Deutscher Bundestag
13. Wahlperiode

Drucksache 13/11002

Vierter Zwischenbericht

der Enquete-Kommission
Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft*)

zum Thema

Sicherheit und Schutz im Netz

*) *Eingesetzt durch Beschluß des deutschen Bundestages vom 5. Dezember 1995 – Drucksache 13/3219.*

Vorwort

Die vom Deutschen Bundestag eingesetzte Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft" hat am 31. Januar 1996 ihre Arbeit aufgenommen. Am 7. November 1996 legte sie ihren ersten Zwischenbericht mit dem Titel „Meinungsfreiheit – Meinungsvielfalt – Wettbewerb. Rundfunkbegriff und Regulierungsbedarf bei den Neuen Medien" vor (Bundestagsdrucksache 13/6000). Die Kommission hat sich seitdem mit zahlreichen weiteren Themen beschäftigt. Sie reichen von den durch die neuen Informations- und Kommunikationstechnik ausgelösten Veränderungen für die Wirtschafts- und Arbeitswelt bis hin zu den durch die rasante technische Entwicklung entstandenen rechtlichen Herausforderungen. Ergebnis dieser Arbeit der Enquete-Kommission sind unter anderem Zwischenberichte zu den Themen Regulierungsbedarf, Urheberrecht, Jugendschutz und Verbraucherschutz.

Der nun vorgelegte Zwischenbericht trägt den Titel „Sicherheit und Schutz im Netz". Er will Antworten auf die Frage geben, wie spezifischen Risiken begegnet werden kann, die mit der Nutzung der modernen Informations- und Kommunikationstechnik einhergehen. Der Bericht behandelt damit ein außerordentlich wichtiges Thema. Weil die neuen Techniken immer stärker alle Lebensbereiche durchdringen, wächst die Abhängigkeit von ihrem reibungslosen Funktionieren. Datenverluste oder Systemzusammenbrüche können – beispielsweise im medizinischen Bereich, aber auch in der Finanzwirtschaft – katastrophale Folgen haben.

Der Zwischenbericht ist in drei Teile untergliedert. Der erste Teil beschäftigt sich mit der Frage, wie die Sicherheit in der Informationstechnik im allgemeinen gewährleistet werden kann. Er untersucht die technischen, organisatorischen und politischen Voraussetzungen für eine sichere informationstechnische Infrastruktur. Ein wichtiger Aspekt dieser umfassenden Themenstellung ist der „Datenschutz" im Sinne des Rechts auf informationelle Selbstbestimmung, das nach der Rechtsprechung des Bundesverfassungsgerichts vom Grundgesetz gewährleistet wird. Wie dieses Recht im Informationszeitalter geschützt werden kann, ist Gegenstand des zweiten Berichtsteils. Er greift damit ein Thema auf, das für die Akzeptanz der neuen Informations- und Komminikationstechniken von großer Bedeutung ist. Der dritte Berichtsteil schließlich behandelt das Thema „Sicherheit und Schutz im Netz" aus strafrechtlicher Perspektive.

Der Zwischenbericht „Sicherheit und Schutz im Netz" geht vor allem auf Arbeiten der Berichterstatter Dr. Manuel Kiper, MdB, Dr. Michael Meister, MdB, Jörg Tauss, MdB, und Hans-Otto Wilhelm, MdB, zurück. Wertvolle Anregungen lieferten eine öffentliche Anhörung von Sachverständigen im Frühling vergangenen Jahres sowie Gespräche, die mit Vertretern von Sicherheitsbehörden geführt wurden.

Der Zwischenbericht empfiehlt unter anderem, den Selbstschutz der Bürger im Informationszeitalter zu fördern. Das setzt freilich ein entsprechendes Bewußtsein der Gefahren und der Möglichkeiten des Selbstschutzes voraus. Der Bericht kann auch als Beitrag dazu angesehen werden, ein solches Bewußtsein zu schaffen.

Die Enquete-Kommission dankt den Sachverständigen, Instituten und Organisationen, die ihre Arbeit unterstützt haben.

Bonn, den 22. Juni 1998

Siegmar Mosdorf, MdB

Vorsitzender der Enquete-Kommission
„Zukunft der Medien in Wirtschaft
und Gesellschaft – Deutschlands Weg
in die Informationsgesellschaft"

Zwischenbericht
Sicherheit und Schutz im Netz

Inhaltsverzeichnis

A. Auftrag und Durchführung der Arbeit der Enquete-Kommission

1. Auftrag der Kommission

Der Deutsche Bundestag hat in seiner 27. Sitzung am 7. Dezember 1997 beschlossen, eine Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft" einzusetzen. Die Kommission, der zwölf Mitglieder des Bundestages und zwölf Sachverständige angehören, hat ihre Arbeit am 31. Januar 1996 aufgenommen. (Drucksache 13/3219)

Die schnelle Entwicklung der Informations- und Kommunikationstechnologien sowie der elektronischen Medien hat gravierende Auswirkungen auf Wirtschaft, Arbeitsmarkt, Gesellschaft, Kultur, Politik und Demokratie. Die Enquete-Kommission des Bundestages will die sich aus dem Einsatz dieser neuen Technologien ergebenden politischen Konsequenzen darstellen und Vorschläge für parlamentarische Initiativen machen, um einerseits die Chancen der Informationsgesellschaft umfassend zu nutzen und andererseits ihre Risiken angemessen zu bewältigen.

Die übergeordnete Themenstellung der Enquete-Kommission ist in sechs Arbeitsschwerpunkte gegliedert worden:

Entwicklungen im 21. Jahrhundert

- Wirtschaft 21
- Technik 21
- Bildung 21
- Umwelt und Verkehr 21
- Gesellschaft 21
- Parlament, Staat und Verwaltung 21

Die Untersuchungsergebnisse dieser Arbeitsschwerpunkte sind Grundlage für die Benennung politischen Handlungsbedarfs auf verschiedenen Gebieten:

- Schaffung eines ordnungspolitischen und rechtlichen Rahmens für die Informationsinfrastruktur
- Schaffung geeigneter Rahmenbedingungen, die eine optimale Nutzung der Technologien in verschiedenen Bereichen zulassen
- Sicherung eines funktionsfähigen Wettbewerbs
- Sicherung von Meinungsvielfalt und Informationsfreiheit
- Datenschutz und Datensicherheit
- Jugend und Verbraucherschutz
- Urheberrecht

Zu Feldern, auf denen Entscheidungen rasch getroffen werden müssen, werden jeweils Zwischenberichte vorgelegt, in denen Handlungsperspektiven aufgezeigt werden. Bisher hat die Enquete-Kommission zusammen mit dem vorliegenden Bericht „Sicherheit und Schutz im Netz" zu vier Themen einen Zwischenbericht vorgelegt. Der erste Zwischenbericht behandelt das Thema „Meinungsfreiheit, Meinungsvielfalt und Wettbewerb bei den Neuen Medien". Im zweiten Zwischenbericht „Neue Medien und Urheberrecht" werden die Auswirkungen der Neuen Medien auf das Urheberrecht dargestellt. Der dritte Zwischenbericht „Kinder- und Jugendschutz im Multimediazeitalter" untersucht die besonderen Herausforderungen der neuen Medien an den Kinder- und Jugendschutz. Mit dem nunmehr vorgelegten Zwischenbericht „Sicherheit und Schutz im Netz" werden die für die Entwicklung der Informationsgesellschaft ebenfalls grundlegenden Themen Datensicherheit und Datenschutz behandelt.

Wichtige Erkenntnisse für ihre Arbeit gewinnt die Enquete-Kommission aus Arbeitssitzungen, Workshops, Anhörungen und wissenschaftlichen Gutachten. Bei den Sitzungen tragen anerkannte Experten und Sachverständige zu bestimmten Themengebieten vor und beantworten Fragen der Mitglieder der Enquete-Kommission.

In dem vorliegenden Bericht sind u. a. das Expertenwissen und die Ergebnisse einer öffentlichen Anhörung zur Datensicherheit, eines Expertengesprächs mit Vertretern von staatlichen Sicherheitsbehörden[1]), der Studie „Information Warfare" des Bundesministeriums der Verteidigung, der Studie „Probleme der Datensicherheit in multimedialen Anwendungen der Medizin" und einer Sitzung zum Datenschutz eingeflossen.

[1]) Im Anhang zu diesem Zwischenbericht sind die Sachverständigen beider Veranstaltungen zusammen mit den Listen der behandelten Fragen aufgeführt.

2. Zusammensetzung der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft

Mitglieder

Vorsitzender:	Siegmar Mosdorf, MdB
Stellvertretender Vorsitzender:	Dr. Michael Meister, MdB

Die Abgeordneten:

Ordentliche Mitglieder:	*Stellvertretende Mitglieder:*
CDU/CSU	
Dr. Maria Böhmer, MdB	Klaus Brähmig, MdB
Dr. Martin Mayer, MdB (Obmann)	Renate Diemers, MdB
Dr. Michael Meister, MdB	Elmar Müller, MdB
Wilfried Seibel, MdB	Johannes Singhammer, MdB
Hans-Otto Wilhelm, MdB	Werner Lensing, MdB
SPD	
Doris Barnett, MdB (Obfrau)	Lilo Blunck, MdB
Eike Hovermann, MdB	Dr. Cornelie Sonntag-Wolgast, MdB
Thomas Krüger, MdB	Ludwig Stiegler, MdB
Siegmar Mosdorf, MdB	Jörg Tauss, MdB
F.D.P.	
Dr. Max Stadler, MdB (Obmann)	Jürgen Koppelin, MdB
BÜNDNIS 90/DIE GRÜNEN	
Rezzo Schlauch, MdB (Obmann)	Dr. Manuel Kiper, MdB
PDS	
Wolfgang Bierstedt, MdB (Obmann)	Gerhard Jüttemann, MdB

Die Sachverständigen:

Dr. Dr. Heike von Benda
Unternehmensberaterin mit Schwerpunkt „Neue elektronische Medien", Nürtingen

Prof. Dr. Jürgen Doeblin
Fachbereich Betriebswirtschaftslehre an der Fachhochschule Nürnberg

Hans-Roland Fäßler
Sprecher der Geschäftsführung G+J Funk- und Fernsehproduktions GmbH, Bertelsmann AG, Hamburg

Kurt van Haaren
Vorsitzender der Deutschen Postgewerkschaft (DPG), Frankfurt a. M.

Prof. Dr. Hans J. Kleinsteuber
Institut für Politische Wissenschaft und Institut für Journalistik, Fachbereich Philosophie und Sozialwissenschaften der Universität Hamburg

Prof. Dr. Herbert Kubicek
Hochschullehrer für Angewandte Informatik mit dem Schwerpunkt Telekommunikation und Informationsmanagement der Universität Bremen

Prof. Dr. Gisela Losseff-Tillmanns
Fachbereich Sozialpädagogik, Fachgebiet Soziologie der Fachhochschule Düsseldorf

Prof. Dr. Wernhard Möschel
Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Arbeitsschwerpunkte Deutsches und Internationales Kartellrecht, Wirtschaftsordnungsrecht und Bankenrecht der Juristischen Fakultät Tübingen

Prof. Dr. Arnold Picot
Institut für Organisation, Seminar für betriebswirtschaftliche Informations- und Kommunikationsforschung, Fakultät für Betriebswirtschaftslehre der Ludwig-Maximilians-Universität München

Prof. Dr. Hans Poerschke
Dipl.-Journalist, Leipzig

Prof. Dr. Reinhart Ricker
Professur für Medienrecht und Medienpolitik am Institut für Publizistik der Universität Mainz

Prof. Dr. Eberhard Witte
Institut für Organisation der Ludwig-Maximilians-Universität München

Kommissionssekretariat:
Der Enquete-Kommission wurde vom Deutschen Bundestag zur organisatorischen und wissenschaftlichen Unterstützung ihrer Arbeit ein Sekretariat zur Verfügung gestellt.

Leiter des Sekretariats:
Dr. Gerd Renken

Stellvertretende Leiterin des Sekretariats:
Isolde Kießling, Diplom-Ökonomin

Wissenschaftliche Mitarbeiter:
Martina Fritsch, Sozialwissenschaftlerin
Andreas Kühling, Diplom-Ökonom; M.Sc.
Dr. Lorenz Müller, Jurist

Sachbearbeiter/Büroleiter:
Klaus Braun, Diplom-Betriebswirt (FH)

Erste Kommissionssekretärin:
Jutta Hardt

Zweite Kommissionssekretärin:
Mechthild Meyer

Die Kommission dankt den Sachverständigen, Instituten und Organisationen, die ihre Arbeit durch Gutachten und die Bereitstellung von Materialien unterstützt haben.

3. Thema und Kontext der Schutzziele für Kinder und Jugend, Verbraucher und Wirtschaft, Bürger, Staat und Verwaltung

Moderne Informationstechnik überwindet räumliche, sprachliche und zeitliche Barrieren. Weltweit über globale Daten- und Telekommunikationsnetze verbundene Computersysteme eröffnen neue vielversprechende Möglichkeiten in zahlreichen Bereichen von Gesellschaft, Wirtschaft und Politik. So wird sich z.B. auch das Gesundheitswesen durch den Einsatz von Informationstechnologie umfassend und nachhaltig verändern. Patientenchipkarte und elektronische Krankenakte erlauben medizinischem Personal einen raschen Zugriff auf wichtige anamnesische und diagnostische Daten des Patienten. Die Faktoren „Zeit" und „Ort" rücken dabei in den Hintergrund, denn der Zugriff kann über das weltweite Datennetz „Internet" erfolgen. Hierbei gewinnt nicht nur der Patient durch einen verbesserten Gesundheitsschutz, sondern auch das Gesundheitswesen durch mehr Effizienz und Kosteneinsparungen.

Über diese Beispiele hinaus, verbinden sich mit dem Begriff „Telemedizin" zahlreiche neuartige Anwendungsmöglichkeiten der Informationstechnik im Gesundheitswesen. Die Chancen, die sich als ganzes in diesem Bereich für die Informationsgesellschaft eröffnen, hängen aber entscheidend davon ab, ob hochsensible Daten – etwa Informationen über Patienten – vor unberechtigtem Zugriff, Kopieren und Manipulieren sowie im Hinblick auf ihre Verfügbarkeit gesichert werden können (IT-Sicherheit), so daß die Privatsphäre von Patienten (Datenschutz) unangetastet bleibt. Aus anderer Perspektive betrachtet bedeutet dies auch, organisatorische Vorkehrungen gegen mögliche Computerdelikte (Strafrecht) zu treffen.

Diese Ambivalenz der gegenwärtigen Übergangssituation in eine vielfach so genannte „Informationsgesellschaft" rückt deutlicher in die öffentliche Aufmerksamkeit: Neben positiven Zukunftsbildern über die Chancen in einer „Informationsgesellschaft" gibt es gleichzeitig immer wieder neue, überraschende und bestürzende Meldungen darüber, wonach es etwa Schülern ohne besonderen Aufwand erneut gelungen sei, den Passwortschutz bei T-Online und American Online (AOL) zu überwinden, was – wenn diese Jugendlichen gewollt hätten – den Zugriff auf sensible, elektronisch gespeicherte Daten von Privaten möglich gemacht hätte.

Die Verquickung von datenschutzrechtlichen wie strafrechtlichen Aspekten mit dem Phänomen von nicht oder unzureichend gegebenem Schutz sensibler digitaler Daten kann als Signatur eben einer Entwicklungsphase hin zur „Informationsgesellschaft" verstanden werden, in der zahlreiche multimediale und interaktive Dienstleistungen allmählich die Labors verlassen und auf dem Weg zur breiten Anwendung sind.

Stichworte wie Telemedizin, Teleshopping, elektronischer Zahlungsverkehr stehen für Beispiele einer „neuen Wirklichkeit", die – dies wird immer klarer – , weit über die heute vorherrschenden Fragen einer technologischen Machbarkeit der elektronisch gestützten Dienstleistungsgesellschaft der Zukunft hinausgehen. Immer deutlicher zeigt sich, daß Probleme der wachsenden Abhängigkeit von offensichtlich nicht beherrschbaren Computerwelten nicht gelöst sind. So steht etwa das aktuell diskutierte „Jahr-2000"-Computerproblem – also daß weltweit die Computersysteme nach dem Übergang zum Jahr 2000 unkorrekt arbeiten oder ganz ausfallen, was zu einem Einsturz der globalen Wirtschafts- und Finanzströme führen könnte – für eine Symptomatik, die das öffentliche Interesse auf einen zwar wichtigen Tatbestand lenkt, daß der Weg in die „Informationsgesellschaft" offenbar mit neuartigen Sicherheitsproblemen belastet ist, die nicht aus dem Kontext eines allein technischen Sicherheitsverständnisses gelöst werden können.

Der ursprüngliche Ansatz, wonach informationstechnische Sicherheit allein durch Herstellung von Vertraulichkeit, Integrität und Verfügbarkeit elektronisch gespeicherter Daten zu gewährleisten sei, wird neuerdings im Rahmen eines „erweiterten" Sicherheitsverständnisses überwunden. Damit werden ausdrücklich auch die Sicherheitsbedürfnisse der handelnden Akteure – etwa das Recht das Bürgers auf Unbeobachtbarkeit bei der Nutzung von Geldautomaten – mit berücksichtigt. Dahinter steht die umfassendere Diskussion, daß es ohne einen besseren Schutz der Privatsphäre, mithin also des Rechts auf informationelle Selbstbestimmung, keine demokratisch verantwortbare „Informationsgesellschaft" geben kann.

Zunehmend rücken deshalb Fragen und erste Antworten in den Vordergrund einer politischen Debatte, die nicht bei den immer klarer erkennbaren Risiken eines von neuen, digitalen Technologien bestimmten Weges in die Zukunft stehenbleiben will, sondern ausdrücklich nach Lösungen sucht, die die Beherrschbarkeit dieser multimedial gestützten Entwicklung auch durch den Einsatz der Technik selbst anstrebt. Ob aber die neuen Formen der Verletzlichkeit der industriellen Gesellschaft durch nicht-sichere Informationstechnik mit technologischen Schutzstrategien rechtsstaatlich und demokratieverträglich gelingen werde, ist eine Frage, die die hier vorgelegten Berichte zum Thema IT-Sicherheit, Datenschutz und Strafrecht verbindet. Deutlich wird gezeigt, daß IT-Sicherheit, Datenschutz und Strafrecht als politisch zu gestaltende Handlungsfelder begriffen werden können, die möglicherweise, werden sie im Sinne des Schutzes und der Entwicklung bürgerlicher Freiheitsrechte genutzt, eine große Chance bieten, die soziale Akzeptanz einer multimedial bestimmten Zukunft zu fördern.

Noch ist der Mehrheit der Bürgerinnen und Bürger, von denen nicht immer ein von vornherein technikfreundliches wie technikaufgeschlossenes Rollenverständnis erwartet werden kann, keineswegs egal, was mit ihren Daten bei der Nutzung der neuen Tele- und Mediendienste, des digitalen Fernsehens, bei der Bezahlung mit Kreditkarten oder beim digitalen Telefonieren geschieht. Sie fürchten, und das mit Recht, daß durch die Datenspuren, die bei diesen elektronischen Aktivitäten immer anfallen, ihr persönliches Konsum- und Freizeitverhalten für unbefugte Dritte immer transparenter wird.

Ob das Projekt der „Informationsgesellschaft" womöglich an ungelösten Fragen des Datenschutzes, an der Sicherheitsproblematik oder an den unzulänglich bleibenden Kontrollmöglichkeiten des Strafrechts scheitert – weil es nicht oder unzureichend gelingt, rechtsstaatliche Errungenschaften in einer virtuell sich betätigenden Dienstleistungsgesellschaft zu gewährleisten –, ist heute noch nicht abschätzbar.

Aber eines steht fest: So wie heute absehbar ist, daß etwa das Geld virtuell wird oder die Telemedizin den Patienten und seine Krankengeschichte auf einen „Datenschatten" reduzieren muß – das Vertrauen der Bürgerinnen und Bürger gegenüber diesen ungewohnt neuen Möglichkeiten scheint im Moment noch keineswegs gesichert. Deutlich ist eine wachsende „Kultur des Mißtrauens" erkennbar, was aber als Chance gesehen werden sollte. Denn damit wachsen die Herausforderungen an IT-Sicherheit, Datenschutz und Strafrecht den nicht-technischen Komponenten dieser Debatte besondere Aufmerksamkeit zukommen zu lassen.

Offensichtlich erfordern die neuen digitalen Technologien auch neue Formen einer kulturell verträglichen Beherrschbarkeit. Diese sind, aus der Perspektive von heute, teilweise schon erkennbar oder werden diskutiert oder bedürfen noch der kreativen Ideenfindung. Tatsache bleibt, daß wir erfahrungslos sind, die notwendige Sozialverträglichkeit des Epochenwechsels, mit den in zunehmender Schärfe erkennbaren, noch nicht voll erkannten Chancen wie bewältigten Risiken in eine demokratiegemäße, die Zukunft der freiheitlichen Gesellschaft offenhaltende Perspektiven zu bringen.

Es ist dieser weite, gesellschaftliche Maßstab, der als zu gestaltender „Kontext" begriffen werden will, um damit dann IT-Sicherheit, Datenschutz und Strafrecht als Aktionsfelder politischen Handelns verstehen zu können. Schließlich geht es darum, das Potential national begrenzter Staatlichkeit zu optimieren, um die aus globalen wie virtuellen Cyberwelten hereinstürmenden neuartigen Chancen (Stichwort: weltweiter elektronischer Handel), aber auch die in ihren nichtbeabsichtigten Folgen kaum oder überhaupt nicht abgeschätzten Konsequenzen dieser Entwicklung für Rechtsstaatlichkeit und soziales Zusammenlegen präventiv und grundrechtsschützend zu gestalten.

In diesem Sinne versteht sich, wie unten gezeigt wird, beispielsweise der „Systemdatenschutz" als ein Ansatz, die neuen multimedialen Technologien von vornherein grundrechtsverträglich zu gestalten, um so dem Verfassungsrecht auf informationelle Selbstbestimmung aus der Logik der digitalen Möglichkeiten heraus eine Chance zu geben. Damit, so wird erwartet, kann dem Orwell'schen Schreckensszenario vom „gläsernen Menschen" wenigstens tendenziell, in weiterer Zukunft vielleicht sogar grundlegend, die Spitze genommen werden. Wird dieses Bemühen ergänzt durch die sich mit den Möglichkeiten der digitalen Technik ergebenden Chancen zum technologischen „Selbstschutz" seiner elektronisch gespeicherten personenbezogenen Daten – zumal es sich dann in der Regel um den Schutz dieser sensiblen Daten in Netzen handelt –, dann greift dieser rein technologische Schutz für die breite Masse der Bürgerinnen und Bürger wohl nur dann, wenn es auch zu einer massiven Aufklärung über die Möglichkeiten zum eigenverantwortlichen Umgang auch mit den Risiken der elektronischen Dienstleistungsangeboten kommt – beispielsweise bei der Eingabe der PIN an offenen Geldautomaten!

