten entsprechend dem Common Logfile Format (CLF) vor. Danach werden für jeden Abruf von einem WWW-Server die IP-Adresse, ggf. Rechner- und Benutzername, Datum, Uhrzeit und URL (Uniform Ressource Locator) aufgezeichnet. Die so gewonnenen umfangreichen Logdateien (siehe Kasten) werden zum Teil über lange Zeit aufbewahrt und können (nicht nur) für Statistiken genutzt werden. Die aufgezeichneten Daten sind Nutzungsdaten im Sinne des Teledienst- bzw. Mediendiensterechtes.

Die Daten sind auch in vielen Fällen über die IP-Nummer personenbezogen. Personenbezogen ist eine IP-Nummer insbesondere dann, wenn sie einem bestimmten Rechner oder Benutzer fest zugeordnet ist. Auch bei dynamischer Vergabe von IP-Nummern, wie sie bei den meisten großen Internet-Providern praktiziert wird, ist zumindest den Access-Providern eine personenbezogene Zuordnung dieser Nutzungsdaten möglich.

Gegen diese Argumentation ist aus Kreisen von Internet-Anbietern eingewandt worden, daß selbst feste IP-Nummern nicht personenbezogen seien, da sich aus ihnen für Dritte nicht direkt ergebe, welche Person sich dahinter jeweils verberge. Würde man dieser Argumen-

tation folgen, wären jedoch weder Telefon- noch Kontonummern oder Autokennzeichen personenbezogen. In Zusammenhang mit diesen Merkmalen ist die Diskussion jedoch weitgehend beendet; Konto-, Telefon- und Autonummern sind nach herrschender Meinung in der juristischen Literatur und Rechtsprechung als personenbezogene Angaben anzusehen und unterliegen den Datenschutzbestimmungen. Gerade für elektronische Kommunikationsbeziehungen gilt darüber hinaus, daß es eine Vielzahl von Suchprogrammen und Hilfsmitteln gibt, die die Zuordnung einer Information zu einer Person erleichtern.

```
141.91.33.38 - - [21/Jan/1997:16:08:58 -0400] "GET /HMB-DSB/hmbdsb.htm HTTP/1.0"
141.91.33.38 - - [21/Jan/1997:16:09:21 -0400] "GET /HMB-DSB/HMBDSB.htm HTTP/1.0"
141.91.33.38 - - [21/Jan/1997:16:15:11 -0400] "GET /HTTP/1.0"
141.91.33.38 - - [21/Jan/1997:16:15:12 -0400] "GET /images/note.gif HTTP/1.0"
141.91.33.38 - - [21/Jan/1997:16:15:12 -0400] "GET /images/htpdicon.gif HTTP/1.0"
97.20.240.136 - - [13/Feb/1996:19:57:29 -0100] "GET /images/note.gif HTTP/1.0"
97.20.240.136 - - [13/Feb/1996:20:02:17 -0100] "GET /httpd-doc/Legal.htm HTTP/1.0"
97.20.240.136 - - [13/Feb/1996:20:02:40 -0100] "GET /httpd-doc/images/icon.gif HTTP/1.0"
97.20.240.136 - - [13/Fe/1996:20:03:01 -0100] "GET /httpd-doc/images/back.gif HTTP/1.0"
```

Beispiel von Einträgen in einer Logdatei entsprechend dem Common Logfile Format

Mit dem Inkrafttreten der neuen Rechtsvorschriften im Sommer 1997 werden die Betreiber von WWW-Servern schon bei der Speicherung der Daten dafür sorgen müssen, daß die IP-Nummer des Nutzers nicht registriert wird. Offensichtlich hat sich diese Anforderung bei betroffenen Unternehmen noch nicht in genügendem Maße herumgesprochen.

Auch die von einigen Anbietern praktizierte, für den Nutzer verdeckte, Übermittlung von e-mail-Adressen im Zuge des Informationsabrufs wird unter den neuen rechtlichen Vorgaben nicht beizubehalten sein. Gleiches gilt auch für die Übermittlung bestimmter anderer personenbezogener Angaben im Rahmen einer Informationsanforderung durch Eingabe einer URL, durch die es dem Anbieter ermöglicht wird, jeden einzelnen Informationsabruf zu registrieren, sofern dies für das einzelne Angebot nicht erforderlich ist.

Cookies

Das neue Recht orientiert sich an der Maxime größtmöglicher Transparenz, d.h. der Nutzer soll wissen, was mit seinem System und was mit seinen personenbezogenen Daten geschieht, insbesondere welche Daten in welcher Form verarbeitet werden und für welchen Zweck und an welchem Ort diese Verarbeitung vorgenommen werden und wer dafür jeweils verantwortlich ist.

Die in letzter Zeit viel diskutierte Cookie-Problematik ist vor dem Hintergrund des neuen Rechts neu zu betrachten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ermöglichen, ist der Benutzer vor Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muß für den Nutzer jederzeit abrufbar sein.

Danach wäre die Praxis von Anbietern illegal, Cookies oder andere identifizierende Informationen auf einem Client-System ohne Kenntnis und Einwilligung des Nutzers zu plazieren und bei späterer Gelegenheit wieder abzurufen. Gleiches gilt auch für Programme oder Programmelemente, die auf dem Rechner des Nutzers ablaufen und durch die personenbezogene Daten offenbart werden können, z.B. Java-Applets.

Absehbare Umsetzungsschwierigkeiten

Auch wenn das neue Recht datenschutzrechtliche Verbesserung aufweist, ist doch vor übertriebener Euphorie zu warnen. Gerade in internationalen Netzen sind die Durchsetzungschancen noch so guter oder gut gemeinter nationaler Regelungen begrenzt. Dem Nutzer ist vielfach nicht klar, in welchem Land eine Datenverarbeitung stattfindet; nicht einmal die Domain-Bezeichnung garantiert, daß man sich im Inland befindet. Das Domain-Kürzel „de" ist allenfalls ein Indiz dafür, daß es sich um einen deutschen Anbieter handelt und daß deshalb deutsches Recht anwendbar ist. Der Rechner mit dem entsprechenden Angebot kann sich jedoch tatsächlich in einem anderen Erdteil befinden. Der Durchgriff der deutschen Datenschutzaufsichts- und Kontrollbehörden wird in diesem Fall kaum gelingen.

Angesichts dieser Problematik wäre es sehr sinnvoll, wenn es gelingen könnte, Qualitätskriterien und Zertifizierungsverfahren zu definieren, mit denen bestimmte, besonders datenschutzfreundliche Angebote und Anbieter festgestellt werden könnten. Entsprechend zertifizierte Angebote könnten vom Nutzer als vertrauenswürdig erkannt werden und hätten somit auch im internationalen wirtschaftlichen Wettbewerb ggf. bessere Durchsetzungschancen. Wenn traditionelle Aufsichts- und Kontrollformen versagen, würde die Zertifizierung von datenschutzfreundlichen Angeboten und Anbietern gleichwohl einen Weg zu einer datenschutzfreundlichen Praxis eröffnen. Einen derartigen Weg weist die Vorschrift zum Datenschutz-Audit im Mediendienste-Staatsvertrag. Zu hoffen ist, daß der Bundesgesetzgeber im weiteren Gesetzgebungsverfahren den Gedanken des Datenschutz-Audits wieder aufgreifen und im Teledienstedatenschutzgesetz verankern wird.

Werner Moritz

Telekommunikations- und Medienrecht im Wandel

Welche Folgen ergeben sich für den Datenschutz?

Im Mai 1995 ist die Fernmeldeüberwachungsverordnung (FÜV), am 19. Juli 1996 die Verordnung für den Datenschutz für Unternehmen, die Telekommunikations-Dienstleistungen erbringen (Telekommunikationsdienstunternehmen-Datenschutzverordnung – TDSV, BGBl I, Nr. 34, S.982) und am 01. August 1996 das Telekommunikationsgesetz (TKG, BGBl I Nr. 39 S. 1120) in Kraft getreten. Zum 31.12.1997 verliert der Rest des Fernmeldeanlagengesetzes (FAG), der derzeit noch in Kraft ist, seine Gültigkeit. Eine neue Fernmeldeüberwachungs- und eine neue Telekommunikationsdatenschutzverordnung, die auf der Grundlage des TKG verabschiedet werden, sind erforderlich.

Weitere Gesetzesvorhaben im Medienbereich laufen: der Mediendienste-Staatsvertrag (MStV) ist zwischen den Ministerpräsidenten der Länder abgestimmt und liegt den Länderparlamenten zur Ratifizierung vor. Der Entwurf des Informations- und Kommunikationsdienstegesetzes (IuKDG) ist von der Bundesregierung in den Bundesrat (Bundesratsdrucksache 966/96) und den Bundestag eingebracht worden. Der Bundesrat hat am 21. Februar 1997 einen Beschluß mit vielen Änderungswünschen gefaßt (BR-Drucksache 966/96 – Beschluß). Am 18. April 1997 hat der Bundestag den Gesetzentwurf in erster Lesung an folgende Ausschüsse verwiesen:

- Innenausschuß
- Rechtsausschuß
- Ausschuß für Bildung, Wissenschaft, Forschung, Technologie und Technikfolgenabschätzung (federführend)
- Ausschuß für Wirtschaft
- Ausschuß für Familie, Senioren, Frauen und Jugend
- Ausschuß für Post und Telekommunikation
- Ausschuß für die Angelegenheiten der Europäischen Union

Mit der Ratifizierung und dem Inkrafttreten des Mediendienste-Staatsvertrages ist ebenso wie mit der Verabschiedung und dem Inkrafttreten des IuKDG noch in diesem Jahr zu rechnen.

Alle diese Gesetze(sentwürfe) beinhalten auch Regelungen zum Datenschutz.

Sowohl Onlinediensteanbieter wie AOL, Compuserve und T-Online (um nur die drei größten der BRD in alphabetischer Reihenfolge zu nennen) als auch MailboxbetreiberInnen und Universitäten (sofern sie E-Mail und News anbieten), fallen unter diese Regelungen:

- Für den Bereich der E-Mail gilt das Telekommunikationsrecht, also in erster Linie das Telekommunikationsgesetz sowie die sich darauf berufenden Verordnungen, aber auch noch die FÜV und die TDSV aus den Jahren 1995 bzw. 1996,
- für den Bereich der (nicht moderierten) Newsgroups (elektronischen Diskussionsforen, Bretter) sowie für den Zugriff auf WWW-Seiten wird das IuKDG gelten und
- für redaktionelle eigene Inhalte der DiensteanbieterInnen wird der Mediendienste-Staatsvertrag zur Geltung kommen. Dies kann auch für MailboxbetreiberInnen gelten, die regelmäßig eigene Inhalte ihren und oder den Netz-NutzerInnen anbieten.

Es könnte also vorkommen, daß wenn einE TeilnehmerIn einer Mailbox oder eines Onlinedienstes eine datenschutzrelevante Eingabe macht, die Kontrollregelungen aller drei Bereiche zur Anwendung kommen und drei verschiedene Institutionen zu prüfen haben, ob es zu Verstößen gegen das Datenschutzrecht gekommen ist.

Telekommunikationsbereich

Im Telekommunikationsbereich stellt sich die Verbindung zwischen „alter" TDSV (vom 18.07.1996) und „neuem" TKG (vom 31.07.1997) als sehr komplex dar.

Die TDSV „regelt den Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten." Die „Bestimmungen gelten für Unternehmen und Diensteanbieter, die der Öffentlichkeit angebotene Telekommunikationsdienstleistungen erbringen oder daran mitwirken." (TDSV, § 1). Dabei sind „Diensteanbieter alle, die ganz oder teilweise geschäftsmäßig Telekommunikationsdienstleistungen erbringen" (TDSV, § 2, Ziff. 2). Nun sind aber „Telekommunikationsdienstleistungen das gewerbliche Angebot von Telekommunikation[1] einschließlich der Übertragungswege [...] und nicht lediglich für die Teilnehmer geschlossener Benutzergruppen" (TDSV, § 2 Ziff. 6). Unternehmen wiederum sind „alle, die nach den Vorschriften des Geset-

1. Hier hat sich eine begriffliche Ungenauigkeit eingeschlichen. Gemeint ist hier sicher das gewerbliche Anbieten von Telekommunikationsdiensten und nicht das der Telekommunikation selbst. Außer Firmenhotlines und gewerblichen AnbieterInnen von Telefonsex fallen mir wenige ein, die Telekommunikation mitsamt KommunikationspartnerInnen selbst gewerblich anbieten. Auch hier zeigt sich, daß die Begriffsbestimmungen in der TDSV und dem TKG mit heißer Nadel gestrickt wurde.

zes über Fernmeldeanlagen eine Fernmeldeanlage betreiben oder daran mitwirken" (TDSV, § 2 Ziff. 7).
Alles klar? Nein? Kein Grund zur Beunruhigung! Das ging – zumindest einigen – ParlamentarierInnen des Bundestages genauso. Eine entsprechende Anfrage ist daher auch auf den Weg gebracht worden.[2] Es wird aber noch verwirrender: Durch das TKG sind viele Paragraphen[3] des Gesetzes über Fernmeldeanlagen (FAG) außer Kraft gesetzt worden. Wie es jetzt einem Unternehmen gelingen soll, nach den Vorschriften des FAG eine Fernmeldeanlage zu betreiben, ist derzeit auch nicht klar.

Gewerblich oder nur geschäftsmäßig?

Für viele MailboxbetreiberInnen ist es überflüssig, sich mit der derzeit gültigen TDSV zu beschäftigen, da ja nur das „gewerbliche Anbieten von Telekommunikation" eine Telekommunikationsdienstleistung darstellt. Das rein geschäftsmäßige Anbieten von Telekommunikationsdiensten unterliegt nicht der noch gültigen TDSV. Da Universitäten, die ihren StudentInnen, MitarbeiterInnen und DozentInnen E-Maildienste zur Verfügung stellen dies im allgemeinen nicht gewerblich tun, trifft auch für diese die TDSV nicht zu. Wer allerdings den Betrieb der Mailbox als Gewerbe angemeldet hat, sollte sich etwas näher mit der TDSV beschäftigen.

Etwas anders sieht es hingegen beim TKG aus: Auch dort wird zwischen „geschäftsmäßigem Erbringen von Telekommunikationsdiensten" (TKG, § 3 Nr. 5) und Telekommunikationsdienstleistungen – gemeint ist „das gewerbliche Anbieten von Telekommunikation"[4] (TKG, § 3 Nr. 18) – unterschieden. Es ist bei den einzelnen Regelungen daher immer darauf zu achten, ob sie für die BetreiberInnen von TK-Anlagen, AnbieterInnen von Telekommunikationsdiensten oder für (gewerbliche) AnbieterInnen von Telekommunikationsdienstleistungen gelten.

Durch die im § 3 des TKG enthaltenen Begriffsbestimmungen (ganze 24 an der Zahl) entfallen einige leidenschaftliche Auseinandersetzungen in der Online- und Mailboxszene. So ist klar definiert, was eine Telekommunikationsanlage (vormals Fernmeldeanlage) ist. Diese Definition schließt Mailboxen - sofern der Dienst E-Mail angeboten wird - eindeutig mit ein. Ebenso ist für den Begriff „geschäftsmäßiges Erbringen von Telekommunikationsdiensten" klargestellt, daß hiermit daß „nachhaltige[5] Angebot von Telekommunikation einschließlich des Angebots von Übertragunsgswegen für Dritte mit oder ohne Gewinnerzielungsabsicht" (TKG, § 3 Nr. 5) gemeint ist.

Eine weitere lang diskutierte Frage ist nun geklärt: JedeR der/die „Telekommunikationsdienstleistungen erbringt, muß die Aufnahme, Änderung und Beendigung des Betriebes innerhalb eines Monats bei der Regulierungsbehörde anzeigen."(TKG § 4 Satz 1). Die bereits seit längerem vom Bundesamt für Post und Telekommunikation (BAPT, es übernimmt für eine Übergangszeit die Aufgaben der im TKG genannten Regulierungsbehörde) durchgeführte Praxis - nur die Anzeigen von Mailboxen mit Gewerbeschein zu registrieren - ist nun gesetzliche Regelung geworden.

Fernmeldeüberwachung und Datenübermittlung an Sicherheitsbehörden

Im 11. Teil des TKG („Fernmeldegeheimnis, Datenschutz und Sicherung") „verstecken" sich zwei Paragraphen, die zumindest den Datenschutz karikieren! So regelt der „§ 88 Technische Umsetzung von Überwachungsmaßnahmen", daß die technischen Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation von BetreiberInnen von Telekommunikationsanlagen auf eigene Kosten zu gestalten sind. Ansonsten übernimmt dieser Paragraph weitgehendst die Regelungen aus der stark kritisierten FÜV[6]. Eine sogenannte Telekommunikationsüberwachungsverordnung, die die FÜV ablösen wird, befindet sich bereits in der Ressortabstimmung.

Im „§ 90 Auskunftsersuchen der Sicherheitsbehörden" ist geregelt, daß alle, die geschäftsmäßig Telekommunikationsdienste anbieten, verpflichtet sind, „Kundendateien zu führen, in die unverzüglich die Rufnummern[7] [...] sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontigenten aufzunehmen sind, auch soweit diese nicht in öffentlichen Verzeichnissen eingetragen sind." Der Regulierungsbehörde wird dabei das Recht eingeräumt, auf Anforderung der Sicherheitsbehörden online diese Kundendaten abzufragen. Dabei hat das Abfragesystem der BetreiberInnen so eingerichtet zu sein, daß die BetreiberInnen nichts von diesen Abfragen merken! Angriffe von Hackern auf diese Verzeichnisse können somit auch nicht festgestellt und kontrolliert werden!

Fernmeldegeheimnis

Erfreulich - zumindest für die TeilnehmerInnen - ist, daß zur Einhaltung des Fernmeldegeheimnisses verpflichtet ist, „wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt" (TKG § 85). Dies gilt somit für fast alle Mailboxen (auch wenn es den FIDO-Sysops, die E-Mail Netmail nennen, nicht passen wird) und ebenso

2. Die Antwort des BMPT, die inzwischen erteilt wurde, macht deutlich, daß sich diese Verwirrung bis in die Regierung fortpflanzt.
3. nämlich der § 1 Abs. 1 bis 3, die §§ 1a, 2a bis 5e, der § 7 Abs. 3, die §§ 9 bis 11, 13 bis 15, 18, 20 bis 24 und 27
4. Nach § 3 Nr. 16 „ist 'Telekommunikation' der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen." Und das sind wiederum „technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können." (TKG, § 3 Nr. 17)
5. der Begriff „nachhaltig" kommt aus dem Finanzrecht und steht – ähnlich wie der Begriff „geschäftsmäßig" im Bundesdatenschutzgesetz (BDSG) – für eine auf Wiederholung oder auf Dauer ausgelegte Tätigkeit.
6. vgl. FIfF-Kommunikation 2/95 Seite 4-5
7. Nach § 3 Nr. 10 „sind 'Nummern' Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen"; also auch die E-Mail-Adressen der TeilnehmerInnen!

für die Onlinedienste und Mailserver, soweit jeweils E-Mail als Dienst angeboten wird.

Datenschutz und -sicherung

Im § 87 TKG wird vorgeschrieben, daß die BetreiberInnen von Telekommunikationsanlagen, „die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen", für diese Anlagen „angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

1. des Fernmeldegeheimnisses und personenbezogener Daten,
2. der programmgesteuerten Telekommunikations- und Datenverarbeitungsanlagen gegen unerlaubte Zugriffe,
3. gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen[8], und
4. von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Eingriffe und Einwirkungen von Katastrophen[9] zu treffen" haben.

Auch die datenschutzrechtlichen Anforderungen aus § 89 TKG gelten für Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken. Dabei ist auch hier vorgesehen, daß eine Verordnung (die Nachfolgeverordnung für die im Juli 1996 in Kraft getretene TDSV) erlassen wird[10], die das nähere regelt. Mindestanforderungen sind aber bereits in diesem Paragraphen genannt. Die wichtigsten Regelungen sind:

- Es dürfen nur die personenbezogenen Daten erhoben werden, die erforderlich sind zur betrieblichen Abwicklung der geschäftsmäßigen Telekommunikationsdienste.
- Die Gestaltung des Einzelverbindungsnachweises muß so erfolgen, daß der Schutz von MitbenutzerInnen und Anrufen bei Institutionen, die grundsätzlich anonym bleibenden AnruferInnen ganz oder überwiegend Beratung in seelischen oder sozialen Notlagen anbieten, gewahrt bleibt.
- Nachrichteninhalte dürfen nur aufgezeichnet, Dritten zugänglich gemacht oder sonst verarbeitet werden, wenn dies für die Diensteerbringung erforderlich ist (z.B. Speicherung der eingehenden Nachrichten im elektronischen Postfach bis zur Abholung durch den/die TeilnehmerIn) oder im Falle der Telekommunikationsüberwachung.
- Für die Nutzung personenbezogener Daten zu Zwekken der Werbung, Kundenberatung oder Marktforschung ist die Einwilligung der KundInnen erforderlich. InhaberInnen der am 01. August 1996 bestehenden Anschlüsse mußten auf ihre Möglichkeit zum Widerspruch gegen diese Nutzung hingewiesen werden. Bei Kenntnis dieses Widerspruchsrechtes gilt das Nichtwidersprechen als Einwilligung.
- Die KundInnen haben ein differenzierteres Widerspruchsrecht bezüglich der Veröffentlichung in gedruckten und/oder elektronischen Verzeichnissen. So ist es möglich, nur in gedruckten Verzeichnissen zu erscheinen, nicht aber in elektronischen Verzeichnissen. Unabhängig hiervon ist die Nutzung der Daten für die Auskunft, für die es ebenfalls ein Widerspruchsrecht gibt. So ist z.B. möglich, nur über die Auskunft erfragbar zu sein, aber in keinem öffentlichem Verzeichnis (z.B. Telefonbuch oder CD-ROM) verzeichnet zu sein.
- „Die geschäftsmäßige Erbringung von Telekommunikationsdiensten und deren Entgeltfestlegung darf nicht von der Angabe personenbezogener Daten abhängig gemacht werden, die für die Erbringung oder Entgeltfestlegung dieser Dienste nicht erforderlich sind."[11]

Datenschutzkontrolle

Die Datenschutzkontrolle für Unternehmen und Personen, die der Datenschutzaufsicht nach § 38 Bundesdatenschutzgesetz (BDSG) unterliegen, wird nicht - wie im § 38 BDSG bestimmt - durch die regional zuständigen Aufsichtsbehörden vorgenommen, sondern ist im TKG dem Bundesbeauftragten für den Datenschutz (BfD) übertragen worden. Begründet wurde dies damit, daß alle Telekommunikationsdienste-AnbieterInnen die gleichen Bedingungen bezüglich der Datenschutzaufsicht unabhängig von ihrem Sitz haben sollen. Auch sollte die Erfahrung des BfD in diesem Bereich, die er bezüglich der Deutschen Telekom AG gesammelt hat, weiter nutzbar bleiben. Allerdings zeigte sich bereits bei Eingaben bezüglich der Deutschen Telekom AG, daß der BfD teilweise wenig Biß hatte. Eine Ausweitung der Kontrollbefugnis auf alle in der BRD ansässigen TK-Dienste-AnbieterInnen würde zumindest bedingen, daß das Personal des BfD für diesen Bereich entsprechend aufgestockt wird.

Informations- und Kommunikationsdienste – Mediendienste

Die Regelungen, die sich durch den Mediendienste-Staatsvertrag und das Informations- und Kommunikationsdienstegesetz ergeben, betreffen nicht nur das Internet[12], sondern auch Mailboxnetze (wie z.B. das /CL-Netz[13] oder FIDO) bzw. deren SystembetreiberInnen sowie OnlinediensteanbieterInnen wie AOL, Compuserve und T-Online, die auch eigene Inhalte, die teilweise nur ihren KundInnen zugänglich sind anbieten.

8. Dies haben BetreuerInnen von Internet-Gateways für PM's und Systeme, über die für andere Systeme PM's geroutet werden besonders zu beachten!
9. So ist der Betrieb z.B. ohne ausreichenden Blitzschutz und vernünftige Backup-Systeme nicht mehr zulässig. Dies ist insbesondere für die kleineren Mailboxsysteme sicherlich ein Problem.
10. ein entsprechender Entwurf befindet sich ebenfalls bereits in der Ressortabstimmung
11. § 89, Abs. 10 Satz 1 TKG
12. vgl. hierzu den Artikel „Tele- und Mediendiensterecht: Neue Maßstäbe für die Verarbeitung personenbezogener Daten im Internet" von Peter Schaar in diesem Heft, Seite 24 ff
13. /CL steht für Computernetze Linkssysteme, vgl. hierzu auch Artikel der Ausgaben 2/95 und 1/97

Presseerklärung

53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in München am 17./18. April 1997

Der derzeitige Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der Bayerische Landesbeauftragte für den Datenschutz, Reinhard Vetter, hat heute die Ergebnisse der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in München vorgestellt. Den Datenschutzbeauftragten lag eine umfangreiche Tagesordnung vor, die ihre Schwerpunkte im Bereich Datenschutz bei Polizei und Strafverfolgungsbehörden, Auskunftsbegehren von Sicherheitsbehörden gegenüber Telediensten, Europol, Datenverarbeitung in der Medizin und Datenschutz durch intelligenten Technikeinsatz und intelligente Organisation hatte. Dazu beschäftigte sich die Datenschutzkonferenz auch mit der Kritik am Datenschutz in Öffentlichkeit und Verwaltung.

Zur Diskussion über die Regulierung von Verschlüsselungsverfahren wiesen die Datenschutzbeauftragten auf ihren Beschluß auf der 52. Konferenz hin, in dem die unabdingbare Notwendigkeit sicherer Verschlüsselungsmöglichkeiten für jedermann für eine sichere Nutzung des Internets zur Übermittlung vertraulicher, persönlicher oder wirtschaftlicher Angaben betont wird. Ohne diese sicheren Verschlüsselungsmöglichkeiten ist das Internet für die Übermittlung solcher vertraulicher Daten wegen der gegebenen Abhör- und Verändermöglichkeiten unbrauchbar. Die Datenschutzbeauftragten betonten zwar Verständnis für die legitimen Interessen der Sicherheitsbehörden an der Wahrnehmung ihrer gesetzlichen Befugnisse, wiesen aber darauf hin, daß angesichts der gegebenen Umgehungsmöglichkeiten die Effektivität einer Regulierung der Verschlüsselung sehr zweifelhaft sei. Sie warnten weiter davor, daß mit einer Regulierung der Verschlüsselung keine flächendeckende Überwachung des Kommunikationsverkehrs verbunden sein dürfe.

Die Datenschutzkonferenz betrachtet das Gesetzgebungsverfahren für datenschutzrechtliche Regelungen in der Strafprozeßordnung – Strafverfahrensänderungsgesetz – mit großer Sorge. Das gilt insbesondere für einen Großteil der Vorschläge des Bundesrates, die gegenüber dem schon nicht ausreichenden Entwurf der Bundesregierung weitere erhebliche datenschutzrechtliche Verschlechterungen bringen. Schon der Entwurf der Bundesregierung enthält einzelne Lücken, wie zum Beispiel keine ausreichenden Bestimmungen für die Informationssysteme der Staatsanwaltschaften, mit der Folge, daß nahezu unbegrenzte Möglichkeiten von Zentraldateien und Speicherungen bestehen und zwar unabhängig von der Schwere der Straftaten und Schuld. Dazu kommen unspezifizierte Zugriffsmöglichkeiten von zahlreichen Stellen, wie z.B. Bewährungshelfer, Führungsaufsicht und Gerichtshilfe. Schließlich fehlt eine gesetzliche Absicherung der notwendigen technischen und organisatorischen Maßnahmen des Datenschutzes.

Der Bundesrat hat im ersten Durchgang die Kritik der Datenschutzbeauftragten nicht aufgegriffen, sondern in seiner Stellungnahme im Gegenteil die Streichung wesentlicher Schutzbestimmungen gefordert; wie z.B. den Richtervorbehalt für die Öffentlichkeitsfahndung und die längerfristige Observation, das Verbot weitere Daten zu speichern nach Freispruch, die Forderung nach Festlegung von Speicher- und Löschungsfristen und schließlich das Kontrollverfahren für automatisierte Abrufverfahren.

Die Datenschutzkonferenz bittet Bundesregierung und Bundestag dringend, im Interesse der Bürger diesen Forderungen des Bundesrates nicht nachzukommen.

Die Datenschutzkonferenz hat sich mit den Fragen der Speicherung von genetischen Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke befaßt. Das kürzlich in Kraft getretene Gesetz zur Regelung der DNA-Analyse im Strafverfahren betrifft nur die Verwendung dieser Methode in einem konkreten Strafverfahren, nicht die Speicherung von Ergebnissen aus der DNA-Analyse für erkennungsdienstliche Zwecke.

Die Datenschutzkonferenz hält eine gesetzliche Regelung, mit der die Speicherung derartiger Untersuchungsergebnisse für erkennungsdienstliche Zwecke zugelassen wird, grundsätzlich für möglich. Im Hinblick auf die spezifischen Risiken der DNA-Analyse – wegen des Fortschritts der Wissenschaft muß immer damit gerechnet werden, daß heute nicht als codierend erkannte Abschnitte in Zukunft doch Rückschlüsse auf die Persönlichkeit zulassen – fordert die Datenschutzkonferenz u.a., daß durch diese gesetzliche Regelung sichergestellt wird, daß Analyseergebnisse, die Persönlichkeitsmerkmale erkennen lassen, nicht gespeichert werden. Sollten sich durch die Fortschritte der Wissenschaft später doch Rückschlüsse auf die Persönlichkeit aus heute nicht codierenden Abschnitten ergeben, muß ein striktes Nutzungsverbot für die eventuell zukünftig möglichen Erkenntnisse festgelegt werden.

Die Datenschutzkonferenz wendet sich entschieden gegen die im Entwurf eines Teledienstegesetzes vorgesehene Verpflichtung der Anbieter von Telediensten, Vertragsdaten ihrer Kunden an Sicherheitsbehörden zu übermitteln. Eine derartige Auskunftsverpflichtung auch gegenüber Nachrichtendiensten und der Polizei brächte eine völlig neue Qualität von Eingriffsmöglichkeiten mit sich. Bisher ist niemand auf die Idee gekommen, Auskunftsverpflichtungen für die Anbieter von Dienstleistungen über ihre Kunden zu schaffen. Auch der Medienstaatsvertrag der Länder sieht derartige Auskunftsverpflichtungen nicht vor. Im Unterschied dazu soll

durch die geplante Regelung eine derartige Verpflichtung für die Anbieter von Telediensten, also z.B. Homebanking, Homeshopping, aber auch für Anbieter von Diskussionsforen, jetzt geschaffen werden. Damit würde die Verpflichtung festgelegt, daß Anbieter von elektronischen Informationsdiensten offenlegen müßten, welche ihrer Kunden welche Dienste z.B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin liegt nach Auffassung der Datenschutzkonferenz ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des einzelnen. Dieser Eingriff ist nicht nur unverhältnismäßig, er ist auch nicht erforderlich, da das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht hinreichende Möglichkeiten enthält, um strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen.

Die Datenschutzkonferenz bittet deshalb den Deutschen Bundestag dringend, diese Regelung bei der Beratung des Teledienstegesetzes nicht zu beschließen.

Die Datenschutzbeauftragten erörterten den Sachstand zu Europol und beschlossen dazu, hinsichtlich nicht Verdächtiger und hinsichtlich solcher Daten, die nicht kriminalitätsbezogen sind, im Zusammenhang mit den Analysedateien die Forderungen des Europäischen Parlaments zu den Analysedateien von Europol zu unterstützen. Das Europäische Parlament fordert, alle höchst sensiblen persönlichen Daten, wie Angaben zu Religion, zu philosophischer Überzeugung, zu Rasse, Gesundheit und sexuellen Gewohnheiten von der personenbezogenen Erfassung in diesen Datenbanken auszuschließen.

Im Themenbereich Datenverarbeitung in der Medizin hat die Datenschutzkonferenz weitere offene Probleme bei der Verwendung von intelligenten Chipkarten im Gesundheitswesen erörtert. Dazu gehören die Risiken, die mit einer zentralen Speicherung von sensiblen Gesundheitsdaten zahlreicher Bürger an einer Stelle verbunden wären, und Forderungen, daß die Krankenversicherungskarte, die jeder gesetzlich Versicherte vor der Inanspruchnahme medizinischer Leistungen vorlegen muß, zur Bekämpfung des Mißbrauchs bei Medikamentenverschreibungen eingesetzt werden kann. Sie beauftragte den Arbeitskreis Gesundheit, für die Datenschutzkonferenz hierzu eine Arbeitsgrundlage vorzubereiten.

Die Datenschutzkonferenz forderte, daß bei einer Auslagerung von Patientendaten außerhalb von Arztpraxen und Krankenhäusern soweit wie möglich von den gegebenen Möglichkeiten der Anonymisierung und Pseudonymisierung unter Einsatz von Verschlüsselungstechniken Gebrauch gemacht wird. Soweit dies nicht möglich ist, stellt sie fest, daß der Schutz des strafrechtlich garantierten Arztgeheimnisses für eine personenbezogene Datenverarbeitung außerhalb der geschützten Räume beim Arzt oder ärztlichen Einrichtungen nicht gewährleistet ist. Von diesem Risiko betroffen wäre eine Patientenchipkarte mit Gesundheits- bzw. Krankheitsdaten des Einzelnen, dieses Risiko betrifft die Auftragsdatenverarbeitung medizinischer Daten, es umfaßt die Verlagerung von Teilaufgaben aus Arztpraxis und Krankenhaus an private Auftragnehmer (Outsourcing), und es betrifft schließlich die Weitergabe von personenbezogenen Patientendaten außerhalb des ärztlichen Bereichs zu Forschungszwecken. Die Datenschutzkonferenz sieht deshalb in einer Auslagerung von personenbezogenen Patientendaten ohne einen dem Arztgeheimnis entsprechenden angemessenen Schutz einen Verstoß gegen wichtige Interessen des Patienten. Sie bittet deshalb den Bundesgesetzgeber, für eine personenbezogene Verarbeitung von Patientendaten außerhalb des Schutzbereichs ärztlicher Einrichtungen, dieses Schutzniveau zu gewährleisten.

Die Datenschutzkonferenz hat einen Bericht des Arbeitskreises Technik über den Stand der Arbeiten eines Konzeptes für die Entwicklung datenschutzfreundlicher Techniken entgegengenommen. Dieses soll allgemeine Kriterien zur Bewertung datenschutzfreundlicher Systeme, als Hilfsmittel zur Entwicklung solcher Systeme und als Entscheidungskriterium für die Förderung solcher Systeme bieten.

Als Bereiche für den Einsatz von datenschutzfreundlichen Techniken, das heißt solcher Techniken, die auf die Verarbeitung personenbezogener Daten überhaupt verzichten können oder die Gefährdungen durch den Einsatz von Pseudonymen möglichst gering halten, kommen u.a. der Medien- und Teledienstebereich, die Bezahlung durch elektronisches Geld, die Telekommunikation und Zahlungs- und Überwachungssysteme im Bereich Transport und Verkehr in Frage. Der Arbeitskreis hat angekündigt, daß für die Herbstkonferenz ein abschließender Bericht vorgelegt werden soll. An den Sitzungen der entsprechenden Arbeitsgruppe des Arbeitskreises hat eine Abgesandte der Europäischen Kommission teilgenommen, die großes Interesse der Europäischen Kommission an dieser Arbeit zum Ausdruck gebracht hat.

München den 18.04.1997

Reinhard Vetter ist derzeitiger Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Der aktuelle 16. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (BfD) für die Jahre 1995 und 1996 ist gerade erschienen. Darüberhinaus gibt der BfD Informationsbroschüren zum Thema Datenschutz heraus, die als Einführung in das Thema für jedermann/frau geeignet sind. Der Bericht und die Broschüren können kostenlos beim BfD (Riemenschneiderstr. 11, 53175 Bonn) angefordert werden.

- BFD-Info 1: Bundesdatenschutzgesetz – Text und Erläuterung
- BFD-Info 2: Der Bürger und seine Daten – Überblick über Stellen, die personenbezogene Daten verarbeiten und speichern
- BFD-Info 3: Schutz der Sozialdaten – Beleuchtet den Datenschutz im Bereich der Sozialversicherungen
- BFD-Info 4: Der behördliche Datenschutzbeauftragte – Bestellung, Befugnisse und Aufgaben

Diese Materialien sind auch elektronisch in der Mailbox des BfD verfügbar unter 0228/371062 oder über ISDN unter 0228/9579726.

FIfF-Stellungnahme

Sachverständiger des FIfF: Prof. Dr. Friedrich-L. Holl (FH Brandenburg)

Der folgende Text ist eine Stellungnahme des FIfF zur Anhörung des Ausschuß für Bildung, Wissenschaft, Forschung, Technologie und Technikfolgenabschätzung des Deutschen Bundestages zum Informations- und Kommunikationsdienstegesetz (IuKDG) am 14.5.1997

(Dokumentation in Auszügen)

Fragen zum Teil 1 der Anhörung: Teledienstegesetz (TDG) und Teledienstedatenschutzgesetz (TDDG)

1. In Artikel 1 des IuKDG, dem Teledienste-Gesetz (TDG), werden in § 2 TDG – in Abgrenzung zu den dem Mediendienste-Staatsvertrag unterliegenden Mediendiensten – Teledienste definiert als Informations- und Kommunikationsdienste, die sich nicht an die Allgemeinheit, sondern individuell an den Einzelnen richten. Wie beurteilen Sie dieses Abgrenzungskriterium (den Begriff der „Allgemeinheit") und die darauf basierende Unterscheidung in Medien- und Teledienste? Halten Sie eine solche Unterscheidung für ausreichend trennscharf? (...) Ist diese Abgrenzung für neu entstehende Angebote und Dienste ausreichend flexibel?
2. Welche Abgrenzungsprobleme ergeben sich möglicherweise aus diesen Unterscheidungen und was wären die Konsequenzen?

Antwort zu 1 und 2:
Die abstrakte Definition ist u.E. nicht ausreichend normenklar. So ist der Begriff „Individuelle Nutzung" zwar akzeptabel, eine Definition wie die von „kombinierbaren Daten wie ..." dagegen weniger. Die damit verbundene Problematik wird insbesondere am Beispiel des in Absatz 2 Nr. 4 definierten Beispiels der Telespiele auffällig, weil hier die Frage gestellt werden muß, welche kombinierbaren Daten der Gesetzgeber in diesem Zusammenhang sieht.

Zusätzlich fällt auf, daß in Verbindung mit dem Mediendienste-Staatsvertrag die dort über den Begriff der Allgemeinheit als Adressaten versuchte Differenzierung Abgrenzungsprobleme mit dem TDG ergibt.

So richten sich beispielsweise WWW-Seiten oder Internet News grundsätzlich an die weltweite Allgemeinheit und werden somit über den Mediendienste-Staatsvertrag geregelt. Dienste nach § 2 (2) 4 u. 5 (TDG), und damit im Prinzip auch WWW, unterliegen jedoch dem TDG. WWW-Anbieter werden also sowohl nach TDG als auch nach dem Mediendienste-Staatsvertrag geregelt. Selbst Internet-Anbieter, die nur textbasierte Dienste per uucp anbieten, unterliegen eigentlich bereits beidem, wenn sie Mail und News anbieten.

Insofern muß die Unterscheidung in individuelle Nutzung und Allgemeinheit nicht als ausreichend trennscharf angesehen werden. Als daraus folgende Konsequenz ergibt sich aus unserer Sicht die Notwendigkeit, daß die Frage der Zuständigkeit letztlich vor Gericht geklärt werden muß, was erhebliche neue Rechtsunsicherheiten bis zu diesem Zeitpunkt bedeutet. Staatsvertrag und TDG haben u.E. allenfalls den Charakter eines gentlemen agreement, solange niemand klagen will, eher aber eines Stillhalteabkommens bis zur Klärung einiger Punkte vor dem BVerfG in Karlsruhe.

Bezüglich der beispielhaften Darstellung der dem TDG unterliegenden Teledienste ergibt sich die grundsätzliche Problematik, daß derartige Aufzählungen immer einen *nicht abschließenden Raum* von möglichen unter das jeweilige Gesetz fallenden Elementen darstellt. Aufgrund der oben beschriebenen Problematik der möglichen Zuweisung von Diensten zu *unterschiedlichen* Gesetzen verschärft sich diese Schwierigkeit und wird ggf. zu erheblichen Abgrenzungsproblemen führen.

5. Wie beurteilen Sie die in § 5 TDG vorgesehenen Regelungen zur Verantwortlichkeit für „eigene" und „fremde" Inhalte? (...) Wie beurteilen Sie die in § 5 Abs. 3 vorgesehene Regelung, derzufolge Diensteanbieter zur Sperrung rechtswidriger Inhalte verpflichtet sind, sofern sie unter Wahrung des Fernmeldegeheimnisses von den Inhalten Kenntnis erlangen und eine Sperrung „technisch möglich und zumutbar" ist? Wann ist eine solche Sperrung „technisch möglich und zumutbar"?

Antwort zu 5:
Die Trennung der Verantwortlichkeit bzgl. eigener und fremder Inhalte und die volle Verantwortung für eigene und die grundsätzliche Nichtverantwortung für fremde Inhalte ist prinzipiell zu befürworten.

Allerdings ist die Zuschreibung der Verantwortlichkeit für fremde rechtswidrige Inhalte bei Kenntnisnahme, und die daraus resultierende potentielle Verpflichtung zur Verhinderung bzw. Sperrung der Nutzung, eher problematisch zu sehen. Hier werden aus unserer Sicht Fußangeln gelegt, die zum einen zu äußerst interpretierbaren Rahmenbedingungen bezüglich der Kenntnisnahme[1] führen, die rechtlich – insbesondere für die Anbieter und hier besonders für kleine und nicht gewerbsmäßig ausgerichtete – äußerst schwer zu beurteilen sind. Dies führt zu erheblicher Unsicherheit und ist nicht geeignet, eine demokratische und wirtschaftlich effiziente Nutzung von Telekommunikationsdiensten zu fördern.

Zum anderen bietet die Klausel „technisch möglich und zumutbar" ebenfalls ein weites Feld möglicher Interpretationen, die im Zweifelsfall restriktiv und die Telekommunikationsdienste behindernd ausgelegt werden. So ist es bspw. grundsätzlich immer technisch möglich, den Zugang zu

1. Wie wird Kenntnisnahme definiert? Reichen Zufallsfunde oder müssen Inhalte immer vom Anbieter her überprüft werden? Reicht eine Kenntnisgabe über Abmahnvereine oder müssen die Inhalte vor ihrer Sperrung auf die Rechtswidrigkeit von Gerichten überprüft werden? Usw.

Inhalten zu verhindern – heute durch die Unmöglichkeit der Sperrung von URLs im Zweifelsfall durch die Sperrung des gesamten Servers.

Die Zumutbarkeit einer solchen Sperrung wird zudem gesellschaftlich unterschiedlich bewertet und unterliegt damit stark der Definitionsmacht der wegen der unklaren Zuständigkeiten differierenden Interessengruppen.

Daneben verhindert die Sperrung einzelner Server oder URLs normalerweise nicht den Zugang zu inkriminierten Inhalten (Mirrors), sondern schränkt vielmehr nur die Nutzung einzelner Server ein, auch wenn deren restliche Angebote keine problematischen Inhalte haben. Eine Gesamtsperrung führt zudem innerhalb der EU zu Problemen, da wegen weniger Einzelangebote das gesamte Waren- und Dienstleistungsangebot eines Anbieters unterdrückt wird, was mit dem Vertrag von Maastricht unvereinbar ist.

Wir sehen hier einen der wesentlichen Problempunkte des gesamten Gesetzes, der unserer Ansicht nach nicht ausreichend gut und rechtssicher geregelt ist und zusätzlich die realen Bedingungen der Telekommunikationsdienste nicht berücksichtigt.

8. Wie beurteilen Sie die Regelung des Gesetzentwurfes in Art. 2 § 5 Abs. 3? Welche Daten zählen zu den Bestandsdaten? Welche Konsequenzen ergeben sich daraus, daß eine solche Regelung im Mediendienste-Staatsvertrag nicht vorgesehen ist? Ist die Aufteilung in Bestands-, Nutzer- und Abrechnungsdaten sinnvoll und praxistauglich?

Antwort zu 8:
Die Regelung des § 5 (3) bestätigt die Tendenz aller Telekommunikationsgesetze, Bestandsdaten für die Strafverfolgung, Verfassungsschutzaufgaben usw. verfügbar zu machen. Durch die große Durchdringung unserer Gesellschaft mit allen Arten von Telekommunikation ergeben sich durch die Nutzung dieser Daten wesentlich zuverlässigere Auskünfte, als dies mittels anderer traditioneller Datenbestände, wie bspw. der Melderegister, möglich wäre. Insofern sind die Begehrlichkeiten der zuständigen Dienste und Behörden verständlich, zeigen aber die Problematik, daß private Anbieter plötzlich dazu gezwungen werden, öffentliche Aufgaben zu übernehmen bzw. Daten für öffentliche Aufgaben vorzuhalten.

Dies entspricht u.E. nicht den Prinzipien eines demokratischen Rechsstaates, in dem den Bürgern ein größtmöglicher Bereich an persönlicher Unbeobachtetheit zuzubilligen ist.

Insofern ist aus unserer Sicht der § 5(3) von vorneherein sehr problematisch zu bewerten, weshalb nur eine konsequente Streichung dieses Absatzes ausreichenden Schutz der informationellen Selbstbestimmung und der in Art 2 GG zugesicherten freien Entfaltung der Persönlichkeit ermöglichen würde.

Die Ermächtigungsgrundlage im gesamten § 5 für die Datenverarbeitung von KundInnendaten hat zudem den gravierenden Nachteil, daß hierin der Begriff Bestandsdaten weiter gefaßt wird als etwa im TKG. Dort sind dies nur Adreßdaten und die Nutzerkennung, hier jedoch zusätzlich auch Daten zur „inhaltlichen Ausgestaltung" des Vertragsverhältnisses, also etwa zusätzlich abonnierte Dienste und Teledienst-Angebote, soweit die Speicherung solcher Daten zur Abwicklung des Dienstes nötig ist. Dies ist dann der Fall, wenn für diese Dienste gesondert Gebühren erhoben oder Passworte vergeben werden. Bei Nutzung solcher technischer Organisationsformen werden auch inhaltliche Vorlieben mit den Bestandsdaten erfaßt und dann auch für einen Abruf gem. Abs. 3 vorgehalten.

In der Begründung wird explizit von einer abschließenden Definition der Bestandsdaten abgesehen und dies von der Organisation des Diensteanbieters abhängig gemacht. Dieser hat damit die Möglichkeit, daraus einen durchaus größeren Umfang an Daten abzuleiten, als nötig. In Hinblick auf Abs. 3 hätte hier durchaus begrifflich besser differenziert und klar auf Daten zur Identitätsfeststellung reduziert werden müssen. Die Einführung von Nutzungs- und Abrechnungsdaten in § 6 macht überdies deutlich, daß es in § 5 insgesamt vornehmlich um die Befugnis zur Weitergabe an Sicherheitsbehörden geht.

Leider ist auch die Abgrenzung in Bestands-, Nutzer- und Abrechnungsdaten nicht ausreichend (§§ 5 u 6). Insbesondere werden Daten, die nicht Nutzer- oder Abrechnungsdaten sind, über den Passus der inhaltlichen Ausgestaltung den Bestandsdaten zugeordnet, was u.E. unzureichend und potenziell gefährdend ist. Für eine handhabbare und trennschärfere Definition sollte eine zusätzliche Kategorie von ebenfalls besonders zu schützenden Daten entwickelt werden, die sich ausschließlich auf die Definition der inhaltlichen Vertragsbeziehungen (Zugehörigkeit/Abonnements zu Newsgruppen, Abonnement von kostenpflichtigen Zusatzdiensten usw.) bezieht und weder auswertbar noch für Dritte zugänglich gemacht werden dürfte.

Fragen zum Teil 2 der Anhörung: Gesetz über die digitale Signatur (SigG)

1. Mit dem Signaturgesetz sollen Strukturen für rechtsverbindliche digitale Signaturen geschaffen werden. Wie beurteilen Sie die Notwendigkeit eines derartigen Gesetzes?

Antwort zu 1:
Systeme zur digitalen Signatur, die bis auf Ausnahmen auch Möglichkeiten zur Verschlüsselung bieten, sind derzeit entweder im Internet frei verfügbar oder werden kommerziell angeboten und zu verschiedenen Zwecken genutzt. Sowohl die Generierung der Schlüssel als auch deren Zertifizierung und Veröffentlichung wird zumeist durch freiwillige und kostenfreie Mechanismen realisiert. Ein gesetzlicher Rahmen scheint zur Entfaltung der Nutzung dieser Systeme zur Zeit nicht notwendig.

2. Wie beurteilen Sie die vorgesehene Infrastruktur für die digitale Signatur?

Antwort zu 2:
Eine privatrechtliche Lösung ist an sich wenig problematisch, jedoch ist die komplexe Infrastruktur aus Zertifizierungsstellen keineswegs besser als andere Modelle geeignet, sichere Signaturen zu erstellen und zu verwalten. Stattdessen birgt sie insofern Probleme, als sich Unternehmen, die etwa ihre Mitarbeiter mit digitalen Signaturen ausstatten wollen, entweder diese Dienstleistung einkaufen oder ein Zertifikat erlangen müssen. Die vorgeschlagene Infrastruktur ist daher wenig flexibel. Sie ist allerdings ein passendes Instrument, um die Verwaltung von und den Zugriff auf Kryptierschlüssel zuverlässig zu leisten.

10. Wie beurteilen Sie die Einführung der digitalen Signatur im Hinblick auf Pläne, teilnehmerautonome Verschlüsselung einzuschränken oder gar zu verbieten?
11. Wie sinnvoll ist Ihrer Ansicht nach eine Trennung von Signaturgesetz und einer Regelung kryptographischer Verfahren?

Antwort zu 10) und 11)
Die der digitalen Signatur zugrundeliegende Technik ist eine Nutzungsvariante kryptographischer Verfahren. Eine Einschränkung derartiger Verfahren hätte daher auch Folgen für die Nutzung der digitalen Signatur. Die gegenseitige Bedingtheit von Signatur und Verschlüsselungssystemen geben einer getrennten Regelung in verschiedenen Gesetzen wenig Sinn. Da eine Regelung von Kryptierverfahren unterbleiben sollte, wäre in einem solchen Gesetz zumindest darauf einzugehen, daß sowohl Kryptierung als auch Signatur wie bisher ohne weitere Regulierung gemeinsam in Systemen nutzbar sein sollten. Allein die Schaffung einer auch für den staatlichen Zugriff auf Kryptoschlüssel geeigneten Infrastruktur von Zertifizierungsstellen gibt dem Signaturgesetz eine gewisse Logik, deren Zweck allerdings verfehlt ist.

Ein Kryptogesetz würde die digitale Signatur massiv schädigen. Die Signatur würde durch einen staatlichen Zugriff auf Kryptierschlüssel, die mittels derselben Infrastruktur verwaltet werden, völlig unglaubwürdig und würden eine Flucht aus zertifizierten Verfahren hin zu staatlich unbeaufsichtigten Verfahren auslösen.

Multimedia-Regelungen – warum überhaupt?

Eine Analyse von Informations- und Kommunikationsdienstegesetz (IuKDG) sowie Mediendienste-Staatsvertrag zeigt deren offensichtliche und schwerwiegende Probleme. Besonders die fehlende definitorische Abgrenzung beider Werke führte dazu, daß auf diese Weise zwei Regelungen auf ein und denselben Dienst zutreffen. Die Frage liegt daher nahe, wie es überhaupt zu zwei konkurrierenden Regelwerken kommen konnte.

Hier hilft ein Blick zurück. Weit vor der Zeit elektronischer Netze wurden die Zuständigkeiten von Bund und Ländern klar aufgeteilt: Dem Bund obliegt die Regelung der Telekommunikation, also der Individualkommunikation, den Ländern die der Presse und jener Medien wie Radio und Fernsehen, die der allgemeinen Willensbildung dienen. Für bundeseinheitliche Regelungen wird dafür alle Jahre wieder ein Rundfunkstaatsvertrag ausgehandelt.

Das heute in IuKDG und Mediendienste-Staatsvertrag offenbare Abgrenzungsproblem zwischen Bund und Ländern hat seinen Ursprung im Bildschirmtext (BTX)-System der 80er Jahre. Kaum anders als sein Nachfolger T-Online, war das ursprüngliche BTX ein zentrales System, dessen Zugang von der Bundespost, später Telekom, gemanagt wird, dessen Anbieter jedoch auch verschiedenste weitere Unternehmen sind, darunter auch Medienanbieter. Da schon vor 15 Jahren offenbar bei BTX niemand genauer wissen wollte, wie bei elektronischen Netzen nun zwischen Individualkommunikation und Massenmedium differenziert werden könnte und sollte, schlossen Bund und Länder den BTX-Staatsvertrag ab, mit dem eine Bund-Länder-Zuständigkeit für derartige elektronische Dienste präjudiziert wurde.

Seither glimmt die Lunte an einem medienpolitischen Pulverfaß, bei dem durch die Entwicklung des Internets noch kräftig nachgelegt wurde: Weder hat der Bund die Befugnis, Medienrecht zu setzen, noch haben die Länder Regelungsbefugnisse für die Individualkommunikation – tertium non datur, dazwischen aber gibt es im Grundgesetz nichts. Nach Artikel 30 darf der Bund nämlich nur das regeln, was ihm im Grundgesetz zugestanden wurde, und diese Regelungsbefugnis endet mit der Individualkommunikation. Zwar fehlte schon dem BTX-Staatsvertrag weitgehend die gesetzliche Grundlage, doch war BTX zu unbedeutend, um daran Grundrechtsfragen durchzufechten.

Vor die Alternative gestellt, das Internet in seine jeweiligen massenmedialen oder individualkommunikativen Einzelteile zu zerlegen, zu regulieren und damit jegliche Grundlage zu entziehen, oder sich zu einem gemeinsamen Wurf zusammenzuraufen, haben sich Bund und Länder nun auf ein politisches Tauziehen eingelassen, dessen Resultat die Versammlung fast aller Nachteile ist, die beide Alternativen jeweils boten. Der Versuch, Internet-Angebote dem einen oder anderen Regelungsbereich zuzuordnen, ist gründlich danebengegangen, gleichzeitig scheint in dem Prozeß alles für einvernehmliche Lösungen verfügbare politische Porzellan zerschlagen zu sein.

Beide Seiten tragen daran ihr gerüttelt Maß an Schuld. Die Länder traten mit der Forderung an, das von ihnen als Abart des digitalen Fernsehens mißverstandene Internet bis hin zu WWW-Seiten regulieren zu wollen. Zukunftsminister Rüttgers ging Anfang 1996 in die Beratungen mit dem Bekenntnis, die Regulierungswut der Länder durch sein Multimediagesetz zu bremsen, das die im BTX-Staatsvertrag eingeschlagene Richtung umkehren sollte. Im Interesse der Bundeskompetenz war einkalkuliert, die Länder zu einem Gang nach Karlsruhe zu treiben. Nur: es gibt im Grundgesetz keine Basis für seine Ansichten.

Diese Machtfrage zwischen Bund und Ländern wird nun auf dem Rücken der Internet-Provider und -Nutzer ausgetragen. Sie haben die Zeche für Profilierungsgehabe, mangelnden politischen Einigungswillen und baren technischen Unverstand zu zahlen. (Ingo Ruhmann)

Ute Bernhardt

Voyeure im Netz

Ein funktionierender und strenger Datenschutz gilt vielen als spezifisch deutsche Eigenart. Beispiele aus den USA zeigen aber, daß auch dort mit zunehmender Kommerzialisierung von Daten der Ruf nach einem verbesserten Schutz der Privatsphäre lauter wird.

Ein Anlaß der Entrüstung war die Datenbank P-Trak der Firma Lexis-Nexis. Die Firma bietet in einer für jedermann zugänglichen Datenbank personenbezogene Daten an. Gespeichert sind in P-Trak Stammdaten wie Name, Geburtsname, Adresse, frühere Adressen, Telefon- und Sozialversicherungsnummer. Das als „personal locator" bezeichnete Personenregister ist eine gigantische Datenbank mit über 300 Millionen Datensätzen, die monatlich aktualisiert wird.

Nach ersten Protesten ist die Sozialversicherungsnummer nur noch als Suchkriterium möglich und damit die gänzlich freie Abfrage ein kleines bißchen eingeschränkt. Dennoch ist die Sozialversicherungsnummer weiterhin in der Datenbank enthalten. Lexis-Nexis vertreibt dabei die Stammdaten der Transunion, einer der größten Kreditauskunfteien der USA und mit der Schufa vergleichbar. Diese beiden Unternehmen nutzen eine Gesetzeslücke im Fair Credit Reporting Act, die diese Daten vom Datenschutz ausnimmt. Die eigentliche Zielgruppe von Lexis-Nexis sind zwar Juristen und Strafverfolgungsbehörden, doch gegen eine Gebühr kann jeder die Dienste in Anspruch nehmen.