Noch ist die Gefahr nicht gebannt, daß die „Informationsgesellschaft" eine erneut geteilte Gesellschaft sein könnte.

Heutige Bemühungen gerade im Bereich von IT-Sicherheit, Datenschutz und Strafrecht haben vorrangig den Schutz der Interessen jener vergleichsweise noch kleinen technikaufgeschlossenen Minderheit im Auge, die fähig sind, wegen ihrer technischen Aufgeschlossenheit auch moderne Schutzmöglichkeiten zu nutzen. Das hat für sich gesehen auch weiterhin hohe Priorität. Zu schwach oder noch gar nicht entwickelt sind dagegen Ansätze und Fragen danach, wie es gelingen kann, die breiten, heute noch technikfernen Bevölkerungskreise für die Chancen, aber eben auch für die simultan immer gegenwärtigen fremdartigen und neuen Risiken – etwa der Möglichkeit des Verlustes digital über Netze verschickten geistigen Eigentums -zu sensibilisieren.

Der Förderung des „Sicherheitsbewußtseins" kommt dabei eine strategisch zu bewertende Schlüsselrolle zu, die, und das ist aus heutiger Sicht erkennbar, weit über die laufenden Aktivitäten zum Stichwort „Medienkompetenz" hinausgehen. So ist etwa die Frage nach didaktischen Ansätzen zur breiten Vermittlung von Verhaltensanforderungen im Versuch, zu einem optimierten Umgang von vorhandenen II-Sicherheitstechnologien zu kommen, kaum oder gar nicht beantwortet – was wirtschaftlichen Innovationen und der sozialen Akzeptanz abträglich sein wird.

Hierzu wäre ein neuartiger bildungspolitischer Ansatz zu entwickeln, der es zuläßt, den strategischen Stellenwert von Fragen nach der „Didaktik des Selbstschutzes mit IT-Sicherheit und Datenschutz" als Chance zu begreifen, um so vielleicht das heute absehbare Auseinanderfallen der „Informationsgesellschaft" – in eine starke Minderheit der „Informationsreichen" und einer großen Mehrheit der „Informationsarmen", also jenen, die es nie lernen konnten, sich und ihre persönlichen Daten zu schützen – zu verhindern.

Zu den neuartigen, aus den Möglichkeiten der digitalen Technologien erwachsenden Chancen zur Herstellung der Authentizität und Vertraulichkeit bei der privaten und geschäftlichen Kommunikation gehören

„Digitale Signaturen" und Verschlüsselungsverfahren.

Die Bundesrepublik Deutschland kann für sich in Anspruch nehmen, auf dem Gebiet des rechtsverbindlichen, gerichtsverwertbaren und vertraulichen Rechtsverkehr mit dem „Gesetz über die „digitale Signatur" (SigG), als Teil des Informations- und Kommunikationsgesetzes (IuKDG) weltweit ein bedeutsames Zeichen gesetzt zu haben. Mit dem SiG werden erstmals die Rahmenbedingungen für die sogenannte „elektronische Unterschrift" gesetzt. Die sich aus diesem Gesetz ableitenden verfahrungsmäßigen und technischen Umsetzungsmaßnahmen – etwa zum Aufbau sogenannter „Trust-Center" und damit, in weiterer Perspektive – zur kulturell verträglichen Herausgestaltung einer sogenannten „Sicherungsinfrastruktur" – werden es erstmals gestatten, verbindliche Rechtsgeschäfte über beliebige – auch unsichere – elektronische Kommunikationswege zu betätigen. Eindeutig: Dies ist ein Schwerpunkt zukunftsorientierter Sicherheitspolitik.

Ein anderer Schwerpunkt wird sicherlich die Antwort auf die Frage zu sein haben, wie hält es eine demokratisch verfaßte und sich offen bezeichnende Gesellschaft mit den Möglichkeiten der Verschlüsselungstechnik.

So ist aus Sicht des Datenschutzes die Nutzung kryptographischer Verfahren ein rechtsstaatliches Gebot des Bürgerschutzes, sozusagen der „elektronische Briefumschlag", um eigene sensible Daten gefahrlos über unwegsame Netze in virtuelle Welten zu schikken.

Aus der Perspektive der jungen, deutschen, sehr innovativen Kryptowirtschaft werden sich viele neue Anwendungen der Informationstechnik nur dann entwickeln und wirtschaftlichen Nutzen bringen können, wenn mittels spezifischer kryptographischer Möglichkeiten und auf benutzerfreundliche wie preiswerte Weise die grundlegende notwendige Vertraulichkeit des Datenaustausches hergestellt werden kann. Denn anzunehmen ist, daß der stetige Fortschritt bei digitalen Technologien die Verwendung von Rechenalgorithmen für die Verschlüsselung noch kostengünstiger machen wird.

Und genau diese Schutzmöglichkeiten, die die Kryptographie bietet, werden sich zum Beispiel die organisierte Kriminalität und politische Extremisten für ihre Zwecke zu eigen machen, womit sie – und das ist absolut neuartig – die staatlichen Möglichkeiten der Strafverfolgung wie Strafvereitelung strukturell und logisch zumindest einschränken kann – wobei die Möglichkeiten zur Nutzung des Internets als Instrument zur präventiven Strafverfolgung einen anderen Aspekt des Spektrums der Chancen wie der Risiken der neuen Technologien betont.

Dieses Dilemma konfligierender Interessen zwischen Datenschutz und IT-Wirtschaft einerseits und Staatsschutzinteressen andererseits ist unter dem Stichwort der „Kryptokontroverse" eine seit etwa 10 Jahren in Deutschland schwelende und ungelöste Debatte, die aber auch in den USA noch keineswegs abschließend beantwortet ist.

Das Verhältnis von IT-Sicherheit, Datenschutz und Strafrecht in der „Informationsgesellschaft" ist bislang von politischer Seite nicht in einem abgewogenen und aufeinander bezogenen Sinne bearbeitet worden. Ob IT-Sicherheit nur als Mittel des Datenschutzes oder des Strafrechtes verstanden wird, oder inwieweit es auch ein Ziel sein sollte und welche politischen Rahmenbedingungen dafür notwendig sind, ist bislang ebenfalls ungeklärt. Dieser Bericht der Enquete versucht daher aus einer Darstellung der Probleme auch Vorschläge für einen vernünftigen Gestaltungsrahmen zu erarbeiten, dem eine integrierte Sicht von IT-Sicherheit, Datenschutz und Strafrecht zugrunde liegt.

Eine nach demokratischen Prinzipien und zum Schutz der bürgerlichen Freiheitsrechte und ihrer zukünfigen Entwicklungen gestaltete „Informationsgesellschaft" bildet die Perspektive in dieser Sichtweise.

4. Berührungspunkte der Schutzziele für Kinder und Jugend, Verbraucher, Bürger, Wirtschaft, Arbeitswelt und Behörden

Das Verhältnis der in den folgenden drei Teilen des Berichts behandelten Bereiche Datenschutz, IT-Sicherheit und Strafrecht ist – wie darin sichtbar wird – durchaus nicht frei von Widersprüchen und Spannungen. Ein Grund dafür ist vor allem in den divergierenden jeweiligen Schutzzielen zu sehen. Andererseits ist auch zu konstatieren, daß zur Umsetzung des Schutzgedankens bei der Nutzung der IT einige Grundprinzipien einheitlich verwirklicht werden müssen. Der folgende Bericht versucht, aus den divergierenden Zielen heraus zu einem recht einheitlichen Blickwinkel zu kommen. Um das damit angelegte Spannungsfeld zu verdeutlichen, sollen in diesem Abschnitt wichtige Bezüge zwischen den drei Berichtsteilen verdeutlicht werden.

Zu den strittigsten Themen bei elektronischen Netzen gehört sicherlich die Debatte über die Zulässigkeit oder Unzulässigkeit unterschiedlicher Angebote im Internet. Hieran lassen sich besonders deutlich die Grenzen und Verknüpfungen einer Betrachtung von IT-Sicherheit, Datenschutz und Strafrecht aufzeigen. Vom technischen Standpunkt der IT-Sicherheit aus ist zu erkennen, daß die Möglichkeiten der Technik zur Filterung von Inhalten im Internet eng begrenzt sind. Auch der Datenschutz ist dadurch kaum

berührt, da es sich bei den umstrittenen Angeboten um öffentlich zum Abruf angebotene Daten und Informationsangebote handelt. Das Strafrecht schließlich kennt nur in wenigen der umstrittenen Fallgruppen überhaupt Strafbarkeitstatbestände, die eben dann zumeist nicht gegeben sind, wenn Angebote im Ausland verfügbar gemacht werden.

Als Hintergrund für diese bisweilen unbefriedigende Sachlage ist zu sehen, daß es dabei um die unterschiedliche Bewertung von Angebotsinhalten geht. IT-Sicherheit, Datenschutz und Strafrecht in elektronischen Netzen orientieren sich dagegen an sehr konkreten Sachverhalten und Risiken bei der Nutzung elektronischer Netze, bei denen überdies bereits eine gewisse, wenngleich deutlich verbesserungswürdige Grundlage an internationalen Übereinkünften besteht. Es geht in diesem Bericht also im Kern um Aussagen zu einer risikoverminderten Nutzung elektronischer Netze, nicht dagegen um eine Auseinandersetzung um in ihnen verfügbare Inhalte.

Dennoch ist es nicht so, daß alle drei in den Berichtsteilen untersuchten Bereiche nahtlos bei einer Risikoabwehr ineinander greifen. Ein offensichtliches Beispiel für die bereits angesprochenen divergierenden Ziele spiegelt sich im Spannungsverhältnis von Datenschutz und Strafrecht wider. Im Interesse der Strafverfolgung wäre es durchaus wünschenswert, jede Aktivität eines Nutzers im Netz zu protokollieren. Damit ließen sich nicht nur Gesetzesbrechern auf die Spur kommen, sondern möglicherweise sogar strafbare Handlungen im Ansatz erkennen und vereiteln. Um dies zu ermöglichen, müßte eine anonyme und vertrauliche Nutzung elektronischer Netze untersagt und statt dessen jede Nutzung mit eindeutigen personenbezogenen Angaben versehen werden. Aufgabe der IT-Sicherheit wäre dabei sicherzustellen, daß derartige Angaben nicht verfälscht werden können.

Abgesehen von den – schon aufgrund der Datenmengen – technischen Problemen mit derartigen Ideen, die bisher nicht einmal in autoritären Staaten realisiert wurden, hat eine solche Form der vollständig überwachten Nutzung elektronischer Netze die entscheidende Eigenschaft, mit einer Vielzahl von Grundrechten und rechtsstaatlichen Prinzipien zu kollidieren: Eine im vorgenannten Sinne extensive Nutzung von IT zur Überwachung von Nutzeraktivitäten ist mit einer demokratischen Verfassung unvereinbar. In einem demokratischen Rechtsstaat muß es daher darum gehen, persönliche Freiheitsrechte und staatliche Befugnisse auch bei der Nutzung elektronischer Netze in einer verfassungsmäßig gebotenen Weise abzuwägen.

Aus der Sicht des Datenschutzes ist es für Nutzer beim Surfen im World Wide Web dagegen bedenklich, daß Informationsanbieter bestimmte Daten nutzen können, um ein Persönlichkeitsbild über ihre Kunden zu gewinnen, das an Feinheit gewinnt, je öfter diese das elektronische Angebot wahrnehmen. Derzeit sind Vertraulichkeit und Anonymität der Nutzer und damit ihr informationelles Selbstbestimmungsrecht dadurch eingeschränkt, daß ihnen kein IT-System eine einfache Kontrolle der von ihnen abgerufenen Daten ermöglicht. Nur wenige Angebote im Internet offerieren die Anonymisierung als Informations-Dienstleistung.

Eine solche Anonymität wird oft als Gegensatz zur Authentizität der Nutzer gesehen. Es wird daher gern argumentiert, daß eine Nutzung von Electronic Commerce-Angeboten zumindest ein nicht-anonymes Surfen, besser noch automatische Authentisierunsgsverfahren voraussetzen. Doch auch beim nicht-anonymen Surfen existiert im Internet-Verkehr keine Technologie, die eine Authentisierung mit einer akzeptablen Korrektheit gewährleistet. Authentisierung in elektronischen Netzen setzt daher immer die Nutzung zusätzlicher Mechanismen wie etwa die digitale Signatur voraus. Damit sind Anonymität und Authentizität in der Praxis kein Gegensatz. Authentizität ist bei einem Informationsabruf meist unwichtig. Auch elektronische Transaktionen lassen sich so gestalten, daß darin anonyme Formen kein Hindernis darstellen müssen: Bei einer Transaktion Bargeld gegen Ware ist die Identität von Käufer und Verkäufer keineswegs durchweg erforderlich. Erst bei Rechtsgeschäften oder bei Finanztransaktionen wird eine Authentizität in vielen Fällen erforderlich. Authentizität beruht letztlich darauf, daß sich zwei Transaktionspartner ihres Gegenübers in dem spezifischen Rahmen sicher sind, wie er für die Transaktion notwendig ist.

Authentizität von Nutzern ist keineswegs nur im Interesse kommerzieller Anbieter. Auch die Angebote staatlicher Verwaltungen, beispielsweise im Internet, sind dann auf einen Authentizitätsbeweis angewiesen, wenn dort über reine Informationsangebote hinaus Dienstleistungen wie die Erledigung von Anträgen oder anderes zur Nutzung bereitgestellt werden, die zum Schutz der Bürger nicht-öffentlich oder vertraulich abgewickelt werden müssen. Wo elektronische Medien genutzt werden, sollte die Möglichkeit einer anonymen Beteiligung nicht generell ausgeschlossen sein.

Mit Informationstechnik ist eine Reihe von kommunikativen und sozialen Funktionen nachzubilden, die sich im Alltag als erforderlich erwiesen haben und die deswegen auch in Rechtsnormen formuliert sind. Technische Maßnahmen zur IT-Sicherheit sind dabei erst die Grundlage zu elektronischen Transaktionen, die sowohl den Rechtsvorschriften entsprechen als auch den Schutz der Persönlichkeitsrechte ermöglichen.

Gemeinsam ist allen diesen Gesichtspunkten, daß sie verschiedene Ausprägungen des Wunsches nach *Zuverlässigkeit oder Verläßlichkeit* zum Ausdruck bringen: IT-Sicherheit befaßt sich vorrangig mit Voraussetzungen an zuverlässige IT-Systeme, der Datenschutz will für eine Verläßlichkeit und damit Vertrauen bei der Verarbeitung und Weitergabe personenbezogener Daten sorgen, das Strafrecht schließlich setzt Grenzen fest, innerhalb derer man sich auf bestimmte Verhaltensformen verlassen kann. Diese drei verschiedenen Formen wurden bislang noch nicht angemessen zueinander in Beziehung gesetzt.

In diesem Spannungsverhältnis steht auch das eingangs angeführte Beispiel des Jugendschutzes. Rechtlich geht es beim Jugendschutz um den altersgemäßen Zugang zu Informationen und Dienstleistungen. In elektronischen Transaktionen geht es auch darum, Kinder und Jugendliche vor den Folgen mangelnder Kenntnisse von Vorschriften zu schützen. Dies umfaßt etwa die Rechtsmündigkeit und damit die Fähigkeit, Rechtsgeschäfte einzugehen. Diese Schutzgedanken implizieren daher im technischen Sinne – in einem weit stärkerem Maße, als es für erwachsene Nutzer rechtlich zulässig ist – entweder die Überwachung von Aktivitäten jugendlicher Internet-Nutzer oder Verfahren, die Jugendlichen den Zugang zu Informationsquellen nicht oder nur – etwa durch Anwendung technischer Verfahren wie des Vier-Augen-Prinzips – in Anwesenheit von Erwachsenen gestatten. Da jede Form der Überwachung jugendlicher Internet-Nutzer die Persönlichkeitsentwicklung nicht fördert, sondern mit Persönlichkeits-rechten konfligiert, ist hier nach Lösungen zu suchen, bei denen die Informationstechnik in flexibler Weise die Bedürfnisse von Eltern und Jugendlichen unterstützt.

Dies verdeutlicht: Das Recht und die Entfaltung der Person stehen in einem wechselseitigen Bezug zu den verfügbaren technischen Möglichkeiten des Schutzes, wie sie die IT-Sicherheit liefern kann. IT-Sicherheitsmechanismen wiederum werden in ihrer Bedeutung für die Nutzung und Gestaltung der Informationstechnik bei weitem noch nicht angemessen anerkannt. Es besteht bislang keine angemessene Verkopplung der Bedürfnisse von Nutzern, den Erfordernissen des Rechts und den Anforderungen an die Gestaltung von IT-Sicherheitsmechanismen. Anders herum wird zu wenig wahrgenommen, worin die technischen Grenzen dieser Bedürfnisse und Erfordernisse liegen und wo sich daher neue Formen des gesellschaftlichen Umgangs mit Informationstechnik entwickeln müssen.

In diesem Sinne geben die drei folgenden Berichtsteile eine Übersicht über die Situation der jeweils getrennt zu sehenden Sachgebiete. Gleichwohl wird in allen drei Teilen versucht, die notwendigen Bezüge zwischen IT-Sicherheit, Datenschutz und Strafrecht mit dem Ziel herzustellen, das Verständnis für eine erweiterte Sicht eines sicheren, geschützten und geordneten Umganges mit Informationstechnik zu wecken.

B. Berichtsteil: Sicherheit in der Informationstechnik

(Verabschiedet am 15. Juni 1998)

1. Ausgangslage

Moderne Gesellschaften sind von der Funktionsfähigkeit ihrer Infrastrukturen in hohem Maße abhängig. Den Infrastruktursystemen der Industriegesellschaft – Elektrizität, Telekommunikation und Verkehr – hat sich beim Wandel zu einer Informationsgesellschaft die Informationstechnik hinzugesellt, die durch ihre Kopplung mit der Telekommunikationstechnik umfassend als Informations- und Kommunikationstechnik (IuK-Technik) gesehen wird. IuK-Technik kommt mittlerweile in nahezu allen Lebensbereichen zur Anwendung, wie folgende Tabelle systematisiert:

Hartmut Pohl: Informationssicherheit der GII

Anwendungsfelder der GII
Erziehung, Bildung und Ausbildung – u.a. Familienplanungsbegleitende sowie berufsbegleitende Veranstaltungen, private Information und Kommunikation.
Konsumorientierte Dienste: Tele- und Homeshopping, Telemarketing, Werbung, Finanzdienstleistungen, individualisierte Publikationen.
Freizeit, Unterhaltung: Bibliotheken, Rundfunk, Fernsehen, Pay-TV, (Near-) Video-on-Demand, Interaktives Fernsehen, Museen, Konzerte, Spiele, ...
Gesundheitswesen: Beratung, Ferndiagnose, Überwachung, Operation, Vorbeugung, ... Notfall-Nutzung bei Krankheit, Unfall, Katastrophen, Höherer Gewalt.
Wissenschaft und Forschung, Teleteaching, Telelearning.
Gebäudesteuerung, Verkehrssteuerung, Fabriksteuerung.
Produktion, Reparaturen, Fernwartung.
Verwaltung: Behördenaktivitäten wie Umweltschutz (Überwachung, Steuerung).
Wahlen, Abstimmungen, Bürgerbegehren, Befragungen.

Quelle: Tauss, S. et al. Deutschlands Weg in die Informationsgesellschaft, Baden-Baden, 1996, S. 363

Die seit den 40er Jahren entwickelte Informationstechnik ist mittlerweile eine Universaltechnologie mit hohem Reifegrad. Nach der Lösung von zentralen Großrechneranlagen und der Migration zu PC-Systemen ist der heute bedeutsame Entwicklungsschritt die weltweite Vernetzung. Dies vollzieht sich zum einen – in Form von Local Area Networks (LANs) oder Intranets – innerhalb von Unternehmen und zum anderen zwischen einer Vielfalt unterschiedlichster Nutzer eines weltweiten Computernetzwerks wie dem Internet.

Das Beispiel Medizintechnik zeigt diese Entwicklung. Sie ist in hohem Maße computergestützt. Beispiele hierfür sind Computertomographen, Kernspintomographen, Operationsroboter, Geräte zur maßgenauen Einzelanfertigung von Prothesen, EKG, EEG sowie Röntgen- und Bestrahlungsgeräte. Mit der verstärkten Integration dieser digital gesteuerten Medizintechnik in Telekommunikationsnetzwerken werden neue Formen der Kommunikation und Datenvermittlung bzw. –verarbeitung im Gesundheitswesen möglich, die unter dem Begriff „Telemedizin"[2]) subsumiert werden.

Das Internet[3]) war ursprünglich ein Datennetzwerkprojekt mit militärisch-wissenschaftichem Forschungs- und Anwendungshintergrund. Durch die technische Entwicklung einer einfach zu bedienenden grafischen Benutzeroberfläche *World Wide Web* für Hypertext-Dateisysteme Ende der 80er Jahre und die von der Bush-Administration initiierte und unter Präsident Clinton forcierte Neuausrichtung der Technologiepolitik[4]) hat sich seit Anfang der 1990er Jahre die Nutzung des Internets rasant ausgebreitet.[5])

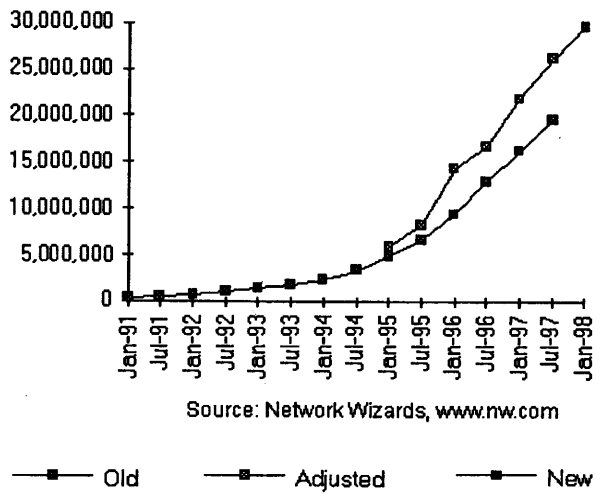
[2]) Vgl. Europäisches Institut für Systemsicherheit/Universität Karlsruhe, Künftige Anforderungen an die Kommunikationssicherheit in der Medizin (Gutachten für die Enquete-Kommission)

[3]) Der Begriff „Internet" beschreibt im eigentlichen Sinne die Kopplung unterschiedlicher technischer Übermittlungsstandards – sogenannter Protokolle wie TCP/IP, ftp, uucp oder Ethernet – in einem elektronischen Netz. Zusätzlich wird dieser jedoch auch benutzt, um die Nutzung gleichartiger Anwendungen in offenen oder geschlossenen Netzen zu umschreiben, bei denen in gleicher Weise – unabhängig von technischer Kompatibilität und organisatorischen Grenzen – auf Daten aus einem geschlossenen Intranet oder aus dem globalen Internet zugegriffen werden kann. Mit der einheitlichen technischen Basis und der abnehmenden Bedeutung organisatorischer Grenzen sollen die Voraussetzungen geschaffen werden, Daten in einem globalen Datenraum greifbar zu machen.

[4]) Vgl. Keil-Slawik, R., Die Zukunft der Informationsgesellschaft oder Bangemannen gilt nicht, in: Tauss, J.; Kollbeck, J.; Mönikes, J.; (Hrsg), Deutschlands Weg in die Informationsgesellschaft: Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik, Bonn, 1996, S. 855–863

[5]) Vgl. zur Geschichte des Internet: A Brief History of the Internet, in: http://www.isoc.org/internet-history.

Internet Domain Survey Host Count



Als Folge der Ausbreitung und intensiven Nutzung dieser neuen Infrastruktur läßt sich eine Konvergenz bislang getrennter Technologien und Medien beobachten, was unter dem Stichwort Multimedia verkürzt zusammengefaßt wird. Kennzeichen des neuen Mediums ist nicht das „Viele", Kennzeichen ist vielmehr das Integrieren der bisher nebeneinanderstehenden Medien in einem einzigen. Das Internet integriert Potentiale der mündlichen Direktkommunikation (Interaktion oder Telefon), der Printmedien (schwarzes Brett, Zeitung und Buch), der audio-visuellen Medien (Rundfunk, Fernsehen, Video). Es steigert deren Kapazität (durch höhere Archivierungs- und Speicherfähigkeit) und Transaktionsdichte (als many-to-many-Medium).

Auch wenn die Datenlage zum Internet als neuer Kommunikationsinfrastruktur aufgrund unterschiedlicher Meßmethoden vage ist, läßt sich ein exponentielles Wachstum nachweisen: Im Jahr 1995 wurden 24 Millionen Internet-Nutzer gezählt, während es 1996 bereits 50 Millionen waren. 1996 waren 300000 Web-Server im Internet, 1998 werden es voraussichtlich 3 Millionen sein[6]).

Die zunehmende Nutzung einerseits und die wachsende Abhängigkeit von der Verfügbarkeit der Informationstechnik andererseits verdeutlichen, daß der Weg in die Informationsgesellschaft mit erheblichen Risiken und Bedrohungen behaftet ist. Bei der zunehmenden Abhängigkeit unserer Gesellschaft von IuK-Technologien gewinnen informationstechnische Sicherheit und Datenschutz den Status eines infrastrukturellen Fundamentes für die Informationsgesellschaft.

Ausgehend von begrifflichen Klarstellungen werden im folgenden mögliche Risikopotentiale aufgezeigt, um mit Hilfe einer Betrachtung der bestehenden Rahmenbedingungen und den daraus abgeleiteten IT-Sicherheits-Schutzzielen zu Handlungsoptionen zu gelangen. Besonders eingegangen wird dabei auf die Problemfelder kryptographische Verfahren und digitale Signatur. Vor dem Hintergrund rechtlicher, sozialer wie technischer Optionen werden abschließend politische Handlungsempfehlungen entwickelt.

Die Diskussion um die Sicherheit der zum Einsatz kommenden informationstechnischen Systeme ist national wie international sehr vielfältig. Sie reicht von den unterschiedlichen Sicherheitsbedürfnissen der Beteiligten am Informationsausstausch über die Fehleranfälligkeit der verwendeten technischen Systeme und den Einsatz kryptographischer Verfahren für die Verschlüsselung von Daten bis zur Gestaltung von Infrastrukturen, die den mehrseitigen Sicherheitserfordernissen in verteilten Systemen und offenen Netzen Rechnung tragen bis hin zur Definition einer nationalen, aber global angemessenen Kryptopolitik.

Es sind unterschiedliche Einflußphären, die die Sicherheit von konkreten IT-Anwendungen bestimmen[7]):

- die informationstechnische Sicherheit der eingesetzten Hard- und Softwareprodukte, d. h. die Eigenschaften der Systeme, sich verläßlich zu verhalten, gegen unabsichtliche und absichtliche Angriffe auf die IT-Sicherheit resistent zu sein, sie erkennen, abwehren und nachvollziehbar machen zu können (technische Sicherheit);
- IT-Sicherheit als Leistungsmerkmal von IT-Systemen, die eine sorgfältige und verläßliche Nutzung der Systemkomponenten ermöglicht (Anwendungssicherheit);
- die an Sicherheit und Datenschutz orientierte Gestaltung der Informations- und Datenflüsse in einer Organisation (organisatorische Sicherheit);
- die Fähigkeit und Bereitschaft der beteiligten Personen, im Sinne der informationstechnischen Sicherheit zu handeln (personelle Sicherheit).

Die Praxis zeigt, daß die Bedeutung dieser Einflußsphäre für die erzielte Sicherheit in der Reihenfolge der hier gewählten Darstellung steigt. Nicht umsonst weisen alle bisher bekannt gewordenen IT-Sicherheitsuntersuchungen nicht hinnehmbare Restrisiken im personellen Bereich auf.

Als allgemein akzeptierte Ziele für den sicheren Einsatz von IT-Systemen werden Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit weitgehend anerkannt. Der „Weg" zur Beherrschbarkeit der neuartigen Sicherheitsrisiken in der Informationsgesellschaft – sollen sie verfassungs- und sozialverträglich für die gesellschaftliche Ordnung gehalten werden – bestimmt sich aus einem zusammenwirkenden Handlungsmix von technologischen, organisatorischen, rechtlichen, sozialen und kulturellen Regelungsebenen, die neben ihrer Multidiziplinarität vor allem in ihrer internationalen Orientierung eine – gerade durch das Internet geforderte – globale Verankerung finden[8]).

[6]) Vgl. hierzu: http://www.unisys.nl/pp/113/tsld003.htm

[7]) Vgl. Berliner Datenschutzbericht, 1995, S. 51

[8]) Vgl. BSI-Tagungsband 1996, S. 13

„Die E-Stufen der ITSEC

- **E0: Unzureichende Vertrauenswürdigkeit**
- E1: Es wurden Sicherheitsziele und -funktionalitäten definiert (Sicherheitsvorgang), eine informelle Beschreibung des Systems wurde geprüft (Architekturentwurf). Es finden Tests zur Überprüfung der Sicherheitsfunktionalität statt.
- E2: Zusätzlich zu E1 muß ein Deigsnentwurf vorgelegt werden (Feinentwurf). Die Entwicklungsumgebung wird überprüft.
- E3: Zusätzlich zu E2 muß der Hersteller den Quellcode zur Verfügung stellen.
- E4: Zusätzlich zu E3 müssen zu den Sicherheitsvorgaben ein formales Sicherheitsmodell, ein formales Sicherheitsmodell, zu den sicherheitsspezifischen Funktionen semiformale Spezifikationsdokumente zur Verfügung gestellt werden.
- E5: Zusätzlich zu E4 muß der enge Zusammenhang zwischen Feinentwurf und Quellcode nachgewiesen werden.
- E6: Zusätzlich zu E5 müssen sicherheitsspezifische Funktionen und der Architekturentwurf in formaler (Beweisbarer) Notation vorliegen, die konsistent mit dem formalen Sicherheitsmodell sind."[9])

Dabei ist IT-Sicherheit keine Konstante, weniger ein erreichter bzw. zu erreichender (Ideal- oder End-) Zustand. IT-Sicherheit ist ein immerwährender Prozeß hinsichtlich der Durchsetzung von Schutzzielen – sozusagen „eine unendliche Geschichte" der wechselseitigen Beziehungen von (effektiver und zuverlässiger) Zweckrealisierung, Bedrohung, Gefahrenabwehr, Akzeptanz und Vertrauen sowie vor allem deren „Ausbalancierung" und „Harmonisierung" – auch unter der Bedingung einer sich verändernden (IT-sicherheitsrelevanten) „Umwelt"[10]).

„Common Criteria" – die neuen Sicherheitskriterien

„Die „Common Criteria for Information Technology Security Evaluation"(CC) sind Ende Januar 1996 nach zweieinhalb Jahren intensiver Arbeit fertiggestellt worden – und gelten ab Oktober 1997 auch in Deutschland. Sie stehen nun für Evaluationen von IT-Sicherheitsprodukten zur Verfügung. Damit ist das internationale Projekt unter Beteiligung Deutschlands, Frankreichs, Großbritanniens, Kanadas, der Niederlande und der USA erfolgreich zu einem Abschluß gekommen.

Die CC sind eine Weiterentwicklung und Harmonisierung der ITSEC. Wie die ITSEC erlauben die CC eine getrennte Prüfung und Bewertung der Funktionalität und der Vertrauenswürdigkeit. Die CC bieten mit fast 200 detailierten Funktionalitätskomponenten sehr viel konkretere Funktionalitätskriterien als die ITSEC, dennoch kann wie bei den ITSEC auch jede sinnvolle sicherheitsspezifische Funktion evaluiert werden, die nicht ausdrücklich in den Kriterien aufgelistet ist.

Basis für die Vertrauenswürdigkeitsbewertung sind sieben (ITSEC: sechs) Vertrauenswürdigkeitsstufen, die inhaltlich etwa den E-Stufen der ITSEC entsprechen.

Das vorrangige Ziel der internationalen Harmonisierung von IT-Sicherheitskriterien ist die formale gegenseitige Anerkennung von Evaluationsergebnissen. Wenn sichergestellt ist, daß von den beteiligten Stellen dieselben Kriterien und dasselbe Evaluationsverfahren in gleicher Weise angewendet werden, ist es möglich, ausreichendes Vertrauen in die Prüfungsergebnisse anderer Stellen zu haben."[11])

Dieses nur dynamisch zu verstehende Verständnis von IT-Sicherheit – in Fachkreisen wird auch von IV-Sicherheit, im Sinne von Informations*verarbeitungs*sicherheit gesprochen – entspricht nicht nur der Entwicklungsdynamik und der hohen Innovationsrate der Informationstechnik, sondern auch dem herkömmlichen Verständnis von Sicherheit überhaupt.

In der aktuellen Debatte um IT-Sicherheit wird ersichtlich, daß dabei neben den unmittelbaren (informations-) technischen Zusammenhängen verschiedenartige *nichttechnische* Komponenten bedeutungsvoll sind: Zwecksetzung, Akzeptabilität, Verfügbarkeit, Beherrschbarkeit, „Nutzerfreundlichkeit", Veränderungsdynamik, Sicherheitsverlangen usw. Diese Komplexität ist nur erklär- und verstehbar, wenn davon ausgegangen wird, daß einzelne und konkrete IT-Sicherheitslösungen in ein „nichttechnisches Umfeld" sozusagen „eingebettet" werden, das von der techniknahen Infrastruktur bis hin zu global wirkenden Akteuren, vom Stand von Wissenschaft und Technik bis zu politischen „Vorgaben", vom geistigen Klima in der Gesellschaft bis zum Wertekanon der teilhabenden Individuen reicht. Dieses gesamte Umfeld wird in der Literatur unter den Begriff des „Nichttechnischen der IT-Sicherheit" subsumiert.[12])

Die Berücksichtigung sowohl der technischen wie der nichttechnischen Dimensionen der IT-Sicherheit ist noch nicht hinreichend gelöst, zumal sie nicht aus der Perspektive von wissenschaftlichen Einzeldisziplinen bearbeitet werden kann. In der fortgeschrittenen Diskussion über IT-Sicherheit ist unbestritten, daß es nicht ausreicht, IT-Sicherheit ausschließlich auf sichere Informationstechnik zu reduzieren. „Neben die technische Sicherheit müssen Anwendungssicherheit, aber auch organisatorische und personelle Sicherheit treten. Das erfordert eine fortgesetzte interdisziplinäre Diskussion, die nicht nur das technisch Machbare und juristisch Sanktionierbare berücksichtigt, sondern sich auch mit den sozialen, psychologischen, kulturellen und ethischen Komponenten wie auch mit den ökonomischen und ökologischen Auswirkungen beschäftigt."[13])

In der interdisziplinären Diskussion über die konzeptionelle Perspektive der IT-Sicherheit besteht Einvernehmen, daß nur ein in diesem Sinne umfassendes Verständnis von IT-Sicherheit überhaupt Ansätze bietet, zu einer politischen Gestaltung der IT-Sicherheit zu kommen. Nur so könne es möglicherweise zu

[9]) BSI-Informationsblatt, Sicherheitskriterien und Evaluierung nach ITSEC

[10]) Banse, G., Nichttechnisches in der IT-Sicherheit – Positionen und Probleme, in: BSI-Tagungsband, Mit Sicherheit in die Informationsgesellschaft, Ingelheim, 1997, S. 187

[11]) BSI-Informationsblatt, Common Criteria, Informationen auch unter http://www2.cordis.lu/infosec/src/crit.html

[12]) Banse, G., Nichttechnisches in der IT-Sicherheit: Positionen und Probleme, in: Bundesamt für Sicherheit in der Informationstechnik (BSI), Mit Sicherheit in die Informationsgesellschaft, Tagungsband 5. Deutscher IT-Sicherheitskongreß des BSI, Bonn 1997, S. 185ff.

[13]) INFORUM 2000/3; Vgl. Rudinger, 1997, S. 146f.; Wehner, 1992, S. 123f.

einer politisch verantwortbaren Beherrschbarkeit einer sich *dynamisch, virtuell* und *vernetzt* entwickelnden neuartigen Techniklandschaft mit ihren ebenso neuartigen, zumeist allerdings kaum abschätzbaren Risiko- und Unsicherheitsphänomenen kommen[14]).

Datensicherheit oder IT-Sicherheit?

„Auf dem Weg in die Informationsgesellschaft muß davon ausgegangen werden, daß Computerkriminalität (Mißbrauch personenbezogener Daten, Finanzmanipulation usw.), Sabotageversuche an Datenverarbeitungssystemen, Spionage im Bereich der Forschung und der Industrie unter Ausnutzung von IT-Systemen und Netzen, Attacken der Hacker und Phone-Freaks („Einbruch" in Systeme über internationale Netzwerke und Manipulation derselben), Computer-Viren und andere Software-Manipulationen nur die Spitze eines Eisberges noch weitgehend unbekannter Risiken und Sicherheitslücken darstellen. Sie können offenbar nicht aus der konventionellen Perspektive des Umgangs mit Unsicherheiten verhindert und bearbeitet werden. Diese nicht-beabsichtigten Folgen der Informationstechnik wurden bislang zu wenig, zu einseitig oder gar nicht beachtet. Aus dieser unbefriedigenden Situation heraus ist schon vor etwa 20 Jahren das Gebiet der *Informationssicherheit* entstanden. Ursprünglich weitgehend auf militärische Bedürfnisse ausgerichtet, hat sich die Informationssicherheit heute zu einem breiten interdisziplinären Arbeitsgebiet entwikkelt, zu dem Aspekte des *Datenschutzes,* der *Ordnungsmäßigkeit* der Datenverarbeitung, aber auch des *Kommunikationsrechts,* die Beachtung der *Sicherheitsqualität,* Normen und Standards, verbesserte Entwicklungsmöglichkeiten und Werkzeuge vor allem zur *Software-Herstellung,* sowie die Untersuchung von Manipulationsmethoden und entsprechender Gegenmaßnahmen gehören.

Vielfach wird auch von IT-Sicherheit, Computersicherheit, Datensicherheit, Datensicherung und Datenschutz gesprochen – alles Begriffe, die zwar nicht gleichbedeutend sind, aber zum gleichen Kontext gehören, nämlich der sicheren Verarbeitung von Informationen.

Während *Informationssicherheit* der umfassendere Begriff ist, beziehen sich die Begriffe Computersicherheit und IT-Sicherheit eher auf die technischen Sicherheitsaspekte in IT-Systemen und IT-Produkten.

Datensicherheit ist ein älterer Begriff für Informationssicherheit – konzentriert sich aber im Schwerpunkt nur auf die Sicherung der *Daten.*

Datensicherung bezeichnet das Teilgebiet der sicheren *Speicherung* von Daten.

Datenschutz meint die rechtlichen, technischen und administrativen Vorgaben bei der Verarbeitung und Speicherung von *personenbezogenen* Daten gemäß der Datenschutzgesetze.

Um aber den komplexen Phänomenen der neuartigen Risiken und heute erkennbaren Sicherheitsdefiziten der Multimediaanwendungen gerechter zu werden, ist ein erweitertes Sicherheitsverständnis, im Sinne einer *mehrseitigen Sicherheit,* erforderlich."

In der sich entfaltenden neuartigen Praxis der IT-Sicherheit wird diese „Hintergrundkomplexität" aber noch kaum gesehen; IT-Sicherheit wird vielmehr von vielen immer noch als lästige, gern vernachlässigte Nebenfolge des – auf den ersten Blick – mehr Effizienz und Rationalität versprechenden Einsatzes von IT-Systemen verstanden. Hier liegt ein hoher, noch nicht bewältigter Bedarf an Aufklärung und Sensibilisierung nicht nur des Bürgers, sondern auch der verantwortlichen Führungskräfte in Unternehmen wie öffentlichen Institutionen, besonders weil hier und in vielen Fällen nicht von vornherein ein technikfreundliches Rollenverständnis erwartet werden kann. Noch wird die Herstellung von IT-Sicherheit kaum als politisch Gestaltungsaufgabe verstanden – was aber die Wirtschaft nicht aus ihrer Verantwortung entläßt, die notwendigen Schritte zum Aufbau eines angemessenen „Sicherheits-Management" zu unternehmen. Die sich derzeit herausbildende neuartige Risikostruktur einer „neuen Wirklichkeit" ist aber immer weniger allein durch technische Maßnahmen kontrollierbar und beherrschbar zu halten.

Diese „neue Wirklichkeit" läßt sich heute mit folgenden Prinzipien beschreiben[15]):

Unsichtbarkeit

Elektronische Information ist als solche nicht lesbar. Der Prozeß der Sichtbarmachung erfordert verschiedene Techniken, wobei dann unterschiedliche informationstechnische Systeme elektronische Informationen auch unterschiedlich wiedergeben können, mit der Folge: Es gibt kein „Original" mehr bzw. nur noch „Originale".

Flüchtigkeit elektronischer Informationen

Die elektronische Information als elektrische Ladung ist extrem leicht veränderbar, sie kann verschwinden, ohne Spuren zu hinterlassen, z. B. durch den überall gegebenen „Einfluß" von elektromagnetischen Feldern.

Immaterieller Charakter elektronischer Informationen

Immaterielle Austauschbeziehungen und Regulationen stehen paradigmatisch dem heutigen Alltag entgegen und basieren auf materiellen Objekten und physikalischen Gesetzmäßigkeiten.

Dies kommt einem gesellschaftlichen Leitbildwechsel gleich – von körperlichen zu unkörperlichen Werten.

Veränderungen zeitlich-räumlicher Relationen

Telekommunikationssysteme führen zur sinnesmäßig nicht mehr erfaßbaren Beschleunigung des Transportes von Informationen über territorial nicht begrenzbare Räume. Damit werden alle gegenwärtig auf die nationalstaatliche Ebene bezogenen Regelwerke, etwa politischer, wirtschaftlicher oder rechtlicher Art, ausgehebelt.

Probleme der IT-Sicherheit werden meist erst dann wahrgenommen, wenn es zu Schäden gekommen ist. Anhand einiger Beispiele sollen Auswirkungen von Ereignissen und die Ursachen für ihr Auftreten aufgezeigt werden[16]):

- Durch einen *Computerfehler* geriet eine Bank in Zahlungsschwierigkeiten. Sie mußte einen Sonderkredit von zwanzig Milliarden Dollar aufneh-

[14]) Vgl. Ulrich 1995d, S. 114f., in: BSI-Handbuch 95b
Kersten, H., Sicherheit in der Informationstechnik. München, Wien 1995

[15]) Vgl. Stransfeld, R. et al., Rechtliche Aspekte des „Information Superhighway". Studie im Auftrag des BMBF, Teltow, 1995, S. 28ff.

[16]) Vgl. BSI-Handbuch 92

men und dafür in kurzer Zeit fünf Millionen Dollar Zinsen zahlen.