Mit einer Flut von Anrufen, Fax und Email versuchen nun besorgte Bürger, ihre Daten zu löschen. Doch das gestaltet sich nicht so einfach. Lexis-Nexis war nicht auf die große Zahl an Löschungswünschen vorbereitet und mußte mehrfach das Verfahren zur Aufnahme von Löschungswünschen ändern, was Kundinnen und Kunden zusätzlich verärgerte. Wer seine Daten aus P-Trak löschen lassen will, sollte zur eindeutigen Identifizierung die Sozialversicherungsnummer angeben. Falls Daten vorhanden sind, werden die Daten gelöscht. Anders ist es aber, wenn kein Datensatz vorhanden ist. Lexis-Nexis lehnt es ab, eine Robinsonliste mit Löschungswünschen anzulegen. Deshalb ist es in diesem Fall nötig, periodisch eine gebührenpflichtige Datenbankabfrage zu veranlassen, um herauszufinden, ob der eigene Datensatz inzwischen existiert. Der Wunsch nach Datenschutz erweist sich dabei für Lexis-Nexis als zusätzliche Einnahmequelle.

Dieser Fall hat vor allem Bürgerinnen und Bürger, aber auch die Behörden in den USA wachgerüttelt. Es wurde gefordert, gesetzlich gegen die stark zunehmende Dienstleistungsbranche, die gegen Gebühr sensibelste Informationen über Personen feilbieten, vorzugehen.

Das Datenschutzproblem, das durch Firmen wie Lexis-Nexis entsteht, ist mit dem bundesdeutschen Problem der Telefonverzeichnisse von D-Info auf CD-ROM vergleichbar. In den USA wie auch hier geraten zunehmend Daten von BürgerInnen und KonsumentInnen ins Visier kommerzieller Anbieter. Mit relativ wenig Aufwand und geringen Kosten werden Datenbanken mit persönlichen Angaben als neue Produkte geschaffen. Die Kritik und das Unbehagen, die diese Verletzungen der Privatheit auslösen, sind groß. Es zeigt sich, daß nur Aufklärung und zahlreicher Widerspruch gegen derartige Entwicklungen helfen, die politisch Verantwortlichen zu einem Umdenken zu bewegen.

Auch in der Bundesrepublik hat sich der Schutz der Daten vor ihrem Ausverkauf als nicht immer unproblematisch erwiesen. Gerade der Hersteller der D-Info CD-ROM betrieb ein juristisches Wettrennen zwischen Hase und Igel. Er umging das Verbot, indem die inkriminierten Exemplare vom Markt genommen und durch eine neue Version ersetzt wurden, gegen die erst wieder ein neuer juristischer Anlauf unternommen werden muß. Auch die TELEKOM bietet mittlerweile die Daten ihrer Telefonkunden auf dem Internet an. Zusätzlichen Nutzen schlägt sie aus den Adreßdaten ihrer Kunden, die zu Sondergebühren bei der Komfortauskunft abrufbar sind.

Der gläserne Surfer

Das Internet selbst liefert in hohem Maße Daten über die Aktivitäten seiner NutzerInnen. Da Speicherplatzprobleme heute keine Rolle mehr spielen, können die Daten von mehr als 15.000 Newsgruppen katalogisiert und indiziert werden, um sie für Recherchen zugänglich zu machen. Die Firma Deja News bietet mit einem Suchprogramm (http://www.dejanews.com) Zugriff darauf, wer was in welcher Newsgruppe geschrieben hat. Damit kann sich jeder über die Diskussionsbeiträge anderer im Usenet ein Bild machen. Der fleißige Teilnehmer an unterschiedlichsten Diskussionsgruppen wird damit mit seinen Ansichten und Interessen transparent. Unangenehm kann es außerdem werden, wenn auf diesem Wege Eltern, Lebensgefährten oder Arbeitgeber durch die Beteiligung an Newsgruppen über politische Meinungen oder gar von sexuellen Vorlieben erfahren. Den Arbeitgeber könnte aber schon interessieren, was seine Mitarbeiter in der Dienstzeit so in den Newsgruppen treiben. Derartige Möglichkeiten, persönliche Interessen zu erfassen, reizen zu personenbezogenen Auswertungen, wie etwa der Erstellung von Nutzerprofilen und zum gezielten Versand von Werbung.

Auch zu welchen Themen im Internet Suchanfragen gestartet werden, läßt sich mittlerweile verschiedentlich – so etwa bei der Firma Magellan – mitlesen. Die eingehenden Anfragen werden auf einer „Voyeur Page" angezeigt (http://voyeur.mckinley.com/voyeur.cgi). Das entsprechende Ergebnis kann ebenfalls hinzugeladen werden, jedoch noch nicht wer diese Suche veranlasst hat. Derartige Daten werden bei der Netznutzung in Betrieben gesammelt, die ihren

Netzzugang mit Firewalls schützen. Hier wird das Kommunikationsverhalten der Mitarbeiter transparent. Unklar ist, in welchem Umfang derartige mitbestimmungspflichtige Leistungs- und Verhaltenskontrollen von den Betriebsräten als Problem erkannt werden.

Datenbanken im Internet

Eine neue Qualität erhalten Datenbanken durch ihre Veröffentlichung im Internet. Für nur 222 Dollar lassen sich die kompletten Daten der KFZ-Zulassungsbehörde des US-Staates Oregon erwerben. Im August 1996 veröffentlichte ein Käufer diese Datenbank im Internet. Jeder Autofahrer in Oregon war nun durch die Eingabe der Ziffern und Buchstaben des Nummernschildes mit Name, Adresse und Geburtsdatum im Internet identifizierbar. Erklärtes Motiv des Käufers war es, Autofahrer durch die fehlende Anonymität in ihrem Verhalten zu disziplinieren.

Mit immerhin 96.000 Anfragen in wenigen Tagen war die Webseite sehr gefragt. Die Daten wurden kurzzeitig aus dem Netz genommen – nicht aufgrund der enormen Proteste der Autofahrer Oregons –, sondern weil sie einige geschützte Daten enthielt. Nachdem diese unzugänglich gemacht worden sind, stünde einer erneuten digitalen Veröffentlichung nichts mehr im Wege. Überdies plant der Käufer der Zulassungsdaten eine Veröffentlichung der Ergebnisse von Restaurant-Inspektionen durch die Gesundheitsbehörden in Oregon.

Die digitale Veröffentlichung erweitert die Verletzung der Privatheit um eine neue Dimension. Gerade die Beeinflussung des Verhaltens durch eine Identifizierbarkeit war einer der Gründe, die das Bundesverfassungsgericht im Volkszählungsurteil 1983 bewogen, zum Schutz der Persönlichkeit ein „Recht auf informationelle Selbstbestimmung" zu definieren. Der Kauf behördlicher Daten und deren weltweite Veröffentlichung im Internet führen nun zu einer neuen Qualität bei der Offenlegung gesammelter Daten. Einzelne, für einen bestimmten Zweck gesammelte Daten werden für die Allgemeinheit abrufbar. Das Internet bietet dann die Möglichkeit, die Inhalte verschiedenster einstmals isolierter und zweckgebundener Datenbanken miteinander zu verknüpfen.

In Ländern, in denen derartiges gesetzlich nicht untersagt ist, führt dies zu einer Art von informationstechnologischem Pranger, bei dem Anonymität zur Bedrohung bei der Überwachung von konformem Verhalten wird. Zur Konformität mit staatlichen Normen kommt nun die Möglichkeit, höchstpersönliche Motive und Willkür walten zu lassen. Vor diesem Hintergrund sollten wir noch auf einige unliebsame Überraschungen gefaßt sein.

Anzeige

Die Zeitschrift

Datenschutz Nachrichten (DANA)

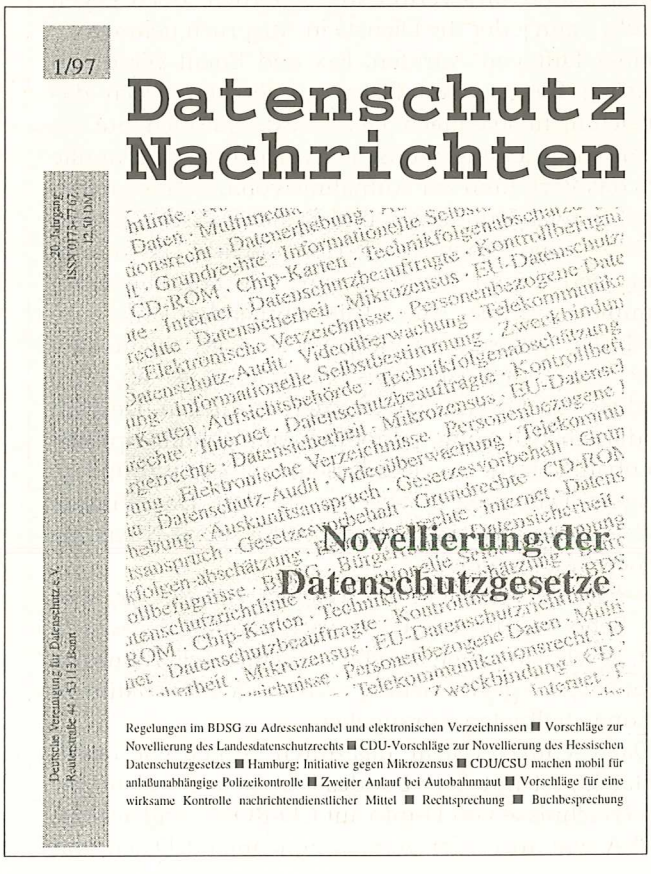
wird herausgegeben von der

Deutschen Vereinigung für Datenschutz

Ziel der DANA und der DVD ist vorrangig, die Bevölkerung über Gefahren und Einsatz elektronischer Datenverarbeitung und der möglichen Einschränkung des Rechts auf informationelle Selbstbestimmung zu beraten und aufzuklären. Neben Aufsätzen und Informationen zu einem Schwerpunktthema berichtet jede Ausgabe der DANA über neue Datenschutzentwicklungen, einschlägige Rechtsprechung und Gesetzgebung, deutsche und internationale Datenschutztrends und bietet Buchbesprechungen sowie Hinweise auf Veröffentlichungen des Bundes- und Landesdatenschutzbeauftragten. Damit ist die DANA auch eine lohnende Lektüre und Arbeitshilfe für behördliche/betriebliche Datenschutzbeauftragte, Personal- und Betriebsräte sowie Rechtsanwälte.

Ein Jahresabonnement der DANA kostet 50,– DM für vier Ausgaben mit je 36 Seiten

Weitere Informationen über
Deutsche Vereinigung für Datenschutz e.V.
Reuterstraße 44 – 53113 Bonn



Nicolas Busch

Geheime „SIRENE“

Garant für Ordnung und Staatssicherheit

Das Schengen Informationssystem (SIS), das polizeiliche Computersystem der Schengen-Staaten, ist wenig mehr als ein Indexsystem im Vergleich mit dem geheimen SIRENE-System für den Austausch „zusätzlicher“ Informationen. Dieser Schluß drängt sich nach der Lektüre des „SIRENE Handbuchs“ auf, eines vertraulichen Dokuments der Schengen-Gruppe. Unter anderem legt das Handbuch spezielle Prozeduren für den Informationsaustausch zwischen Geheimdiensten fest.

Bewegungsfreiheit unter polizeilicher Überwachung

Politiker und Beamten der beteiligten Regierung präsentieren Schengen gern als ein Mittel zur Abschaffung der Grenzkontrollen in Europa und zur Erhöhung der Bewegungsfreiheit von Personen innerhalb Europas. Den Bürgern der Schengen-Staaten soll erlaubt werden, „ohne Ausweis“ von Finnland bis Portugal zu reisen. Der größte Teil des Schengen-Verbundes hat jedoch nur wenig mit der Ausweitung der Bewegungsfreiheit, weit mehr jedoch mit der verstärkten Überwachung von Personen zu tun.

Die 1990 verabschiedete Schengen-Konvention erlaubt nicht nur die extensive Polizeikooperation zur Verfolgung von Straftaten, sondern ebenso die proaktive Überwachung im Interesse der „öffentlichen Ordnung und Sicherheit“ wie auch der „Staatssicherheit“. Dies beinhaltet das Sammeln von Informationen und den umfassenden Datenaustausch über Personen, die keines Verbrechens verdächtigt werden. Der proaktive Charakter und der bemerkenswert weite Umfang von polizeilicher Kooperation und Aktivitäten, die die Schengener Konvention erlaubt, verdeutlichen besonders vier Vorschriften des Vertrags.

Die Konvention erklärt im Artikel 39.1, daß sich die Polizeibehörden der Unterzeichnerstaaten in „Übereinstimmung mit nationalen Regelungen und innerhalb ihrer Zuständigkeiten gegenseitig zum Zweck der Prävention und Entdeckung von Straftaten helfen dürfen, soweit nationales Recht nicht vorschreibt, daß die Anfrage nur an die Justizbehörden zu richten ist und sofern sichergestellt ist, daß die Anfrage oder deren Ausführung nicht die Anwendung von Zwangsmaßnahmen des angefragten Unterzeichnerstaates beinhaltet“. Dies kommt einem Blankoscheck für die „Polizeibehörden“ gleich. Statt des uneingeschränkten Verbots jeder Form von Kooperation und Informationsaustausches, der nicht explizit durch das Gesetz der beteiligten Unterzeichnerstaaten gedeckt ist, werden die „Polizeibehörden“ generell ermächtigt und dazu eingeladen, alles zu tun, was nicht explizit verboten ist. Die Formulierung verweist auch auf eine Machtverschiebung von den Justizbehörden zur Polizei hin. Sie empfiehlt, die Justizbehörden der beteiligten Staaten wo immer möglich aus den gegenseitigen Kontakten zur Verhinderung aund Aufdeckung von Verbrechen herauszuhalten.

Gemäß Artikel 46 der Konvention darf jede Vertragspartei „unabhängig von einer Anfrage der entsprechenden Vertragspartei jede Information übersenden, die für diese von Interesse sein könnte, um Straftaten, Ordnungswidrigkeiten oder Bedrohungen der öffentlichen Sicherheit und Ordnung verhindern zu helfen“. Beide Artikel legen fest, daß Beihilfeersuchen und der Informationsaustausch prinzipiell über eine „für die internationale Polizeikooperation verantwortliche Zentalstelle“ in jedem Schengen-Land abgewickelt werden soll, die darauf achten soll, daß Beihilfeersuchen und Anfragen schnell die zuständigen Stellen erreichen.

SIS: Die Spitze des Eisbergs

Zwar ist das Schengen Informationssystem SIS als gemeinsame Datenbank das bekannteste, aber bei weitem nicht das einzige Instrument zum schnellen Austausch von Informationen zwischen den Schengener Vertragsstaaten.

Das SIS ist sicherlich nicht nur eine Datenbank für Kriminalfälle. Nach Artikel 93 der Konvention ist ihr Zweck, „öffentliche Ordnung und Sicherheit, einschließlich der staatlichen Sicherheit zu erhalten“ und die Regelungen zur Kontrolle von Personen aus Nicht-Schengen-Staaten sowie zur Kontrolle des Aufenthalts von Personen. Obwohl in der Konvention Geheimdienste nicht unter den Behörden genannt werden, die direkten Zugriff auf das SIS haben, legt der Artikel 93 eine starke Rolle dieser Behörden nahe.

„Diskrete Überwachung" für die staatliche Sicherheit

Im Artikel 99.3 der Konvention wird schließlich geregelt, daß „auf Anforderung der Behörden der staatlichen Sicherheit" Berichte über Personen im SIS zum Zwecke „diskreter Überwachung" oder „spezifischer Überprüfungen" gespeichert werden können, sofern „konkrete Anhaltspunkte für den Verdacht vorliegen", daß die dadurch gewonnenen Informationen „notwendig ist für die Verhinderung einer schwerwiegenden Bedrohung durch die entsprechende Person oder andere Bedrohungen der inneren oder äußeren staatlichen Sicherheit". Diese Regelung ist besonders fragwürdig, weil sie eine geheime Registrierung im SIS nicht nur erlaubt, wenn von einer Person ein vermuteter Verdacht ausgeht, sondern auch dann, wenn „andere Bedrohungen" vermutet werden, also solche, die nicht von der entsprechendne Person ausgehen. Auf diese Weise ermöglicht die Schengener Konvention eine annähernd unbeschränkte Erfassung und Überwachung unschuldiger Bürger aus politischen Gründen.

Keine Regelungen über Geheimdienstkooperation

Trotz derartiger Klauseln legt die Konvention keine Regelungen und Prozeduren für die Kooperation von Geheimdiensten und Staatssicherheits-Behörden fest. Der direkte Zugriff auf das SIS oder seine Teile ist explizit auf die Behörden beschränkt, die mit Grenz- und Zollkontrollen innerhalb von Schengenstaaten sowie Polizeilichen Aufgaben betraut sind sowie die Ausländerbehörden. Geheimdiensten und Staatssicherheits-Behörden werden nicht erwähnt.

Überdies wurde ein ursprünglich vorgesehener Abschnitt über die „gegenseitige Unterstützung zwischen den Staatssicherheitsbehörden" kurz vor Unterzeichnung der Konvention 1990 aus dem Vertragstext offenbar deshalb getilgt, um wachsende Bedenken in einigen Ländern zu zerstreuen, daß Schengen zu einer Politischen Polizei jenseits demokratischer Kontrolle führen könnte. Die Streichung des umstrittenen Abschnitts stellt sich nun als rein kosmetische Maßnahme zur Täuschung der Öffentlichkeit heraus.

Dies ist der einzige Schluß, der sich aus dem nun vorliegenden SIRENE Handbuch ergibt.

Das SIRENE Handbuch

SIRENE – für „Supplementary Information Request at the National Entry" also etwa: Zusätzliche Informationsanfrage bei der nationalen Eingabestelle – läßt sich am besten als komplexe, netzwerkartige Struktur für die bi- und multilaterale Polizei- und Sicherheitskooperation zwischen den Schengenländern beschreiben, die die zentralen nationalen Behörden und ein ausgeklügeltes Informationssystem umfaßt, das einen Austausch von „Zusatz"-Daten vor dem Einstellen eines Berichts in das SIS oder dem Verfolgen eines positiven Suchergebnisses erlaubt.

Verglichen mit dem Umfang und der Sensitivität der Informationen, die von den SIRENE-Büros gespeichert und ausgetauscht werden können, ist das SIS wenig mehr als ein Indexsystem. Obwohl die Konvention zur Implementation von Schengen umfangreiche Regeln für das SIS aufstellt, geht sie auch nicht mit einem Wort auf das SIRENE-Netzwerk ein.

Dieser bemerkenswerte Mangel jeglicher rechtlichen Grundlage wurde sogar von der Gemeinsamen Überwachungsstelle (ACC) der Schengenländer bemängelt. Im Februar 1995 bat die ACC die Schengen Zentralgruppe – die machtvolle Runde hoher Beamter, die alle Entscheidungen der Schengen-Minister vorbereitet – „Hinweise auf die von den Vertragsparteien insgesamt oder von ihnen einzeln angestrebten Maßnahmen, die den (SIRENE-) Büros eine angemessene rechtliche Basis geben". Die ACC erwog, daß die Schengenländer – in Ermangelung einer Regelung in der Konvention – „auf einer zentralen Ebene" die erforderlichen Regelungen für die Kompetenzen der SIRENE-Büros in jeweiliges nationales Recht in abgestimmter Weise integrieren sollten. Unseres Wissens haben die Vorschläge der ACC bislang noch zu keiner Reaktion der Zentralgruppe oder des Schengen Exekutivkommitees geführt.

Ein schwer definierbare „unverzichtbare Struktur"

Da die Konvention SIRENE nicht einmal erwähnt, muß man auf das vertrauliche Handbuch zurückgreifen, um zur Wahrheit vorzustoßen. Dort werden die SIRENE-Einrichtungen definiert als eine

- „unverzichtbare Struktur [die französischer Fassung spricht von „Organisation"] für das Funktionieren des Schengen Informationssystem",
- als eine „summarische Beschreibung der Vorgänge", die den Behörden einer Vertragspartei die Übermittlung zusätzlicher Informationen erlauben soll, die die empfangende Partei für die Entscheidung über weitere Schritte nach einem positiven Suchergebnis im SIS benötigt, sowie
- als eine „operationale Organisation".

Ein offizieller Belgischer Bericht von 1994 beschreibt SIRENE zuerst als „die Behörde, die den menschlichen

Vermittler in der Computerstruktur des SIS für die Behandlung der Berichte", später dann als eine „zusätzliche Struktur für die Unterstützung der computergestützten Anwendung".

Ungeachtet der Unklarheiten besteht das SIRENE Netzwerk letztlich aus einem zentralen SIRENE-Büro jeder Vertragspartei und einem Computersystem, das es den SIRENE-Büros erlaubt, Informationen auszutauschen. Die nationalen SIRENE-Büros sind die einzigen Kontaktpunkte zum Austausch von Zusatzinformationen zwischen den Mitgliedsstaaten.

Unterschiede zwischen SIS und SIRENE

Das Handbuch bezieht sich auf Artilkel 108 der Schengen-Konvention als rechtliche Grundlage für SIRENE. Dieser Artikel verpflichtet die Vertragsstaaten jedoch nur dazu, eine zentrale Stelle zu benennen, die für die in der Konvention vorgesehenen nationalen Informationssysteme (N-SIS) verantwortlich ist. Vertreter der Schengen-Organisation haben versucht, die Legitimität des SIRENE-Systems zu rechtfertigen, indem sie es als ein Teil des SIS präsentieren. Diese Interpretation kann jedoch nicht überzeugen. Die SIRENE-Stellen unterscheiden sich von den N-SIS-Behörden deutlich sowohl in ihrer technischen Ausstattung als in ihrem Zweck. Ersteres wird daran deutlich, daß die Daten in den N-SIS-Systemen mit den relativ eingeschränkten Daten identisch sind, die im Straßburger zentralen SIS vorgehalten werden. Letzteres daran, daß ein direkter Datenaustausch zwischen den einzelnen N-SIS, den nationalen Systemen also, in der Konvention nicht gestattet und technisch nicht möglich ist. Im Gegensatz dazu ermöglicht das SIRENE System den direkten und computergestützten Austausch weit umfassender Informationen rund um die Uhr zwischen zwei oder mehr Vertragsparteien, einschließlich der Übermittlung von Textdaten unbegrenzter Länge und unfassender personenbezogener Informationen, die im SIS nicht gespeichert werden dürfen.

Jede andere „nützliche Information"

Überdies ist die Nutzung von SIRENE nicht auf Informationen beschränkt, die im Zusammenhang mit Berichten im SIS stehen. Das Handbuch stellt sogar fest, daß „die SIRENE-Stellen der Vertragsparteien jede nützliche Information austauschen können, die innerhalb der nationalen Grenzen der Anwendung der Artikel 39 und 46 [der Konvention] liegen" (so Kapitel 3.2.1). „Die Kooperation zwischen den Vertragsparteien und Polizeiexperten kann nicht auf die Nutzung nur der Informationen beschränkt bleiben, die im SIS gespeichert sind (...) Das Finden eines Berichts [im SIS] kann die Entdeckung eines Vergehens oder einer schwerwiegenden Bedrohung der öffentlichen Ordnung oder Sicherheit nach sich ziehen. Daher kann es sich als notwendig erweisen, eine Person oder ein Objekt mit Präzision zu identifizieren". Dafür muß der schnelle Austausch von Fotos und Fingerabdrücken möglich sein. Artikel 39 und 46 [der Konvention] ermöglichen dies.

Die Kommunikation zwischen den SIRENE-Stellen umfaßt mündliche und schriftliche Nachrichten ebenso wie Bilder. Nachrichten können als freier oder Standardtext versandt werden, Bilder können Photos oder Fingerabdrücke sein. Texte und Bilder sollen möglichst per E-Mail über das SIRENE-eigene Netzwerk übermittelt werden, Nachrichten dagegen hauptsächlich mündlich per Telefon. Die SIRENE-Stellen sollen auf Informationsanfragen binnen 12 Stunden reagieren. Daher soll die SIRENE-Stelle jeder Vertragspartei über alle zusätzlichen Informationen verfügen, über die sie Berichte an das SIS weitergegeben hat (Kapitel 2.1.3.a des Handbuches). Dies scheint zu implizieren, daß entweder die nationalen SIRENE-Stellen ihre eigenen Register mit den gewünschten Informationen führen oder, daß sie elektronischen Zugang zu entsprechenden Registern der verschiedenen nationalen Behörden haben.

Die die Informationen empfangende SIRENE-Stelle soll die Akten und Nachrichten anderer SIRENE-Stellen entsprechend ihren nationalen Datenschutzregelungen speichern. Diese zusätzlichen Informationen „sollten, wenn möglich, nicht länger auf der SIRENE-Ebene gespeichert werden, sofern der entsprechende SIS-Bericht gelöscht worden ist".

Das Handbuch führt die nationalen Behörden auf, die für die SIRENE-Büros in sechs Schengen-Mitgliedsstaaten verantwortlich sind. Während etwa Belgien ein spezielles Büro, das Belgische SIRENE-Büro, eingerichtet hat, ist das SIRENE-Büro in der Bundesrepublik Teil des Bundeskriminalamtes (BKA). In verschiedenen Mitgliedsstaaten ist die Verantwortung für die SIRENE-Stelle der nationalen Polizei zugeordnet. Portugal hat sie der Abteilung für Fremde und Grenzen (im Innenministerium), Griechenland dem Ministerium für öffentliche Ordnung zugeordnet.

In allen Mitgliedsstaaten operieren die SIRENE-Stellen auf einer im Handbuch als „nationale Arrangements" bezeichneten schmalen Grundlage – also keiner von den Parlamenten abgestimmten gesetzlichen Regelung, sondern lediglich Verordnungen oder ministeriellen Direktiven.

1994: Zugriff durch 63 Behörden

Die Zahl der auf das SIS zugreifenden Behörden – Polizei, Zoll, Justiz, Ausländer- und Staatssicherheitbehörden – betrug 1994 insgesamt 63 Stellen in neun Mitgliedsstaaten (Belgien: 13; Bundesrepublik: 8; Griechenland: 5; Spanien: 6; Frankreich: 7; Italien: 5; Luxemburg: 5; Niederlande: 7; Portugal: 7). Aus diesem Grund setzt sich das Personal in den SIRENE-Stellen aus verschiedenen Behörden zusammen.

Auf der einen Seite betont das Handbuch, daß die SIRENE-Stellen „in den meisten Fällen" nicht mehr als eine formale Anlaufstelle sind, deren Aufgabe in der Hauptsache darauf beschränkt ist, Informationen an die verantwortlichen Stellen weiterzuleiten. Auf der anderen Seite stellt das Handbuch ebenso fest, daß „in anderen Fällen die von den SIRENE-Stellen wahrgenommenen Kompetenzen auf nationaler Ebene definiert werden müssen", was im Abschnitt zu „spezifischen Kompetenzen bei Polizei und Sicherheitsdiensten" (Kapitel 3.2.2. des Handbuchs) ausgeführt wird, in dem zu lesen ist: „In Abschnitt II der Schengen-Konvention werden eine Vielzahl innovativer Vorschriften bei der Kooperation von Polizei und Justiz niedergelegt. Die SIRENE-Stellen bieten eine operative Organisation, die sich in bestimmten Fällen als sehr nützlich erweisen kann, während sie gleichzeitg das Bedürfnis bestimmter Vertragsparteien verringert, verschiedene zusätzliche Strukturen zu etablieren".

Diese Konzeption der SIRENE-Stellen als „operative Organisationen" steht in scharfem Gegensatz zu der im Handbuch an früherer Stelle gegebenen Definition als bessere Poststellen. Darüberhinaus legt die Zahl und Breite der auf das SIS zugreifenden – und damit auch in den Informationsaustausch der SIRENE-Stellen eingebundenen – Behörden nahe, daß die SIRENE-Büros in einer exzellenten Position sind, um schleichend zu einer zwischenbehördlichen Informations- und Koordinationsstelle im breiten Feld der öffentlichen Sicherheit und Ordnung ausgebaut zu werden.