- Die Fernvermittlungsstelle einer deutschen Großstadt fiel vermutlich durch einen *Softwarefehler* zweimal aus – über 100000 Teilnehmer waren jeweils für mehrere Stunden von der Außenwelt abgeschnitten.
- *Computer-Viren* befallen seit einigen Jahren in steigendem Maß vor allem Programme auf Personal Computern. Gefährlich sind ihre unkontrollierte Verbreitung und die Wirkungen einer eventuell vorhandenen Schadensfunktion. Eine Firma mußte für sechs Wochen schließen und alle Daten neu eingeben, weil ein Virus – durch das Ungeschick einer Operateurin – alle Sicherungskopien unbrauchbar gemacht hatte. Der Verlust wurde auf eine Million US-Dollar geschätzt.
- Bei einer Bank dauerte die Restaurierung des Plattenspeichers zehn Stunden, mit einem Folgeschaden von mehr als zwei Millionen DM. Die Ursache war ein Fehler in einem Systemprogramm.
- Bei einer internationalen Großbank in Frankfurt hat ein DV-Systemberater gemeinsam mit einer weiteren Person betrügerisch einen Betrag von 2,8 Millionen US-Dollar über das „Electronic Banking" erlangt.
- Die nachrichtendienstlichen Organe der ehemaligen DDR haben den über Rundfunk und Satelliten geführten Fernmeldeverkehr systematisch – mit Unterstützung von Computern – abgehört und dabei Gerätekennungen und Paßwörter erfaßt. Mit diesen Kenntnissen sind Zugriffe zu Informationen auf IT-Systemen in Behörden und Wirtschaft erfolgt. Der dadurch verursachte Schaden kann im einzelnen nicht beziffert werden.
- Durch eine Bombenexplosion an der verglasten Außenwand des Rechenzentrums einer Maschinenfabrik entstand ein direkter Schaden von zwei Millionen DM. Die Folgeschäden durch Produktionsausfall lagen bei neun Millionen DM.
- Ein Unwetter überschwemmte den Installationsboden eines Rechenzentrums, weil das Dach undicht wurde. Die notwendige Neuverkabelung dauerte fast drei Tage. Der Folgeschaden betrug 800000 DM.
- Ein „frustrierter" Operator verursachte mehrmals täglich „unerklärliche" Systemzusammenbrüche, die jedesmal umfangreiche Wiederanlauf-Arbeiten notwendig machten. Der Schaden belief sich auf 1,4 Millionen DM.
- Ein gekündigter Programmierer modifizierte ein häufig benutztes Programm derart, daß in einer zentralen Datenbank zufällige Veränderungen vorgenommen wurden. Die Manipulation wurde erst nach zwei Jahren zufällig entdeckt. Die Rekonstruktion der Datenbank kostete 1,2 Millionen DM.
- Durch die Presse ging ein Fall, bei dem ein Programmfehler tödliche Folgen hatte. Weil die Software des radio-therapeutischen Bestrahlungsgeräts Therac die Strahlung für Krebspatienten in US-Kliniken falsch dosierte, starben 1987 zwei Menschen. Mindestens drei weitere wurden schwer verstrahlt.
- Mit einem ganz bestimmten Befehl lassen sich Intel Pentium- und Pentium-MMX-Prozessoren und damit alle damit arbeitenden *Systeme lahmlegen.* Der US-Chipproduzent Intel bestätigte, daß ein Fehler auf den beiden Prozessortypen die Sabotage von Computersystemen ermöglicht. Diesen Fehler könnten allerdings nur Spezialisten kennen, heißt es bei Intel.[17])
- Ein Computerfehler legte für fast zwei Tage den Eisenbahnfernverkehr in Hamburg-Altona lahm. Der 63 Mio. DM teure Rechner wurde an einem Sonntag im März 1995 angeschlossen. Er sollte das neue Stellwerk in Hamburg-Altona regulieren. Am Montagmorgen schlug dann ein Fehler im Speichersystem zu: Zwei Tage lang mußten Fernverkehrszüge über zwei andere Bahnhöfe umgeleitet werden, es gab im Nah- und Fernverkehr bis zu 40 Minuten Verspätung. Erst nach der Simulation der Vorgänge fanden die Techniker den Fehler.[18])
- Es waren Programmierfehler, die dazu führten, daß die Meteorologen den großen Sturm im Oktober 1987 in Großbritannien nicht vorhersagen konnten.[19])
- Ein Bürger von Agnes Waters, Australien, war für sechs Stunden eingesperrt worden, weil er ein Bußgeld angeblich nicht bezahlt hatte. In Wirklichkeit war dieses Bußgeld von ihm schon fünf Jahre zuvor bezahlt worden. Die Polizei führte dieses Mißverständnis auf einen Computerfehler zurück.[20])

Nicht allein die Fragilität und Störanfälligkeit der IT-Systeme selbst stellt nunmehr ein Risiko dar. Die zunehmende Vernetzung von IT-Systemen führt zu einer Potenzierung der Risiken. So wächst nicht nur die Gefahr eines Befalls mit Computerviren oder das Risiko ungewollter Zugriffe von außen über die Erreichbarkeit des eigenen IT-Systems durch Dritte:

- In einem internationalen *Netz-Verbund* wurde die lawinenartige Vermehrung eines Programmes entdeckt, das infolge seines hohen Rechenzeit- und Speicherplatzverbrauchs die Verfügbarkeit der befallenen Rechner drastisch reduzierte. Der *„Internet-Wurm"* hatte einige tausend Rechner befallen. Der Aufwand zur Wiederherstellung der Systeme wurde auf 100 Millionen US-Dollar geschätzt.
- Deutsche *„KGB-Hacker"* haben sich eigener Rechner und der weltumspannenden elektronischen Datennetze bedient, um in Rechner in den USA einzudringen und dort ausgespähte Informationen an den sowjetischen Geheimdienst zu verkaufen. Der Nachweis ihrer Aktivitäten war tech-

[17]) Vgl. PC Tip Nr. 4/1997
[18]) Vgl. http://www.infosec.ch/faelle/fall177.htm
[19]) Vgl. http://www.infosec.ch/faelle/fall169.htm
[20]) Vgl. The Risks Digest Volume 19 Issue 58, in: http://catless.ncl.uk/Risks/19.58.html#sub

nisch und personell außerordentlich aufwendig. Der Schaden läßt sich nicht in DM beziffern.

- Wegen eines *Anschlages* von Computerhackern blieben am 23. Oktober 1997 126000 Haushalte in San Francisco während vier Stunden ohne Strom. Cyberterroristen hatten zuerst das computergesteuerte Alarmsystem des Energiekonzerns Pacific Gas & Electric lahmgelegt, dann gelang es ihnen, den Strom abzuschalten.[21])

- Ein britischer *Hacker* veränderte 1994 die Rezepte auf dem Rechner eines Krankenhauses. Ohne die Aufmerksamkeit einer Krankenschwester wäre ein neunjähriger Junge durch die so entstandene hochgiftige Mixtur gestorben.[22])

Der Verlust, die Manipulation und der Diebstahl von sensiblen Daten können nicht nur existenzbedrohende finanzielle Schäden hervorrufen und die organisatorische Funktionsfähigkeit aufheben, sondern auch unbeteiligten Dritten erheblichen Schaden zufügen. An einigen zentralen Funktionsbereichen der Gesellschaft sollen die möglichen Risikopotentiale im privaten, geschäftlichen und öffentlichen Bereich aufgezeigt werden.

Die Funktionsfähigkeit und die Sicherheit des elektronischen Bankennetzes hat eine vitale Bedeutung für die gesamte Wirtschaft. Der Ausfall des Rechenzentrums einer Bank kann durch ein parallel arbeitendes System aufgefangen werden. Ein Ausfall der Verbindung einer Bank mit dem elektronischen Interbanken-Netzwerk würde dagegen binnen Stunden zu deren Zahlungsunfähigkeit führen, wenn sie elektronische Finanztransaktionen nicht mehr ausführen kann. Bei Versicherungen beträgt diese Zeitspanne eine Woche.

Hochsensibel ist beispielsweise auch jede Form der Speicherung privater Gesundheitsdaten – sei es in Form elektronischer Patientenakten oder auch beim Datenaustausch über Arzt- und Kliniknetze oder offene Telekommunikationsnetze – sowie die Funktionsfähigkeit digital gesteuerter technischer Medizinsysteme, weil Gesundheit und Leben von Patienten davon abhängen.

Informationstechnische Sicherheitsprobleme und Datenschutz spielten im Entwicklungszusammenhang des Internets keine Rolle,[23]) woraus die heute zu beobachtende Verschärfung der IT-Sicherheitsprobleme durch die globale Vernetzung folgt. Erst in den 80er Jahren entwickelten die US-Militärs aus ihren Bedürfnissen heraus die ersten IT-Sicherheitskriterien und -techniken (das Orange Book), wickelten zugleich aber zunehmend ihren Datenverkehr über abgeschottete Netzteile ab. Für die Netzkooperation der auf dem Internet neben den Militärs vornehmlich vertretenen Wissenschaftler untereinander bestand kaum Bedarf für IT-Sicherheit.

Die mangelhaften Sicherheitsmechanismen des Internets sind also keine Versäumnisse, sondern Folge des Umstandes, daß das Internet nicht für die heutige breite Nutzungspalette entwickelt worden war. Die hochdynamische Entwicklung des Internets hat bislang noch nicht zu der Notwendigkeit geführt, Sicherheitsaspekte stärker in den Mittelpunkt zu rükken. Erst mit der kommerziellen Nutzung und mit der Übertragung von sensitiven Kunden- und Unternehmensdaten oder elektronischen Geldes führt dies nun zu einer erhöhten Problemwahrnehmung.

Die Ursachen für Störungen und Ausfälle von IT-Systemen lassen sich in drei Kategorien untergliedern:

1. Systemimmanente Fehler
   - Fehler der Hardware
   - Fehler in der Software (auch im Sinne mangelnder Bedienungsfreundlichkeit bzw. mangelnder Robustheit gegenüber Fehlbedienung)
   - Grundsätzlicher Mangel an IT-Sicherheit in offenen Netzen, beispielsweise dem Internet.
2. Fehler bei der Einrichtung und Bedienung von IT-Systemen
   - Fehler beim IT-Systemschutz (etwa mangelhafte Zugangskontrollen und Abschottung gegenüber Dritten, aber auch mangelhafte Sicherung von wichtigen Datenbeständen)
   - Fehler bei der Bedienung von IT-Systemen
   - Mangelndes Problembewußtsein
3. Bewußte Manipulation von IT-Systemen und Angriffe von außen
   - Bewußte Manipulation von Daten und IT-Systemen.
   - Angriffe von außen in IT-Systeme mit dem Ziel des Eindringens, Ausspähens und Manipulierens.

An der KES[24])-Utimaco-Sicherheitsstudie 1996 beteiligten sich 183 Unternehmen. Ihre wichtigsten Ergebnisse sind:

- „Irrtum und Nachlässigkeit von Mitarbeitern, software-bedingte technische Defekte und Software-Anomalien gelten neben den hardware-bedingten technischen Defekten unverändert als die schwerwiegendsten Gefahrenbereiche.
- Irrtum und Nachlässigkeit von Mitarbeitern, software-bedingte technische Defekte und Software-Anomalien werden in Zukunft noch größere Bedeutung für die Informationssicherheit erlangen. Hardware-bedingte technische Defekte werden dagegen abnehmen.
- Nur ein Drittel der Firmen hält die Informationssicherheit im eigenen Haus für gut. Informationssicherheit ist in den Unternehmen nicht unbedeu-

[21]) Vgl. Infosec Internet News, in: http://www.infosec.ch/faelle/infonews.htm

[22]) Vgl. Der Spiegel vom 28. Februar 1994, S. 243; Vgl. hierzu auch den Abschnitt 4.5. Delikte im Berichtsteil Strafrecht

[23]) Vgl. hierzu: The World Wide Web Security FAQ, in: http://www.w3.org/security/Faq

[24]) Die Zeitschrift für Kommunikations- und EDV-Sicherheit (KES) untersucht zusammen mit UTIMACO in regelmäßigen Abständen die Sicherheitssituation von DV-Anwendern.

tend, hat aber doch in vielen Unternehmen keinen vorrangigen Stellenwert.

- Das größte Hindernis für die Verbesserung der Informationssicherheit liegt in einem Mangel an Sicherheitsbewußtsein, fehlenden kompetenten Mitarbeitern und Geldmangel.
- Obwohl viele Schutzmöglichkeiten und Sicherheitsmaßnahmen angeboten werden oder in den Unternehmen bereits verfügbar sind, werden sie doch vielfach erstaunlich wenig genutzt."

Zusammenfassend ist herauszuheben, daß zwei Faktoren bestimmend sind: fehlerhafte Software und der „Fehler-Faktor" Mensch. Bei „Software-Anomalien" liegt das IT-Sicherheitsproblem originär auf der Seite der Software-Hersteller. „Bedienungsfehler" und „nachlässiger Umgang mit IT-Sicherheit" sind eher „hausgemachte Probleme" des DV-Anwenders. Einschränkend muß an dieser Stelle jedoch gesagt werden, daß das Problem der „Bedienungsfehler" nicht grundsätzlich dem Anwender zugeordnet werden kann, da Software häufig nicht bedienungsfreundlich und fehlerrobust ist.

Fehlertoleranz als Gestaltungsoptionen

Richtig ist, daß der Mensch generell die größte „Schwachstelle" beim IT-Einsatz ist, weil die meisten Fehler bei der Bedienung und Benutzung des IT-Systems durch ihn entstehen. Dabei ist zu bedenken, daß auch Software von Menschen hergestellt wird und deshalb im allgemeinen fehlerhaft ist. Die gegenwärtige IT-Sicherheitsstrategie geht davon aus, durch sicherheitsmäßige „Härtung" der Software und Hardware die immanente Fehlerträchtigkeit von IT-Systemen so zu unterlaufen, daß „aufgesattelte" Kontrolltechnologien („Sicherheits-Technik kontrolliert fehlerbelastete Basistechnologie") wie beispielsweise „Firewall-Computer", Virenschutzprogramme, Benutzerhierarchien, Verschlüsselungsfunktionalitäten usw. die Berechtigung des Nutzers zum Zugang zum Rechner bestimmen.

Dieser Grundgedanke bestimmt alle IT-Sicherheitsmaßnahmen mit der Konsequenz, daß die angestrebte „offene, multimediale Dienstleistungsgesellschaft der Zukunft" die notwendige Zuverlässigkeit und Vertraulichkeit nur dadurch erreichen kann, daß eine zusätzliche IT-Sicherungsinfrastruktur auf die im Aufbau befindliche nationale wie globale Informations-Infrastruktur mit „aufgesetzt" werden muß – was sofort wieder zu der Frage nach Zuverlässigkeit und Vertraulichkeit der IT-Sicherungsinfrastruktur führt.

Eine alternative IT-Sicherheitsstrategie – die den Menschen nicht ausschließt, sondern seine nur ihm gegebenen Fähigkeiten zum Lernen aus Fehlern aktiv nutzt – geht von folgender These aus: Menschen machen immer Fehler. Weil Menschen Fehler machen und dadurch Schäden und Unfälle verursachen – Fehler sogar eine evolutionär wichtige Rolle spielen –, kann es nicht darum gehen, die Fehler auszumerzen, weder durch die jedem Fehler vorbauende Technik und Organisation, noch durch rechtliche und moralische Selbstbeschränkungen des Individuums. Vielmehr muß eine positive Haltung dem Fehler gegenüber ausgebildet werden. Das setzt jedoch voraus, daß nur solche Technik zum Einsatz kommen darf, die fehlerfreundlich ist, d.h. deren mögliche Fehlerfolgen tolerabel sind, so daß die Menschen und die Gesellschaft daraus lernen können. Es darf keine Technik eingesetzt werden, in der keine Fehler auftreten dürfen, weil deren mögliche Konsequenzen katastrophal wären. Die Gestaltungsorientierung an der Prämisse, daß Menschen Fehler machen, ist Ausdruck einer prinzipiellen Umorientierung. Das Maß für das, was technisch gemacht wird, sind in diesem Fall die menschlichen, nicht die technischen Möglichkeiten.[25])

Sogenannte „Software-Provisorien" werden derzeit in Wirtschaft, Wissenschaft, Verwaltung und sozialem Alltag als Grundlage einer digital vernetzten Dienstleistungsgesellschaft implementiert. Diese Unzuverlässigkeit ist eine der ersten Erfahrungen, die jeder Anwender von Softwaresystemen macht. Fehlerhafte Software kann verbessert werden. Es wäre daher zu erwarten, daß Systeme mit zunehmenden Alter reifen und zuverlässiger werden. Dies ist für komplexe Systeme jedoch nicht gewährleistet. Vielmehr führen die vielfältigen Abhängigkeiten einzelner Komponenten untereinander zu kontraproduktiven Effekten bei der Fehlerbeseitigung. Die Fachliteratur geht von 1,5 % bis 2,5 % fehlerhaften Anweisungen in größeren Systemen aus. Dabei liegt der Anteil der Spezifikations- und Entwurfsfehler bei jeweils 30 % und der von Kodierungsfehlern bei etwa 40 %[26]). Von den Entwicklungsfehlern sind nach Abschluß der Implementierungsphase ein Drittel noch nicht entdeckt. In großen Softwaresystemen muß daher mit einer entsprechenden Anzahl latenter Fehler gerechnet werden.

Ein wichtiges Hilfsmittel zur Fehlersuche ist das Testen. Tests können allerdings nur das Vorhandensein von Fehlern, nicht die Fehlerlosigkeit zeigen. Statistische Testverfahren können zur Korrektur von Fehlern führen, aber keineswegs die Korrektheit des Produkts garantieren. Sind Fehler erkannt, zeigt die Erfahrung, daß bei deren Korrektur oft neue Fehler entstehen. Die Struktur von Software-Systemen kann sich durch Erweiterungen und Anpassungen stark verändern. Angenommen wird, daß ab einem bestimmten Alter eines Softwareprodukts die Fehlerrate mit jeder neuen Korrektur oder Ergänzung zunimmt. Insgesamt ist unumstritten, daß heute und in absehbarer Zukunft die Software-Programme nicht fehlerfrei oder innerhalb einer vorgegebenen Fehlerwahrscheinlichkeit erstellt werden können.

Vor diesen software-inhärenten (also systematischen) Problemen ist es richtig, davon auszugehen, daß die von IT-Systemen ausgehenden Schadenspotentiale noch deutlich zunehmen werden. Da die Gesellschaft in nahezu allen Bereichen vom richtigen Funktionieren dieser Technik-Systeme abhängig sein wird, lassen sich gesamtgesellschaftliche Katastrophen durch den Ausfall wichtiger sozialer Funktionen, die den IT-Systemen übertragen wurden, nicht ausschließen.

Die Ergebnisse der überwiegenden Mehrzahl der bisher vorliegenden IT-Sicherheitsstudien legen den Schluß nahe, daß diesen Problemen eine wesentlich größere Bedeutung zukommt, als den häufig als Hauptproblemen gesehenen Phänomenen der Computerkriminalität. Trotz zunehmender absoluter Fallzahlen schwankt der auf Computerkriminalität zurückzuführende Anteil von IT-Sicherheitsproblemen

[25]) Vgl. Wehner, Th. Sicherheit als Fehlerfreundlichkeit, Opladen, 1992.

[26]) Vgl. Rossnagel, A. et. al, Verletzlichkeit der Informationsgesellschaft, Opladen, 1989, S. 113

seit den 80er Jahren um etwa 15 %. Die Zunahme der elektronischen Datenverarbeitung und -übermittlung, sowie die wachsende Bedeutung kommerzieller Transaktionen über elektronische Netze, stellen natürlich auch ein Angriffsziel der Kriminalität dar. Auch geheimdienstliche Operationen und die Wirtschaftsspionage sind hierbei zu betrachten.

Diese Gefahr ist empirisch evident. So zitierte die Computer Zeitung vom 28. August 1997 unter dem Titel „Computerkriminalität in Deutschland ist 1996 weiter gestiegen: Offene Systeme locken Kriminelle" den Leiter der Abteilung Computerkriminalität im Bayerischen Landeskriminalamt, Werner Paul: „Seit Jahren schon steigen die Delikte im Computerbereich, und dieser Trend wird leider verstärkt durch die Anbindung an offene Systeme." Für 1996 wurde ein Anstieg der Computerkriminalität von 15,1 Prozent ausgewiesen. Dabei ist aber als grundlegendes Problem der Bewertung dieses IT-Risikos die unsichere statistische Datenlage zu beachten: Unzureichendes Meldeverhalten von Polizeidienststellen, Unternehmen und Privatpersonen sowie statistische Abgrenzungsprobleme lassen eine erhebliche Dunkelziffer in diesem Deliktbereich vermuten.[27])

Zur Abwehr dieser Gefährdungen wurden Kriterien zur Bewertung und Gestaltung von IT-Systemen entwickelt, die zur Formulierung grundlegender IT-Sicherheitsziele geführt haben. Diese allgemein anerkannten IT-Sicherheitsziele dienen heute der Politik, Wirtschaft und Wissenschaft als Handlungsorientierung. Dabei bilden die im folgenden genannten vier IT-Sichheitsziele die Grundlage aller IT-Sicherheitskonzepte:

- **Vertraulichkeit:** als die Sicherheit vor der ungewollten (unauthorised) Einsichtnahme in Informationen.[28])
- **Integrität:** als „die Eigenschaft eines Systems, die besagt, daß es nur erlaubte und intendierte Veränderungen der in ihm enthaltenen Informationen zuläßt. Eine Information ist integer, wenn an ihr nur zulässige Veränderungen vorgenommen wurden."[29])
- **Verfügbarkeit als** die Vermeidung ungewollter Zurückhaltung von Informationen oder Systemressourcen.[30])
- **Authentizität als** „die Übereinstimmung der behaupteten Identität mit der tatsächlichen."[31])

Als weitere wichtige Bausteine einer umfassenden IT-Sicherheitsarchitektur können genannt werden:

- IT-Sicherheit als **funktionaler Bestandteil von IT-Systemen**
- **Gewährleistung von IT-Sicherheit** auf der Seite der Diensteanbieter

Im Kontext der beiden letztgenannten IT-Sicherheitszielen geht es darum,

- IT-Anwender, IT-Hersteller und IT-Dienstleister für Fragen der IT-Sicherheit zu sensiblisieren
- Maßnahmen zur Verbesserung der IT-Sicherheit von IT-Produkten, -Systemen und -Dienstleistungen aufzuzeigen und
- in breiter Anwendung die IT-Sicherheitszertifizierung zu fördern, um IT-Komponenten hinsichtlich der IT-Sicherheit überprüfen und damit hinsichtlich ihrer Vertrauenswürdigkeit bestätigen zu können.

Im Schutzziel **Vertraulichkeit** wird der Bezug zum Datenschutz offensichtlich[32]). In verbesserter IT-Sicherheit und der Kryptographie als Instrument zur Unterstützung der Vertraulichkeit sehen Datenschützer Mittel zu einem besseren Schutz der informationellen Selbstbestimmung.[33])

Ein darüber hinaus gehendes Verhältnis zwischen IT-Sicherheit und Datenschutz kommt im Begriff der „mehrseitigen Sicherheit" zum Ausdruck: „Mehrseitige Sicherheit bedeutet die Berücksichtigung der Sicherheitsanforderungen nicht nur einer der beteiligten Parteien. Da sich die Beteiligten, speziell bei offenen Kommunikationssystemen, nicht per se vertrauen, sind sie auch sämtlich als potentielle Angreifer zu sehen. Entsprechend sind die Anforderungen mehrseitiger Sicherheit bei für universelle Nutzung gedachten öffentlichen Kommunikationsnetzen besonders anspruchsvoll." [34])

Damit erweitert der Begriff der „mehrseitigen Sicherheit" den Kanon der eher technikzentrierten IT-Sicherheitziele um soziale, organisatorische und rechtliche Anforderungen. Die „sieben Bausteine für Sicherheitskriterien", in denen die Anforderungen mehrseitiger Sicherheit beschrieben werden, weisen bei drei „Bausteinen" Überschneidungen zu den bereits vorgestellten IT-Sicherheitszielen auf. Diese sind: „Vertraulichkeit", „Unabstreitbarkeit" (die dem IT-Sicherheitsziel „Authentizität" entspricht) und „Übertragungsintegrität" (die dem IT-Sicherheitsziel „Integrität" entspricht). Als ergänzende kommen hinzu:

- **Unbeobachtbarkeit:** Eine „kommunikative Handlung", etwa ein Telefonanruf, muß durchgeführt werden können, ohne daß ein Außenstehender (auch der Netzbetreiber sollte als Außenstehender angesehen werden) davon erfahren kann.

---

[27]) Dieses Thema wird ausführlich im Abschnitt 4.5 des Berichtsteils Strafrecht behandelt.

[28]) Vgl. Information Technology Security Evaluation Criteria/ ITSEC, in: http://ftp.tu-chemnitz.de

[29]) Vgl. Amann, E.; Atzmüller, H.; IT-Sicherheit was ist das?, DuD 6/92, S. 287

[30]) Vgl. Information Technology Security Evaluation Criteria/ ITSEC, in: http://ftp.tu-chemnitz.de

[31]) Vgl. Amann, E.; Atzmüller, H. a.a.O., S. 287; Vgl. auch: Common Criteria For the Evaluation of IT Security, in: http://ftp.cse.dnd.ca

[32]) Vgl. dazu auch den Berichtsteil Datenschutz.

[33]) Vgl. Bäumler, H., Wie geht es weiter mit dem Datenschutz?, in: DuD 1997, S. 446–452 (450)

[34]) Vgl. Ranneberg, K; Pfitzmann, A.; Müller, G.; Sicherheit, insbesondere mehrseitige IT-Sicherheit, in: Müller, G.; Pfitzmann, A. (Hrsg.), Mehrseitige Sicherheit in der Kommuniktionstechnik: Verfahren, Komponenten, Integration, 1997, S. 21–29, hier S. 26

- **Anonymität:** Ein Benutzer muß die Möglichkeit haben, auch ohne Preisgabe seiner Identität, Informationen und Beratung zu erhalten, analog zum anonymen Kauf einer Zeitung am Kiosk oder dem anonymen Anruf bei einem „Sorgentelefon".
- **Unverkettbarkeit:** Mehrere „kommunikative Handlungen", etwa zwei Anrufe bei nahen Verwandten, dürfen nicht miteinander in Verbindung gebracht werden können, da auf diese Weise erstellte Informationssammlungen die Anonymität und Unbeobachtbarkeit untergraben können.
- **Pseudonymität:** Wer anonymen Benutzern kostenpflichtige (Informations-)Dienste anbietet, muß imstande sein, auf sichere Weise zu seinen Einnahmen zu kommen.
- **Unabstreitbarkeit:** Besonders bei kommerziellen Anwendungen sind unabstreitbare Garantien dafür wichtig, daß jemand eine bestimmte Nachricht, etwa Bestellungen oder Stornierungen, tatsächlich selbst erfaßt bzw. tatsächlich und fristgerecht erhalten hat. Entsprechend müssen Unterschriften von Personen oder Einschreibebriefe digital bzw. elektronisch nachgebildet werden.[35])

1.1. Risikopotentiale im privaten, geschäftlichen und öffentlichen Bereich (Eindringen, Profilbildung und Manipulation von Daten)

Derartige Sicherheitskonzepte erweisen sich als unabdingbar, da Versagen, Ausfälle oder Manipulation von IT-Systemen zu gravierenden Schäden führen können. Informationstechnik ermöglicht vielfältig schädigende Aktionen und damit *Kumulationsschäden*. Sie kann zu einer Vervielfachung eines Schadens und damit zur Verursachung von *Multiplikationsschäden* genutzt werden. Die Zentralisierung von Daten und bei Kommunikationsinfrastrukturen kann zu einem hohen Einzelschaden führen. In vernetzten Systemen können sich Schäden in viele angeschlossene Systeme ausbreiten und einen *Komplexschaden* hervorrufen. Schließlich werden durch standardisierte Software selbst weit verteilte und isolierte Systeme sehr eng gekoppelt und können durch deren Multiplikation sogar allesamt gleichzeitig ausfallen. Die Abhängigkeit von IT-Systemen und damit das spezifische Schadenspotential wird in dem Maße ansteigen, wie die vernetzte Informationstechnik bisherige Formen der Informationsverarbeitung verdrängt.

Diese Abhängigkeit von der Verfügbarkeit letztlich nicht fehlerfreier IT-Systeme kann dadurch reduziert werden, daß Substitutionsmöglichkeiten erhalten bleiben. Macht sich die Gesellschaft von einem einzigen Techniksystem oder von einem Softwareprodukt eines Monopolisten abhängig, kann der Ausfall dieses IT-Systems zu Katastrophen mit nationalem Ausmaß führen.

Fehlende Langzeitverfügbarkeit gespeicherter Daten

Katasterämter, Sozial- und Krankenversicherungen, auch Statistik- und Finanzämter usw. gehen seit einiger Zeit dazu über, ihre jeweils unterschiedlichen Daten, gemäß den neuen Möglichkeiten der Informationstechnik, auf elektromagnetisch funkionierenden Speichermedien (etwa Magnetband, Laser-Disk), gemäß der gesetzlichen Vorschriften, auf „ewig" abzuspeichern, so zumindest die Absicht.

Bekannt ist, daß die heute auf magnetische oder optoelektronische Träger abgespeicherten Daten nur eine Lebensdauer von zwanzig Jahren haben, wobei dies im Sinne von „Halbwertzeiten" gelesen werden muß: In der genannten Zeit sind mindestens die Hälfte der Träger nicht mehr brauchbar. (Weitere Beispiele: Die „Halbwertzeit" von Papier, so es jünger als 150 Jahre ist, beträgt 100 Jahre, von Fax-Papier zwischen zwei und zehn Jahren.) Bekannt ist des weiteren, daß es selbst heute schon sehr schwierig, wenn nicht schon unmöglich, ist, etwa vor nur zehn Jahren gespeicherte Daten zu reproduzieren, entweder weil die mittlerweile überalterte Speichertechnologie nicht mitkonserviert wurde, und/oder weil das Wissen über die damals benutzte Software verlorengegangen ist.

Bei einer notwendigen Dauerkonservierung von Daten muß deshalb die zeitliche Konservierungsfähigkeit eines Speichermediums berücksichtigt werden.

Verfügbarkeit stellt jedoch nur einen Aspekt der möglichen Risikodimensionen. So ist der Schutz der Vertraulichkeit eine nicht nur dem Datenschutz obliegende Aufgabe. Im Zentrum des Datenschutzes steht das nach der Rechtsprechung des Bundesverfassungsgerichtes im Grundgesetz verankerte Recht auf *informationelle Selbstbestimmung*. Jedem Bürger wird damit das Recht zugesprochen, „grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[36]) Diesem Grundrecht kommt im Hinblick auf offene Datennetze eine ganz besondere Bedeutung zu, weil jeder Nutzer offener Netze mit seinen Bewegungen und Handlungen Spuren hinterläßt, die erfaßt und ausgewertet werden können. Dabei können Datenprofile mit großer Schärfentiefe entstehen – der „gläserne Nutzer" wird Wirklichkeit. Diese Gefahr besteht auch bei Electronic Commerce. Es ist für Unternehmen, die sich auf diesem virtuellen Marktplatz engagieren, von großem Reiz – etwa im Rahmen des Data-Warehousing – Datenprofile von Kunden zu gewinnen und diese systematisch auszuwerten. Solche Profildaten nützen nicht nur dem eigenen Marketing und Vertrieb, sondern sind selbst ein wertvolles Wirtschaftsgut, mit dem sich Geld verdienen läßt.

War das Motiv des Datenschutzes in seinem Ursprung, den Bürger vor Übergriffen staatlicher Behörden zu schützen, so erweitert sich der Fokus bei offenen Datennetzen darüber hinaus auf das Verhältnis von privatem Internetnutzer und den kommerziell engagierten Netzunternehmern. Ähnliches gilt in der Arbeitswelt für die Intranets. Die technisch gegebene Möglichkeit, jede Bewegung und Handlung eines Arbeitnehmers aufzuzeichnen und analytisch aufzubereiten, läßt den Arbeitnehmer gegenüber seinem Unternehmen transparent erscheinen.

Als problematisch sind auch Data-Warehouse-Konzepte zu sehen. Mit diesen elektronischen Informati-

[35]) Vgl. Rannenberg, K. et al, Mehrseitige Sicherheit als integrale Eigenschaft von Kommunikationstechnik, in: Kubicek, H. et al. (Hrsg.), Telekommunikation & Gesellschaft, 1995, S. 254–260. Siehe auch: http://www.iig.uni-freiburg.-de/dbskolleg/public/JTK_95/JTK_erschienen.htm

[36]) BVerfGE 65, 1 (43); Vgl. hierzu auch den Abschnitt 3.2., Der Begriff des Datenschutzes im Berichtsteil Datenschutz.

onssytemen werden heterogene Unternehmensdaten integriert und für bestimmte Bedarfsfelder, etwa in den Bereichen Vertriebsunterstützung, Marketing, Kundeninformation und Produktanalyse, aufbereitet zur Verfügung gestellt. So soll mit Hilfe von Data-Warehouse-Resultaten entschieden werden, mit welchen Kunden in welchem Umfang Geschäfte getätigt werden können und welche Strategien zur Kundenbindung verfolgt werden müssen. Dabei werden Informationen über die Profitabiltät, die Bonität und die Zahlungsmoral der Kunden vorrätig gehalten. Diese Form der Informationsaufbereitung unterstützt Unternehmen in ihrem Bemühen, Kunden zu binden, ein kundenorientiertes Marketing zu entwickeln und sich vor riskanten Geschäftsabschlüssen zu schützen. Datenschutzrechtlich wird Data-Warehouse dann problematisch, wenn von dritter Seite – etwa einem Kreditkartenunternehmen – Kundeninformationen gekauft und diese mit eigenen Daten so aufbereitet werden, daß umfassende Kundenprofile entstehen.[37]) Eine solche Verarbeitung und Verknüpfung personenbeziehbarer Daten ist mit dem Grundrecht auf informationelle Selbstbestimmung unvereinbar. Data-Warehousing kann ebenso genutzt werden, um Arbeitsverhalten und Leistung von Arbeitnehmern zu erfassen und zu bewerten. In Analogie zum „gläsernen Nutzer" und „gläsernen Bürger" kann hier vom „gläsernen Arbeitnehmer" gesprochen werden.

Data-Mining

Während der Datenschutz immer noch von der Datenbank-Technologie der 70er Jahre mit großen und nach gleichartigen Kriterien aufgebauten Datensammlungen ausgeht, liefert die Informationstechnik heute die Möglichkeit, heterogene Datenbestände auf interessante Daten und Zusammenhänge hin zu durchsuchen. Bei dieser Verknüpfung von Dateien, die nach herkömmlichem technischem Verständnis nicht zusammen bearbeitbar sind, werden statistische und heuristische Methoden angewandt, um logisch in Beziehung stehende Datensätze miteinander zu verknüpfen und daraus Information zu gewinnen.

Anwendungsgebiete von Data-Mining-Werkzeugen sind heute vor allem Großunternehmen, wie etwa Versicherungen, die aufgrund ihrer Vertriebs- oder Produktstruktur über verschiedenartige Datenbestände verfügen und daraus Zusatzwissen über ihre Kunden gewinnen möchten. Gleiches gilt jedoch auch für die Analyse von Datenmengen aus Kursentwicklungen bei Banken oder andere Datenbestände.

Bei den Zielen wird unter dem Begriff Data-Mining sowohl das Zusammenführen von Daten zu einer Person aus verschiedenen Datenbeständen – also etwa das Sammeln aller Daten zu einer Person im gesamten Unternehmen – als auch das Zuordnen von zusätzlichen Informationen zu personenbezogenen Datensätzen aus disjunkten Datenbeständen – also etwa die Extraktion gruppenspezifischer Verhaltensdaten aus unspezifischen Kundendateien und deren näherungsweise Zuordnung zu „passenden" Personen – zusammengefaßt. Ebenso läßt sich aber auch in großen Produktionsdatenbeständen nach Fehlerquellen von Produktmängeln suchen. Das Internet liefert mit seiner Vielfalt von heterogenen Datenbeständen umfangreiches Quellenmaterial für vielfältige Data-Mining-Anwendungen. Diese für Marketing und Produktion nützliche Methode bringt durch die extensive Möglichkeit zur Zusammenführung von personenbezogenen Daten erhebliche Datenschutz-Gefahren mit sich. Eine Folge ähnlicher Möglichkeiten war etwa die Einschränkung der Weitergabe anonymisierter Daten aus Mikrozensuserhebungen schon Ende der 80er Jahre, da ein Abgleich solch hochqualitativer Daten mit anderen Quellen die statistische Anonymität der Betroffenen erheblich gefährdete. Data-Mining liefert nun die Technik, um ausführliche Personenprofile zu erstellen und droht gleichzeitig, durch die Verknüpfungsmöglichkeiten die anonyme und pseudonyme Nutzung elektronischer Dienste zu gefährden.

Diese Risiken der Profilbildung erklären das Interesse an einer anonymen Nutzung des Internets. Dabei scheinen Anonymität und die für elektronische Geschäftsprozesse benötigte Authentizität zunächst ein Gegensatzpaar zu sein: Wer anonym surft, kann sich nicht automatisch authentisieren. Doch auch, wer nicht-anonym surft, nutzt damit noch keine Technologie, die eine Authentisierung auch nur mit einer akzeptablen Korrektheit gewährleistet. Authentisierung in elektronischen Netzen setzt daher immer die Nutzung zusätzlicher Mechanismen voraus. Damit spielt der Gegensatz von Anonymität und Authentizität in der Praxis in der Regel keine Rolle. Authentizität ist bei einem Informationsabruf meist unwichtig, bei Rechtsgeschäften oder Finanztransaktionen dagegen in vielen Fällen erforderlich. Ein auch im Rahmen des Informations- und Kommunikationsdienstegesetzes (IuKDG) verabschiedeten Teledienste-Datenschutzgesetz (TDDSG)[38]) gewählter Lösungsansatz sind daher Pseudonyme, bei denen eine Zuordnung von Person und Pseudonym durch eine vertrauenswürdige Stelle vorgenommen wird. Ein festes Pseudonym erlaubt eine Authentisierung, die Identität der Person muß aber nur in Zweifelsfällen aufgedeckt werden. Authentizität liefert aber keine Mailadresse oder ähnliches, sondern spezielle Mechanismen wie die digitale Signatur. Wenn aber Authentizität die nicht-anonyme Nutzung nicht voraussetzt, sondern davon völlig unabhängig ist, so läßt sich zwischen Anonymität und Authentizität auch kein prinzipieller Gegensatz konstruieren.

Gefährdungen der Kommunikation im Netz

Eine der größten Gefährdungen bei der Benutzung des Internet stellt der Verlust der Vertraulichkeit durch ein Mitlesen der versandten Daten und der Verlust der Integrität durch die Manipulation der Daten dar. Viele der im Internet benutzten Dienste übertragen die Benutzernamen und Paßwörter offen, so daß jeder, der privilegierten Zugang zu einem der an der Übertragung beteiligten Gateways, Router oder Server hat, diese Daten lesen oder verändern kann. Das Mitlesen der versandten Daten ermöglicht auch sogenannte Replay Attacks, bei denen einmal zur Authentisierung benutzte Daten, wie z. B. verschlüsselte Paßwörter, von einem Angreifer bei einem späteren Zugangsversuch wieder eingespielt werden.

Mit der Notwendigkeit zu digitalen Signaturen erweist sich der technische IT-Sicherheitsbaustein „Kryptographie" als neue und ergänzende Option des Datenschutzes und des Schutzes der Vertraulichkeit. Neu ist auch, daß die Erzeugung von Vertraulichkeit durch die Nutzung kryptographischer Werkzeuge in der Verantwortung des einzelnen Nutzers

[37]) Vgl. Hönicke, I., Das Warehouse-Konzept schürt die Angst vor dem gläsernen Bürger, in: ComputerZeitung vom 3. Juli 1997

[38]) Vgl. hierzu den Berichtsteil Datenschutz, Kapitel 3.5

von Informationstechnologie liegt. Die Erreichung der IT-Schutzziele „Vertraulichkeit", „Authentizität" und „Integrität" und der damit verbundenen Datenschutzziele wird durch die verantwortungsvolle Nutzung von kryptografischen Werkzeugen und der Digitalen Signatur durch den einzelnen IT-Nutzer möglich. *IT-Selbstschutz* und *Selbstdatenschutz* kennzeichnen hierbei begrifflich die Eigenverantwortung des Nutzers informationstechnischer Systeme.

Derartige Werkzeuge können auch das Risiko von Manipulationen in Datennetzen reduzieren, denn: Solange Daten im Klartext von Netzknoten zu Netzknoten weitergegeben werden und dabei mitgelesen, also auch kopiert und manipuliert werden können, verbietet es sich zum Beispiel für den Verbraucher, Kreditkartendaten und für ein Unternehmen, sensible Unternehmensdaten über Datennetzwerke zu schicken. Eine Reihe von Beispielen über Angriffe auf Datenströme und Computer mit dem Ziel Kreditkartendaten zu erlangen, unterstreicht die Bedeutung des Schutzes vor Manipulation. Ähnliches gilt für die Telemedizin: Die Sicherheit vor Manipulation von Patientendaten muß im vollen Umfang auch dann wirksam sein, wenn eine elektronische Patientenakte via Datennetzwerk vom Krankenhaus zum Arzt wandert.

Die Telemedizin stellt weitere spezifische Anforderungen an die Wahrung der IT-Sicherheit: Der medizinische Bereich ist durch eine Besonderheit gekennzeichnet, nämlich das mögliche Vorliegen eines Notfalls, der die plötzliche Anforderung höchster Verfügbarkeit mit sich bringt. Sicherheitsanforderungen wie Vertraulichkeit, Authentizität und Integrität haben jedoch zum Ziel, die Verfügbarkeit für den Angreifer zu minimieren und können sich dann als gefährlich erweisen, wenn sie der im Notfall benötigten Verfügbarkeit entgegenstehen, weil der behandelnde Arzt nicht oder nicht schnell genug als befugter Benutzer erkannt werden kann und ihm der möglicherweise dringend notwendige Zugang verweigert wird.

Die angeführten Konflikte in der IT-Sicherheit zwischen Verfügbarkeit und Authentizität, Authentizität und Anonymität, die Abhängigkeit von einer Verfügbarkeit von IT-Systemen sowie die Nutzbarkeit kryptographischer Verfahren unterstreicht erneut, daß Sicherheit nicht allein durch technische Maßnahmen herzustellen ist, sondern Sicherungsstrategien voraussetzt, die Mensch und Gesellschaft umfassend einbeziehen. Da Angriffe künftig wahrscheinlicher und schadensträchtiger werden und nur eingeschränkte Möglichkeiten bestehen, IT-Systeme in Konflikten angemessen zu schützen, wird es zum einen notwendig sein, die Sicherungslinie in die Gesellschaft hinein vorzuverlegen. Die Technisierung gesellschaftlicher Funktionen (nicht nur, aber auch durch die IT-Technik) erfordert immer nachdrücklicher gesellschaftliche Stabilität und Vertrauen in das sozialkonforme Verhalten jedes Einzelnen. Diese Aufgabe legitimiert den Einsatz von Überwachungselektronik und wird das Überwachungspotential von Staat und Unternehmen anwachsen lassen – mit allen Risiken für eine sich frei entwickelnde Demokratie. Sicherheit setzt zum anderen die Vertrauenswürdigkeit der Beschäftigten voraus. Diese muß gewährleistet werden durch Überprüfungen, Verhaltensüberwachung und Arbeitskontrollen. Sicherheit kann aber auch eine Überwachung von Nutzern bedeuten. Firewall-Software protokolliert die Nutzung von Netzressourcen. Expertensysteme werden eingesetzt, um auffälliges und gefährdendes Nutzerverhalten zu erkennen, bevor Schäden entstehen. Es ist also zu fragen, in welchem Umfang der Einsatz von Überwachungstechnologie erforderlich ist, um Defizite der IT-Sicherheit auszugleichen. Überwachungssysteme beobachten jedoch nur die Nutzung vorhandener Sicherheitslücken. Sicherheitsdefizite lassen sich dagegen weit effektiver durch eine bessere Systemgestaltung beheben als durch nachträgliche Maßnahmen, wie dies auch Überwachungssysteme darstellen.

Die Sicherung der Informationstechnik scheint somit ohne Freiheitseinschränkungen nicht möglich zu sein. Und die Bereiche, in denen Freiheitseinschränkungen unumgänglich werden, wachsen mit der IT-Nutzung. Damit setzt sich die Informationsgesellschaft einem Sicherungszwang aus, der möglicherweise weder technisch noch gesellschaftlich beherrschbar ist und dessen Dynamik im ungünstigen Fall in sozialunverträgliche, politische und soziale Verhältnisse zu führen droht.

Diese Dystopie einer Informationsgesellschaft als „Sicherungszwangsgesellschaft" (Foucault) folgt aus dem Schadenspotential und der Bedrohung von IT-Systemen. Da die Gründe für eine solche Bedrohung zu unterschiedlich und zu komplex sind, um sie politisch zu steuern, bleibt als Instrument zur Regulierung des Sicherungszwangs nur die Beeinflussung der Schadensmöglichkeiten. Macht sich die Gesellschaft jedoch von Hochrisikosystemen abhängig, setzt sie sich dem Dauerzwang zur Ernstfallvermeidung aus.

Sie verliert die Fähigkeit, den Sicherungszwang zu beherrschen, da dessen Stärke dann von der nicht beeinflußbaren künftigen Bedrohung bestimmt wird. Steigt diese an, entsteht eine Dynamik immer größerer Sicherungsanstrengungen. Dies kann durch einige katastrophale Schäden beschleunigt werden. Je sicherer die Informationsgesellschaft jedoch wird, desto weniger wird sie dem Bild entsprechen, das sich heute viele von ihr machen: Ihre Verletzlichkeit fordert eine hohe gesellschaftliche Stabilität und erlaubt keine gesellschaftlichen Experimente. Eine demokratische Informationsgesellschaft setzt daher eine an freiheitssichernden Zielen ausgerichtete politische Gestaltung der IT-Sicherheit voraus.