SIRENE und Staatssicherheit

Das Handbuch schreibt auch spezielle Verfahren zur Kooperation von Staatssicherheits- und Geheimdiensten in Fällen vor, bei denen Personen im SIS – gemäß Artikel 99.3 der Konvention – zur beobachtenden Fahndung und „spezifischen Kontrollen" ausgeschrieben sind. Kapitel 4.1.2. des Handbuchs schreibt vor: „Diese sehr sensible Materie benötigt ein spezielles Verfahren, um die Vertraulichkeit bestimmter Informationen zu bewahren. Deshalb ist es ratsam, die Kontakte zwischen Behörden der staatlichen Sicherheit von denen zwischen den SIRENE-Stellen zu trennen." In Fällen der Staatssicherheit sollen die SIRENE-Stellen nur auf die Gesetzmäßigkeit der Konsultationsprozedur achten und die Resultate dokumentieren, während der Austausch zusätzlicher Informationen direkt zwischen den speziellen Behörden der Vertragsparteien abgewickelt wird. Vor dem Einstellen eines Eintrags in das SIS kontaktiert die betreffende Sicherheitsbehörde die der anderen Vertragsparteien. Die betreffenden Dienste tauschen Informationen aus, woraufhin die eine Einstellung veranlassende Stelle die nationale SIRENE-Stelle über das Ergebnis der Konsultation – zum Beispiel Einwände anderer Vertragsparteien – informiert. Die SIRENE-Stelle ihrerseits informiert die anderen SIRENE-Stellen, die ihre Bewertung abgeben können. Erst nach erfolgreicher Konsultation kann eine Einstellung der Daten in das SIS erfolgen.

Dies erlaubt den Schluß, daß die Schengen-Staaten durch das SIRENE-Netzwerk eine organisatorische und technische Struktur geschaffen haben, die einen schnellen Informationsaustausch und Konsultationen zwischen ihren Geheimdiensten über Fragen der „staatlichen Sicherheit" erlauben. Die sehr vage Formulierung der Artikel 46 und 99.3 der Konvention impliziert, daß der Datenaustausch auch solche Personen umfassen wird, die einer Straftat weder schuldig noch überhaupt verdächtigt sind. Diese Kooperation der Geheimdienste nutzt sowohl das SIS als auch ihre „Erweiterung" SIRENE. Der mangelnde Direktzugriff der Geheimdienste auf das SIS und ihre fehlende Repräsentanz in den SIRENE-Büros hat keine praktische Bedeutung, da die Geheimdienste Daten in das SIS einstellen lassen können und über Daten im SIS über die SIRENE-Stellen informiert werden.

Datenschutz eine Illusion

Die abgeschottete SIRENE-Struktur macht jedes Wort über Datenschutz und rechtliche Kontrolle bei der polizeilichen Kooperation der Schengenländer zu Wunschglauben. Welche – nationale oder internationale – Datenschutzbehörde wird das Budget, das Personal und die technische Ausstattung haben, um die Rechtmäßigkeit des andauernden Stroms von Informationen – von Telefonaten bis zu Bilddateien – zu kontrollieren? Wie läßt sich irgendeine Rechtssicherheit herstellen, wenn die Regeln der Verarbeitung, Speicherung und Weitergabe von Daten in allen Schengenstaaten unterschiedlich sind?

Es trifft zu, daß eine Vertragspartei anderen nur dann Daten übermitteln darf, wenn dies ihrem nationalen Recht entspricht. Nach der Übermittlung jedoch werden die Daten nach dem nationalen Recht des Emp-

fängerstaates gespeichert und verarbeitet. Dieser darf korrekterweise die Daten im Prinzip nur für die Zwecke der Anfrage nutzen, Ausnahmen bedürfen der Bestätigung durch den Übermittlerstaat. Doch wie will dieser die Verwendung der Daten im Empfängerstaat effektiv kontrollieren? Gibt es daran überhaupt ein Interesse? Diese Fragen sind umso bedeutsamer, da die Formulierungen der Vorschriften in der Konvention und die Arbeit der SIRENE-Stellen deutlich machen, daß es nicht die Justiz-, sondern die Polizei- und Geheimdienstbehörden sein werden, die die meisten Informationen des Schengen-Verbundes produzieren und kontrollieren.

Schengen, Interpol, Europol: Verlangen nach „Zusatzinformationen"

Die Entstehung von SIRENE zeigt, daß die Errichtung jedes Informationssystems fast automatisch zu einem Zusatzbedarf nach „Zusatzinformation" führt – also Informationen, die in anderen Informationssystemen und Datenbanken zu finden sind. Daher überrascht nicht, daß das SIRENE-Handbuch das Bedürfnis nach „Kooperationsregeln zwischen SIRENE-Büros und den zentralen Interpol-Büros der Vertragparteien" hervorhebt und daß deren Informationsaustausch durch nationale Gesetze geregelt werden soll. Ein Bericht der K.4-Gruppe vom Februar 1996 betont, daß das Europol-Computersystem „oder eher ein Ensemble von Systemen" in einer Weise aufgebaut werden soll, die die „Anbindung mit den nationalen Systemen" erlaubt. Er schlägt weiter vor, „andere nationale und internationale Systeme wie das Schengen Informationssystem und das von Interpol in die Planung einzubeziehen".

Die Weitergabe von Information zieht den Bedarf nach „Zusatzinformationen" nach sich. Wie sowohl Europol als auch SIS/SIRENE zeigen, werden aus Informationssystemen schnell „Ensembles von Systemen", die wiederum schnell mit anderen „Ensembles" verbunden werden, und das nicht nur auf europäischer Ebene.

(Aus dem Englischen übersetzt von Ingo Ruhmann)

Quelle: „Fortress Europe?" Circular Letter, No. 49, December 1996/January 1997

Literatur

SIRENE Manual, Brussels, 28.3.94, SCH/OR.SIS-SIRENE (92) 26, 9 rev, 7 corr, vertraulich (alle Zitate sind Übersetzungen aus dem Dänischen oder Französischen);

Das Schengen Information System und seine Implementation in Belgien, Report des belgischen SIRENE-Büros, Dezember 1994;

Schengen Implementing Convention, 19.6.90;

Liste der Behörden mit direktem Zugriff auf die Daten im Schengen Informationssystem, Comitee d'orientation SIS, Bruxelles, 17.6.94, SCH/OR.SIS (94) 18, 3 rev (auf Französisch);

Decision de l'Autorite de Controle Commune Provisoire: Fondement juridique des bureaux SIRENE et du Manuel SIRENE, Brussels, 22.2.95, SCH/Aut-contr (94) dec. 3 rev.;

The Europol Computer System and Draft of the additional budget for 1996 for the post-Convention phase of Europol, Bericht an den JHA Rat, 12869/95, verabschiedet am 26-27.2.96.

In eigener Sache

Das vom FIfF herausgegebene „Datendschungelbuch. Ein pfiffiger Wegweiser für Ihren persönlichen Datenschutz" ist leider schon seit längerem vergriffen. Doch jetzt ist es als elektronische Version zu haben. Und zwar ist das Heft nun unter

http://www.bawue.de:80/~ernie/index.html

wieder für alle Interessierte verfügbar.

Thilo Weichert

Brauchen wir EUROPOL?

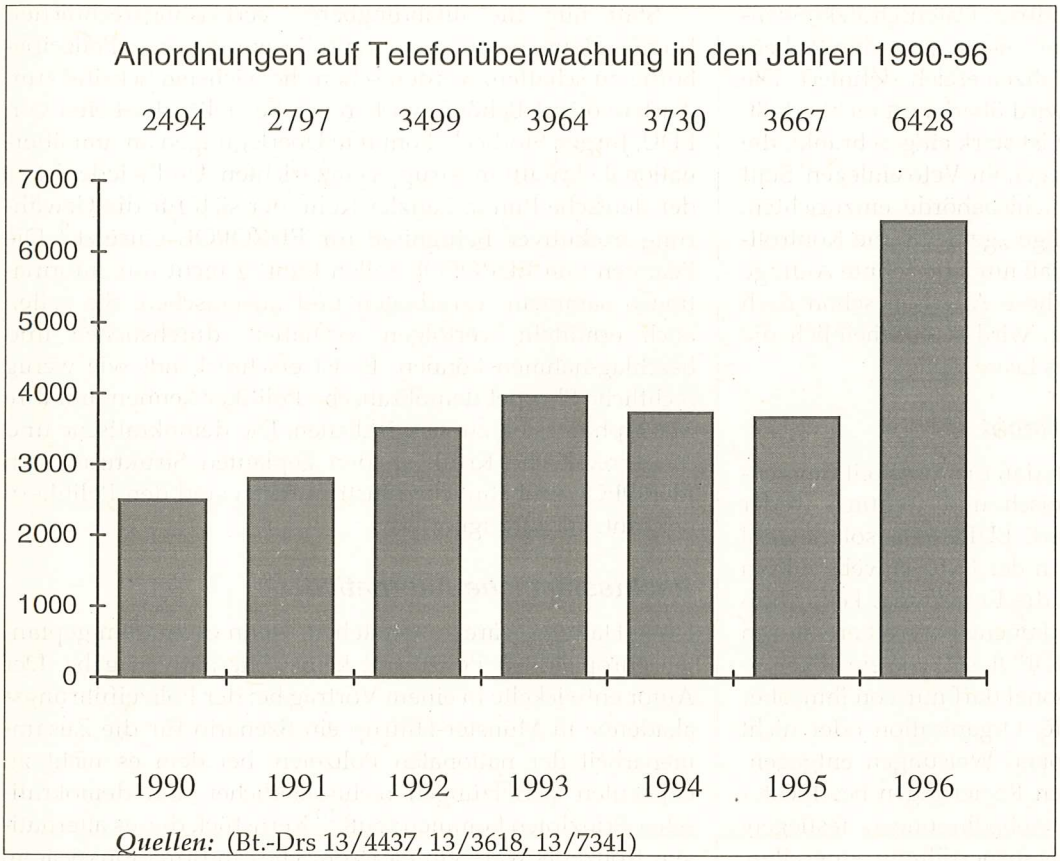
Es ist immer wieder und überall zu hören und zu lesen: Wegen der zunehmenden internationalen Kriminalität benötigt die Polizei für sich neue Befugnisse und neue Institutionen. Schon 1974 kritisierte der für seine unkonventionellen Ideen bekannte, ja berüchtigte Präsident des deutschen Bundeskriminalamtes, Horst Herold, die Dritte-Welt-Länder wären bei der Internationalen Kriminalpolizei-Organisation Interpol ein Klotz am Bein der europäischen Polizeikooperation. Es bedürfe für die europäische Zusammenarbeit der Polizei neuer Strukturen.[1] Ein zentrales europäisches Polizeiamt mußte her. Bundeskanzler Helmut Kohl hatte dann auch Ende der 80er Jahre eine „EG-Bundespolizei" vor Augen, ein „Euro-FBI". Und der damalige Innenminister von Baden-Württemberg, Dietmar Schlee, träumte bereits 1987 von „einer Art Weltpolizei" mit hoheitlichen Befugnissen, zumindest aber von einem „Europäischen Kriminalamt".[2] Im Rahmen der informellen Kooperation der EU-Innen- und Justizministerien unter dem Namen TREVI[3] wurden die Vorarbeiten für die Einrichtung eines europäischen Polizeiinformationssystems zur Ermittlungsunterstützung durchgeführt.[4] Am 7.2.1992 wurde der Vertrag über die Europäische Union (EUV) von Maastricht unterzeichnet. In Art. K.1. Nr. 9 dieses Vertrags wird „zur Verwirklichung der Ziele der Union ... die polizeiliche Zusammenarbeit zur Verhütung und Bekämpfung schwerwiegender Formen der internationalen Kriminalität ... im Rahmen eines Europäischen Polizeiamtes (Europol)" verabredet. Bezüglich des Zieles bestand Einigkeit, nicht aber über die notwendige demokratische und rechtliche Kontrolle dieser Superpolizeibehörde, über Fragen des Schutzes der Beschuldigten im Ermittlungsverfahren oder über die Beachtung der Grundrechte. Es schien zu genügen, daß Art. F EUV ohne nähere Präzisierung die Beachtung der Menschenrechte versprach. 1994 wurde nach mehrmaligen Verzögerungen von den EU-Kern-Staaten in Straßburg das Schengen Informationssystem, die Keimzelle eines europäischen elektronischen Fahndungssystems, in Betrieb genommen. Ohne völkerverträgliche Absicherung, lediglich auf Grund einer Ministervereinbarung (Ministerial Agreement) der EU-Innen- und Justizminister, wurde außerdem Anfang 1994 mit der Arbeit der Europäischen Drogeneinheit (European Drugs Unit – EDU) in Den Haag/NL begonnen. Am 27. Juni 1995 wurden auf dem EU-Gipfel in Cannes die wesentlichen Strukturen der künftigen europäischen Polizeibehörde, von EUROPOL, in einer Konvention festgelegt.[5] Diese Konvention befindet sich derzeit vor den Parlamenten der EU-Mitgliedstaaten im Ratifizierungsverfahren.

Die Tätigkeitsberichte von EDU scheinen beeindruckend. Schon im Jahr 1994 unterstützte EDU 595 Ermittlungsverfahren. 1995 gab es in 1474 Verfahren Ermittlungshilfen durch EDU. Im Jahr 1996 waren es ca. 2000 Fälle, bei denen die inzwischen 120 Bediensteten aus den 15 Mitgliedstaaten von EDU beteiligt waren. Diese Form der Kooperation ist von Anfang an äußerst kostenintensiv: Ohne Berücksichtigung des Europol-Computersystems (TECS – The Europol Computer System) kostete der Betrieb von EUROPOL 1994 schon 4,13 Mio. Mark, mit steigender Tendenz. Für 1997 sind die Kosten der Institution EDU, die formal juristisch eigentlich noch überhaupt nicht existiert, auf 11,2 Mio. Mark angesetzt. Hinsichtlich der Effektivität von EDU ist Skepsis angebracht. Selbst der kommissarische Leiter (Koordinator) Jürgen Storbeck meinte: „Internationale Ermittlungen gegen weltweit oder europaweit agierende Organisationen finden nicht statt. Erfolge wurden gegen solche kriminellen Organisationen als Ganzes oder ihre Chefs trotz aller Erfolgsmeldungen praktisch nie erzielt." Statt aber die Berechtigung der verfolgten EUROPOL-Konzeption aufgrund dieser Erfahrungen in Frage zu stellen, meint Storbeck, seiner zentralen Behörde müßten zusätzliche Ermittlungskompetenzen zugestanden werden.[6] Der Grundstein für eine europäische Superpolizeizentrale ist gelegt. Die symbolische politische Bedeutung dieser Stelle und die in diese gesetzten Erwartungen werden dabei immer größer sein als das, was sie leistet. Das Konzept von EDU/EUROPOL ist auf Expansion von Kompetenzen und Aufwand angelegt. Wer dieses Konzept in Frage stellt, setzt sich dem Vorwurf aus, die internationale Kriminalität zu unterstützen.

Polizeibehörde aus vordemokratischer Zeit?

CDU und SPD sind von der Notwendigkeit EUROPOLs überzeugt. Es ist vor allem die Partei Bündnis 90/Die Grünen, die in den Parlamenten Kritik äußert. Auch die öffentlichen Medien enthalten Lobeshymnen über die europäischen „Kämpfer" gegen die internationale Kriminalität. Kritik kommt lediglich von Datenschutzbeauftragten und Bürgerrechtsorganisationen. Diese Kritiker haben nichts gegen internationale Verbrechensbekämpfung. Sie haben aber wohl etwas gegen eine Polizeibehörde, deren Tätigkeitsbeschreibung an vordemokratische Zeiten erinnert. Die Kritik an EUROPOL und an den damit verbundenen Projekten richtet sich nicht generell gegen Europa, sie ist nicht nationalistisch motiviert. Im Gegenteil: Die Notwendigkeit einer verbesserten europäischen Zusammenarbeit bei der Strafverfolgung ist unumstritten. Diese kann aber nur zugelassen werden, wenn eine ausreichende demokratische und rechtli-

1. Fijnaut, The internationalization of criminal investigation in Western Europe, in: Fijnaut/Hermans, Police Cooperation in Europe, Lochem/NL, 1987, S. 37.
2. Weichert, Europolizei – Die Entfesselung der Exekutive vom Recht, Forum Recht 3/1989, 21.
3. Steht für „terrorisme, radicalisme, extremisme, violence internationale".
4. Busch, Grenzenlose Polizei? Neue Grenzen und polizeiliche Zusammenarbeit, Münster 1995, S. 303 ff.
5. Die Grünen im Europäischen Parlament: Mit EUROPOL grenzenlos sicher? Hearing zu Europol, Bruxelles/Bonn 1995.
6. EDU als EUROPOL-Vorgänger erfolglos? Datenschutznachrichten (DANA) 1/1997, 28 f.



Quellen: (Bt.-Drs 13/4437, 13/3618, 13/7341)

che Legitimation und Kontrolle erfolgt. Und davon kann bei den europäischen Planungen keine Rede sein.

Wer meinte, daß EDU bzw. EUROPOL gegen Wirtschaftskriminelle, z.B. gegen EG-Subventionsbetrüger, gegen internationale Müllschieber oder illegale Waffenhändler eingesetzt würde, der wird enttäuscht. Zunächst ist EDU als EUROPOL-Vorgänger für Drogen-, Schleuser-, Kraftfahrzeug- und Nuklearkriminalität zuständig. Insbesondere die Drogenbekämpfung wird zum Türöffner für die europäische Polizeikooperation benutzt, obwohl sich in allen Staaten auch bei der Polizei immer mehr die Erkenntnis durchsetzt, daß repressive Methoden hier keine Lösung des Problems bringen können. Nicht die tatsächliche Gefährlichkeit der Kriminalitätsbereiche, sondern das Schielen auf hohe gesellschaftliche Akzeptanz war ausschlaggebend für die Auswahl der ersten EDU/EUROPOL-Zuständigkeiten.

Daten, Daten, Daten

Solange einer europäischen Polizeibehörde keine exekutiven Eingriffsmöglichkeiten eingeräumt werden, liegt deren Tätigkeitsschwerpunkt bei der Informationsverarbeitung. Nach der EUROPOL-Konvention werden nicht nur Daten über Straftäter und Verdächtige gesammelt und verarbeitet, sondern auch über sogenannte Risikopersonen, über Personen, denen man Beziehungen zu Kriminellen unterstellt oder von denen man vermutet, daß sie künftig Straftaten begehen könnten. Hinzu kommt die Speicherung der Daten von potentiellen oder tatsächlichen Zeugen, Informanten, Opfern und Kontaktpersonen (Art. 8 I, 10 I). Voraussetzung dieser Speicherung in Analysedateien ist nicht die Einwilligung oder zumindest die Benachrichtigung der Betroffenen. Richterliche oder staatsanwaltliche Anordnungen sind nicht vorgesehen; entscheidend sein sollen die nicht näher zu begründenden polizeilichen Hypothesen. Nicht weniger suspekt ist die mögliche Datenbeschaffung in „Drittstaaten", z.B. bei der türkischen Polizei, oder bei Geheimdiensten (Art. 10 IV Nr. 4, 4 V Nr. 3). Insbesondere in den Analysedateien werden nicht nur „harte" Informationen gesammelt und ausgetauscht, sondern vor allem ungesicherte Verdächtigungen, Hinweise, Spuren, Vermutungen. Zielsetzung ist weniger die konkrete Ermittlungsunterstützung. Mit den Daten sollen Lagebilder über die internationale Kriminalität erstellt werden. Die Nutzung von personenbezogenen Angaben über hochsensible Sachverhalte, die mit einer konkreten Tat nichts zu tun haben, wie sexuelle Neigungen, ethnische Zugehörigkeit oder politische Überzeugung, ist geplant.

Bei EUROPOL sollen die Daten aus allen EU-Ländern zusammengeführt werden, von denen jedes ein eigenes Datenschutzrecht hat. Diese nationalen Regelungen enthalten Festlegungen über Zweckbindung und Verwendungsbeschränkungen, Löschungs- und Sperrvorschriften, Einwilligungs- und Benachrichtigungserfordernisse, Akteneinsichts- und Auskunftsrechte vor allem bei der Datenweitergabe ins Ausland. Derartige strenge Regelungen sind in der EUROPOL-Konvention nicht zu finden. Die Konsequenz: EUROPOL eignet sich vorzüglich als „Datenwaschanlage", mit der nationale Datenschutzvorschriften umgangen werden können. Durch die Abgabe eigener Daten an EUROPOL geht auch die Verantwortung hierüber an die übernationale Organisation über. Selbst wenn bestimmte Formen der Datenverarbeitung nach nationalem Recht unzulässig wären, über den Umweg EUROPOL können die Daten ohne größere rechtlichen Probleme gespeichert, weiterverarbeitet, wieder abgerufen und genutzt werden. Fatal kann dies insbesondere bei der Datenübermittlung durch EUROPOL in Länder außerhalb der EU werden. Unter minimalen Anforderungen dürfen z.B. Informationen über kurdische „Terroristen" an türkische Behörden weitergegeben werden. Die algerische fundamentalistische Regierung kann sich bei EUROPOL über Emigranten aus dem eigenen Land informieren.

Trotz der hohen Sensibilität der zentral verarbeiteten Daten tendiert das Datenschutz-Niveau in der EUROPOL-Konvention gegen Null: Dieses Niveau wird durch den Ver-

weis auf eine nicht direkt anwendbare Datenschutzkonvention des Europarates und eine noch unverbindlichere Datenschutzempfehlung zum Polizeibereich definiert. Die sensible Verarbeitung in Akten wird überhaupt nicht erfaßt. Die Auskunft an die Betroffenen ist stark eingeschränkt, die datenbesitzende Stelle kann dagegen ihr Veto einlegen. Statt eine wirksame Datenschutzaufsichtsbehörde einzurichten, ist zur Kontrolle eine schwerfällige „gemeinsame Kontrollinstanz" vorgesehen. Dadurch, daß nur jede zehnte Anfrage protokolliert werden soll und diese Angaben schon nach sechs Monaten zu löschen sind, wird wahrscheinlich die Datenschutzkontrolle zumeist ins Leere laufen.

Frei schwebend über dem Recht

Nicht weniger problematisch ist, daß die Tätigkeit der zentralen Polizeibehörde demokratisch und rechtlich weder legitimiert noch kontrolliert wird. EUROPOL soll sowohl politisch als auch juristisch frei in der Luft schweben: Kein Staatsanwalt oder Richter leitet die Ermittlung, kein Minister ist verantwortlich, kein Parlament kontrolliert dessen Tätigkeit. Der Direktor von EUROPOL soll wie ein absolutistischer Fürst regieren. Sein Personal darf nur von ihm, aber von „keiner Regierung, Behörde, Organisation oder nicht EUROPOL angehörenden Personen Weisungen entgegennehmen" (Art. 30 I). Ein von den Regierungen beschickter Verwaltungsrat darf nur Rahmenbedingungen festlegen, nicht aber in die konkrete Aufgabenerfüllung eingreifen. Das deutsche Bundesverfassungsgericht hat in seinem „Maastricht"-Urteil klargestellt, daß das deutsche Grundgesetz derartige unkontrollierte und unzureichend legitimierte EU-Institutionen nicht zuläßt.[7] Auch die Rechtskontrolle ist löcherig. Die monatelange Kontroverse über die Zuständigkeit des Europäischen Gerichtshofes für Streitigkeiten zu EUROPOL zwischen den meisten EU-Staaten und Großbritannien verstellt den Blick dafür, daß von EUROPOL betroffene Bürger in keinem Fall das Gericht in Straßburg anrufen können.

Als Zwischenergebnis kann festgehalten werden, daß die Regelungen für die geplante zentrale europäische Polizeibehörde gegen grundlegende rechtsstaatliche und demokratische Prinzipien verstoßen. Die Beachtung von Bürgerrechten und der Anspruch auf ein faires Ermittlungsverfahren sind nicht sichergestellt. Die EUROPOL-Konvention verstößt gegen deutsches Verfassungsrecht.[8] Problematisch ist jedoch, daß das deutsche Verfassungsrecht keine umfassende Vorabkontrolle vor der Ratifizierung ermöglicht. Eine vergleichbare verfassungsrechtliche Kritik ist aus anderen EU-Mitgliedstaaten zu vernehmen. Die EU besteht aus Staaten, die den Menschenrechten, der Demokratie und der Rechtsstaatlichkeit traditionell verpflichtet sind. Die Schaffung von EUROPOL würde einen Bruch mit dieser Tradition darstellen.

Statt nun die unabdingbaren verfassungsrechtlichen Voraussetzungen für eine zentrale europäische Polizeibehörde zu schaffen, werden schon die nächsten Schritte zum Ausbau dieser Behörde vorbereitet. So stellte der Leiter von EDU, Jürgen Storbeck, konkrete Überlegungen an, um übernationale Ermittlungstrupps einzurichten. Und wieder ist es der deutsche Bundeskanzler Kohl, der sich für die Gewährung exekutiver Befugnisse für EUROPOL einsetzt.[9] Die Beamten von EUROPOL sollen künftig nicht nur Informationen sammeln, verarbeiten und austauschen. Sie sollen auch ermitteln, verfolgen, verhaften, durchsuchen und beschlag-nahmen können. Es ist erschreckend, wie wenig rechtliche Skrupel demokratische Politiker kennen, um ihre Machtphantasien zu verwirklichen. Die demokratische und bürgerrechtliche Kritik an den geplanten Strukturen von EUROPOL und ähnlichen Instrumenten sind den Politikern bekannt. Sie wird ignoriert.

Rechtsstaatliche Alternative

Diese Haltung wäre zu verstehen, wenn es zu dem geplanten europäischen Polizeiamt keine Alternativen gäbe. Der Autor entwickelte in einem Vortrag bei der Polizeiführungsakademie in Münster-Hiltrup ein Szenario für die Zusammenarbeit der nationalen Polizeien, bei dem es nicht zu eklatanten Verletzungen rechtsstaatlicher und demokratischer Prinzipien kommen muß.[10] Kernstück dieses alternativen Konzepts wäre ein elektronisches Informationssystem, zu dem die nationalen Strafverfolgungsbehörden automatisierten Zugriff haben. In einer völkerrechtliche Regelung müßte nur die Grundstruktur dieses Informationssystems vereinbart werden. Welche Daten in dem System zur Verfügung gestellt werden und wer auf diese Daten Zugriff nehmen darf, soll aber ausschließlich von der jeweiligen nationalen Polizei nach dem jeweils geltenden nationalen Recht festgelegt werden. Ziel wäre es nicht, riesige Daten-Pools zu schaffen, sondern eine effiziente Vermittlungsstelle für Informationen zu internationalen Verbrechenszusammenhängen aus nationalen Ermittlungsverfahren. Über Indexangaben könnten die Behörden der anderen EU-Staaten zwar feststellen, daß Ermittlungen in einem bestimmten Kriminalitätsbereich stattfinden. Um aber die Ermittlungsergebnisse auszutauschen, müßten die beteiligten nationalen Dienststellen direkt Kontakt miteinander aufnehmen. Dies hätte den Vorteil, daß nicht fernab von der konkreten Ermittlungsarbeit in einem bürokratischen Wasserkopf sachfremde Entscheidungen getroffen würden, sondern daß vielmehr die Ermittler kooperieren, die an den Fakten am nächsten dran sind. Das Modell hätte weitere Vorteile: Durch die flexible Konstruktion des Informationssystems könnte dieses kontinuierlich unter Berücksichtigung der bisherigen Erfahrungen weiterentwickelt werden. Aber auch die Rücknahme problematischer Kooperation wäre leichter möglich. Erweist sich, daß ein Staat die Kooperation zweck- und rechtswidrig mißbraucht, so können diesem die Zugriffsmöglichkeiten wieder entzogen werden. Die Staaten müßten ihre Souveränität für die öffentliche Sicherheit und

7. BVerfG, NJW 1993, 3051 ff.
8. Wächter, Demokratische Steuerung und Kontrolle einer europäischen Polizei, ZRP 1996, 167 ff., Weichert, EUROPOL-Konvention und Datenschutz, DuD 1995, 450 ff.; Zieschang, Der Austausch personenbezogener Daten mittels Europol, ZRP 1996, 427 ff., Lavranos, Datenschutz in Europa, DuD 1996, 405; Di Fabio, Die „Dritte Säule" der Union, DöV 1997, 101; Werner, Schengen und Europol, CR 1997, 34 ff.
9. Focus 50/1996, 42; Der Spiegel 11/1997, 20.
10. Weichert, A Sketch of an entirely different Europol, Fortress Europe? – CL No. 46 August 1996, 10 ff.