1.2 Kulturelle und soziale Rahmenbedingungen

1.2.1 Mangelndes IT-Sicherheitsbewußtsein in der Gesellschaft

Das Problem der wachsenden Abhängigkeit von unbeherrschbaren Computerwelten ist nicht gelöst. Die täglichen Meldungen über neue Formen von Computerviren, von Hackern, die in fremden Netzen und

Datenbanken ihr Unwesen treiben und die Software manipulieren, von kostenintensiven oder lebensgefährdenden Datenabstürzen, von erpresserischem Handeln mit abgefangen vertraulichen Daten, von abhörbaren Telefonnetzen, erregen zunehmend die öffentliche Aufmerksamkeit und können – werden sie nicht abgestellt – einer breiten sozialen Akzeptanz der „Informationsgesellschaft" im Wege stehen.

Noch aber wird IT-Sicherheit von vielen als lästige, gerne vernachlässigte Nebenfolge des mehr Effizienz und Rationalität versprechenden Einsatzes von IT-Systemen gesehen. Zu wenig wird IT-Sicherheit als Chancen öffnendes, in die Zukunft weisendes Gestaltungsprinzip von IT-Systemen gewertet. Einerseits hat sich die Zahl der Software-Programmierer in Deutschland innerhalb weniger Jahre vervierfacht und andererseits gibt es kaum eine unabhängige Institution, die die Verläßlichkeit und Korrektheit der Programmierarbeiten testet. Die Schere zwischen Softwareproduktion und Evaluation hat sich in den letzten Jahren noch geweitet. Allerdings hatte die Qualitätskontrolle im Rahmen der allgemeinen ISO 9000 Zertifizierung auch positive Auswirkungen auf die Qualität der Softwareerstellung. Gleichwohl wird eine immer komplexer werdende, vernetzte Software zum entscheidenden Träger einer modernen Dienstleistungsgesellschaft. Aber vernetzte Software, von deren einwandfreien Funktionieren zunehmend eine moderne Gesellschaft abhängig wird, wovon gar, sollte es zu einem Absturz kommen, das Leben vieler Menschen abhängen kann, muß sich in keiner Weise einem Gewährleistungstest durch unabhängige Stellen unterwerfen.

Die nicht vollständig regelbaren Nebenfolgen der unsicheren, angreifbaren und manipulierbaren Informationstechnik stellen ein Dilemma dar. Die absehbaren neuen Konflikte, die aus diesem Dilemma entstehen, werden kaum in dem Umfang diskutiert wie dies angesichts der Informationsrevolution im 21. Jahrhundert angemessen erscheint. Neue Forschungsgebiete an den Universitäten, die den Querschnittsaufgaben der künftigen Sicherheitswissenschaft gerecht werden können, sind noch nicht hinreichend entwickelt. Ein allein ingenieurwissenschaftlich ausgelegtes Sicherheitsverständnis greift angesichts einer Risikosymptomatik, die dynamisch, virtuell und vernetzt angelegt ist, zu kurz.

Durch „Technikfolgenabschätzung" *könnte* nicht nur ein wichtiger Impuls gegeben werden, sondern die komplexen Sicherheitsprobleme einer rasch fortschreitenden informationstechnischen Durchdringung der Gesellschaft systematisch dargestellt, analysiert und in Hinblick auf Lösungsstrategien aufgearbeitet werden.

„Das Jahr-2000-Problem

„Weltweit drohen Computersysteme nach dem Übergang zum Jahr 2000 unkorrekt zu arbeiten oder ganz auszufallen. Der Grund liegt darin, daß wichtige Funktionen in Hardware- oder Softwarekomponenten von Berechnungen mit dem aktuellen Datum abhängen, diese Berechnungen aber nur zweistellige Jahreszahlen nutzen. Die aus Gründen der Speicherökonomie genutzte zweistellige Codierung von Jahreszahlen läßt sich nur mühsam in Computersystemen aufspüren und beseitigen. Auch eine Korrektur der Systeme garantiert jedoch keine zuverlässige Verfügbarkeit der IT-Systeme nach dem 1. Januar 2000: Die Nebenfolgen einer Softwareänderung können ebenso gravierend sein wie eine falsche Datumsberechnung selbst. Langwierige Tests sind daher nötig, bevor die gewohnte Verfügbarkeit wiederhergestellt ist. Das Problem erweist sich daher als eines der größten Risiken der Informationstechnik.

Schätzungen zufolge wird die Umstellung aller Systeme weltweit 1 Billion Mark verschlingen und werden weltweit 30 % der Budgets für Informationstechnologie in den nächsten Jahren für die Lösung dieses Problems ausgegeben. (1) In den USA werden die Gesamtkosten auf 600 Milliarden Dollar geschätzt, die Abschätzungen für die Computerumstellung der US-Bundesbehörden bewegen sich zwischen 2,3 und 30 Milliarden.

(2) Betroffen ist nicht nur die Software, sondern auch einige Hardwarekomponenten, die selbst auf Datumsfunktionen zugreifen oder diese steuern. Dies betrifft Festplatten ebenso wie PCs, bei denen vielfach BIOS-Festspeicher und die System Clock ausgewechselt werden müssen.

Weit komplexer als der Austausch von Hardware-Baugruppen ist die Fehlersuche in Software. Vom Betriebssystem über Standardsoftware bis zur selbstprogrammierten Softwareanwendung drohen hier Ausfälle. Sicherheit bietet nur eine Überprüfung aller Systemteile. Diese ist jedoch fast unmöglich, da nur bei Eigenprogrammierungen überhaupt kontroll- und modifikationsfähiger Sourcecode vorliegt. Die Hersteller von Betriebssystemen und Standardsoftware jedoch können kaum die Vielfalt aller am Markt vertriebenen Software und damit mögliche Fehlerquellen überblicken. Somit ist nur davon sicher auszugehen, daß nach dem 1. Januar 2000 eine Vielzahl von Computerfehlern auftreten wird.

Die Folgen dieser Fehler und ihre Schwere hängen von den getroffenen Vorsichtsmaßnahmen ab. Lethale Folgen können Systemabstürze und Fehler in sicherheitsempfindlichen Bereichen – von der Flugsicherung bis zur Steuerung von Kernkraftwerken oder chemischen Analgen – und beim menschennahen Einsatz – vor allem in der Intensivmedizin – haben. Die ökonomischen Folgen beginnen bei einem Run auf Bargeld vor dem 1. Januar 2000 und reichen von schweren Störungen des Zahlungsverkehrs bis zu Firmenzusammenbrüchen, die als Konsequenz bei 15 % der bundesdeutschen Unternehmen vermutet werden.

Ein gleichzeitiger und schwerwiegender Ausfall größerer Teile der Informationstechnik dürfte mit hoher Wahrscheinlichkeit zu einem erheblichen Vertrauensverlust in die Funktionsfähigkeit und Zuverlässigkeit der gesamten Informationstechnologie führen. Maßnahmen zur Schadensminderung auf allen Ebenen sind eine der dringlichsten Aufgaben." [39])

Die Wirkungskomplexität der Informationstechnik einerseits und mit diesem Wirken der Informationstechnik konstitutiv erzeugte Probleme der IT-Sicherheit erfordern es, Sicherheitsbetrachtungen in einem erweiterten soziotechnischen Kontext vorzunehmen, der nicht nur die technischen Systeme, sondern auch ihre (z. B. soziale, ökonomische, rechtliche, kulturelle) Funktion in der jeweiligen Anwendungsumgebung einbezieht. Mit einem rein technisch orientierten IT-Sicherheitsbegriff, wie er heute in den Sicherheitskriterien (ITSEC, und den Common Criteria), dem Sicherheitshandbuch des Bundesamtes für Sicherheit in der Informationstechnik oder anderen relevanten Standards verwendet wird, ist keine um-

[39]) Vgl. 1.) EXPO direkt Nr. 3, 1997;
2.) The Day the World Shuts Down, in: Newsweek, S. 44, 46

fassende, der Komplexität möglicher Wirkungen gerecht werdende Betrachtung möglich.

1.2.2 IT-Sicherheit als soziotechnische Systemgröße

Mit dem im einleitenden Kapitel vorgestellten Begriff der „mehrseitigen Sicherheit" ist bereits angedeutet worden, daß IT-Sicherheit die Grenzen eines rein technisch verstandenen Sicherheitsbegriffs überschreitet.

In diesem Begriff enthaltene IT-Sicherheitsforderungen, wie „Unbeobachtbarkeit" und „Unverkettbarkeit" zielen weniger auf technische Gestaltungsoptionen informationstechnischer Sicherheit ab, als vielmehr auf Gestaltungsmaßnahmen des sozialen und organisatorischen Umfelds, in dem die Interaktion von Mensch und informationstechnischer Maschine stattfindet. Gerhard Banse[40]) spricht in diesem Zusammenhang vom „Nicht-Technischen" der IT-Sicherheit: „Zwecksetzung, Akzeptabilität, Verfügbarkeit, Beherrschbarkeit, Nutzerfreundlichkeit, Veränderungsdynamik, Sicherheitsverlangen u. v. a. m. in Bezug auf IT-Sicherheit sind nur erklär- und verstehbar – und damit auch bzw. erst berücksichtigbar –, wenn davon ausgegangen wird, daß die einzelne und konkrete IT-Sicherheitslösung in ein *nichttechnisches Umfeld* sozusagen *eingebettet* ist, das von der techniknahen Infrastruktur bis hin zu global wirkenden Akteuren, vom Stand der Wissenschaft und Technik bis zu politischen Vorgaben, vom geistigen Klima in der Gesellschaft bis zum Wertekanon der teilhabenden Individuen reicht. Dieses gesamte Umfeld wird [...] unter dem Begriff *Nichttechnisches* subsumiert."[41])

Ein in diesem Sinne „ganzheitlicher" IT-Sicherheitsbegriff bezieht sich auf alle Facetten eines *soziotechnischen Systems,* also der produktiven Kombination von Mensch – und in unserem Fall – *informationstechnischer* Maschine[42]). Dabei entfaltet der Begriff „Sicherheit" seine Bedeutung als strukturelle, konzeptionelle und strategische Antwort auf die unterschiedlichen Manifestationen von „Risiko". Risiko, bezogen auf soziotechnische Systeme, bedeutet, daß nichtintendierte Folgen menschlichen Handelns mit technischen Systemen nachhaltig negative Folgen auch über das jeweilige Handlungssystem bzw. technische System hinaus haben können. Die negativen Folgen betreffen Individuen, aber auch die Gesellschaft als Ganzes. Die bewußte Wahrnehmung dieser Risiken aus empirischer Erfahrung oder die antizipatorische Projektion möglicher Risiken wird „Risikobewußtsein" genannt. Aus diesem Risikobewußtsein heraus werden strukturelle, konzeptionelle und strategische Antworten auf Risiken mit dem Ziel entwickelt, Sicherheit zu gewinnen, indem die nichtintendierten Folgen sichtbar gemacht werden, um sie dann ggf. begrenzen oder vermeiden zu können. Eine so verstandene ganzheitliche IT-Sicherheit ist das Ergebnis einer umfassenden Reflexion von Risiken, die aus der Kombination von Mensch und informationstechnischer Maschine erwachsen. Deshalb ist es notwendig, über die im Eingangskapitel skizzierten „offensichtlichen" IT-Sicherheitsrisiken hinaus sozial und kulturell wirksame Tendenzen in der Entwicklung von IuK-Technologien mit Blick auf ihre informationstechnischen Sicherheitsfolgen zu betrachten.

1.2.3 Nichtwahrnehmbarkeit von Datenverarbeitungs- und Telekommunikationsvorgängen

Datenverarbeitungs- und Telekommunikationsvorgänge sind für den Menschen im allgemeinen nicht mit seinen eigenen Sinnen wahrnehm- oder durchführbar. Der Mensch braucht stets eine Mensch-Maschine-Schnittstelle, z. B. einen Bildschirm, bedrucktes Papier, ein Mikrophon, einen Lautsprecher, eine Tastatur, eine Maus oder eine graphische Benutzeroberfläche. Diese Schnittstelle ist für sich betrachtet selbst wieder ein risikobehaftetes Datenverarbeitungssystem. Der Mensch kann die Korrektheit der Funktion dieser Schnittstelle deshalb ebenfalls nicht unmittelbar durch eigene Wahrnehmung feststellen. Er bräuchte dazu weitere Mensch-Maschine-Schnittstellen usw.

Die korrekte Funktion der Schnittstelle kann in der Regel nur durch den Hersteller garantiert werden. Der Mensch kann deshalb nicht unmittelbar handeln und wahrnehmen. Es ist nicht gewährleistet, daß augenscheinliche und tatsächliche Funktionen und Vorgänge übereinstimmen.

Benutzerschnittstelle: Der Unterschied zwischen Schein und Sein

a) Der Benutzer eines Computers löscht eine Datei und die ordnungsgemäße Durchführung wird angezeigt. Der Benutzer kann aber nicht unmittelbar feststellen, ob die Datei wirklich logisch und physikalisch gelöscht, oder ob nur der Verweis im Inhaltsverzeichnis als ungültig markiert wurde.

b) Der Benutzer eines Telefons mit Freisprecheinrichtung ist darauf angewiesen, daß das Bestehen einer Verbindung optisch angezeigt wird. Geschieht dieses nicht, so besteht die Möglichkeit, daß der Raum unbemerkt über die Freisprecheinrichtung abgehört wird.

Der Mensch ist als Nutzer der EDV nicht mehr der ausschließlich Handelnde. Jedes System basiert auf komplexer Software, die von vielen verschiedenen Programmierern erstellt wurde. Der Benutzer bestimmt daher nicht mehr allein die Handlung, seine Entscheidungskompetenz kann hinter die sich in der Software niederschlagenden Absichten des Programmierers zurückgedrängt werden.[43]) Der Entscheidungswille des Benutzers muß auch nicht mehr kausal für die Aktion sein. Aktionen des Systems können

[40]) Prof. Dr. sc. Phil Gerhard Banse, Brandenburgische Technische Universität Cottbus; Europäische Akademie zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen GmbH Bad-Neuenahr-Ahrweiler

[41]) Banse, G., Nichttechnisches in der IT-Sicherheit: Positionen und Probleme, in: Bundesamt für Sicherheit in der Informationstechnik (BSI), Mit Sicherheit in die Informationsgesellschaft, Tagungsband 5. Deutscher IT-Sicherheitskongreß des BSI, Bonn 1997, S. 185–204, S. 187

[42]) Vgl. ebenda, Fußnote 11

[43]) Vgl. Schöne, B., Wenn der Dritte anonym bleibt, in: Süddeutsche Zeitung vom 15. Januar 1998

daher nicht uneingeschränkt und ohne genauere Betrachtung dem Inhaber oder Benutzer des Systems zugeordnet werden. Der Bürger läuft damit ständig Gefahr, sich Handlungen, Erklärungen und Entscheidungen zurechnen lassen zu müssen, von denen er gar nichts weiß. Gleichzeitig stehen aber auch die Strafverfolger vor dem Problem, daß sich der „virtuelle Straftäter" jederzeit auf Kontrollverlust oder gar Fremddisposition berufen kann und ihm dies auch nicht ohne weiteres zu widerlegen ist.

1.2.4 Selbststeuernde IT-Systeme

In der Entwicklung von IT-Systemen gibt es einen starken Trend, informationstechnische Systemwelten mehr und mehr autonom vom steuernden oder kontrollierenden „Zugriff" des menschlichen Nutzers zu gestalten. Autonom entscheidende Softwaresysteme kommen in vielfältigen Bereichen zum Einsatz, beispielsweise:

Der Pilot im Cockpit eines vom „Autopiloten" gesteuerten Großflugzeuges; der Fluglotse im Tower eines Großflughafens, bei dem die Steuerung des Anflugverkehrs auf Computer-Empfehlung beruht; der Lokführer eines computergesteuerten ICE-Zuges; der Stationsarzt in der computergestützten Intensivstation eines Krankenhauses; der „Facharbeiter" in der automatisierten, rechnergestützten Fabrik; der Chemiker am Steuerungspult chemisch-industrieller Verfahren; der Soldat an „intelligenten" Waffensystemen ...

All diese Personen stehen Systemen, technischen Prozeduren, in Programmen gefaßten Eigengesetzlichkeiten der IT-Systeme gegenüber, die, obwohl sie diese eigentlich steuern und kontrollieren sollen, längst unabhängig vom „steuernden" Menschen in der Regel „alles im Griff haben". Diese Tendenz ist ambivalent zu bewerten.

Auf der einen Seite könnte ein ICE ohne Computerunterstützung – die bestimmte logische Entscheidungsroutinen einschließt, – keine Geschwindigkeit von 250 Km/h relativ sicher fahren. Auch wäre es für den Piloten eines Tornado-Kampfflugzeuges ohne Computer-Unterstützung ausgeschlossen, mit Überschallgeschwindigkeit unterhalb feindlichen Radarempfangs zu fliegen. Und ob der Airbag im Auto aufspringt, kann sinnvollerweise auch nur über ein autonomes informationstechnisches System entschieden werden. Die soziale und kulturelle Kehrseite dieses Trends einer „Materialisierung von Verhaltensregeln" in Form von Computerprogrammen führt aber dazu, menschliche Fähigkeiten den technischen Qualitäten der scheinbar dem Menschen überlegenen Maschine entweder unterzuordnen oder den Menschen ganz aus den technischen Funktionsabläufen herauszunehmen. Dabei findet ein „Verantwortungstransfer" von menschlicher Verantwortung auf Maschinen bzw. Programme statt, die, wie bereits gezeigt wurde, durchaus fehlerbehaftet und unfertig sein können. Maschinen bzw. Programme sind aber weder natürliche noch juristische Personen, die Verantwortung im Sinne von Haftung übernehmen können. Daraus leitet sich als Konsequenz ab, daß bei einer zunehmenden, vom Nutzer nicht mehr kontrollierbaren Selbststeuerung von IT-Systemen sich die Verantwortung für etwaige negative Folgen dieser Selbststeuerung im Sinne eines justitiablen Haftungsbegriffes auf die Hersteller informationtechnischer Systeme verlagern muß.

1.2.5 Wachsende IT-Systenkomplexität

Gewährleistung und Überprüfung der Sicherheit und Qualität von Software und die Beurteilung ihrer Wirkung sowie der von ihr ausgehenden Gefahren setzen das Verständnis der gesamten Arbeitsweise und die Erfassung der funktionalen Zusammenhänge voraus. Die heute marktübliche Software weist jedoch eine Größe, einen Funktionsumfang und eine Komplexität auf, die selbst Fachleute überfordert. Während der Umfang des Betriebssystems und der Anwendungsfunktionen ständig ansteigt, steigt nämlich auch die Geschwindigkeit der Fortentwicklung, weil immer mehr Personen an der Entwicklung beteiligt sind. Aktuelle Systeme sind innerhalb der Zeit zwischen erster Verfügbarkeit und Veraltung nicht mehr ausreichend zu erfassen.

Vor diesem Problem stehen auch die Hersteller, wie aufgedeckte und veröffentlichte Sicherheitslücken qualitativ und quantitativ belegen.

Die Folge ist, daß Anwender und Entscheidungsträger, die selbst nicht auf das jeweilige Gebiet spezialisiert sind, mit der Benutzung, dem Verständnis der Funktionalität und der Abschätzung der Wirkung überfordert sind. Die Gefahr der Fehlbedienung auf Anwenderseite steigt damit erheblich an. Trotzdem verfügt die weit überwiegende Mehrzahl der Anwender nicht über eine fundierte Schulung, sondern nur über oberflächliche, grob lückenhafte und teilweise falsche Einzelkenntnisse.

Gleichzeitig verlieren die Systeme durch steigende Komplexität an Robustheit und Fehlertoleranz. Schon geringfügige Fehlkonfigurationen und kleine Bedienungsfehler können unabsehbare Folgen haben.

Die zunehmende Komplexität und Funktionenvielfalt ist mit der Verwendung durch immer größere Anwendergruppen mit immer geringeren Fachkenntnissen unverträglich.

Als ein Beispiel für die Diskrepanz zwischen informationstechnischen Abläufen und mangelndem Nutzerverständnis kann die internetbasierte Anwendung „Email" dargestellt werden.

Die genaue Funktionsweise von Email, Mailinglisten und dem Usenet ist vielen Benutzern dieser Systeme nicht ausreichend klar. Wegen der engen Verwandtschaft und der sehr ähnlichen Erscheinungs- und Darstellungsweise dieser Dienste und ihrer nichttrivialen Funktionsweise kommt es immer wieder zu Mißverständnissen, Verwechslungen und Bedienungsfehlern.

Oft können Benutzer zwischen dem Senden einer Email an eine Privatperson, dem Senden an alle Personen der Cc:- und Bcc:-Zeilen, dem Senden an Mailinglisten und dem Posten in Newsgruppen nicht unterscheiden. Die Unterscheidung wird zusätzlich erschwert durch Programme wie Web-Browser, die

alle diese Funktionen hinter (vermeintlich!) leicht zu bedienenden graphischen Benutzeroberflächen ohne augenfällige Differenzierung verbergen.

So passiert es immer wieder, daß Anwender in dem Glauben, eine persönliche Email an eine bestimmte Person zu schicken oder in einer Newsgruppe nur einen lokalen Bekanntenkreis zu erreichen, vertrauliche Informationen einem größeren Personenkreis oder gar gleich weltweit offenlegen. Im harmlosesten Fall führt dies zur Verwunderung darüber, von wildfremden Menschen aus anderen Kontinenten wohlwollende Antworten zu erhalten.

Ein drastisches Beispiel ist der Vorfall bei der Firma Siemens Nixdorf[44]). Dort wurden monatelang unbemerkt firmeninterne Mitteilungen an einen außerhalb gelegenen Empfänger versandt, weil Email-Benutzer den Domain-Namen verwechselten und an Empfänger in **Münch**en statt an **mch.sni.de** an **sni.mch.de** und damit an den Inhaber der **mch.de,** nämlich das **M**arketing-**C**enter **H**andwerk" versandten. Der Umfang der Verwechslungen ist nicht allein mit Flüchtigkeitsfehlern zu erklären. Hier haben eine Vielzahl von Benutzern das Funktionsprinzip der Domainnamen und des Mail-Transports nicht genau verstanden. Das ist insoweit beunruhigend, als es sich hier sogar um Mitarbeiter eines EDV-Herstellers handelt.