Strafverfolgung nicht aufgeben, hätten aber dennoch ein wirksames Instrument der Zusammenarbeit in der Hand. Es bedürfte in jedem der EU-Staaten eines Gesetzes, das den rechtlichen Rahmen für die internationale Zusammenarbeit festlegt. Ein weiterer Vorteil dieses System bestünde darin, daß es sich nicht auf die Staaten der EU beschränken müßte. Internationale kriminelle Verbindungen machen nicht an den Außengrenzen der EU halt. Das vorgeschlagene Informationssystem würde es erlauben, die Verfolgungsbehörden der Herkunftsländer vieler internationaler Straftäter mit einzubeziehen.

Nicht möglich wäre mit dem alternativen Konzept polizeilicher Zusammenarbeit das Lieblingskind der EUROPOL-Planer: die Erstellung von detaillierten Lagebildern über bestimmte Szenen mit Hilfe übernationaler Analysedateien. Eine solche aus England und Holland stammende elektronische Kartierung bestimmter angeblich krimineller Personengruppen ist heute in vielen EU-Staaten selbst auf nationaler Ebene noch nicht üblich. Über Europa soll so den nationalen Polizeien die neue Richtung gewiesen werden. Diese Pläne haben jedoch Schwachstellen: Von vielen Polizeipraktikern wird eine derartige Erfassung von Risikomilieus als viel zu aufwendig und uneffektiv abgelehnt. Entscheidend aber ist, daß diese Methode zwangsläufig zu einer Stigmatisierung und polizeilichen Vorverurteilung gesellschaftlicher Randgruppen führen würde. Ein Verzicht auf derartige polizeiliche Methoden wäre verbunden mit einem Gewinn an gesellschaftlicher Offenheit und Toleranz.

Die derzeit äußerst schwerfälligen nationalen Gesetze zur internationalen Zusammenarbeit der Polizei sollten nicht dazu führen, daß gesetzlose Institutionen geschaffen werden. Solange nicht versucht wurde, die nationalen Regelungen zu verbessern, gibt es keinen Grund, sich durch Schaffung supranationaler Institutionen den Fesseln des nationalen Rechts zu entziehen. Subsidiarität ist ein Grundprinzip der Kooperation in Europa. Erst wenn sich erwiesen hat, daß dezentrale Rezepte nicht greifen, darf nach zentralen Problemlösungen gesucht werden. Von akzeptablen zentralen Lösungen sind wir aber noch weit entfernt, da die Einzelstaaten nicht bereit sind, nationale, teilweise nationalistisch anmutende Vorbehalte zurückzustellen. Voraussetzung für eine zentrale europäische Polizeieinheit wäre es, daß ein klarer Katalog von Straftaten definiert wird, für den diese zuständig ist. Diese Straftaten müssen in allen Mitgliedstaaten verfolgt werden können.[11] Zumindest bezüglich der Ermittlungen der zentralen Einheit bedürfte es einer europäischen Strafprozeßordnung mit staatsanwaltlicher und richterlicher Beteiligung. Ein europäisches Ermittlungsinstrument müßte vom europäischen Parlament politisch und von europäischen Gerichten rechtlich kontrolliert werden können. Weitere Voraussetzungen sind ein – derzeit noch fehlendes – Datenschutzrecht mit einer europäischen Datenschutzkontrolle sowie Informationsrechte zur Sicherung demokratischer Transparenz. Je weiter ein bürokratischer Apparat von den Menschen entfernt ist, desto wichtiger sind Instrumente, die diesen Apparat für die Politik und letztendlich für die Menschen durchschaubar machen. Von diesen demokratischen Selbstverständlichkeiten sind wir noch weit entfernt. Solange diese Selbstverständlichkeiten nicht realisiert sind, solange darf es auch keine zentrale europäische Polizeibehörde geben.

11. Dannecker, Strafrecht in der Europäischen Gemeinschaft, JZ 1996, 879 f.

Anzeige

WECHSEL WIRKUNG

Zeitschrift für
NATURWISSENSCHAFT, TECHNIK
GESELLSCHAFT & PHILOSOPHIE

WECHSELWIRKUNG berichtet über gesellschaftliche Auswirkungen von Naturwissenschaft und Technik.

WECHSELWIRKUNG analysiert die soziale, politische und ökonomische Funktion von Wissenschaft und Technik und zeigt deren Perspektiven und Alternativen auf.

WECHSELWIRKUNG erscheint alle zwei Monate im Buchhandel.

Schwerpunktthemen bisheriger Ausgaben:
- Gentechnik auf dem Vormarsch (Aug.´95)
- Schöne neue Arbeitswelt (Okt.´95)
- Multimediale Visionen (Febr.´96)
- 10 Jahre nach Tschernobyl (April´96)
- Fragwürdige Biomedizin (Juli´96)
- „Künstliche Intelligenz" (Aug.´96)
- Meere und Menschen (Okt.´96)
- Gehirn (Dez.´96)
- Internet (Febr.´97)

Schwerpunktthemen kommender Ausgaben:
- Energie (April ´97)

FIFF

Bestellen Sie mit diesem Coupon
- ☐ ein Probeheft für 3 DM in Briefmarken
- ☐ das aktuelle Heft für 12 DM
- ☐ ein Probeabonnement für 6 Monate für 25 DM

WECHSELWIRKUNG, Rott 53, NL-6294NL Vijlen

Nicolas Busch

EUROPOL
Keine Aussicht auf Löschung sensitiver Daten

Wie ein Papier der derzeitigen Irischen Präsidentschaft der EU-Innen- und Justizminister zeigt, haben die mit der Neufassung von Regeln für die Implementation der sogenannten Analysedaten beschäftigten Vertreter der K.4-Gruppe nicht die Absicht, ihre Pläne eines umfassenden Registers von Personen, die keiner Straftat verdächtigt sind, aufzugeben. Das unsägliche Vokabular der Vorversion nährt den Verdacht, daß die K.4-Bürokraten trotz heftiger Widerstände unter anderem des EU-Parlaments Nebelkerzen zünden wollen, um ihre Pläne durchzusetzen.

Artikel 5 der geplanten Regeln über „besondere personenbezogene Daten" ist trotz des Wortkonvoluts eindeutig: „Die Sammlung personenbezogener Daten allein aus Gründen der Rasse, Religion oder anderer Glaubensüberzeugungen, politischer Meinung, Sexualverhalten oder Gesundheit soll untersagt werden. Derartige Daten dürfen nur gesammelt, gespeichert und verarbeitet werden, wenn sie andere personenbezogene Daten in Analysedateien ergänzen und für den Zweck der Datei absolut notwendig sind". In anderen Worten: Wenn „absolut notwendig", können diese Daten gesammelt werden. Die Einschränkung, daß diese Daten nicht allein um ihrer Willen gespeichert werden dürfen, macht absolut keinen Sinn. Oder sollten wir dies etwa so lesen, daß sensitive personenbezogene Daten – außer Daten über Rasse, Sexualverhalten und politische Meinung – per se von EUROPOL gesammelt und verarbeitet werden dürfen, auch wenn dies für den Zweck einer Analyse nicht „absolut notwendig" ist?

„Genaue" und „absolut notwendige" Daten

Artikel 6 ist ein anderes Beispiel einer Nebelkerze. Der englischen Version des Artikels 6.2 gemäß „sollen personenbezogene Daten in den Analysedateien spezifisch und auf solche Daten beschränkt sein, die absolut notwendig sind". Die deutsche Version ist noch verwirrender. Sie lautet: „Die Speicherung personenbezogener Daten [...] beschränkt sich auf genaue Daten sowie auf unbedingt nötige Daten". Oder anders: unnötige Daten können gespeichert werden, wenn sie „genau" sind und ungenaue Daten, wenn sie „nötig" sind. Sowohl die deutsche als auch die englische Version lassen uns im Unklaren darüber, was mit „absolut nötig" und „genau" oder „spezifische Daten" gemeint ist.

„Genaue" bzw. „spezifische" Daten sind jedoch offensichtlich nicht dasselbe wie faktenbasierte, verifizierte und zuverlässige Informationen. Gemäß Artikel 6.3 sollen in der Tat Daten in den Analysedateien unterschieden werden „in Übereinstimmung mit der Bewertung der Quelle und dem Grad der Genauigkeit oder Zuverlässigkeit der Information. Faktenbasierte Daten sollen von Daten unterschieden werden, die auf Meinungen oder persönlichen Bewertungen beruhen".

Darüberhinaus sollte man beachten, daß viele Typen der zu verarbeitenden Daten – also personenbezogene Daten über Personen, die womöglich Verbrechen in unbestimmter Zukunft begehen werden, Informationen über „Charakterschwächen" oder Lebensstile – sich nicht auf Fakten beziehen, sondern eindeutig auf persönlichen Ansichten beruhen. Können solche Daten ernsthaft als „spezifisch" oder „genau" bezeichnet werden? Eins wird damit deutlich: Der Entwurf verfehlt die für Rechtsdokumente nötigen Mindeststandards der Normenklarheit.

Sechs Kategorien

Die EUROPOL-Konvention sieht für Sammeln, Verarbeiten und Nutzen von personenbezogenen Daten sechs Kategorien von Personen vor:

1. Verdächtige und Überführte einer Straftat (Artikel 10.1.2),
2. Personen, die möglicherweise eine Straftat begehen werden (Artikel 8.1.2),
3. Mögliche zukünftige Zeugen (Artikel 10.1.2),
4. Opfer und mögliche zukünftige Opfer (Artikel 10.1.3),
5. „Kontaktpersonen" und „Begleiter" (Artikel 10.1.4),
6. Auskunftspersonen für die zu untersuchende Straftat (Artikel 10.1.5)

Während die Konvention noch die umfangreichen Kategorien von Personen aufzählt, die registriert werden dürfen, unterläßt sie bemerkenswerterweise die Spezifikation der Personen, die in den Analysedateien gespeichert werden dürfen. Stattdessen sollen diese Fragen in den Umsetzungsregelungen geklärt werden.

Im Gegensatz zu früheren Entwurfsversionen, unterscheiden die Umsetzungsregelungen der Irischen

Präsidentschaft formal zwischen den Kategorien 1 und 2 sowie 3 bis 6, also zwischen (zukünftigen) Beschuldigten und nicht Beschuldigten.

„Lebensstil" und „Charakterzüge"

Der Artikel 3.1. des Entwurfs erlaubt die Sammlung, Speicherung und Verarbeitung von nicht weniger als 52 (!) Typen von Daten über Personen der Kategorien 1 und 2. Diese 52 Datentypen sind unter 11 Kategorien gruppiert, darunter: persönliche Details (15 Datentypen), äußere Erscheinung, Identifikation und Dokumente, Beruf und Fähigkeiten, wirtschaftliche Daten sowie „Verhaltensdaten". Diese beinhalten Daten zu „Lebensstil und -weise" und „Charakterzüge".

Schließlich wird eine Kategorie bezeichnet als „andere Datenbanken, in denen Informationen über die betreffende Person gespeichert sind". Dies bezieht sich auf Datenbanken von EUROPOL, Polizeibehörden, internationalen Organisationen, öffentliche und – höchst bemerkenswert – private Einrichtungen.

Gemäß Artikel 3.2 können alle der genannten Kategorien und Typen von Daten in Bezug auf „Kontakte" und „Begleitpersonen" auf der Basis von Artikel 10.1.4 der EUROPOL-Konvention verarbeitet werden, sofern dies „notwendig" ist und „vorausgesetzt, daß alle Daten relevant sind aus Sichtweise von Kontakten solcher Personen zu [Straftätern und Verdächtigen und möglichen zukünftigen Straftätern]". Zusammengefaßt bedeuten diese Regelungen die ungehinderte Sammlung und Verarbeitung von Daten so gut wie jeder vorstellbaren Art. Diese umfassende Überwachung richtet sich nicht gegen überführte Kriminelle oder Verdächtige, sondern auch gegen im Sinne der Gesetze unschuldige Personen.

Bezüglich der anderen in Artikel 10.1 der EUROPOL-Konvention genannten „anderen Personen" erklärt der Artikel 3.3 des Entwurfs der Implementierungsregelungen, daß die „folgende Information gespeichert werden darf, sofern sie für die Zwecke der Analyse notwendig ist". Der nächste Paragraph sagt jedoch nichts über die Kategorien oder Typen aus, sondern, daß „der Inhalt der entsprechenden Kategorien in einem Nutzerhandbuch spezifiziert wird." Eine Fußnote verrät weiterhin, daß die Expertengruppe rät, ein solches Handbuch zu erstellen, dies „kann jedoch nicht der in Titel VI [des Maastrichter Vertrags] genannten Prozedur unterfallen, da es sich um ein Instrument für Nutzer handelt".

Fazit

Schon früher wurde die Besorgnis darüber geäußert, daß die Typen der in den Analysedateien EUROPOLs zur Verarbeitung zugelassenen Daten nicht in einer abschließenden und eingeschränkten Form in der Konvention definiert werden, der von den Parlamenten der Mitgliedsstaaten zugestimmt werden muß. Stattdessen werden die entsprechenden Regeln in „Implementationsregelungen" festgelegt, die lediglich von den Justiz- bzw. Innenministern auf Vorschlag des EUROPOL Direktoriums einstimmig angenommen werden müssen – unter Ausschluß der Parlamente.

Offenbar glauben die kreativen Beamten der K.4, nicht nur einen Weg zur Umgehung parlamentarischer Kontrolle gefunden zu haben, sondern auch die Zustimmung der Innen- und Justizminister zu den detaillierten Vorschriften über die personenbezogenen Daten in EUROPOLs Analysedateien überflüssig zu machen. Wir können annehmen, daß die K.4-Expertengruppe nie gewagt hätte, einen derartigen Vorschlag zu unterbreiten, ginge sie nicht von der stillschweigenden Zustimmung der Innen- und Justizminister aus. So verwundert nicht, daß unserer Kenntnis nach nicht ein einziger Innen- oder Justizminister auch nur eines EU-Mitgliedsstaates der umfassenden Speicherung personenbezogener Daten in den Analysedateien EUROPOLs widerspricht. Einige Minister fanden es jedoch belastend, eine derartige Haltung in der Öffentlichkeit zu vertreten. Einige Minister mögen darauf spekulieren, sich eine unliebsame öffentliche Debatte zu ersparen, wenn die kontroversesten Aspekte einer Speicherung personenbezogener Daten weder in der Konvention noch in den Implementierungsregularien enthalten sind, sondern in einem internen Handbuch, das ihrer Zustimmung nicht bedarf.

Der von den K.4-Experten genutzte Begriff „Handbuch" legt nahe, daß dessen Inhalt genau wie schon eine Reihe anderer Handbücher – zur Kontrolle der Außengrenzen, Visapolitik und SIS/SIRENE – geheimgehalten werden wird.

Es ist zu erwarten, daß wie üblich die Ratspräsidentschaft und die Innen- und Justizminister der Mitgliedsstaaten parlamentarische und öffentliche Beunruhigung über den Entwurf der Implementierungsregelungen dadurch zu entkräften suchen, daß ein solcher Entwurf nicht mehr als ein Arbeitspapier darstelle, das umfangreiche Änderungen durchlaufen wird, bevor ihm der Rat zustimmt. Kritiker wird dies hoffentlich nicht von der Tatsache ablenken, daß sowohl der Rat als auch die K.4-Bürokraten entschlossen sind, eine umfassende Polizeiüberwachung unschuldiger Bürgerinnen und Bürger zu erlauben – außerhalb parlamentarischer Kontrolle und politischer Verantwortung. Jetzt – vor der Ratifizierung der EUROPOL-Konvention – ist die Zeit zu handeln.

(Aus dem Englischen übersetzt von Ingo Ruhmann)

Quellen: Proposal for rules applicable to analysis files, Council Presidency, Brussels, 25.6.96, 4038/3/96 Rev 3, limite, EUROPOL 2, Englische und Deutsche Version; Plattform Fortress Europe No.39, p.1, No.41, p.1.

Professor Dr. Alexander Roßnagel

Globale Datennetze
Ohnmacht des Staates – Selbstschutz der Bürger

Thesen zur Änderung der Staatsaufgaben in einer „civil information society"

Weltweit offene Netze schaffen neue Herausforderungen für Staat und Recht. Beide sind nicht mehr in der Lage, im neuen immateriellen Sozialraum der Netze Gemeinwohlbelange durchzusetzen und die Bürger zu schützen. Zugleich aber bieten moderne Informationstechniken jedem vielfältige Möglichkeiten, sich selbst zu schützen. Unter diesen Umständen wandelt sich die Erfüllungsverantwortung des Staates zu einer Strukturverantwortung. Er wird seiner Schutzpflicht gerecht, wenn er Strukturen schafft, die seine Bürger befähigen, ihre Interessen in der Welt der Netze selbstbestimmt zu schützen.

I. Weltweite offene Datennetze

Datennetze wie das Internet verbreiten sich mit extrem hohen Wachstumsraten über den gesamten Globus. Von den bisher bekannten Netzen wie dem Telefon- oder dem Telexnetz unterscheiden sie sich durch spezifische techniksystemische Charakteristika. Das Internet ist aus dem militärischen ARPA-Net hervorgegangen. Das US-Verteidigungsministerium wollte mit ihm ein Datennetz entwickeln, das auch nach Atomschlägen noch funktioniert. Es wurde daher als ein dezentrales, von einer zentralen Administration unabhängiges Vermittlungsnetz konzipiert. Mit Hilfe eines weltweit gleichen Adressierungschemas und eines sehr einfachen Übertragungs- und Vermittlungsprotokolls (TCP/IP) kann sich im Internet jedes Nachrichten-Paket selbst seinen Weg von Vermittlungsrechner zu Vermittlungsrechner bis zum Zielrechner suchen. Tritt irgendwo eine Störung auf, wird die Nachricht über andere Knoten umgeleitet. Das Netz wird erweitert, indem sich ein Interessent mit seinem Rechner an einen der bestehenden Millionen Knoten anhängt. Als „Netz der Netze" stellt das Internet global Verbindungen zwischen unübersehbar vielen lokalen und regionalen Netzen her.

Seine hohe Attraktivität verdankt das Internet zum einen den in ihm angebotenen Anwendungen wie der elektronischen Post, dem Arbeiten auf fremden Rechnern, dem Fernkopieren von Daten und Software, elektronischen schwarzen Brettern und global vernetzten Informationsangeboten wie „World Wide Web". Zum anderen ist hierfür der über die Telefonleitung jedem mögliche Zugang zum Netz und seine durch grafische Oberflächen inzwischen einfache Nutzung verantwortlich. Als globales Netz verknüpft es über mehr als hundert Staaten hinweg etwa 50 Mio. Arbeitsplätze und Haushalte. In ihm sollen sich elektronische Marktplätze, elektronischer Zahlungsverkehr und elektronische Verwaltungskontakte entwickeln. Mit ihnen verbinden sich große Hoffnungen auf neue Märkte, neue Arbeitsplätze, umweltverträgliches Wirtschaftswachstum, unbeschränkte Informationsfreiheiten und Stärkung demokratischer Willensbildung. Weltweite offene Netze erzeugen aber auch neue Herausforderungen für die rechtliche Ordnung.

II. Entwurf eines Multimedia-Gesetzes

Ihnen versucht die Bundesregierung gerecht zu werden. Das Bundesforschungsministerium hat hierzu den Referentenentwurf eines „Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG)" vorgelegt. Er verfolgt zum einen das Ziel, Netzanwendungen zu fördern. Er behandelt die neuen Informations- und Kommunikationsdienste, die eine individuelle Übermittlung von kombinierten Daten ermöglichen nicht als Rundfunk. Sie sollen daher keiner Anmeldung oder Zulassung bedürfen. Die Anbieter solcher Teledienste sollen nicht für fremde Inhalte, die sie zur Nutzung bereithalten, verantwortlich sein, es sei denn, sie sind ihnen bekannt und sie können ihre technische Verbreitung verhindern. Als Rahmengesetz soll es mehrere bestehende Gesetze an die neuen Sachverhalte anpassen – etwa das Strafgesetzbuch, das Gesetz über die Verbreitung jugendgefährdender Schriften, das Urheberrechtsgesetz und das Preisauszeichnungsgesetz.

Der Schwerpunkt des Entwurfes sind zwei eigenständige Regelungskomplexe, die die neuen Anwendungen ermöglichen und absichern sollen.[1] Der erste betrifft den spezifischen Datenschutz. Das Gesetz verpflichtet die Anbieter zu Datensparsamkeit. Sie haben ihre technischen Einrichtungen für die Inanspruchnahme von Telediensten so auszuwählen und zu gestalten, daß möglichst keine personenbezogene Daten zu erheben und zu verarbeiten sind. Außerdem haben sie im Rahmen ihrer Möglichkeiten anonyme oder pseudonyme Nutzungs- und Bezahlungsformen anzubieten. Die Datenerhebung und -verarbeitung setzt grundsätzlich eine Einwilligung voraus, die auch elektronisch erklärt werden kann.

Der zweite eigenständige Regelungskomplex betrifft die Rechtssicherheit des elektronischen Rechtsverkehrs.[2] Um sie zu ermöglichen, schafft der Entwurf Rahmenbedingungen für die Sicherungsinfrastruktur für digitale Signaturen.[3] Der Entwurf enthält Anforderungen an die Technik, sieht ein Lizenzierungsverfahren für Zertifizierungsinstanzen vor, bestimmt deren Betreiberpflichten und regelt die Kontrollmöglichkeiten der Regulierungsbehörde. Details sollen einer gesonderten Verordnung überlassen werden.

1. S. zu ihnen auch provet, Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online-Multimedia-Anwendungen, Gutachten für den BMBF, 1996.
2. S. zu diesem Roßnagel, NJW-CoR 1994, 96 ff.; Alcatel SEL Stiftung, Rechtverbindliche Telekooperation, 1996.
3. S. hierzu Hammer (Hrsg.), Sicherungsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht, 1995.

Dieser Entwurf enthält Aspekte eines neuen Ansatzes, Persönlichkeitsrechte in einer global vernetzten Informationsgesellschaft zu schützen. Er bietet sich daher als Bezugspunkt an, über die Schutzaufgaben von Staat und Recht in einer multimedial vernetzten Welt nachzudenken.

III. Neue Herausforderungen

In der neuen Welt der Netze sind Staat und Recht mit der Aufgabe, ihre Bürger zu schützen, überfordert. Sie sind als Nationalstaat und Nationalrecht konzipiert, basieren auf national ausgerichteter Demokratie. In der Netzwelt wird sich der demokratische Rechtsstaat an Ohnmachtserfahrungen gewöhnen müssen.

1. Ohnmachtserfahrungen des Staates

Globale Datennetze sind von ihm nicht mehr zu kontrollieren. Sie erlauben jedem, sich allgemeinverbindlichen Vorgaben zu entziehen. In einem weltweiten, dezentral organisierten Netz wie dem Internet sind gezielt steuernde Eingriffe eines Nationalstaates ohne durchschlagenden Erfolg.[4] Zum einen gibt es keinen zentralen Betreiber, sondern Millionen. Diese sind für das Netzgeschehen kaum verantwortlich zu machen.[5] Zum anderen würden diejenigen, gegen deren Interessen der Eingriff wirkt, vielfältige Möglichkeiten finden, – etwa durch Umleitungen über andere Knoten[6] oder durch Verschleierung ihrer Identität[7] – den Eingriff zu konterkarieren. Niemand weiß, wer und wieviele am Internet teilnehmen und was diese tun – auch kein Nachrichtendienst und keine Polizei.[8]

Versuchen diese einen bestimmten Teilnehmer zu beobachten, kann der sich der Kontrolle entziehen. Er kann seine Nachrichten über einen Anonymisierungsrechner schicken und damit ihren Ursprung verschleiern.[9] Er kann seine Nachrichten verschlüsseln und so gegen Kenntnisnahme schützen. Selbst wenn sie aufgezeichnet werden, bleibt ihr Inhalt den Behörden verschlossen. Ein Verbot der Verschlüsselung ist sinnlos. Wer seine Kommunikationsinhalte verbergen will, wird über starke Verschlüsselungsverfahren verfügen. Von irgendwo auf der Welt kann er sie immer beziehen. Ein Verbot wäre auch nicht vollziehbar. Denn über das Internet sind Steganografie-Programme kostenlos zu erhalten. Mit ihrer Hilfe können Nachrichten in anderen Nachrichten so verborgen werden, daß sie nicht zu erkennen sind – beispielsweise in bestimmten Farbpixeln eines Bilddokuments oder in den Hintergrundgeräuschen eines Telefongesprächs.[10]

Der demokratische Rechtsstaat muß feststellen, daß er viele Gesetze, die er aufstellt, in den Netzen nicht vollziehen kann. Er kann weder Gemeinwohlbelange durchsetzen noch seinen Bürgern Schutz gewähren:

Zielsetzungen etwa der Außenhandelskontrolle oder des Datenschutzes werden bei länderübergreifender Datenübermittlung obsolet. Im Netz gibt es keine Grenzkontrollen. Exportverbote sind ebensowenig durchsetzbar wie Zweckbegrenzungen oder Löschungsgebote für die Verarbeitung personenbezogener Daten.[11]

Im Gegenteil: Jede Aktion im Netz hinterläßt Datenspuren, die zum Verursacher zurückverfolgt werden können.[12] Dies eröffnet die Möglichkeit, Kommunikationsprofile zu erstellen. Die informationelle und kommunikative Selbstbestimmung können im Internet nicht gewährleistet werden.

Das gleiche gilt für den Schutz der Privatsphäre und aller rechtlich geschützten Geheimnisse. Alle Inhalte sind für alle am Transport elektronischer Nachrichten Beteiligten einsehbar:[13] sie entsprechen einer für jeden lesbaren Postkarte. Mit speziellen Programmen, „Packet Sniffern", kann im ganzen Netz gezielt nach interessanten Daten wie Paßwörtern oder Kreditkartennummern gesucht werden.[14] Übertragene Nachrichten können verändert, gefälscht, verzögert, wiedereingespielt oder unterdrückt werden.[15]

Im Netz herrscht keine Rechtssicherheit. Elektronische Willenserklärungen können jederzeit spurenlos verändert werden. Die Identität des Erklärenden läßt sich nicht überprüfen, die Willenserklärungen ihm nicht beweisgeeignet zuordnen. Zu leicht kann die Identität eines anderen vorgetäuscht werden.[16]

Inhaltskontrollen sind im Netz kaum durchsetzbar.[17] Erfolgt die Kommunikation international, entschwindet sie dem nationalen Einflußbereich. Gewaltverherrlichung[18], Pornographie[19], unlauterem Wettbewerb, Urheberrechts[20]- oder Ehrverletzungen kann der Staat nicht wirkungsvoll entgegentreten. Wenn er irgendwo eine Information unterdrückt, wird sie weltweit in vielen anderen Servern „gespiegelt".[21] Wenn er Kommunikationswege sperrt, sucht sich die Nachricht einen Umweg. Auch durch Satellitenübertragung wird die Standortfrage nahezu irrelevant.[22] Theresa Orlowski wurde hier die Lizenz für ihren Pornokanal verweigert. Jetzt sendet sie aus Großbritannien. Aufgaben von gesellschaftlichem Interesse, wie zum Beispiel der Jugendschutz, können in der Netzwelt nicht mehr vom Staat wahrgenommen werden. Sie werden ausschließlich auf die Eltern verlagert.[23]

4. S. z.B. auch Hoffmann-Riem, in: Kubicek/Müller/Neumann/Raubold/Roßnagel (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft 1995: Multimedia – Technik sucht Anwendung, 1995, 106; Guéhenno, Das Ende der Demokratie, 1994, 26 ff.
5. S. z.B. Jäger/Collardin, CR 1996, 236 ff.
6. S. z.B. „Bombt Deutschland", Der Spiegel 2/1996, 108.
7. S. hierzu Damker/Federrath/Schneider, DuD 1996, 286 ff.
8. S. z.B. Kleinsteuber, Wechselwirkung, Dezember 1994, 25.
9. S. hierzu z.B. „Netzbeschmutzer ausgeklinkt", Die Zeit 4/1996, 16.
10. S. z.B. Huhn/Pfitzmann, DuD 1996, 23 ff.
11. Datenexporte zur Umgehung von Datenschutzanforderungen sind zwar nach Art. 25 der EG-Datenschutzrichtlinie verboten. Wer aber will dies kontrollieren?
12. Die Standard-Software eines WWW-Servers protokolliert automatisch jeden Zugriff mit Rechneradresse, Datum, Zeitpunkt, Aktion und Zugriffsobjekt.
13. S. z.B. Schallbruch, Datenschutznachrichten 5/1995, 12.
14. S. hierzu z.B. Schaar, CR 1996, 172; Fuhrberg, KES 6/1995, 43.
15. S. z.B. Fuhrberg, KES 6/1995, 43.
16. S. hierzu näher Roßnagel, Die Infrastruktur sicherer und verbindlicher Telekooperation, Gutachten für die Friedrich-Ebert-Stiftung, 1996.
17. S. z.B. auch van Haaren, in: Kubicek/Müller/Neumann/Raubold/Roßnagel (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft 1995: Multimedia – Technik sucht Anwendung, 1995, S. 68.
18. S. z.B. „Schweinkram drauf", Der Spiegel 7/1996, 157f.
19. S. z.B. „Bombt Deutschland", Der Spiegel 2/1996, 106.
20. S. z.B. „Raubkopie im Internet", NJW 9/1996, XLV.
21. S. z.B. „Schweinkram drauf", Der Spiegel 7/1996, 157f.
22. S. Zweites Deutsches Fernsehen, Das ZDF vor den Herausforderungen des digitalen Fernsehens, ZDF-Schriftenreihe, Heft 48, 1994, S. 21; Eberle, in: Becker (Hrsg.), FS f. Kreile, 1994, S. 169.
23. S. z.B. Zweites Deutsches Fernsehen (o. Fußn. 23), S. 21 ff.

Neue Risiken entstehen für den Schutz der Persönlichkeit: Personenbezogene Daten können leicht von einem Medium in ein anderes übertragen werden. Ein Interview kann als Text, ein Text als Rede erscheinen. Alle Medien können einfach manipuliert, Bild- und Sprachaufnahmen etwa in nicht erkennbarer Weise verändert werden. Simulationen ermöglichen, künstliche Realitäten zu schaffen und Personen in diese einzufügen. Schein und Wirklichkeit verschwimmen im Netz. Wer soll den Wirklichkeitsgehalt von Informationen gewährleisten?

Der Staat kann nur da eingreifen, wo die immaterielle Welt des Netzes in die körperliche Welt übergeht: Er kann Täter festnehmen, Geräte und Datenträger beschlagnahmen, wenn diese sich körperlich in seinem Herrschaftsbereich befinden. Er kann die Befolgung seiner Gesetze erzwingen, wo er seine Zwangsgewalt körperlich ausüben kann. In der körperlosen Netzwelt aber ist er weitgehend machtlos.

Alle diese Beispiele verweisen auf einen neuen Tatbestand: Die Netze konstituieren einen neuen körperlosen Sozialraum. Auf diesen werden zunehmend mehr soziale Kontakte, wirtschaftlicher Austausch und rechtlicher Verkehr übertragen. In ihm herrschen andere Bedingungen als in den Sozialbeziehungen der körperlichen Welt. In dieser neuen Welt hat der Staat keine Zwangsmittel, kein Gewaltmonopol und keine Souveränität.

2. Gefährdung von Rechtsstaat und Demokratie

Recht bedarf zur Durchsetzung der Macht. Der demokratische Rechtsstaat ist auf Hoheitsgewalt und Gesetzesgehorsam angewiesen. Nur durch sie kann er demokratische Beschlüsse allgemeinverbindlich durchsetzen und die Grundrechte der Bürger gegen Übergriffe Dritter schützen.[24] Dies zu gewährleisten, ist der fundamentale Zweck, um dessentwillen der moderne Staat besteht.[25] Sein Schutzauftrag gilt weiterhin. Er hat sich aber mit der zivilisatorischen Entwicklung erweitert. Während bei Hobbes der Schutz von Leib und Leben im Vordergrund stand, kamen bei Locke der Schutz von Freiheit und Eigentum hinzu, und in diesem Jahrhundert angesichts neuer Gefährdungen auch der Schutz der Persönlichkeit.[26] Heute erstreckt sich die staatliche Schutzpflicht auf die Schutzgüter aller Grundrechte.[27]

Die Durchsetzungsmacht der Staaten aber ist auf die Gebietshoheit in dem körperlichen Raum ihrer Staatsgebiete beschränkt.[28] Ihre Hoheitsgewalt gründet auf der Macht, als einzige in diesem Raum legitime körperliche Gewalt auszuüben. Diese Hoheitsgewalt stößt im immateriellen Raum globaler Netze an Grenzen.

Wenn der Bürger aber in der Sonderwelt der Netze vom Staat keinen Schutz mehr erfährt und der Staat dort keine Gemeinwohlbelange mehr durchsetzen kann, ist insoweit seine Basislegitimation gefährdet.[29] Nach Thomas Hobbes kann „die Verpflichtung der Bürger gegen den Oberherrn ... nur so lange dauern, als dieser imstande ist, die Bürger zu schützen."[30] Mit dem Grund für die Gehorsamspflicht der Bürger entfällt aber auch die Möglichkeit demokratischer Einflußnahme auf die gesellschaftliche Entwicklung. Können demokratische Entscheidungen nicht mehr durchgesetzt werden, ist auch die gesamte Konstruktion des Rechtsstaats, der Gleichheit und Allgemeinheit der Gesetze in dieser Sonderwelt gefährdet.

IV. Neue Lösungen

Wo sind Lösungen zu suchen? Der Schutz von Individual- und Gemeinwohlinteressen allein durch Ge- und Verbote wird in der immateriellen Welt der Netze weitgehend obsolet. Die rein normativ orientierte Strategie ist durch einen neuen Ansatz zu ersetzen: dieser ist gekennzeichnet durch ein neues Verständnis der Staatsaufgaben und durch die Strategie der rechtlichen Technikgestaltung.[31]

1. Rechtliche Technikgestaltung

- Selbstschutz
  Wenn der demokratische Rechtsstaat seine Bürger im neuen Sozialraum der Netze nicht mehr zuverlässig schützen kann, muß er sie zum Ausgleich zum Selbstschutz befähigen.[32] Er muß sie stark machen, eigene Instrumente zu ihrem Schutz selbstbestimmt einsetzen. Er muß den Einzelnen gegen die steigenden Kontroll- und Steuerungsmöglichkeiten von Großorganisationen handlungsfähig machen.[33] Hierfür bieten die Informations- und Kommunikationstechniken vielfältige Möglichkeiten:

  - Verschlüsselung[34] und Steganografie[35] ermöglichen jedem, die Vertraulichkeit seiner Nachrichten und Speicher zu sichern und seine rechtlich anerkannten Geheimnisse zu schützen.

  - Digitale Signaturen schaffen Rechtssicherheit im Netz. Sie bieten jedem die Möglichkeit, Verfälschungen zu erkennen und die Zuordnung einer Nachricht zu einer Person nachzuweisen.[36]

  - Pseudonyme ermöglichen jedem, seine Teleüberweisungen, Teleeinkäufe, Telebuchungen, Teleberatungen und Informationsnachfragen ohne rückverfolgbare

24. S. hierzu z.B. Kant, Über den Gemeinspruch: Das mag in der Theorie richtig sein, taugt aber nicht für die Praxis, 1793, A 232 ff., in: ders., Werke (hg. v. Weischedel), Bd. VI, 1964, S. 143 ff., s. auch Isensee, Staat und Verfassung, Handbuch des Staatsrechts, Band I, 1987, 622f.
25. Hobbes, Leviathan, deutsche Übersetzung von J. P. Mayer, Stuttgart 1980, S. 193: „Friede und Schutz (sind) der allgemeine Endzweck bei der Errichtung eines Staates"; s. auch S. 119, 155f., 160, 195 ff.; Isensee, Das Grundrecht als Abwehrrecht und staatliche Schutzpflicht, Handbuch des Staatsrechts, Band V, 1992, S. 157f., 162, 186f.
26. S. z.B. Isensee (o. Fußn. 25), S. 623; Isensee (o. Fußn. 26), S. 198f.
27. S. z.B. Alexy, Theorie der Grundrechte, 1985, 410, 420f.; Isensee (o. Fußn. 26), S. 187.
28. S. z.B. Vitzthum, Staatsgebiet, Handbuch des Staatsrechts, Band I, 1987, 713 ff.
29. S. z.B. Robbers, Sicherheit als Menschenrecht, 1987, 34, 42.
30. Hobbes (o. Fußn. 26), S. 197.
31. S. hierzu Roßnagel, Rechtswissenschaftliche Technikfolgenforschung, 1993, S. 241 ff.
32. S. zum technischen Selbstschutz z.B. auch Roßnagel/Wedde/Hammer/Pordesch, Digitalisierung der Grundrechte? 1990, S. 240 ff., 297f. Roßnagel (o. Fußn. 32), S. 152 ff., 224 ff.; Roßnagel, in: Wolfinger, (Hrsg.), Innovationen bei Rechen- und Kommunikationssystemen, 24. Jahrestagung der Gesellschaft für Informatik im Rahmen des 13th World Computer Congress, 1994, 267 ff.
33. Roßnagel, in: Nickel/Roßnagel/Schlink (Hrsg.), Die Freiheit und die Macht – Wissenschaft im Ernstfall –, FS für Podlech, 1994, S. 240 ff.
34. S. Zimmermann, PGP – Pretty Good Privacy, 2. Aufl. 1994; Grimm, DuD 1996, 27 ff.
35. S. Huhn/Pfitzmann, DuD 1996, 23 ff.
36. S. hierzu provet/GMD, Die Simulationsstudie Rechtspflege, 1994, 54 ff.; Roßnagel (o. Fußn. 17).

Datenspuren, aber dennoch rechtssicher abzuwikkeln.[37]

- Certified Electronic Mail ermöglicht, den elektronischen Zugang einer Nachricht nachzuweisen, ohne einen Dritten einschalten zu müssen, der die Daten dieses Vorgangs speichert.[38]
- Mit Programmen wie Ecash oder CAFE können elektronische Geldscheine und Geldbörsen realisiert werden, die – wie bei Bargeld – einen sicheren und anonymen Zahlungsverkehr ermöglichen.[39]
- Agentenprogramme wie General Magic können Informationen im Netz sammeln und Aufträge wie das Buchen eines Tickets ausführen, ohne daß dabei personenbezogene Verbindungsdaten ihres Besitzer entstehen.[40]
- Mit Erreichbarkeitsmanagementprogrammen kann jeder seine kommunikative Selbstbestimmung durch die technikunterstützte Vereinbarung von Telekommunikationswünschen unterstützen.[41]
- Mobilfunk ohne Bewegungsprofile ist möglich, wenn der eigene Computer zu Hause die Aufenthaltsdaten verwaltet und der Netzbetreiber sie nicht zu kennen braucht.[42]
- Mit Programmen wie Watch Patrol können Eltern verhindern, daß Jugendliche Zugriff auf gefährdende Informationsangebote erhalten.
- Mit Sicherheitsmanagementprogrammen können alle diese Selbstschutzmöglichkeiten unterstützt und leicht bedienbar zur Verfügung gestellt werden. Statt im Netz, ist die „Intelligenz" im Endgerät.
- Und diese Endgeräte können leistungsfähige, vertrauenswürdige portable Benutzerendgeräte sein, die manipulationsresistent und teilnehmerkontrollierbar sind.[43] Auf ihnen können die Daten des Benutzers gespeichert werden und machen es in vielen Fällen überflüssig, sie im Netz oder auf fremden Rechnern verfügbar zu halten.

37. S. hierzu Roßnagel/Wedde/Hammer/Pordesch (o. Fußn. 33), S. 240 ff., 297f.; Roßnagel (o. Fußn. 32), S. 152 ff., 225 ff.
38. S. z.B. Bahreman/Tygar, Certified Electronic Mail, Proceedings of the Internet Society Symposium on Network and Distributed System Security, 1994, S. 3 ff.
39. S. hierzu z.B. Grimm, in: GMD (Hrsg.), 6. GMD-SmartCard-Workshop, Darmstadt 1996; Chaum, Scientific America, August 1992, 96; Weber et al., Secure International Payment and Information Transfer. Towards a Multi-Currency Electronic Wallet, 1995.
40. S. hierzu z.B. Römer/Quendt/Stenz, c't 3/1996, 156 ff.
41. S. hierzu z.B. Hammer/Pordesch/Roßnagel/Schneider, Vorlaufende Gestaltung von Telekooperationstechnik – am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft, GMD-Studien Nr. 235, 1994; Schneider/Sarbinowski, GMD-Spiegel 4/93, 62 ff.; Bertsch/Damker/Federrath, it+ti 4/1996.
42. S. z.B. Pfitzmann, DuD 1993, 451 ff.; Hetschold, Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformationen im Gewahrsam des Endbenutzers unter Erhaltung der GSM-Funktionalität eines Funknetzes, GMD-Studien Nr. 222, 1993; Federrath/Jerichow/Kesdogan/Pfitzmann/Spaniol, it+ti 4/1996.
43. S. hierzu z.B. Pfitzmann/Pfitzmann/Schunter/Waidner, in: Brüggemann/Gerhardt-Häckl (Hrsg.), Verläßliche IT-Systeme, Proceedings der VIS'95, 1995, S. 329 ff.

Techniken dieser Art bilden die Basistechnologie des Bürgerschutzes in der Informationsgesellschaft. Sie ermöglichen einen teilnehmerkontrollierbaren Selbtsschutz. Sie stärken das Individuum. Statt dem Recht des Stärkeren herrscht gleichberechtigte mehrseitige Sicherheit. Und jeder kann individuell und im konkreten Fall entscheiden, ob er von diesen Möglichkeiten Gebrauch machen will.

Manche dieser Mittel – zum Beispiel das Verschlüsselungsprogramm PGP – können ohne jede Vorleistung genutzt werden. Hier muß der der Staat nur auf hinderliche Regelungen verzichten. Andere – wie digitale Signaturen – sind auf eine Infrastruktur angewiesen, die dem Einzelnen ermöglicht, die Selbstschutzinstrumente zu nutzen. Der Abhängigkeit von infrastrukturellen Vorleistungen kann auch der Bürger der Informationsgesellschaft nicht entfliehen. Aber es macht einen entscheidenden Unterschied, ob der Einzelne über den Einsatz von selbstkontrollierten Schutzmechanismen selbst bestimmen kann, oder ob ihm der Staat oder eine andere Großorganisationen einen Schutz bieten, auf den er keinen Einfluß hat.

Sommerakademie '97

Zum vierten Mal veranstaltet die Datenschutzakademie Schleswig-Holstein am 28.5.1997 im Kieler Landhaus eine Sommerakademie. Das Thema lautet diesmal:

Computermedizin und Patientengeheimnis

Die älteste bekannte Datenschutzvorschrift ist der Eid des Hippokrates. Er verpflichtet den Arzt seit mehr als zweitausend Jahren, über das zu schweigen, was der Patient ihm anvertraut hat. Diese Pflicht blieb, bei allen Änderungen im Detail, im Kern über die Jahrhunderte erhalten und findet sich bis jetzt in den ärztlichen Berufsordnungen und im Strafgesetzbuch wieder. Die elektronische Datenverarbeitung, die heute in der Medizin eine immer größere Rolle spielt, hat gravierende Auswirkungen auf Inhalt und Reichweite der ärztlichen Verschwiegenheitspflicht. Wem vertraut der Patient seine Geheimnisse an, wenn Computer, von Softwarehäusern gewartet, selbsttätig Diagnosedaten erheben und speichern? Wer kann Kenntnis nehmen, wenn Krankheitsdaten im Rahmen der Telemedizin über tausende von Kilometern und dutzende von Knotenrechnern ausgetauscht werden? Ist die konventionelle Krankenakte sicherer zu handeln als eine hochkomplexe Datenbank? Sind die Patienten gut beraten, ihre Krankendaten besser selbst, z.B. auf einer Chipkarte, zu verwahren? Müssen wir es unter dem gegenwärtigen Kostendruck akzeptieren, daß die Krankenkassen über die Erkrankungen der Versicherten immer besser Bescheid wissen? Und schliesslich: Soll – und wenn ja, unter welchen Bedingungen – die medizinische Forschung Vorrang vor dem Patientengeheimnis haben?

Die Sommerakademie 1997 wird sich mit diesen Fragen auseinandersetzen. Ärzte, Techniker, Forscher, Juristen und Datenschützer haben Gelegenheit, über die Voraussetzungen zu diskutieren, unter denen auch im Computerzeitalter das Patientengeheimnis wirksam geschützt werden kann.

Anmeldung beim:
Landesbeauftragten für den Datenschutz
Düsternbrooker Weg 82, 24105 Kiel, Tel: 0431/988-1200
email: ldsh@netzservice.de

Ein Teil dieser Infrastrukturleistungen sind ergänzende Rechtsregelungen. In vielen Fällen muß Recht erst die Möglichkeit schaffen, die Selbstschutztechniken zu nutzen. Um die alten Ziele Freiheit und Selbstbestimmung auch im neuen Sozialraum der Netze zu schützen und zu bewahren, muß das Recht gerade neue Techniken ermöglichen und fördern.

- Systemschutz
  Die notwendigen Infrastrukturen müssen freiheitstauglich sein. Sie dürfen die Selbstschutztechniken nicht konterkarieren. Sie sind daher präventiv zu gestalten – und zwar dort, wo die Netzwelt physisch aufgebaut wird. Anzusetzen ist an den Stellen, wo die Netzwelt zur körperlichen Welt in Kontakt tritt. Hier kann der Gesetzgeber Selbstschutz durch Systemschutz[44] ergänzen.
  Systemschutz kann er einmal erreichen, indem er – zumindest für die Bundesrepublik Deutschland – die Infrastrukturen technisch-organisatorisch gestaltet – etwa indem er die Wahlfreiheit für anonyme Abrechnungsverfahren, die permanente Anzeige der entstandenen Gebühren oder die technische Dauersignalisierung von Werbung oder nicht jugendfreien Angeboten sicherstellt.
  Zum anderen kann er neue Machtkonzentrationen verhindern. Er baut in die neuen Infrastrukturen organisatorische Sicherungen ein, wie die Teilung physischer und informationeller Gewalt, schafft konkurrierende Instanzen mit gegenseitigen Kontrollkompetenzen, institutionalisiert spezifische Schutzinteressen und behindert bewußt einseitige Effizienz.[45] Ein Beispiel hierfür ist die organisatorische Trennung zwischen Betreibern von Multimedia-Servern und Anbietern von Multimedia-Programmen.[46]
  Der Referentenentwurf des Gesetzes über Informations- und Kommunikationsdienste enthält hierzu hoffnungsvolle Ansätze: Es führt den Grundsatz der Datensparsamkeit ein, ermöglicht anonymes Bezahlen und pseudonymes Handeln und schafft einen Rahmen für die Sicherungsinfrastruktur digitaler Signaturen.

2. Neues Leitbild: zivile Informationsgesellschaft

Die Ohnmachtserfahrungen des Staates und die Schutzmöglichkeiten der Individuen bieten die Chance zu einem neuen Verständnis der Staatsaufgaben in der Informationsgesellschaft. Wir sollten die Diskussion um eine moderne Zivilgesellschaft[47] aufnehmen und versuchen, die Aufgaben des Staates und der Gesellschaft neu zu strukturieren.

Dieses Gesellschaftsmodell ist von der Freiheit des Individuums her zu konstruieren.[48] Es darf allerdings nicht in einer rein individualistischen Rechtskonstruktion aufgehen. Vielmehr sind gerade die systemischen Bedingungen individueller und gesellschaftlicher Freiheit zu thematisieren.[49] Für die Konstruktion einer zivilen Informationsgesellschaft ist daher zu fragen: Welche Strukturmerkmale sind erforderlich, um dem Individuum zu ermöglichen, seine gesellschaftliche Rolle selbst zu definieren, seine Schutzbedürftigkeit selbst zu bestimmen und sich entsprechend dem eigenen Bedürfnis zu schützen?

Die Fragen so zu stellen, ermöglicht, den Staat von Überforderungen zu befreien. Er muß nicht mehr alle Funktionen, die ihm historisch zugewachsen sind, selbst erfüllen. Einige kann er der gesellschaftlichen Selbstorganisation überlassen und sich auf die Vorgabe der Spielregeln beschränken. Die Willensbildung und -durchsetzung im konkreten Fall können vielfach die Beteiligten vor Ort übernehmen. Zu fairen Regeln gehört in diesem Spiel allerdings auch, jedem den Zugang zu Netzen und Informationen sicherzustellen. Eine Aufgabe des informationellen Sozialstaats ist, die Kluft zwischen Informationsarmen und Informationsreichen zumindest durch eine Grundversorgung mit Informationsmöglichkeiten zu lindern.[50]

Für den Schutz seiner Bürger ist der Staat zwar weiterhin verantwortlich. Wo er diesen aber nicht mehr selbst gewährleisten kann, genügt er seiner Schutzpflicht, wenn er für Systemschutz sorgt und Selbstschutz ermöglicht. Denn die staatliche Schutzpflicht besteht nur im Rahmen des Möglichen.[51] Das ihm Mögliche muß der Staat aber zum Schutz seiner Bürger ergreifen.[52] Der Staat reduziert seine Verantwortung von einer Erfüllungsverantwortung zu einer Strukturverantwortung.

Die Vision einer „civil information society" ließe sich so zusammenfassen: In ihr stehen Entfaltung und Schutz der Persönlichkeit, Informationsfreiheit, Kommunikation, Assoziation und demokratische Willensbildung im Vordergrund. In ihr werden die Verwirklichungsbedingungen von Grundrechten durch die individuellen Nutzungsmöglichkeiten moderner Informations- und Kommunikationstechniken nicht nur gewahrt, sondern verbessert. Datennetze könnten es ermöglichen, daß die Bürger sich selbstbestimmt informieren, organisieren und entscheiden. Sie könnten informationelle und kulturelle Vielfalt bieten und sichern. In dieser Informationsgesellschaft kommt dem Staat eine beschränkte, aber entscheidende Rolle zu. Um die im Grundgesetz verankerten Entwicklungsziele unserer Gesellschaft zu verwirklichen, schafft er durch Infrastrukturvorgaben Systemsschutz und die Rahmenbedingungen für den Selbstschutz der Bürger. Diese erhalten dadurch die Möglichkeit, sich frei zu informieren, Konflikte in freier Selbstorganisation anzugehen, gegenseitige Sicherheit auszuhandeln und zu praktizieren, ohne dabei auf größere Brüder angewiesen zu sein.

Quelle: Überarbeiteter Teil eines Vortrags auf der Tagung der Alcatel-SEL-Stiftungsprofessur „Rechtliche Gestaltung der Informationstechnik – Zwischen rechtlicher Regulierung und technischem Selbstschutz" in der Technischen Hochschule Darmstadt am 26./27.6.1996. Nachdruck mit freundlicher Genehmigung aus der Zeitschrift für Rechtspolitik 1/1997, 26 - 30.

44. S. hierzu auch Podlech, in: Brückner/Dalichau (Hrsg.), FS f. Grüner, 1982, S. 451 ff.
45. S. hierzu z.B. Schlink, VVDStRL 48 (1990), 260f.
46. S. hierzu z.B. §§ 82 ff. LMedienG Baden-Württemberg – s. hierzu auch Roßnagel/Bizer, Multimediadienste und Datenschutz, 1995.
47. S. zu dieser z.B. Cohen/Arato, Civil Society and Political Theory, 1992; Van den Brink/van Reijen (Hrsg.), Bürgergesellschaft, Recht und Demokratie, 1995.
48. S. hierzu auch Podlech, in: Steinmüller (Hrsg.), Verdatet und vernetzt, 1988, S. 123 ff.
49. S. hierzu Roßnagel (o. Fußn. 34), S. 240 ff.
50. Ebenso z.B. van Haaren (o. Fußn. 18), 69; Hoffmann-Riem (o. Fußn. 5), 108; Schmid/Kubicek, Media-Perspektiven 1994, 406; Roßnagel, DuD 1995, 259 ff.
51. S. z.B. BVerfGE 33, 303 (333); 46, 160 (164f.).
52. S. z.B. Isensee (o. Fußn. 26), S. 222.

Marit Köhntopp

Datenschutz durch Technik?!

Datenschutz versus Technik

Betrachtet man die Bereiche Datenschutz und Informationstechnik, fallen einem zunächst eher die Gegensätze als die Gemeinsamkeiten ein. Für die Datenschützer war die Technik lange Zeit Feindbild Nummer eins. Tatsächlich bringt die elektronische Datenverarbeitung im Gegensatz zur herkömmlichen, ausschließlich papierenen Welt eine neue Qualität mit sich, aus der Gefahren für den Datenschutz resultieren:

EDV-Datenbestände kann man leicht nach beliebigen Kriterien auswerten und mit weiteren Informationen koppeln. Man denke nur an den Telefonbuchdatenbestand auf Festplatte oder CD-ROM, der im Gegensatz zu den Papierbüchern vielfältig recherchierbar und auswertbar ist und leicht mit anderen Datenbanken zusammengeführt werden kann.

Außerdem werden die Speichermedien immer kleiner bei zugleich zunehmender Kapazität. Die Akten ganzer Unternehmen oder Verwaltungen passen auf einem Datensicherungsband in jede Hemdtasche. Da die Speicherpreise sinken, wird häufig keine Notwendigkeit gesehen, datensparsam zu arbeiten. Während Akten spätestens dann vernichtet werden, wenn auch im hintersten Lagerraum kein Platz mehr ist, löst in der EDV eine neue Festplatte etwaige Engpässe, ohne daß auf die bisher gespeicherten Daten verzichtet werden muß. Wer weiß, wozu man die Daten später einmal gebrauchen kann? Die Auswertungsmöglichkeiten sind nahezu unbegrenzt und müssen nicht im voraus festgelegt werden. Archive können riesige, umfassend erschließbare Datensammlungen bergen, die ein detailliertes Bild über Personen zeichnen und beispielsweise ein barmherziges „Vergessen" etwaiger früherer Verfehlungen unmöglich machen. Doch selbst das „Löschen" hinterläßt auf den Datenträgern oft genügend Spuren, um die Informationen größtenteils oder vollständig rekonstruieren zu können.

Dazu kommt, daß die Hard- und Software-Systeme, die sich zum Marktstandard entwickelt haben, häufig die geringsten Anforderungen der Datensicherheit nicht erfüllen. Paßwortschutz, die Möglichkeit zur Vergabe benutzerbezogener Zugriffsrechte und eine Protokollierung bestimmter Zugriffe gehören längst nicht zur Standardfunktionalität beim Systemkauf. Keiner durchblickt, was im Rechner gerade abläuft. Dies wird besonders interessant, wenn das System an ein Netz angebunden ist. Die drohende Vision, daß unbemerkt die Festplatte ausgelesen wird und die Informationen über das Netz einem interessierten Empfänger zugehen, kann längst real sein.

Die Durchdringung aller Lebensbereiche mit Computern verstärkt auch die Abhängigkeit von diesen technischen Systemen. Häufig hat der Benutzer keine andere Wahl, als ein bestimmtes technisches System zu benutzen. Bewußt haben sich viele Datenschützer der 70er und 80er Jahren in die technikfeindliche Ecke gestellt, um von dort aus – die diffuse Technikangst der Bevölkerung nutzend – gegen den technischen Fortschritt zu mobilisieren. Techniker hatten im Datenschutzbereich ihre Daseinsberechtigung allenfalls im Segment der Datensicherheit. Der eigentliche Datenschutz spielte sich im juristischen Bereich ab.

„Datenschutz"

„Datenschutz" bedeutet in erster Linie Schutz der Menschen, deren personenbezogene Daten gespeichert werden. Das Fundament für den neueren Datenschutz hat in Deutschland das Bundesverfassungsgericht 1983 mit dem Volkszählungsurteil gelegt, in dem aus dem Grundgesetz das Recht auf informationelle Selbstbestimmung abgeleitet wird: „Jeder hat das Recht zu wissen, wer was wann über ihn weiß."

Zu den Datenschutzkriterien gehören die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, eine strikte Zweckbindung der Datenverarbeitung sowie die Datensicherheit. Da nur diejenigen personenbezogenen Daten verarbeitet werden dürfen, die für die jeweilige Aufgabe erforderlich sind, gilt das Prinzip der weitgehenden Datenvermeidung und -sparsamkeit.