Man führe sich vor Augen, welche Folgen es gehabt hätte, wenn sich solche Vorfälle in einer Klinik ereignet hätten und über mehrere Monate hinweg Patientendaten, Befunde, Röntgenbilder usw. unkontrolliert an zufällige Empfänger verschickt oder gar versehentlich in eine Newsgruppe gepostet und damit gleich weltweit veröffentlicht worden wären.

Passierte solches mit Wirtschaftsdaten oder Firmengeheimnissen, wäre der Bestand des Unternehmens, ja sogar anfälliger Volkswirtschaften, durchaus in Frage gestellt.

1.2.6 Handlungs- und Gestaltungsoptionen

In der bisherigen Beschreibung der Wechselbeziehung von Mensch (Sozialer Sphäre) und IT-System (Technischer Sphäre) ist deutlich geworden, wie durch die Gestaltung von Technik menschliche Handlungs- und Gestaltungsmöglichkeiten beeinflußt und determiniert werden. Die im soziotechnischen System durch das Technische dominierte und vorgegebene Handlungsmöglichkeiten des Menschen mit der IT-Maschine beeinflußt nachhaltig die Kultur des Umganges mit IT-Sicherheit und ihre soziale Einbindung. Daß dabei erhebliche Defizite zu verzeichnen sind, ist durch zahlreiche Beispiele illustriert worden.

Es soll nun erörtert werden, welche Gestaltungsoptionen existieren, um die angezeigten „systemimmanenten" Sicherheitsrisiken des sozio-*informations*technischen Systems zu begrenzen oder zu vermeiden.

Dabei muß unterschieden werden zwischen Gestaltungsoptionen in der „Technischen Sphäre" und in der „Sozialen Sphäre".

Die technischen Gestaltungsoptionen werden u. a. in den Abschnitten „Ziele der IT-Sicherheit" und „Möglichkeiten der Technik" ausführlich vorgestellt und diskutiert. Im Rahmen dieses Abschnittes „Kulturelle und soziale Rahmenbedingungen" sollen zunächst die Handlungs- und Gestaltungsoptionen dargestellt werden, die auf eine soziale und kulturelle Beherrschung von IT-Sicherheitsproblemen abzielen.

1.2.7 IT-Sicherheit als Thema von Forschung und Lehre an der Hochschule

Entwurf, Anfertigung und Verifikation von Software sind Arbeiten, die hohe Anforderungen an Zuverlässigkeit, Erfahrung, Ausbildung und an die akademischen und „handwerklichen" Fähigkeiten der damit befaßten Personen stellen. Die Erstellung von hochwertiger Software setzt umfangreiches Wissen aus den Kerngebieten der Informatik, themenspezifisches Wissen und Wissen aus angrenzenden Randgebieten voraus, wie sie durch das wissenschaftliche Informatikstudium vermittelt werden.

In der Realität fehlen diese Voraussetzungen oftmals. Eine Ursache hierfür ist der steile Anstieg des Bedarfs an Programmierkräften, der in dieser Geschwindigkeit von den Hochschulen nicht befriedigt werden konnte, denn ein intensives Informatikstudium an einer deutschen Hochschule benötigt über 10 Semester, und die Anzahl der Informatikabsolventen ist zu niedrig.

Es gibt eine Vielzahl von Softwareentwicklern, die aus anderen Berufsfeldern stammen und das Programmieren von Software autodidaktisch, ohne eine ausreichende fachliche Ausbildung durchlaufen zu haben, erlernt haben. Weder hier noch in den USA bestehen Normen zur Bewertung IT-spezifischer Fachkenntnisse. Ein weiteres Problem besteht darin, daß Software normalerweise nach bestimmten Anforderungen bzw. Spezifikationen erstellt wird oder werden sollte, die Sicherheit der Software aber oftmals nicht Teil der Spezifikation ist. Sicherheit wird zu oft als überflüssige Belastung statt als Qualitätsmerkmal verstanden. In der Folge werden Sicherheitsanforderungen ignoriert oder nur scheinbar und unzureichend erfüllt.[45])

Aus der grundlegenden Bedeutung informationstechnischer Sicherheit für alle Ebenen der Gesellschaft erwächst die Notwendigkeit, Belange der IT-Sicherheit systematisch als Curricula in die Ausbildung der Informatiker einzubinden. Vorrangiges Ziel sollte dabei die Vermittlung von informationstechnischen Sicherheitsanforderungen als Parameter bei der Konzeption und dem Aufbau von IT-Systemwelten sein. Entsprechend der hohen Komplexität und des interdisziplinären Formats, wie es durch den Begriff der „Mehrseitigen Sicherheit" zum Ausdruck

[44]) Vgl. Focus 3/1998, Loch im Datennetz, S. 158ff.

[45]) Dies äußert sich z. B. in der Verwendung wertloser Chiffren oder dem regelrechten Vortäuschen von Sicherungsmaßnahmen.

kommt, muß die IT-Sicherheitsausbildung interdisziplinär angelegt werden. Hierzu ist die Politik auf Bundes- und Länderebene gefordert, entsprechende Anstrengungen zu unternehmen.

Der Bedarf einer verstärkten Integration von Curricula zur IT-Sicherheit in der Informatiker-Ausbildung korrespondiert mit der Notwendigkeit einer verstärkten Forschungsförderung.

Dabei ist die besondere Bedeutung des „Faktors Mensch" im Zusammenhang mit IT-Sicherheitsunfällen ein Hinweis darauf, daß ausgehend von einem Paradigma des soziotechnischen Systems, die Frage, wie IT-Sicherheit im Mensch-Maschine-Interaktionsprozeß systematisch eingebunden werden kann, vordergründig zu stellen ist.

1.2.8 Förderung von IT-Sicherheit als Bestandteil der Alltagskultur

Elektronische Textverarbeitung, Email, Telebanking, Teleshopping, Telearbeit, Electronic Commerce, Telefonie sind nur einige wenige Beispiele für IT-Anwendungen, die sich immer stärker in der Lebens- und Wirtschaftskultur unserer Gesellschaft etablieren. Diese Anwendungen werden zunehmend über das globale Internet integriert. Bedingt durch den erheblichen Mangel an Sicherheit im Internet werden die den einzelnen Anwendungen anhaftenden Sicherheitsmängel durch die Netzeinbindung verstärkt. Daraus entsteht die Gefahr, daß „sofern die Endanwender nicht sicher sein können, daß ihre digitale Kommunikation unverfälscht beim Adressaten ankommt, die Nachrichteninhalte Unberechtigten nicht zugänglich sind und die Kommunikation von Dritten nicht überwacht wird (Datenschutz, Vertraulichkeit), die „Global Information Structure" weder von Unternehmen noch von Privaten in der Form angenommen werden, wie es heute vielfach geplant ist."[46]) Auf der anderen Seite ist das Risikobewußtsein der Nutzer von IuK-Technologien gering ausgebildet. Was hinter dem Sichtbaren des Bildschirms passiert, entzieht sich menschlicher Wahrnehmung und Kontrolle. Die Komplexität informationstechnischer Prozesse wird heute selbst von Experten nicht mehr verstanden. Deshalb sind Risiken in IT-Systemen wenig spür- und greifbar. Diese Situation stellt sich auch als Herausforderung anwendungsorientierter IT-Forschung und Technikgestaltung dar: Nämlich IT-Systemwelten so zu gestalten, daß zu jeder Zeit der Mensch den Status eines IT-Systems mit seinen sinnlichen und rationalen Möglichkeiten erfassen und kontrollieren kann. Auf der gesellschaftspolitischen Handlungsebene ist die Herausforderung, Belange der IT-Sicherheit bei der informationstechnischen Ausbildung – auch unterhalb der Hochschulausbildung – systematisch zu berücksichtigen. Damit ist auf der einen Seite das Ziel verbunden, das Verständnis informationstechnischer Systemwelten und ihre Risiken zu erhöhen. Auf der anderen Seite gilt es, dem IT-Nutzer einfache, kostengünstige und robuste Werkzeuge des IT-Selbstschutzes in die Hand zu geben und ihren Gebrauch zu vermitteln.

Die Politik ist hier auf Bundes- und Länderebene gefordert, Maßnahmen zu ergreifen, die sowohl auf eine Erhöhung des Risikobewußtsein der IT-Nutzers abzielen als auch die Kompetenz der IT-Nutzer beim IT-Selbstschutz erhöhen. Hierzu zählen Maßnahmen der Aufklärung der Bürger und der Wirtschaft über Sicherheits- und Datenschutzrisiken sowie mögliche Schutzstrategien, die verstärkte frühzeitige Abschätzung von Risiken und die Verankerung informationstechnischer Sicherheitsbelange in die IT-Ausbildung in Schule und Wirtschaft. Im Zentrum dieser Bemühungen sollte die Förderung der Nutzung der Digitalen Signatur und Verschlüsselungssoftware (Kryptographie) stehen.

1.3 Die politische Bedeutung der IT-Sicherheit

Ein hervortretendes Merkmal der neuen IuK-Technologien ist ihre Einbindung in globale Telekommunikationsnetze. Die damit geschaffene Struktur für einen global vernetzten Datentransfer erlaubt den Austausch und Zugriff von Informationen ohne zeitliche oder räumliche Restriktionen. Diese Möglichkeit stellt den Kern dessen dar, was mit Informationsgesellschaft bezeichnet wird. Wie bereits mehrfach in diesem Berichtsteil gezeigt wurde, ist dieser globale Informationsaustausch weder von seinen technischen Voraussetzungen her sicher, noch existieren hinreichende Möglichkeiten des Schutzes vor Angriffen. Die Abhängigkeit und Verletzbarkeit technisch hochentwickelten Gesellschaften von weltweit verteilten Datenverarbeitungsprozessen erzeugen die politische Notwendigkeit, bestimmte IT-Sicherheitsstandards im Rahmen internationaler Vereinbarungen und Verträge zu sichern und verbindlich durchzusetzen.

Die Bundesrepublik Deutschland ist deshalb aufgefordert, im Rahmen der G8-Konferenzen und der EU auf international verbindliche Regulierungen der IT-Sicherheit hinzuwirken.

In Verbindung mit der Etablierung verbindlicher internationaler IT-Sicherheitsstandards steht die Aufgabe, die Voraussetzung für eine internationale wirksame Rechtsverbindlichkeit – etwa in Fragen der Haftungsregulierung – zu schaffen. Im Hinblick auf neue Formen der Computer– und Netzkriminalität stellt sich der Politik die Aufgabe auch hier über internationale Vereinbarungen die Voraussetzungen zu schaffen, eine effiziente Strafverfolgung in grenzüberschreitenden Netzwerken möglich zu machen. Ein weiteres Aufgabengebiet ist die Herstellung eines internationalen Konsens über die Kompatibilität sicherer digitaler Zahlungsmittel und der damit zusammen hängenden Sicherheitsfragen.

Die politische Förderung von IT-Sicherheit durch die Vereinbarung international verbindlicher Standards und anderer rechtlicher Regulierungen trägt entscheidend dazu bei, eine höhere Akzeptanz von IuK-Technologien in Wirtschaft und Gesellschaft zu errei-

[46]) Pohl, H., Informationssicherheit der Global Information Infrastructure (GII), in: Tauss, J.; Kollbeck, J.; Mönikes, J. (Hrsg.), Deutschland Weg in die Informationsgesellschaft, Bonn, 1996, S. 366

chen. Eine in solcher Form institutionell verankerte IT-Sicherheit wirkt als Katalysator bei der Entfaltung einer neuen digitalen Ökonomie. Ohne die globale Verankerung von IT-Sicherheitsmechanismen werden sich die bestehenden IT-Sicherheitsrisiken als Wachstumshemmnisse sowohl beim elektronischen Handel als auch im Hinblick auf eine breite Akzeptanz der neuen Medien in der Gesellschaft auswirken.

Auf Seiten der Bundesrepublik Deutschland wurde mit dem Signaturgesetz ein erster wichtiger Schritt zum Aufbau einer nationalen Sicherheitsinfrastruktur unternommen. Mit diesem Gesetz wurde die rechtliche Grundlage für die Schaffung einer Infrastruktur für die Bereitstellung und Nutzung der digitalen Signatur gelegt.[47])

Mit diesem auch im Ausland vielbeachteten Gesetz hat die Bundesrepublik Deutschland über die eigenen Ländergrenzen hinweg einen wichtigen Impuls für informationstechnische Sicherheit gegeben.

Wie bereits im Zusammenhang mit dem Begriff der „mehrseitigen Sicherheit" verdeutlicht wurde, ist IT-Sicherheit heute auch eine wichtige Voraussetzung, um Datenschutzziele zu erreichen. Mit der Feststellung des informationellen Selbstbestimmungsrecht durch das Bundesverfassungsgericht obliegt der Politik die Aufgabe, alle Instrumente, die diesem Ziel dienen, zu fördern und ihre Verbreitung zu unterstützen.

In diesem Kontext ist zu beachten, daß die globale Dimension und Körperlosigkeit virtueller Netzräume die selbstverantwortliche Nutzung von IT-Sicherheitsinstrumenten, wie z.B. Kryptosystemen, durch den Netzteilnehmer erfordert. Der Staat hat hier nur noch begrenzte Eingriffs- und Schutzmöglichkeiten. Aus dieser Situation stellt sich dem Staat die Aufgabe, die materiellen, strukturellen und organisatorischen Voraussetzungen für den IT-Selbstschutz durch den Netzteilnehmer zu schaffen. Diese staatliche Aufgabe leitet sich aus der Pflicht des Staates ab, die Sicherung der Persönlichkeitsrechte, wie sie auch durch das informationelle Selbstbestimmungsrecht zum Ausdruck kommen, zu gewährleisten.[48])

1.3.1 Information Warfare als Bedrohungspotential nationaler Sicherheit

Die nationale Sicherheit eines Landes wird im Informationszeitalter durch vielfältige Angriffsformen im Netzraum bedroht.

Informationen und Datenverarbeitungsprozesse, die über elektronische Netze laufen, sind grundsätzlich potentielle Objekte gegnerischer Angriffe. Angriffe auf Informationen bzw. auf Informationen basierende Prozesse sowie auf die Informationstechnik selbst werden mit dem Begriff: „Information Warfare" bezeichnet. Informationen Warfare ist also eine Form der Kriegsführung mit Mitteln der Informationstechnik und beinhaltet die gezielte Ausnutzung von Schwachstellen in der IT- Sicherheit zur Durchsetzung von politischen Interessen. Dabei werden zwei unterschiedliche Intensitätsstufen unterschieden. So wird ein Netwar gesehen als ein informationsbezogener Konflikt auf der Ebene von Staaten und Gesellschaften, bei dem das Wissen der Bevölkerung eines Konfliktgegners und deren Schaubild Ziel der Auseinandersetzung ist. Diese Sichtweise resultiert aus der Nähe von Informationen Warfare zu Elementen psychologischer Kriegsführung und verdeutlicht, daß es hierbei nicht allein um militärische Konflikte geht. Ein im herkömmlichen Sinne militärisches Konzept ist ein Cyberwar, der die Durchführung und Vorbereitung militärischer Operationen nach informationsbezogenen Prinzipien bedeutet. Dies umfaßt die Störung des Wissens eines Gegners über die eigene Lage und Stärke und die Zerstörung seiner Informations- und Kommunikationssysteme. Information Warfare Angriffe können über internationale Netzwerke und von weit entfernten Orten aus geführt werden. Die herkömmlichen, traditionellen, nationalen Grenzen, die als Front dienen, verlieren im Informationskrieg ihre Bedeutung. Der organisatorische, technische und finanzielle Aufwand für Angriffe oder Störungen von IuK-Netzen und der Informationsstruktur eines Landes ist gering im Vergleich mit herkömmlichen militärischen Angriffen. Die Bedrohung geht beim Information Warfare immer seltener von Hackern, sondern von fremden Geheimdiensten aus, die vertrauliche Wirtschaftsinformationen ausspähen. So wurde im Jahr der Veröffentlichung dieses Berichtes bekannt, daß vom deutschen Außenposten des amerikanischen Geheimdienstes *National Security Agency* systematisch Wirtschaftsunternehmen ausgespäht wurden. Die Bedrohung kann aber auch von befreundeten europäischen Nachbarländern ausgehen: „Siemens Manager bestätigen, daß Südkorea das französische Zugsystem TGV dem deutschen ICE vorzog, nachdem die Franzosen während der Verhandlungen die deutschen Preisforderungen aus dem Internet abhorchten und prompt unterboten."[49]) Die Politik ist hier dringend gefordert, die Voraussetzungen für den Aufbau einer nationalen Sicherheitsinfrastruktur zu schaffen, die allen Bedrohungsformen des Information Warfare geeignete Schutz- und Abwehrstrategien entgegen setzt.

Dabei stellen sich folgende grundlegende Aufgaben:

- Beschreibung und Analyse der „Information Warefare-Bedrohungspotentiale",

[47]) Die digitale Signatur ist ein wichtiges IT-Sicherheitsinstrument zur Herstellung von Rechtssicherheit bei elektronischen Dokumenten. Vgl. hierzu die Abschnitte 3.2.7 und 4.1.1

[48]) Vgl. hierzu auch die Abschnitte 1.3 und 4.1.3

[49]) Klagges, H., Kleine Lauschangriffe unter Freunden: Die USA hören in Europa offenbar systematisch Telephone, Faxe und E-Mails ab, in: Süddeutsche Zeitung vom 20. Januar 1998, S. 28; vgl. außerdem hierzu Nürnberger, C., Feind hört mit: Technische und elektronische Überwachung auf dem Vormarsch, in: Süddeutsche Zeitung vom 26. März 1998, S. 15; Einen umfassenden Überblick zu diesem Thema gibt die im Auftrag des Europäischen Parlaments erarbeitete Studie AN APPRAISAL OF TECHNOLOGIES OF POLITICAl CONTROL. Diese Studie kann entweder direkt über das Europäische Parlament oder über die Internetadressen http://jya.com/stoa-atpc.htm bzw. http://www.heise.de/tp bezogen werden.

- Technologiepolitische Anstrengungen der Bundesrepublik Deutschland zum Ausbau einer IT-Sicherheitsinfrastruktur,
- Beteiligung Deutschlands an einer gezielt überlegenen IT-Sicherheitstechnik der westlichen Verbündeten bei gleichzeitiger Wahrung nationaler Interessen,
- Entwicklung gemeinsamer Sicherheitsstrategien im „Cyberspace" seitens der NATO-Länder,
- Verstärktes koordiniertes Vorgehen in Fragen des Schutzes globaler Informationsnetze gegen Computerspionage und -sabotage,
- Initiierung internationaler Verhandlungen zum Schutz der Informations-Infrastruktur gegen Angriffe und Manipulationen.
- Kontinuierliche Aufklärung, Überwachung und Kontrolle von „Cyberwar", Bedrohung der staatlichen und globalen Informationssysteme auf der Basis internationaler Zusammenarbeit.[50])

Neben dem Ausbau der materiellen, institutionellen und organisationellen Voraussetzungen zum Aufbau einer nationalen IT-Sicherheitsinfrastruktur ist es gleich bedeutsam, daß der Staat die Verbreitung und den Einsatz von IT-Sicherheitsinstrumenten in seinen Institutionen fördert. Dies ist nicht nur notwendig um Sicherheit bei der eigenen Daten- und Informationsverarbeitung zu erreichen, sondern um die Akzeptanz und den Gebrauch von Sicherheitsinstrumenten beim IuK-Nutzer zu fördern. Hinzu kommt, daß staatliche Institutionen und öffentliche Verwaltungen eine hinreichende Größenordnung bieten, um so die Verbreitung und Nutzung in die Gesellschaft zu verstärken.

Die Frage, inwieweit bestimmte Formen der IT-Sicherheit den Strafverfolgungsinteressen der Sicherheitsbehörden entgegenlaufen und Kriminellen die Möglichkeit von geschützter Kommunikation bieten, wird im Abschnitt „Die Kryptographie" im Kapitel 2.4 erörtert.

1.4 Die wirtschaftliche Bedeutung von IT-Sicherheit

1.4.1 Einführende Bemerkungen

Die strukturelle Bedeutung von IT-Sicherheit für die Wirtschaft wächst parallel mit der zunehmenden Verbreitung und wirtschaftlichen Anwendungsintensität von IuK-Technologien. Die damit verbundene zunehmende Abhängigkeit vom einwandfreien Verlauf datenverarbeitender Prozesse bedeutet umgekehrt, daß auch die Risiken wachsen, die mit einem Ausfall oder einem Angriff auf ein informationsverarbeitendes System verbunden sind. Datamonitor beziffert den Schaden, der durch mangelnde IT-Sicherheit weltweit in einem Jahr verursacht wird, auf 16 Milliarden Dollar.[51]) Die Bedeutung von IT-Sicherheit als risikominderndes technisches, soziales und organisatorisches Maßnahmenbündel ist im einleitenden Kapitel behandelt und soll in diesem Abschnitt nicht weiter vertieft werden. Ein Schwerpunkt dieses Abschnittes wird vielmehr die Behandlung von IT-Sicherheit im Hinblick auf digitale Märkte[52]) sein. Die wirtschaftliche Bedeutung von IT-Sicherheit erschließt sich in diesem Zusammenhang insofern, als daß Unternehmen erst durch die Reduktion von informationstechnischen Risiken die Wettbewerbsvorteile des Electronic Commerce ausschöpfen können. Dabei wirkt IT-Sicherheit als vertrauensbildender Faktor, ohne den Unternehmen und Verbrauchern den Schritt in den „digitalen Handel" scheuen würden.

IT-Sicherheit als vertrauensbildender Faktor offenbart seine wirtschaftliche Bedeutung indirekt, denn der Marktteilnehmer kann grundsätzlich die „digitale Ökonomie" meiden und seine Transaktionen über die nicht-digitalen Märkte ausführen. Erst über die Betrachtung der kostenreduzierenden und damit wettbewerbswirksamen Mechanismen der „digitalen Ökonomie" werden die wirtschaftlichen Folgen einer mit IT-Sicherheitsrisiken begründeten Nichtteilnahme am Electronic Commerce deutlich. Deshalb wird die wirtschaftliche Bedeutung von IT-Sicherheit in diesem Zusammenhang über eine Betrachtung der Ökonomie des „digitalen Marktes" eingeleitet.

Mit dem wachsenden Bedürfnis nach informationstechnischer Sicherheit entsteht eine Nachfrage für IT-Sicherheitsprodukte und Dienstleistungen, die einen Markt für IT-Sicherheit initiiert. Dieser Markt und die Wettbewerbsposition, die europäischen Unternehmen in diesem einnehmen, werden im zweiten Teil dieses Abschnittes betrachtet.