Bei der Ausbildung für EDV-Berufe kam wiederum der Datenschutz oft gar nicht vor. Insbesondere an Hochschulen wurden derlei Wünsche der Studenten mit dem Hinweis abgebügelt, die naturwissenschaftlich geprägte Ausgestaltung des Studiums lasse nur die Betrachtung „harter Fakten" zu. „Weiche Wissenschaften" wie z.B. Jura, die auslegungsfähig oder -bedürftig sind, wurden dort nicht anerkannt. Datenschutz und selbst der Datensicherheitsbereich gehören bis heute nicht überall zum Standardrepertoire einer EDV-Ausbildung. Hinzu kommt die hohe Geschwindigkeit des technischen Fortschritts ohne eine Phase der Besinnung: „Unter hoher Wachstumsgeschwindigkeit hat die Informatik kein professionelles Selbstverständnis entwickelt, das per se zuverlässig und bedachte Konstruktionen zum beruflichen Normalfall werden läßt." [Coy_92]

Schon grundlegende Informatikvorgaben, die rein technisch betrachtet logisch und sinnvoll sind, können mit dem Persönlichkeitsrecht kollidieren. So stellt z.B. die Vermei-

dung von Redundanzen ein fundamentales Ziel beim Design von Datenbanken dar, um Anomalien bei Änderungen von Teilen des gedoppelten Datenbestandes zu vermeiden. Unterwirft man die Datenbankkonzeption ausschließlich diesem technischen Prinzip, ist eine weltweite Zentraldatenbank für alle Informationen zu jeder Person die einfachste und „natürlichste" Lösung. Mit einem geeigneten Datenbankschema ließen sich dort Redundanzen vermeiden. Bei Bedarf könnten Replikationsverfahren die Netzlast beim Abfragen eines solchen Zentralregisters reduzieren.

Selbst wenn alle möglichen Zugriffsbeschränkungen technisch ausgereizt würden, stünden den Datenschützern bei einem solchen Plan die Haare zu Berge: So wäre allein die Existenz eines Zentralregisters bedenklich, in dem alle möglichen Informationen über Personen zusammengeführt sind und sich zu Profilen z.B. über Lebensgewohnheiten und Persönlichkeit verdichten lassen. Ein solcher Datenpool würde Begehrlichkeiten wecken bei den Interessenten für derartige Persönlichkeitsprofile, z.B. Marketing-Abteilungen, Arbeitgeber, Versicherungen, Kriminelle und Geheimdienste. Einige würden weder Kosten noch Mühen scheuen, um sich einen Zugriff auf die Daten zu verschaffen. Die Zentralität brächte mit sich, daß sich alle Angreifer auf diesen einen Punkt konzentrieren und dort nach Sicherheitslücken im technischen oder organisatorischen Bereich fahnden könnten.

„Datensicherheit"

Unter „Datensicherheit" versteht man den Schutz der Datenvor unberechtigten Zugriffen und Zerstörung. Die drei klassischen Grundbedrohungen der Datensicherheit, denen es zu begegnen gilt, sind der Verlust der Verfügbarkeit (Daten und technische Systeme stehen nicht mehr zur Verfügung), der Verlust der Integrität (Veränderung von Daten, Manipulation von technischen Einrichtungen und Programmen) und der Verlust der Vertraulichkeit (unberechtigte Kenntnisnahme von Informationen). Manchmal wird außerdem der Verlust der Verbindlichkeit (Fälschungen von Nachrichten, Absender und Empfänger nicht zweifelsfrei zuordenbar) hinzugenommen. [Kers_91]

In Deutschland wäre das geschilderte umfassende Zentraldatenbankkonzept nicht durchsetzbar, da der Gesetzgeber die Abschottung bestimmter Bereiche voneinander gesetzlich festgeschrieben hat. Es reicht nicht immer aus, dies über Zugriffsbeschränkungen zu realisieren, denn Änderungen in einem Bereich dürfen bei einer vollständigen Abschottung nicht in anderen Bereichen sichtbar werden. Solche Informationen müssen redundant vorgehalten werden – mit dem Nachteil, daß Aktualität, Vollständigkeit und Übereinstimmung der Daten nicht sichergestellt werden können. Der Betroffene soll nämlich weitgehend selbst in der Hand haben, wer welche Daten über ihn verarbeitet oder an wen weitergibt.

Jedoch passen auch die Prinzipien der Rechtsnormen nicht unbedingt auf die Welt der Techniker. So ist es einigen Gesetzen und Verordnungen anzumerken, daß bei ihrer Verabschiedung die technische Realität sehr verschieden von heutigen Verhältnissen war oder kaum eine Rolle spielte. Ein Beispiel sind die internationalen Netze, die von nationalen Gesetzen nicht so recht einzufangen sind. Hier ist den meisten inzwischen die Problematik bewußt, doch befriedigende Lösungen sind nicht in Sicht. Manchmal scheint es auch so zu sein, daß absichtlich die technischen Verhältnisse nicht zur Kenntnis genommen werden und die Politiker gänzlich unbeeinflußt von der „realen Welt" diskutieren. Dies fällt zur Zeit besonders in der Kryptodebatte auf, in der z.B. Berlins Innensenator Jörg Schönbohm (CDU) behauptet, alles andere als ein Verschlüsselungsverbot „käme dem Eingeständnis gleich, daß der Staat bereits vor der Technik kapituliert hat" (Der Spiegel, 17.3.97).

Leitbildwechsel

Dabei ist Technik nur ein Werkzeug: Nutzen und Schaden hängen vom Menschen ab, der es einsetzt oder steuert [Zema_96]. Wie jedes Werkzeug kann sie ein „Mittel der Veränderung" [Weiz_77] sein. Ebenso wie die Technik fungieren Rechtsnormen als Werkzeug. In beiden Bereichen kommt es stets darauf an, was man daraus macht. Ein generelles Verdammen solcher Werkzeuge ist fehl am Platz und auch weitgehend wirkungslos. So läßt sich der Weg in die Informationsgesellschaft kaum mehr aufhalten – aber er läßt sich noch entscheidend gestalten. Mit moderner „Technik vom Feinsten" kann oft sogar ein besserer Datenschutz ermöglicht werden als beim herkömmlichen Vorgehen.

Die Idee, Datenschutz auch technisch zu realisieren, ist nicht neu. So haben bereits 1984 die Informatiker Günter R. Koch und John Favaro bei der Beschäftigung mit kryptographischen Verfahren erkannt: „So wie es bisher schon einen auf Gesetze und Konventionen gegründeten und organisatorisch implementierten Schutz von personenbezogenen oder sicherheitssensiblen Daten gab, so läßt sich dieser Schutz auch technisch realisieren, sogar ohne daß es dazu übergeordneter Einflußnahme bedürfte." [KoFa_84]

„Datenschutz durch Technik" ist jedoch kein Selbstgänger, sondern eine wirkliche Herausforderung für Datenschützer und Techniker, die nur durch intensive Zusammenarbeit gemeistert werden kann. Es reicht nicht, sich auf die Datensicherheit im herkömmlichen Sinne zu beschränken, die häufig vorwiegend Hersteller oder Betreiber von EDV-Systemen schützen soll. Statt dessen bedarf es einer „mehrseitigen Sicherheit", in der die Sicherheits- und Datenschutzinteressen aller beteiligten Parteien berücksichtigt werden [RDLM_95]. Mögliche Zielkonflikte, die sich aus den unterschiedlichen Interessen ergeben können, lassen sich beispielsweise durch ein wechselseitiges „Aushandeln" lösen. Da der von der Datenverarbeitung Betroffene zumeist die schwächste Partei bildet und oft faktischen Zwängen unterliegt, muß sein Interesse im Zweifel Vorrang haben vor anderen Sicherheitsinteressen [Bäum_97].

Die Datenschutzbeauftragten des Bundes und der Länder messen dem Thema „Datenschutz durch Technik" große Bedeutung bei und erarbeiten Vorschläge, wie sich z.B. im Telekommunikationsbereich personenbezogene Daten weitgehend vermeiden lassen. Künftig soll es auch bei der Europäischen Kommission ein Programm zur Förderung von datenschutzfreundlichen Technologien geben. Dieser Trend hat bereits Eingang in die Gesetzgebung gefunden: Im Multimedia-Bereich wird das Prinzip der datenschutzgerechten Technik durch den Mediendienste-Staatsvertrag (Md-StV) der Länder gesetzlich festgeschrieben; der Entwurf des Teledienstedatenschutzgesetz (TDDSG) des Bundes sieht gleichlautende Regelungen vor [Bund_96]. So hat sich „die Gestaltung und Auswahl technischer Einrichtungen ... an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen" (§3 Abs. 4 TDDSG-Entwurf, § 12 Abs. 5 Md-StV).

Weiterhin hat der Diensteanbieter dem Nutzer die Inanspruchnahme von Diensten und ihre Bezahlung „anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist" (§ 4 Abs. 1 TDDSG-Entwurf, § 13 Abs. 1 Md-StV). Mit dieser Formulierung geht die Verpflichtung der Anbieter weiter als andere Gesetze, in denen lediglich vorgeschrieben wird, „den Stand der Technik zu berücksichtigen" (z.B. § 87 Abs. 1 TKG). Die Multimedia-Rechtsvorschriften verpflichten damit die Anbieter, in Bereichen, in denen noch keine marktgängigen „Stand-der-Technik"-Lösungen existieren, in zumutbarem Rahmen auch eigene datensparsame Verfahren zu entwickeln.

Der Mediendienste-Staatsvertrag sieht außerdem die Möglichkeit eines Datenschutz-Audits vor, so daß der Anbieter sein Datenschutzkonzept und die technischen Einrichtungen vor Inbetriebnahme durch unabhängige Gutachter prüfen und bewerten lassen kann.

Grundsätze der datenschutzgerechten Technikgestaltung

Noch sind die Anforderungen, die im Datenschutz-Audit untersucht werden, nicht abschließend definiert. Ein Patentrezept für datenschutzfreundliche Technikgestaltung kann es nicht geben, es lassen sich jedoch dafür allgemeine Grundsätze formulieren ([FSch96] [Ross_97][LDSH_97]):

- ***Technikfolgenabschätzung:*** Bereits im Vorfeld der Entwicklung neuer Technologien sind die sozialen und rechtlichen Folgen unter Mitwirkung der Betroffenenverbände, Datenschützer und unabhängiger Experten (z.B. Sozialwissenschaftler, Juristen und Informatiker) abzuschätzen. Sinnvoll gestaltete und umfassend ausgewertete Pilotprojekte können dabei helfen. Sollte sich herausstellen, daß die Risiken einer neuen Technik zu groß werden und nicht beherrschbar sind, muß auf ihre Realisierung verzichtet werden.
- ***Systemkonzeption unter Datenschutzaspekten:*** Beim Gestalten neuer Technologien müssen Maßnahmen zu Datenschutz und Datensicherheit von Anfang an einbezogen werden. Nachträglich ist es meist nur schwer möglich, Schutzmechanismen wirkungsvoll in bestehende Strukturen zu integrieren.
- ***Datensparsame Technik:*** Nur die wirklich erforderlichen Daten dürfen erhoben und gespeichert werden. Sobald sie nicht mehr erforderlich sind, müssen sie unverzüglich gelöscht werden, Oft können organisatorische Regeln oder spezielle Angebote umfangreiche Datensammlungen vermeiden, z.B. bei Abrechnungssystemen durch Pauschaltarife oder vorausbezahlte anonyme Chipkarten (Prepaid-Chipkarten). Wo auf die Speicherung individueller Daten nicht verzichtet werden kann, reichen häufig Pseudonyme aus, also zusätzliche Identitäten, die der Benutzer selbst wählt oder die ihm zugeordnet werden. Sofern diese Zuordnung bei vertrauenswürdigen Stellen gespeichert wird, darf sie nur unter bestimmten strengen Voraussetzungen aufgedeckt werden, z.B. auf richterlichen Beschluß bei Verdacht von Straftaten.
  Um zu bestimmen, welche personenbezogenen Daten wirklich erforderlich sind, muß man sämtliche Module des zu untersuchenden Verfahrens betrachten. Das universelle Konzept des Identity Protectors aus den Niederlanden [Regi_95] hilft, die einzelnen Prozesse (insbesondere authorization, identification and authentication, access control, auditing, accounting) in den Systemen zu analysieren. In den Fällen, in denen die Information über die Identität des Nutzers nicht notwendig ist, kann mit technisch generierten oder selbstgewählten Pseuso-Identitäten gearbeitet werden.
- ***Zugriffsschutz:*** Für die gespeicherten Daten muß eine strikte Zweckbindung garantiert werden. Hier geht es um die klassische Datensicherheit: Unbefugte dürfen die Daten weder zur Kenntnis nehmen noch verändern, fälschen oder zerstören können. Ein Zugriffsschutz läßt sich beispielsweise mit Paßworten, Vergabe von maßgeschneiderten Zugriffsrechten und einer wirksamen Verschlüsselung erreichen. Einen Schutz gegen unbemerkte Veränderung bietet die digitale Signatur. Flankierende Maßnahmen sind das regelmäßige Anfertigen von Sicherungskopien und eine umfassende Zugriffsprotokollierung, die nicht manipulierbar sein darf.
- ***Kontrolle durch den Betroffenen selbst:*** Eine effektive Verfügungs- und Kontrollgewalt über die eigenen Daten läßt sich beispielsweise dadurch erreichen, daß die Daten dezentral beim Betroffenen selbst gespeichert werden (z.B. auf einer Chipkarte) und für den Zugriff und eine etwaige weitere Verwendung durch Dritte extra vom Betroffenen freigeschaltet werden müssen. Portable Benutzerendgeräte, die vertrauenswürdig, manipulationsresistent und teilnehmerkontrollierbar sind, können Sicherheits- und Datenschutzfunktionen realisieren [PPSW_95].
- ***Transparenz und Nachprüfbarkeit:*** Die technischen Systeme müssen so transparent aufgebaut sein, daß der Anwender sowohl erkennen als auch steuern kann, wo welche seiner Daten gespeichert und übertragen wer-

den. Sicherheitsrisiken müssen vom Benutzer einzuschätzen sein. Gütesiegel, Zertifikate, Qualitätskontrolle, Verifikation und auch die Meinung unabhängiger Experten können das Vertrauen des Nutzers in das technische System erhöhen. Damit verbunden ist eine Offenlegung der Konzepte und Realisierungen von Hard- und Softwarekomponenten gegenüber Zertifizierungsstellen oder noch besser gegenüber der öffentlichkeit, so daß eine breite Diskussion der interessierten Experten und Laien möglich ist.

Zusätzlich sind Datenschutz-Tools denkbar wie Prüf- und Kontrollwerkzeuge für bestimmte Regelungen der Datenschutzgesetze: In [Wäch_96] wird die Idee verfolgt, die Vorgaben des BDSG zur Anwendbarkeit des Gesetzes auf eine Datei, zur Benachrichtigung des Betroffenen, zur Auskunfterteilung sowie zur Berichtigung, Löschung oder Sperrung von personenbezogenen Daten technisch umzusetzen und so Datenschutz zu automatisieren. Dies kann helfen, die gesetzlichen Anforderungen einzuhalten und gegebenenfalls selbst einen besseren Überblick über die eigene Datenverarbeitung zu gewinnen.

Ausblick

Experten sehen die datenschutzgerechte Gestaltung des Informationszeitalters als unbedingt erforderlich für die Akzeptanz der Verbraucher an [BMWi_96]. Gemeinsam müssen nicht nur Datenschützer und Techniker, sondern auch Wissenschaftler und Verbrauchervertreter das rechtliche, technische und organisatorische Umfeld bürgerfreundlich bestimmen. Dies bedeutet, daß frühzeitig eine stärkere wechselseitige Einbindung nötig ist, um in allen Bereichen praxisorientierte Lösungen zu erreichen, z.B. in der Gesetzgebung, in der politischen Diskussion und in der Technikgestaltung. Erste Ansätze in den gesetzlich neu geschaffenen Datenschutzanforderungen im Multimedia-Bereich sind vielversprechend. Die diskutierte rechtliche Regulierung der Kryptographie wäre allerdings ein großer Schritt in die falsche Richtung. Da Kryptographie die Basistechnologie der Informationsgesellschaft ist, auf der nicht nur Verschlüsselung und digitale Signatur, sondern auch Datenvermeidungsstrategien beruhen, wäre bei Kryptoverboten oder -einschränkungen die Datensicherheit und der Datenschutz gefährdet.

Betreiber und Hersteller sollten offensiv die konstruktiven Vorschläge für mehr Datenschutz durch Technik umsetzen. Datenschutzfreundliche Gestaltung von Dienstleistungen und der zugrundeliegenden Technik kann ihnen bei einer sensibilisierten Bevölkerung entscheidende Wettbewerbsvorteile verschaffen.

Technikgestaltung wird als gesellschaftliches „Regulierungsinstrument" neben staatliche Regulierung treten. Die technische Möglichkeit zum „Selbst-Datenschutz" [Ulri_96] kann jeder bekommen. Dies ist rechtlich in allen Bereichen, in denen der Staat die Sicherheit nicht gewährleisten kann, sogar geboten [Ross_97]. Dennoch bleiben einige Fragen offen [Pomm_96]:

- Was muß ein Mensch über die Technik wissen, um verantwortungsvoll damit umgehen und sein Recht auf informationelle Selbstbestimmung wirkungsvoll wahrnehmen zu können?
- Wird der Bürger mit der Aufgabe überfordert, sein eigener Datenschützer zu sein?
- Wem kann man vertrauen in einer immer komplexer werdenden Technikwelt, die man nicht selbst überprüfen kann?

Für diese Probleme gibt es keine rein technischen Lösungen, sondern es müssen die subjektive Einschätzungen jedes einzelnen Bürgers ernst genommen werden. Hier sind alle Beteiligten gefragt, ihre Ideen und Vorstellungen einzubringen, um zu einer gesellschaftlich tragfähigen Lösung zu kommen. Von besonderer Bedeutung wird künftig die Frage der Vertrauenswürdigkeit sein. Hier sind die Datenschützer gefragt, sich auch das technische Know-how anzueignen, um ihre bisherige Vertrauensstellung auch in der Informationsgesellschaft ausfüllen zu können.

Literatur

[Bäum_96] Bäumler, Helmut: „Eröffnungsrede des Landesbeauftragten für den Datenschutz Schleswig-Holstein zur Sommerakademie 'Datenschutz durch Technik – Technik im Dienste der Grundrechte'", DuD 11/96, 647-649.

[Bäum_97] Bäumler, Helmut: „IT-Sicherheit – für wen?", erscheint im Tagungsband des 5. Deutschen IT-Sicherheitskongresses „Mit Sicherheit in die Informationsgesellschaft" des BSI, 28.-30.04.97, Bonn.

[BMWi_96] Der Bundesminister für Wirtschaft: „Info 2000 – Deutschlands Weg in die Informationsgesellschaft", Bericht der Bundesregierung, Bundesratsdrucksache 140/96, Bonn, 13.02.96.

[Bund_96] Bundesregierung: Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG), Bundesratsdrucksache 966/96, Bonn, 20.12.96.

[Coy_92] Coy, Wolfgang: „Informatik – Eine Disziplin im Umbruch?", in: Wolfgang Coy u.a. (Hg.): Sichtweisen der Informatik, Vieweg, Braunschweig 1992, 1-9.

[FSch_96] Fischer-Hübner, Simone; Schier, Kathrin: „Der Weg in die Informationsgesellschaft – Eine Gefahr für den Datenschutz", in: Britta Schinzel (Hg.): Schnittstellen – Zum Verhältnis von Informatik und Gesellschaft, Vieweg, Braunschweig 1996, 215-239.

[Kers_91] Kersten, Heinrich: „Einführung in die Computersicherheit", Oldenbourg, München 1991.

[KoFa_84] Koch, Günter R.; Favaro, John: „Die technische Dimension", in: Günter Myrell (Hg.): Daten-Schatten, Rowohlt Taschenbuch Verlag, Reinbek bei Hamburg 1984, 131-172.

[LDSH_97] Der Landesbeauftragte für den Datenschutz Schleswig-Holstein: „19. Tätigkeitsbericht", Kiel, März 1997, http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/TB19/.

[Pomm_96] Pommerening, Klaus: „Chipkarten und Pseudonyme", FIFF-Kommunikation 1/96, 9-12.

[PPSW_95] Pfitzmann, Andreas; Pfitzmann, Birgit; Schunter, Matthias; Waidner, Michael: „Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule", Proc. Verläßliche Informationssysteme (VIS '95), Vieweg, Braunschweig 1995, 329-350.

[RDLM_95] Rannenberg, Kai; Damker, Herbert; Langenheder, Werner; Müller, Günter: „Mehrseitige Sicherheit als integrale Eigenschaft von Kommunikationstechnik", in: Kubicek, Müller, Neumann, Raubold, Roßnagel (Hg.): Jahrbuch „Telekommunikation & Gesellschaft" 1995, R. v. Decker_s Verlag, Heidelberg 1995, 254-260.

[Regi_95] Registratiekamer: „Privacy-enhancing technologies: The path to anonymity", Volume II, Achtergrondstudies en Verkenningen 5b, Rijswijk, Niederlande, 1995.

[Ross_97] Roßnagel, Alexander: „Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger", in diesem Heft, Seite 48, oder ZRP 1997, Heft 1, 26-30.

[Ulri_96] Ulrich, Otto: „Leitbildwechsel: dem (sicherheits-)technologisch aktivierten Datenschutz gehört die Zukunft", DuD 11/96, 664-671.

[Wäch_96] Wächter, Michael: „Datenschutz als 'Software-Routine' – Ein datenschutzrechtlicher Implementierungsvorschlag", DuD 5/96, 272-278.

[Weiz_77] Weizenbaum, Joseph: „Die Macht der Computer und die Ohnmacht der Vernunft", Suhrkamp, Frankfurt am Main 1977.

[Zema_96] Zemanek, Heinz: „Werkzeug Computer: Verstärker von Intelligenz und Sorglosigkeit", in: Britta Schinzel (Hg.): Schnittstellen – Zum Verhältnis von Informatik und Gesellschaft, Vieweg, Braunschweig 1996, 31-47.

FIfF

Forum
InformatikerInnen für
Frieden und gesellschaftliche
Verantwortung e.V.

FIfF

2. Ankündigung

FIfF-Jahrestagung 1997

Zur Rolle kritischer ExpertInnen in der Informationsgesellschaft

14.-16. November 1997
Paderborn

Ursprünglich sollte die FIfF-Jahrestagung in Kombination mit einem internationalen Treffen kritischer europäischer und amerikanischer Initiativen stattfinden, um die Fragen und Probleme der Globalisierung auch im internationalen Zusammenhang zu behandeln. Um eine Teilnahme der internationalen Gruppen zu ermöglichen, sollte die Tagung – abweichend vom üblichen Turnus – im Sommer stattfinden. Leider war die internationale Resonanz auf unseren Aufruf so gering, daß wir uns entschließen mußten, den internationalen Teil der Tagung zu streichen. Das hatte Folgen: Offensichtlich war der Sommertermin für viele FIfFerlinge und Interessierte sehr ungünstig. Nachdem der wesentliche Grund für einen sommerlichen Termin entfallen war, hat der Vorstand des FIfF zusammen mit dem Beirat beschlossen, die FIfF-Jahrestagung wie üblich im November durchzuführen.

Deshalb möchte die FIfF-Regionalgruppe Paderborn Euch erneut zur FIfF-Jahrestagung zum oben angegebenen neuen Termin nach Paderborn einladen. Die Tagung wird vom 14. bis 16. November an der Universität-GH Paderborn, Warburger Str. 100, 33098 Paderborn durchgeführt. Da wir die gesamte Zeitplanung auf dieses Datum anpassen, ergeben sich somit neue Termine für die Anmeldung von Arbeitsgruppen sowie die Anmeldung zur Teilnahme:

Anmeldung von Arbeitsgruppen bis 31. Juli 1997 per E-Mail an c5@uni-paderborn.de oder an das Tagungsbüro.
Anmeldung zur Tagungsteilnahme: 10. Oktober 1997 (Frühzahlungstarif)

Diesen Abschnitt bitte ausgefüllt
(Rückseite nicht vergessen)
und ausreichend frankiert
(z. B. im Fensterbriefumschlag)
an die angegebene Adresse senden!

Name, Adresse:

Universität-GH Paderborn
Sekretariat Informatik und Gesellschaft
Carmen Buschmeyer
Fürstenallee 11

33102 Paderborn

Tel. dienstl.:

Tel. privat:

Preise:

- DM 100,- Normaltarif (DM 80,- Frühzahlungstarif)
- DM 50,- für Studierende und Menschen in vergleichbarer Situation (DM 40,- Frühzahlungstarif)

Tagungskonto:

- Dieter Engbring, Volksbank Paderborn BLZ: 472 601 21 Kto. Nr.: 880 8988 900

Das ausführliche Programm und die angebotenen Arbeitsgruppen werden in der FIfF-Kommunikation 3/97 veröffentlicht. Weitere Informationen gibt es auch im WWW unter der Adresse: http://hyperg.uni-paderborn.de/FIFF_JT_97

Wir freuen uns auf Eure Anmeldung.

Tagungsbüro:

Carmen Buschmeyer
Sekretariat Informatik und Gesellschaft
Universität-GH Paderborn
Fürstenallee 11
33102 Paderborn

Tel.: ++49 +52 51 60-64 12
Fax: ++49 +52 51 60-64 14
E-Mail: carmen@uni-paderborn.de

Einladung zur FIfF-Mitgliederversammlung 1997

An alle FIfF-Mitglieder!
Der Vorstand lädt herzlich ein zur FIfF-Mitgliederversammlung im Rahmen der diesjährigen Jahrestagung am

Samstag, den 15. November 1997 von 17:30 Uhr bis 20:30 Uhr in der Universität GH Paderborn, Warburger Str. 100, 33098 Paderborn

Tagesordnung:

1. Wahl der Versammlungsleitung und der Protokollführung
2. Beschlußfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion des Vorstandsberichts und der Kassenprüfung
6. Entlastung des Vorstands und der Kassenprüfer
7. Neuwahl des Vorstands:
   - Wahl der WahlleiterIn
   - Wahl einer Wahlkommission
   - Wahl der/des Vorsitzenden
   - Wahl der/des stellvertretenden Vorsitzenden
   - Wahl der übrigen Vorstandsmitglieder (BeisitzerInnen)
8. Neuwahl der Kassenprüfer
9. Satzungsänderung
10. Diskussion aktueller Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
11. Verschiedenes

Wir freuen uns auf eine rege Teilnahme und ein Wiedersehen in Paderborn,
mit FIfFigen Grüßen

Ute Bernhardt (stv. FIfF-Vorsitzende)

Anmeldung zur Jahrestagung '97 in Paderborn

Hiermit melde ich mich verbindlich zur 13. FIfF-Jahrestagung „Zur Rolle kritischer ExpertInnen in der Informationsgesellschaft" an. Der Tagungsbeitrag beträgt:

	bei Zahlungseingang vor dem 10. Okt. 97	nach dem 10. Okt. 97
für Verdienende	80,- DM	100,- DM
für Studierende/Nichtverdienende	40,- DM	50,- DM

Den Beitrag in Höhe von _____ DM habe ich am _____ 1997 auf das Konto Dieter Engbring (Nr. 880 8988 900 bei der Volksbank Paderborn eG, BLZ 472 601 21) überwiesen.

Ich wünsche die Vermittlung einer (einfachen) privaten Unterkunft für ◯ 14./15. Nov ◯ 15./16. Nov

Ich bitte um die Vermittlung von Pension/Hotel (◯ Einzelzimmer) für ◯ 14./15. Nov ◯ 15./16. Nov

Ich möchte gerne eine Arbeitsgruppe mit dem

Thema _____ anbieten.

_____
Datum, Unterschrift

FIFF e.V. FIFF Überall

FIFF–Vorstand

- **Prof. Dr. Reinhard Keil-Slawik (Vorsitzender)**
  U-GH Paderborn,
  Fürstenallee 11
  33102 Paderborn
- **Ute Bernhardt (stellv. Vorsitzende)**
  Paulstraße 15,
  53111 Bonn
- **Peter Bittner**
  Hochstraße 56,
  64285 Darmstadt
- **Johannes Busse**
  Derendingerstraße 106,
  72072 Tübingen
- **Prof. Friedrich-Lothar Holl**
  Hektorstraße 7,
  10711 Berlin
- **Prof. Dr. Hans-Jörg Kreowski**
  Uni Bremen,
  FB 3,
  Postfach 33 04 40,
  28334 Bremen
- **Werner Moritz**
  Uhlandstraße 17,
  27576 Bremerhaven
- **Ingo Ruhmann**
  Paulstraße 15,
  53111 Bonn
- **Jürgen Ditz Schroer**
  Graf-Schenck-Straße 4a,
  82299 Türkenfeld
- **Dr. Cornelia Teller**
  Kittlerstraße 27,
  64289 Darmstadt

Beirat

Prof. Dr. Wolfgang Coy (Berlin); **Prof. Dr. Leonie Dreschler-Fischer** (Hamburg); **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Prof. Dr. Michael Grütz** (Konstanz); **Dr. Rolf Günther** (München); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Hans-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppung); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Hamburg); **Dr. Hermann Rampacher** (Bonn); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Roßnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Dr. Gabriele Schade** (Ilmenau); **Prof. Dr. Britta Schinzel** (Freiburg); **Prof. Dr. Dirk Siefkes** (Berlin); **Dr. Marie-Theres Tinnefeld** (München); **Prof. Dr. Josef Weizenbaum** (Freiburg/Cambridge, Mass.); **Dr. Gerhard Wohland** (Wankheim)

Regionalgruppe Bremen

Censorship in Cyberspace

Am 30. Mai 1997 hielt Marsha Woodbury an der Universität Bremen auf Einladung der FIFF-Regionalgruppe (in Kooperation mit dem Informatik-Kolloquium der Universität) einen Vortrag mit dem Titel „Censorship in Cyberspace: What are the Issues". Marsha Woodbury ist Mitglied des Vorstands der Computer Professionals for Social Responsibility (CPSR) und arbeitet an der Graduate School of Library and Information Science der University of Illinois, Urbana-Champaign, USA. In ihrem Vortrag stellte sie zunächst einige der nationalen und kulturellen Unterschiede und Gemeinsamkeiten im Umgang mit „unerwünschten" Inhalten im Internet dar: Sie ging dabei ebenso auf die deutschen Verhältnisse und Fallbeispiele ein (z.B. als Compuserve als Reaktion auf Ermittlungen in Deutschland weltweit den Zugang zu bestimmten Newsgruppen sperrte) wie auf China, Singapur oder Saudi Arabien, die durch wenige, staatlich kontrollierte Gateways und/oder durch restriktive Auflagen für die Provider den Zugang zum Internet beschränken. Und auch in den USA, die hierzulande vor allem als Anwälte des Rechts auf freie Meinungsäußerung wahrgenommen werden, gibt es – vor allem im Bereich sexuell expliziter Inhalte und Pornographie – staatliche Eingriffe (vgl. die Diskussionen um den „Communications Decency Act"). Kritisch diskutiert wurde die Frage der Wirksamkeit solcher Zensurmaßnahmen. Marsha Woodbury: „Internet treats censorship like a damage: it's going around". Neben „Umwegen" gibt eine Reihe von Möglichkeiten, Zensurbeschränkungen zu vermeiden oder zu umgehen (z.B. Verschlüsselung, anonyme Remailer, Mirroring gesperrter Web-Sites u.a.m.) Neben staatlicher Zensur ging Marsha Woodbury in ihrem Vortrag auch auf „Commercial Censorship" ein, eine ihrer Ansicht nach aufgrund zunehmender Monopolisierungstendenzen im Medien- und Telekommunikationsbereich steigenden Gefahr: Kommerzielle Interessen bestimmen die Inhalte - sowohl was zur Schlagzeile wird als auch was (wegen Gefährdung kommerzieller Interessen) nicht weiter verbreitet wird. Abschließend ging Marsha Woodbury auf Maßnahmen jenseits von Zensur und technischen Filtern ein und berichtete beispielsweise über das Vorgehen der American Library Association, die ausgehend von ihrem Auftrag Informationen zu vermitteln (und nicht zu unterdrücken) vorangig auf eine Erziehung zur Selbstverantwortung setzen. Neben Festlegungen in der Benutzungsordnung öffentlicher Terminals gibt es daher Sammlungen mit Links empfehlenswerter Web-Sites. Und für alle diejenigen, die sich doch das ein oder andere ansehen wollen, was vorbeigehende Besucher der Bibliothek belästigen könnte, werden die Terminals so angebracht, daß sie nicht mehr öffentlich im Blick sind. Nach ihrem Vortrag vor ca. 40 Personen gab es noch ein sehr nettes „Postkolloquium" in einem sonnigen Biergarten, bei dem – neben vielem anderen – auch über Unterschiede und Gemeinsamkeiten von FIFF und CPSR gesprochen wurde. *(Ralf E. Streibl)*

Termine

21.6.97

Bonn, Vorstands- und Beiratssitzung.

5.7.97

Berlin, Treffen des Dortmunder Kreis im Willy-Brandt-Haus.

11.10.97

Darmstadt, Vorstands- und Beiratssitzung. Infos zu den Terminen bei der FIfF-Geschaeftsstelle

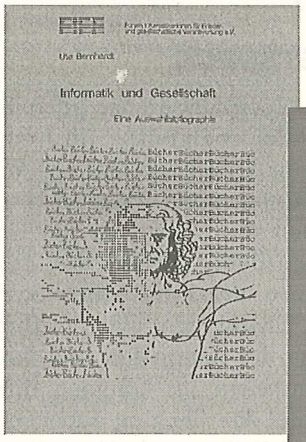
14.-16.11.97

Paderborn, Jahrestagung des FIfF (siehe vorige Seite)

29.-31.5.1998

Osnabrück, European Peace Congress – Vom Westfälischen Frieden zu einem friedensstiftenden Europa
Nähere Informationen über
PeaceCongress1998@t-online.de
http://www.dfg-vk.de/peacecongress1998

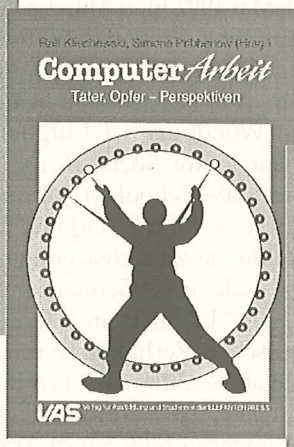
FIFF Bibliothek



Ute Bernhardt: Informatik und Gesellschaft. Eine Auswahlbibliographie

Ein thematisch gegliederter Einstieg in die Literatur zu Informatik und Gesellschaft

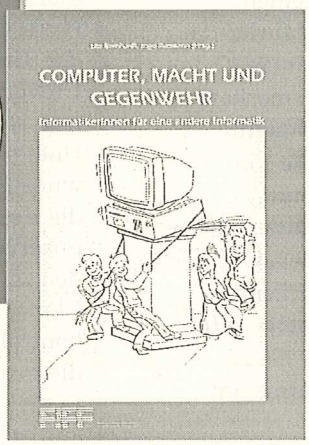
26 Seiten, Bonn 1990, 3,– DM



Ralf Klischewski, Simone Pribbenow (Hrsg.): ComputerArbeit. Täter, Opfer – Perspektiven

Das demokratische Potential der Neuen Fabrik · Maschinelle Intelligenz – Industrielle Arbeit · Arbeitnehmer und Betriebsräte zur Informatik im Betrieb.

190 Seiten, Berlin 1989, 19,80 DM



Ute Bernhardt, Ingo Ruhmann (Hrsg.): Computer, Macht und Gegenwehr – InformatikerInnen für eine andere Informatik

Protected Mode · Computersicherheit: militärisch oder zivil · Computer und Umwelt · Technologiepolitik und Technikfolgenforschung · Partizipative Entwicklung von Systemen · EU: Grundrechte als Handelshemmnisse? · u.v.a.

216 Seiten, Bonn 1991, 12,80 DM

Jutta Schaaf (Hrsg.): Die Würde des Menschen ist unverNETZbar.

Netzknoten Frankfurt · Automatisierung des Zahlungsverkehrs · Rüstungshaushalt und Informationstechnik · Verfassungsverträglichkeit als Kriterium der Technikbewertung · Ethik und Technik · Theorie der Informatik · u.v.a.; **300 Seiten, Bonn 1990, 12,80 DM**

NEU: „Datendschungelbuch – *Ein pfiffiger Wegweiser für Ihren persönlichen Datenschutz" als elektronische Version unter*
http://www.bawue.de:80/~ernie/index.html
wieder für alle Interessierte verfügbar.

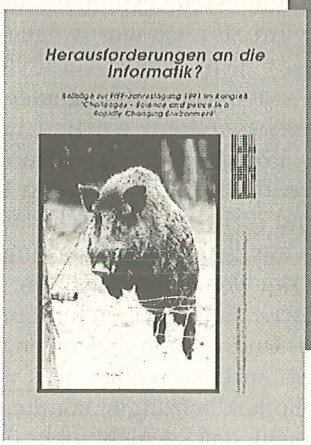
Ute Bernhardt, Ingo Ruhmann (Hrsg.): Ein sauberer Tod: Informatik und Krieg.

Informations- und Kommunikationstechnik – seit ihren Anfängen politisch geformt · Computer auf dem Schlachtfeld · Dual-Use: zivil geforscht – militärisch genutzt? · „Wehrtechnik und Landesvertidigung" – Zur Forschung in der Bundesrepublik · Weiter so oder umsteuern? · u.v.a.

320 Seiten, Marburg 1991, 20,– DM

Rudolf Kitzing, Ursula Linder-Kostka, Fritz Obermaier (Hrsg.): Schöne neue Computerwelt – Zur gesellschaftlichen Verantwortung der Informatiker

Beherrschbarkeit von Systemen, ihre Verletzlichkeit und die Verantwortung von Informatikern · Neue Wege in der Informatik · Psychosoziale Folgen des Computereinsatzes; **256 Seiten, Berlin 1988, 19,80 DM**



Heike Dörr (Hrsg.): Herausforderungen an die Informatik? – Science in a Rapidly Changing Environment

Wissenschaft und Ethik · Computergestützte und Elektronische Kriegsführung · Curricula und Forschungs- & Entwicklungs-Ansätze in der Informatik – den Anforderungen des 21. Jahrhunderts gerecht werden · Computertechnologie – ein angemessenes Mittel gegen die Armut der 3. Welt? · (Kredit-)Kartenzahlung im Licht von Daten- und Verbraucherschutz · Vernetzung von Friedensgruppen · Texte in englisch und deutsch. **126 Seiten, Bonn 1992, 12,80 DM**

Alle Bücher zzgl. Porto zu beziehen bei: FIFF-Geschäftsstelle, Reuterstr. 44, 53113 Bonn

Vielzweck-Schnipsel

Kopieren, ausfüllen und einsenden an: FIFF e.V., Reuterstraße 44, 53113 Bonn

FIFF

Das möchte ich:

- ❒ **Ich möchte ❒ aktives / ❒ förderndes Mitglied des FIFF werden** *(Mindestjahresbeitrag ist für Verdienende **100,- DM**, für Studierende und Menschen in vergleichbarer Situation **25,- DM** pro Jahr. Mitglieder in den neuen Bundesländern zahlen **60%** des Beitrags.)*
- ❒ **Ich möchte die FIFF-Kommunikation zum Preis von 25,- DM jährlich frei Haus abonnieren.**
- ❒ **Ich überweise den Mitglieds- bzw. Abobeitrag auf das Konto 480 00 798 bei der SPK Bonn, BLZ 380 500 00.**
- ❒ **Der Mitglieds- bzw. Abobeitrag soll per Lastschriftverfahren von meinem Konto abgebucht werden** *(siehe unten).*
- ❒ **Ich möchte meine neue/korrigierte Anschrift mitteilen** *(siehe unten).* **Meine alte/falsche Anschrift:**

  Straße: _____ *Wohnort:* _____
- ❒ **Ich möchte dem FIFF etwas spenden:**
- ❒ *Verrechnungsscheck über* _____ *DM liegt bei* ❒ *Spendenquittung am Ende des Kalenderjahres erbeten*
- ❒ **Ich möchte mehr über das FIFF wissen, bitte schickt mir:** _____
- ❒ **Ich möchte gegen Rechnung, zuzüglich Portokosten, bestellen:** _____
- ❒ **Ich möchte das FIFF über einen Artikel/ein Buch informieren:** ❒ **Zitat** *(siehe unten)* ❒ **Kopie** *(liegt bei)*
- ❒ **Ich möchte zur FIFF-Kommunikation beitragen mit:** ❒ **einem Manuskript zur Veröffentlichung** *(liegt bei)* ❒ **einer Anregung** *(siehe unten)*

  Bemerkungen/Ergänzungen: _____
  _____
  _____
- ❒ **Ich möchte einen richtigen Brief schreiben. Der Vielzweck-Schnipsel ist nichts für mich.**

Die/der bin ich:

Name: _____ *Straße:* _____

Wohnort: _____ *ggf. Mitgliedsnummer:* _____

Telefon (privat): _____ *(Arbeit):* _____ *E-Mail:* _____

Einzugsermächtigung

Hiermit ermächtige ich das FIFF e.V. widerruflich, meinen Mitgliedsbeitrag durch Lastschrift einzuziehen. Wenn das Konto keine Deckung aufweist, besteht keine Verpflichtung des Geldinstituts, die Lastschrift auszuführen.

Name: _____ *Jahresbeitrag:* _____ *DM, erstmals* _____

Konto-Nr.: _____ *BLZ:* _____ *Geldinstitut:* _____

Straße: _____ *Wohnort:* _____

Datum: _____ *Unterschrift:* _____

(Wir werden Ihre Daten nach §28 BDSG nur für eigene Zwecke verarbeiten und keinem Dritten zugänglich machen.)

Was will das FIFF?

Im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. haben sich InformatikerInnen zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen ihres Fachgebiets verantwortlich fühlen und entsprechende Arbeit leisten wollen:

- *Kritik üben, denn wir haben das Know-how dazu*
- *uns für eine Abrüstung der Informatik engagieren*
- *uns am Diskurs über Technik und Wissenschaft beteiligen*
- *die Öffentlichkeit warnen, wenn wir Entwicklungen in unserem Fachgebiet für schädlich halten*
- *möglichen Gefahren eigene Vorstellungen entgegensetzen*
- *die Informations- und Kommunikationstechnik nicht gegen, sondern für den Menschen gestalten*
- *uns für eine zivile und gerechte Welt einsetzen; eine Welt, in der die Grundrechte aller Menschen gewahrt werden, eine Welt, die menschenwürdig ist*
- *last not least nicht alles machen, was machbar ist*

Geplante

Themen-schwerpunkte

für die FIFF-Kommunikation im Jahr 1997:

3/97 **»Sicherheitsinfrastrukturen«**

zuständig: *Kathrin Schier, Claus Stark*

4/97 **»Arbeit«**

zuständig: *Ditz Schroer, Friedrich Holl*

Die FIFF-Kommunikation bittet um Beiträge!

Die FIFF-Kommunikation lebt von der aktiven Mitarbeit ihrer LeserInnen! Interessante Artikel sowie Fotos und Zeichnungen zur Illustration (mit Quellengaben) sind immer herzlich willkommen. Die Bearbeitung wird erleichtert, wenn Beiträge elektronisch und zusätzlich auf Papier der Redaktion zugehen. Die Redaktion behält sich Kürzungen und Titeländerungen vor.

Impressum

Die FIFF-Kommunikation ist das Mitteilungsblatt des »Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.« (FIfF). Die Beiträge sollen die Diskussion unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder. Nachdruck genehmigung wird nach Rücksprache mit der Redaktion in der Regel gerne erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Heftpreis: 6 DM. Der Bezugspreis für die FIFF-Kommunikation ist für FIFF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIFF-Kommunikation für 25 DM/Jahr (inkl. Versand) abonnieren.

Erscheinungsweise: einmal vierteljährlich

Erscheinungsort: Bonn

Auflage: 2000

Herausgeber: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIFF)

Verlagsadresse: FIFF-Geschäftsstelle, Reuterstr. 44, 53113 Bonn, Tel. (0228) 21 95 48

ISSN 0938 – 3476

Druck: Printwerkstatt Rambow, Auguststr. 10, 53229 Bonn, Tel. (0228) 46 22 14

Layout: Markus Hoff

Titelfoto: Hygienemuseum Dresden; Copyright Stephan Moses, München

Redaktionsadresse: FIFF-Kommunikation, Reuterstr. 44, 53113 Bonn, Tel. (0228) 21 95 48, Fax (0228) 21 49 24, E-Mail: fiffko@uni-paderborn.de

FIFF-Überall: In dieser Rubrik der FIFF-Kommunikation ist jederzeit Platz für Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an: hubert.biskup@sdm.de

Lesen, Schluß-PFIFF: Beiträge für diese Rubriken bitte per Post an Claus Stark (Heilbronn) oder per E-Mail an: stark@fh-heilbronn.de

Redaktionsschluß für die Ausgabe 3/97: 31.07.1997

Redaktions-Team FIFF-Kommunikation 2/97: Ute Bernhardt, Markus Hoff, Ingo Ruhmann, Claus Stark, Harald Selke (verantwortlich)

Hinweis: Postvertriebsstücke wie die FIFF-Kommunikation werden von der Post auch auf Antrag nicht nachgesandt, daher bitten wir alle Mitglieder und Abonnenten, dem FIFF-Büro jede ***Adreßänderung*** rechtzeitig bekanntzugeben!

Adressen

Berlin
Irina Piens
Schmidtstraße 3
10179 Berlin
piens@prz.tu-berlin.de

Bonn
Manfred Domke
Am Wildpfad 12
53639 Königswinter
manfred.domke@gmd.de

Braunschweig
TU Braunschweig
Fachschaft Informatik
AStA-Fach
Katharinenstraße 1
38106 Braunschweig

Bremen
Prof. Dr. Hans-Jörg Kreowski
Uni Bremen
FB Informatik/Mathematik
Postfach 330440
28334 Bremen
Tel.: (0421) 218-2956
fiff@informatik.uni-bremen.de
http://www.informatik.uni-bremen.de/~res/fiffhb.html

Darmstadt
Peter Bittner
Jens Woinowski
Hochstr. 56
64285 Darmstadt
Tel.: 06151/41805
bittner@mathematik.th-darmstadt.de
woinowsk@iti.informatik.th-darmstadt.de

Erlangen/Fürth/Nürnberg
Klaus Thielking-Riechert
Sommerstraße 10
90762 Fürth
k.thielking@link-n.cl.sub.de

Frankfurt
Ingo Fischer
Dahlmannstraße 31
60385 Frankfurt am Main

Hamburg
Simone Pribbenow
Hein-Köllisch-Platz 5
20359 Hamburg
Tel.: (040) 54715-366
pribbeno@informatik.uni-hamburg.de

Hannover
Bernhard Pfitzner
Rosenbergstraße 14a
30163 Hannover

Heilbronn
Claus Stark
Tel.: (07131) 33299
stark@fh-heilbronn.de

Kaiserslautern
Frank Leidermann
Moltkestraße 58
67655 Kaiserslautern
f_leider@informatik.uni-kl.de

Karlsruhe
Thomas Freytag
Institut AIFB
Universität Karlsruhe
76128 Karlsruhe
Tel.: (0721) 6084063 (d)
(0721) 815416 (p)
E-Mail: tfr@aifb.uni-karlsruhe.de

Kiel
Hans-Otto Kühl
Alte Kieler Landstraße 118
24768 Rendsburg
Tel.: (04331) 201-2187

Koblenz
Dr. Michael Möhring
Uni Koblenz-Landau
FB Informatik
Rheinau 3–4
56075 Koblenz
Tel.: (0261) 9119477
Fax: (0261) 37524
moeh@infko.uni-koblenz.de

Köln
Manfred Keul
Landsbergstraße 16
50678 Köln
Tel.: (0221) 317911
100031.12@compuserv.com

Konstanz
Volker Schuchardt
Jungerhalde 78
78464 Konstanz

Leipzig
Dr. Rolf Stranzky
Freiburger Allee 9
04416 Markkleeberg
Tel.: 0341/35690-0

München
Bernd Rendenbach
Leerbichlallee 19
82031 Grünwald
Tel.: (089) 6410547

Münster
Werner Ahrens
Hohe Geest 120
48165 Münster
Tel.: (02051) 3054 (p)
(0251) 491-429 (d)

Oldenburg
Universität Oldenburg
Fachschaft Informatik
Ammerländer Heerstraße
26129 Oldenburg
Fachschaft.Informatik@informatik.uni-oldenburg.de

Paderborn
Harald Selke
Heinz Nixdorf Institut
U-GH Paderborn
Fürstenallee 11
33102 Paderborn
Tel.: (05251) 606518
hase@uni-paderborn.de

Regensburg
Paul Hilmer
Zollerstraße 13
93053 Regensburg
Tel.: (0941) 706542
Fax: (0941) 706540
P.Hilmer@LINK-R.de

Stuttgart
Kurt Jaeger
Schozacher Straße 40
70437 Stuttgart
Tel.: (0711) 8701309
(0711) 90074-23
Fax: (0711) 7289041
pi@lf.net

Tübingen
Jochen Krämer
Sand 13
72076 Tübingen
Tel.: (07071) 29-5957
fiff@informatik.uni-tuebingen.de
http://www-fiff.informatik.uni-tuebingen.de

Ulm
Universität Ulm
Fachschaft Informatik
Bernhard C. Witt
Oberer Eselsberg
89081 Ulm
wittbe@pcpool1.informatik.uni-ulm.de

Überregionale Arbeitskreise

AK »RUIN« (Rüstung und Informatik)
Ingo Ruhmann
Paulstraße 15
53111 Bonn
Tel.: (0228) 634816
fiff@fiff.gun.de

AK »FIFF in Europa«
Dagmar Boedicker
Daiserstraße 45
81371 München
Tel.: (089) 7256547

AK »Informationstechnik für eine lebenswerte Welt«
Ralf Klischewski
Universität Hamburg
FB Informatik
Vogt-Kölln-Straße 30
22527 Hamburg
Tel.: (040) 54715-367
Fax: (040) 54715-311
klischew@informatik.uni-hamburg.de

FIFF-Mailingliste
Beiträge an:
fiff-l@dia.informatik.uni-stuttgart.de
An- und Abbestellungen an:
fiff-l-request@dia.informatik.uni-stuttgart.de

FIFF-WWW-Seiten
http://hyperg.uni-paderborn.de/~FIFF

FIFF-Geschäftsstelle
Reuterstraße 44
53113 Bonn

Tel.: (0228) 219548
Fax: (0228) 214924

E-Mail: fiff@fiff.gun.de

Dienstags 9 bis 15 Uhr,
Donnerstags 16 bis 19 Uhr

Kontoverbindung: 48000798
Sparkasse Bonn, BLZ 380 500 00

WahnsinnsWissenWachstum oder WeltWeiter Wahn?

von Stephan Ehlers, mit freundlicher Genehmigung

Erfahrungen mit dem WWW. Weitgehend Wahr Weitergegeben

Hand aufs Herz - WWW, diese drei Buchstaben beschäftigen Sie. Oder lesen Sie etwa keine Zeitung? Hören Sie kein Radio? Ihren Fernseher haben Sie in den letzten Wochen und Monaten auch nicht eingeschaltet? Ist ja auch nicht schlimm - Sie befinden sich in bester Gesellschaft. Laut einer Umfrage geben 80% der Deutschen (ab 14 Jahre) zu, schon etwas von WWW gehört zu haben. Egar ob Tagespresse oder Bäckerblume, ob öffentliche oder private Hörfunk- oder Fernsehsender - nicht nur die Medienmacher stolpern der Reihe nach ins weltweite Netz. Auch die Mediennutzer, sogenannte OnlineUser, bieten ihre Informationen im sogenannten Netz der Netze an. Alle machen mit - jeder teilt jedem mit, daß man sich was mitteilen kann. Kurzum: das WWW-Fieber ist ausgebrochen - allesamt getragen vom www-Leitmotiv: widersetzen womöglich waghalsig. Deutsche Manager setzen neuerdings fest aufs WWW: Womöglich-Wachstums-Wirksam.

Was ist nun dran am WWW ?

WirtschaftsWunderWaffe oder doch nur WeltWeiter Wahn? Derzeit tendiere ich eher zu letzterem. Zwar habe ich (noch) nicht alle Entwicklungsstufen der InternetUmgangs hinter mir. Dennoch war meine bisherige WWW-Nutzung durchaus erlebnisreich - diese Zwischenergebnisse möchte ich nun an Sie WWW-gemäß, sprich: weitgehend wahr weitergeben.

Noch völlig ohne Internet-Kenntnisse zeigten die „großartigen" WWW-Ankündigungen in den Medien ihre Wirkung auf mich: WWW ist für Außenstehende soetwas wie ein Wildfremdes WunderWerk. Ich war also vor meinen ersten Gehversuchen im Internet durchaus guten Mutes: Wohlgelaunt-Wissensdurst-Wettmachen, getragen von der Hoffnung, Wissen Wunschgemäß Weiterzuentwickeln. Ich Witterte WissensWertes. Diese www-Situation (was wäre wenn?) dauerte nicht all zu lange und habe mir also das Nötigste für den WWW-Anschluß besorgt. Der Erstkontakt mit dem Netz als Willig-Wackerer Web-Anfänger hatte mich sehr beeindruckt -allerdings negativ. Denn ich fand Widersinniges WirrWarr. Anstatt stürmisch das Tor zur Informationswelt aufzustoßen, fand ich Wirklichkeitsfremden WildWuchs vor. Das ganze angereichert durch Werbe-Wischi-Waschi. (Allen Erstsurfern und NochNichtWWWlern sei an dieser Stelle gesagt: dies ist mein ganz persönlicher - also höchst subjektiver Eindruck. Sie müssen nicht, können aber solche Erlebnisse machen). Aus den anfangs großen W's wurden auf einmal kleine w's: „wühlen wir weiter?" oder „weswegen weitermachen?"

Schnell hatte ich eine der wesentlichen Nutzungsvoraussetzungen für das WWW kapiert: Willenskraft Wird Wertvoll. Doch irgendwann finden auch Erstbenutzer den Weg zu den sog. Suchmaschinen ... Webseiten-WegWeiser. Haben Sie schon mal in so einer Suchmaschine (als Anfänger!) auf Anhieb etwas Brauchbares gefunden? Man sucht und sucht und sucht ... dies könnte eine mögliche Erklärung dafür sein, warum diese Einrichtungen Such- und nicht Findmaschinen heißen.

Weiterhin wunderbar wahnsinnig

Zusammenfassend habe ich folgende WWW-Erfahrungen gemacht. DieKunst der InternetNutzung für Neugierige und Wißbegierige besteht im Widerstehen Wirrer Wahlmöglichkeiten, und ich befürchte: Willensschwache Werden Weich. Für diese Personengruppe besteht durchaus die Gefahr vom WWW- zum WwWwWw-Nutzer zu mutieren, so daß sie zum Werkzeug windiger Werbeanbieter wertloser Waren werden. Also: Willensschwache Hände weg vom Internet! NNN (Noch-Nicht-Nutzer) interessiert sicherlich die Frage, wer im Großen und Ganzen die WWW-Nutzer sind. Es sind - natürlich WWWs: Wißbegierige, Wichtigtuer und Wartezeit-Inkaufnehmende. Vor allem letztere Personengruppe hat sich längst an World-Wide-Wait gewöhnt. Aus meinen bescheidenen Praxiserfahrungen heraus sollten folgende Personen das WWW meiden: Willensschwache, Widerspruchslose und Wichtigtuer. Jedem NNN muß ich leider die WWW-Illusion nehmen, Internet sei ein Wunderschönes WunderWerk. Konzentrieren Sie sich vor der Internet-Nutzung lieber auf die drei wesentlichen W's: Erstens: Weshalb? Zweitens: Wieso? Drittens: Warum? - Wenn Sie dann drin sind - also im WWW - dann kommen Ihnen die drei anderen W-Fragen ganz alleine und schneller als Sie denken: Wo? Wo? Wo?

Gelernt habe ich auch, daß eine bewußte, kritische, stets konzentrierte Wahrnehmung für die Internet-Nutzung von besonderer Bedeutung ist ... hierzu kann ich Ihnen eine kleine Eselsbrücke anbieten: Sie lautet abgekürzt - nein, nicht WeWeWe, sondern WaWaWa:

Wachsame Wahrnehmung Wahren.

Abschließend kann ich Ihnen für eine persönliche WWW-Nutzung noch ein WiWiWi empfehlen: Wichtigtuerische Wirkungen Widerstehen. Ich bedanke mich, daß Sie dieses WortWirrWarr bis hierhin durchgehalten haben. Eine weiterhin wunderbar-wahnsinnige und wissenswerte WWW-Nutzung wünscht Ihnen

Stephan Ehlers, Berlin

PS: Wer es wirklich wissen will: WWW heißt korrekt übersetzt „World Wide Web" - WWW-Experten finden Sie in Ihrer unmittelbaren Umgebung, das Aufsagen der drei Buchstaben reicht völlig. Glauben Sie's nicht? Probieren Sie's mal!

Erschienen in: ZUKÜNFTE Nr. 19, Frühjahr 1997

Geeignete Texte für den Schluß-PFIFF bitte mit Quellenangabe an Claus Stark (Adresse siehe Adreßverzeichnis) senden.