Mit dem Entstehen digitaler Märkte offenbart sich auch das Problem geeigneter digitaler Zahlungsmittel, die die Prinzipien einer einfachen Handhabung, Anonymität und vor allem Sicherheit miteinander verbinden. Ähnlich wie das reale Geld umfassende Sicherungsmaßnahmen auf allen Ebenen seines Lebenszyklus erfordert, muß Sicherheit auf allen Stufen des „digitalen Geldkreislaufes" systematisch angelegt sein, wenn „digitales Geld" nicht von Anfang an zum Scheitern verurteilt sein soll. Dabei kommt der Sicherheit vor Fälschung eine ganz besondere Rolle zu.

Im dritten Teil dieses Abschnitts werden digitale Zahlungsmittelsysteme näher betrachtet.

1.4.2 Die Ökonomie des digitalen Marktes

Im Erscheinungsjahr dieses Berichtes – 1998 – war Electronic Commerce das zentrale Thema auf der weltweit größten Computermesse CeBIT.

Es herrscht Aufbruchstimmung, die inzwischen auch deutsche Unternehmen erfaßt zu haben scheint. Trotz unterschiedlicher Parameter, die zur Beurteilung des internationalen Wettbewerbs herangezogen werden können, ist eindeutig, daß die Bundesrepublik in der

[50]) Vgl. die Aussage der Stiftung Wissenschaft und Politik während der Anhörung der Enquete-Kommission am 12. Mai 1997

[51]) Datamonitor „Internet/Extranet Security – Executive Summary" (1997) S. 5

[52]) Diese Märkte werden im folgenden mit dem Begriff *Electronic Commerce* bezeichnet.

Internet-Nutzung deutliche Fortschritte gemacht hat. Die Umrisse der künftigen „digitalen Ökonomie" werden sichtbar. Das Internet zählt weltweit rund 80 Millionen Nutzer sowie 400000 kommerzielle Anbieter und ist Basis für ein Handelsvolumen von Milliarden Dollar.[53]) Auch in Deutschland nimmt das Interesse am „Electronic Business" quer durch alle Branchen zu.[54])

Die Feststellung eines wachsenden Interesses deutscher Unternehmen am Electronic Commerce erklärt noch nicht die wettbewerbsrelevanten Vorteile, die Unternehmen in der digitalen Ökonomie für sich ausschöpfen können. Um diese zu verstehen, ist es notwendig, einen Teil der Bedingungen zu betrachten, unter denen seit Anfang der 1990er-Jahre eine digitale Ökonomie sich entfalten konnte.

Der wichtigste Antriebsfaktor in dieser Entwicklung ist der beispiellose Preisverfall für Computertechnologie und technisch vermittelter Kommunikation.

Möglich wurde dieser rapide Preisverfall durch eine sehr hohe Innovationsgeschwindigkeit in der Computertechnologie. Immerhin werden 80 Prozent des Umsatzes in diesem Markt mit Produkten gemacht, die nicht älter als zwei Jahre sind.

Zwischen Technologieinnovation, Preisverfall und Wachstum des Marktvolumens formiert sich eine Wechselbeziehung zwischen *Technologie und Ökonomie:* Der Preisverfall auf dem Markt für Computertechnologie führt zu einer wachsenden Nachfrage und damit zu einer immer stärkeren Verbreitung dieser Technologie, die gleichzeitig ständigen Innovationen unterliegt.

Bei der weiter zunehmenden Computerisierung und informations-technischen Durchdringung von immer mehr Bereichen in der Gesellschaft, ist schwer zu erkennen, wann die Grenzen dieser Wechselbeziehung erreicht sein könnten. [55])

Dabei handelt es sich nicht um eine grundsätzlich neue Entwicklung, denn schon vor dem Internet wurden zunehmend geschäftliche Vorgänge mit Unterstützung von Computern abgewickelt. Mit der Einbindung geschäftlicher Aktivitäten in Telekommunikationsnetzwerke ist es möglich geworden, geographisch weit verteilte Ressourcen ohne zeitliche Einschränkungen zu nutzen und zu bündeln. So entwickeln beispielsweise große Automobilkonzerne ihre neuen Modelle, indem Entwicklungsingenieure aus verschiedenen Erdteilen am Computermodell zusammenarbeiten. Eine erhebliche Verkürzung der Entwicklungszeit mit entsprechenden Kostenvorteilen ist das Ergebnis einer solchen Form netzbasierter Kooperation.

Die Suche nach dem preiswertesten Anbieter eines bestimmten Produktes oder Dienstleistung kann heute vom heimischen Schreibtisch über das Internet zu erheblich verringerten Kosten erfolgen. In Zukunft werden „intelligente Agenten" die Recherche im Internet erleichtern.[56]) Speziell auf die Informationsbedürfnisse des individuellen Nutzers eingestellt, werden diese elektronischen Helfer das Netz durchsuchen und die gewünschten Informationen auf seinem Bildschirm präsentieren.

Die Organisation von Unternehmen verändert sich unter dem Einsatz von IuK-Technologien. Die Spannweite reicht vom Managementinformationssystem über Telearbeit bis hin zum virtuellen Unternehmen, das sich bezogen auf den individuellen Kunden bzw. auf die jeweilige Aufgabenstellung durch die Aktivierung und organisatorischen Bündelung standortverteilter Ressourcen über Telekommunikationsnetze aufgabenbezogen flexibel formiert.[57]) Für die beteiligten Akteure ist dabei wichtig, daß die IT-Sicherheitsziele Vertraulichkeit der Recherche, Integrität und Verfügbarkeit der Daten, sowie deren Authentizität realisiert werden.

Die oben genannten Beispiele lassen erkennen, daß die Möglichkeiten der „digitalen Ökonomie" erhebliche Kosteneinsparungen erlauben. Dies gilt insbesondere für Transaktionskosten. Heute können Informationen über Anbieter von Waren und Dienstleistungen zu sehr geringen Kosten auch von kleinen und mittleren Unternehmen[58]) weltweit über das Internet ermittelt werden. Kontakte und Geschäftsanbahnungen können dann sofort via E-Mail über den Bildschirm erfolgen. Und schließlich können Produkte- und Dienstleistungen direkt über das Netz vermarktet und sogar vertrieben werden.[59])

Bedingt durch die weltweite Ausbreitung des Internet wird Electronic Commerce den Wettbewerb verschärfen und weiter globalisieren.

Die durch die globale Vernetzung von Rechnern möglich gewordene weltweite Vergleichbarkeit von Anbietern und Preisen, die geringe Markteintritts- und Geschäftsanbahnungskosten sowie die potentielle weltweite Erreichbarkeit von Kunden – all diese neuartigen Bedingungen einer globalen und digitalen Ökonomie erzeugen erheblichen Anpassungsdruck nicht nur für Unternehmen, sondern für ganze Volkswirtschaften.[60])

Verstärkt wird die Bedeutung des Electronic Commerce durch den erklärten politischen Willen, den elektronischen Handel durch eine der „digitalen Ökonomie" angepaßte Gestaltung internationaler Handelsbedingungen zu fördern. So tagte vom 6. bis 8. Juli 1997 in Bonn die internationale Konferenz

[53]) Die Internet Data Corporation prognostiziert für Westeuropa einen Anstieg von Internetumsätzen von 1 Milliarde Dollar in 1997 auf 30 Milliarden Dollar im Jahr 2001; Vgl. http://www.idc.com/F/HNR/225.htm

[54]) Vgl. Die Bundesrepublik holt beim Internet auf, in: Süddeutsche Zeitung vom 23. März 1998

[55]) Vgl. hierzu: Sieben Knöpfe, in: Der Spiegel vom 16. März 1998, S. 204–206

[56]) Vgl. Martin, G. Virtuelle Assistenten helfen beim Einkauf, in: Handelsblatt vom 17. März 1998

[57]) Vgl. Picot, A.; Neuburger, R. Der Beitrag virtueller Unternehmen zur Marktorientierung, in: Bruhn, M.; Steffenhagen, H. (Hrsg.) Marktorientierte Unternehmensführung Wiesbaden 1997, S. 126

[58]) Vgl. Große Märkte für kleine Unternehmen, in: Mittelständische Wirtschaft (1997, Bd. 19, Nr. 3) S. 26–27

[59]) So setzt etwa der Computerhersteller Dell jeden Tag für 1 Million Dollar Computer über das Internet ab.

[60]) Vgl. hierzu Schmidt, H., Auf Mausklick naht ein Konkurrent: Die Ökonomie des Internet, in: FAZ vom 26. November 1997

„Global Information Network". Mit ihrem „Framework for Global Electronic Commerce" setzten der amerikanische Präsident Clinton und der Vizepräsident Gore ein deutliches Signal für eine konsequente Liberalisierung des Electronic Commerce. Sie wollen über das Internet eine globale Freihandelszone ohne neue Steuern und Zölle schaffen, einen globalen virtuellen Markt, der ohne staatlichen Dirigismus nur seinen eigenen ökonomischen Regeln folgt. Dieser von amerikanischer Seite gesetzte Akzent blieb nicht ohne Wirkung. Es ist in den entwickelten Industrieländern in Hinblick auf die wirtschaftliche Nutzung des Internet eine deutliche Liberalisierungstendenz zu erkennen.[61])

Obwohl Electronic Commerce sich zur Zeit noch in einer offenen Entwicklungsphase befindet, in der sich herausstellen wird, welche wirtschaftlichen Aktivitäten sinnvoll über den Cyberspace unternommen werden können, besteht für nicht online-fähige Unternehmen die große Gefahr, Marktanteile an Wettbewerbern zu verlieren, die für sich die Informations- und Transaktionskostenvorteile des Electronic Commerce aussschöpfen.

1.4.3 IT-Sicherheit und internationale Wettbewerbsfähigkeit

Für die Sicherung der internationalen Wettbewerbsfähigkeit wird die Teilnahme von Wirtschaftsunternehmen am Electronic Commerce und die Nutzung der globalen Informations- und Kommunikationsinfrastruktur zunehmend bedeutsamer. Die Transaktionskostenvorteile und die mit ihnen verbundenen Wettbewerbsmechanismen, die sich durch die Nutzung von Multimediaanwendungen im weltweiten Telekommunikationsnetz ergeben, werden durch die generelle Globalisierung der Wirtschaft noch verstärkt. Diese Entwicklung äußert sich z. B. in virtuellen Unternehmen oder der zunehmend genaueren Integration von Zulieferfirmen in die Produktionsabläufe eines weltweit verteilten Unternehmens[62]).

Für die Integration einer so zunehmend funktional differenzierten und global standortverteilten Wirtschaft ist die intensive Nutzung von IuK-Technologien unverzichtbar, weil diese Strukturen einen sehr hohen Bedarf an Koordination und Kommunikation erzeugen. In einem nur sehr eingeschränkten Umfang kann der hierzu notwendige Datenaustausch über geschlossene Systeme erfolgen. Der in der Regel über offene Telekommunikationsnetze durchgeführte Datenaustausch ist Risiken ausgesetzt, die sich auch auf die internationale Wettbewerbsposition von Unternehmen negativ auswirken können. Dies gilt insbesondere für mangelnde Vertraulichkeit und Verfügbarkeit sowie die Verletzung der Integrität von elektronischen Dokumenten. Deshalb sind informationstechnische Sicherheitsmaßnahmen auch ein Schutz vor möglichen Schäden, die zu Wettbewerbsnachteilen führen können.

In diesem Zusammenhang muß auch das IT-Sicherheitsziel „Verfügbarkeit" betont werden. Immer mehr Unternehmensvorgänge sind abhängig von komplexen Datenverarbeitungs- bzw. Informationsmanagementprozessen. Eine Einschränkung der Verfügbarkeit von Daten und Informationen bedeutet in der Regel eine empfindliche Beeinträchtigung von Funktions- und Koordinationsabläufen. Die Folge sind erhebliche Kostennachteile und eine möglicherweise verschlechterte Wettbewerbsposition.

Bei allen IT-Sicherheitspostulaten darf aber auch nicht die softwareergonomische Gestaltung von IT-Sicherheitslösungen unbeachtet gelassen werden. Besonders bei länderübergreifendem Datenaustausch ist es sehr wichtig, IT-Sicherheitslösungen zu wählen, die die Akzeptanz aller Beteiligten finden. Hierzu sind internationale Vereinbarungen über Standards, Aufklärung und Beratung über Risiken und Schutzmöglichkeiten sehr wichtig. Aber auch die direkt beteiligten Akteure müssen sich über ein sinnvolles IT-Sicherheitsdesign verständigen.

Bei der Betrachtung des Zusammenhangs von IT-Sicherheit und internationaler Wettbewerbsfähigkeit stellt sich auch die Frage nach den Wettbewerbswirkungen von Key-Recovery-Systemen.

Dabei muß unterschieden werden zwischen dem Wirkungsgefüge von Key-Recovery, nämlich die Herstellung von Vertraulichkeit durch Verschlüsselungssoftware und ihre Bedeutung für den Electronic Commerce auf der einen Seite und dem wettbewerbswirksamen Einfluß von Key Recovery auf die Anbieter von IT-Sicherheitslösungen.

Die Wettbewerbswirkungen von Key Recovery geht über betroffene Verschlüsselungsprodukte hinaus. Häufig fragen Kunden nach IT-Sicherheitssystemlösungen, in denen Verschlüsselungsprodukte ein Feature unter zahlreichen anderen sind. Grundsätzlich wird mit einem Key-Recovery-System die durch Verschlüsselungssoftware hergestellte Vertraulichkeit eingeschränkt. Dies ergibt sich alleine schon durch den Umstand, daß eine Schlüsseldublette außerhalb der Kontrolle des Schlüsselinhabers existieren würde. Es kann grundsätzlich nicht ausgeschlossen werden, daß diese Schlüsseldublette in falsche Hände gerät. Als besondere Bedrohungsform kommt hinzu, daß Key Recovery für Wirtschaftsspionage durch Geheimdienste genutzt werden kann. Außerdem kann eine zentrale Hinterlegungsstelle selbst Ziel von Angriffen werden. Dieses Risiko wäre dann besonders evident, wenn es jemals zu dem von den USA vorgeschlagenen weltweiten Key-Recovery-System käme. Mit Blick auf den internationalen Wettbewerb muß ein obligatorisches Key-Recovery-System als wettbewerbsnachteilig für die betroffenen Unternehmen betrachtet werden. Dies gilt insbesondere im Verhältnis zu Unternehmen aus Ländern, in denen kein obligatorisches Key-Recovery-System existiert. Bei einem weltweiten Key-Recovery-System würde sich

---

[61]) Vgl. FAZ/Blick durch die Wirtschaft vom 8. Juli 1997; Diese Politik ist während der WTO Ministerkonferenz im Mai 1998 nocheinmal ausdrücklich bestätigt worden; vgl. hierzu http://www.wto.org/anniv./ecom.htm. A Framework For Global Electronic Commerce, in: http://www.whitehouse.-gov/WH/New/Commerce

[62]) Besonders gut ist dies in der Automobilindustrie erkennnbar. Dort angewandte Logistikkonzepte wie Just-in-Time-Fertigung unterstreichen die Tendenz einer immer feineren Abstimmung zwischen Unternehmen und ihren Zulieferern.

die Wettbewerbsfrage allerdings auf eine andere Ebene verschieben: Die Position einer nationalen Wirtschaft im globalen Wettbewerb würde in einem erheblichen Umfang von den organisatorischen und technischen Möglichkeiten der eigenen Geheimdienste abhängen, verschlüsselte Dokumente von fremdländischen Wettbewerbern abzufangen, zu entschlüsseln und die Informationen der eigenen Wirtschaft zur Verfügung zu stellen.

Ein obligatorisches Key Recovery-System beschädigt auch die internationale Wettbewerbsfähigkeit von betroffenen Anbietern entsprechender Verschlüsselungssoftware gegenüber jenen Anbietern die Key Recovery-freie Verschlüsselungsprodukte anbieten können. Dieser Umstand erklärt den massiven Widerstand auch von amerikanischen Anbietern gegen die Key Recovery-Pläne der US-Regierung. Gleichzeitig erklärt diese Sachlage aber auch das Interesse von Regierungen an einem standardisierten weltweiten Key Recovery-System, denn dies würde die Zugriffsmöglichkeiten des veranlassenden Staates auf verschlüsselte Daten ermöglichen, ohne daß es für die eigenen Anbieter zu Wettbewerbsnachteilen kommen würde.

Die Schlußfolgerung ist, daß ein obligatorisches Key-Recovery-System zu Wettbewerbsnachteilen für die Wirtschaft führt. Über die dargelegten Gründe hinaus muß zusätzlich beachtet werden, daß Key Recovery-Systeme Zusatzkosten in einem erheblichen Umfang erzeugen. Auch dies würde die Wettbewerbsfähigkeit von Key Recovery-pflichtigen Unternehmen im Vergleich zu Anbietern aus Ländern ohne Key Recovery-Verpflichtung zusätzlich verschlechtern. Andersherum bedeutet dies aber auch, daß deutsche Anbieter ohne Key Recovery-Verpflichtung gegenüber ihren wichtigsten Mitbewerbern in den USA solange Wettbewerbsvorteile haben, wie diese Key-Recovery-Module in ihre Software einbauen müssen.

1.4.4 Wirtschaftsfaktor IT-Sicherheit und Datenschutz

Die größte Eintrittsbarriere in den Electronic Commerce ist für Unternehmen und Verbraucher der Mangel an Sicherheit im elektronischen Netz. Mangelnde Vertraulichkeit, manipulierbare IT-Systeme und Rechtsunsicherheit erzeugen Risiken, die kein Vertrauen auf Seiten der Unternehmen und Verbraucher gegenüber dem digitalen Handel entstehen lassen. Solange nicht sicher ausgeschlossen werden kann, daß unbefugte Dritte sensible Daten mitlesen können, die Authentizität eines Dokuments verletzt und die Identität eines Absenders manipulierbar ist, sind die potentiellen Folgekosten zu hoch, die ein Angriff auf eine geschäftliche Transaktion im Datennetz nach sich ziehen könnte. Die mit den Risiken verbundenen wirtschaftlichen Nachteile müssen sowohl auf Unternehmens- als auch Verbraucherseite höher als die Vorteile des Electronic Commerce eingeschätzt werden.

In einem ersten Schritt wurden in Bezug auf Rechtssicherheit[63]) vom Gesetzgeber mit dem Gesetz zur Digitalen Signatur die gesetzlichen Voraussetzung für die Erzeugung einer Infrastruktur zur Digitalen Signatur geschaffen, jedoch müssen die Hürden der Umsetzung dieses Gesetzes und zur tatsächlichen Nutzbarmachung der Digitalen Signatur noch überwunden werden.[64])

In ökonomischer Lesart bedeutet Sicherheit im Netz die Vermeidung von Risiken, die sich aus nicht geschütztem Daten- und Informationsaustausch im Rahmen von Electronic Commerce ergeben können. Diese Risiken halten Unternehmen von einem Eintritt in den „digitalen Handel" ab. Risiken sind dabei die potentiellen Folgekosten eines erfolgreichen Angriffs einer dritten Partei auf geschäftliche Transaktionen eines Unternehmens bzw. eines Kundens über ein offenes Netz. Wenn z. B. ein Unternehmen für ein bestimmtes Produkt oder eine Dienstleistung über das Internet einem Nachfrager ein Angebot unterbreitet, so kann es fatale Folgen haben, wenn diese Information von einem Wettbewerber mitgelesen wird. Der Mit-Wettbewerber kann mit diesem Informationsvorsprung das Angebot gezielt unterbieten. Der Mangel an informationstechnischer Sicherheit kann zu einer Wettbewerbsverzerrung führen, bei dem nicht nur ein Unternehmen geschädigt werden kann, sondern auch volkswirtschaftliche Schäden entstehen können.

Die Folgekosten eines erfolgreichen Angriffs auf die Online-Transaktionen eines Unternehmens würden die Transaktionskostenvorteile des E-Commerce in unserem Beispiel bei weitem zunichte machen. Allein die Möglichkeit eines erfolgreichen Angriffs auf die Online-Transaktionen eines Unternehmens reicht, um Vertrauen in den „digitalen Handel" zu unterminieren. Der Umstand, daß Verbraucher mit ihren Bewegungen und Transaktionen Datenspuren im Netz hinterlassen, die von Unternehmen ohne deren Wissen gesammelt, ausgewertet und zu detaillierten Profilbildern aufgearbeitet werden können, bedeutet bei nicht vorhandener Einwilligung des Nutzers nicht nur eine eklatante Verletzung des Grundrechtes auf informationelle Selbstbestimmung, sondern unterminiert auch das Vertrauen der Verbraucher in den digitalen Handel. In diesem Zusammenhang ist es sehr wichtig, daß Verbraucher ähnlich wie im „realen Kaufhaus" Kauf- und Zahlungsakte im Netz anonym durchführen können. Mit der Entwicklung von „Digitalen Geld", das auf sogenannten „Blinden Signaturen" beruht, ist in diese Richtung ein erster Schritt getan. Dieses Konzept wird im folgendem etwas ausführlicher vorgestellt.

Die wirtschaftliche Folge der Nichtnutzung von E-Commerce aufgrund mangelnder IT-Sicherheit wäre, daß die Kostenvorteile des Electronic Commerce nicht realisiert werden könnten. Die langfristige Folge wären Wettbewerbsnachteile großer Teile einer Volkswirtschaft im globalen Wettbewerb.

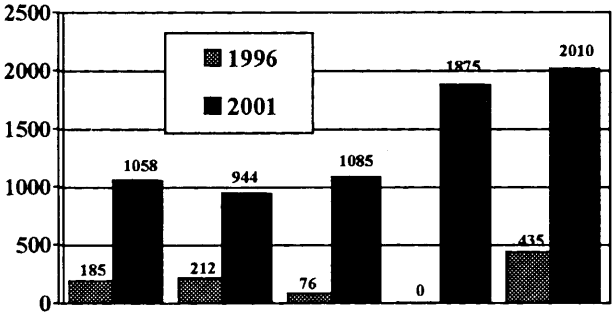
[63]) Vgl. hierzu auch die Ausführungen im Abschnitt 4.1.1

[64]) Vgl. Die Bundesrepublik holt beim Internet auf, in: Süddeutsche Zeitung vom 23. März 1998

1.4.5 Der Markt für IT-Sicherheit

Mit der rasch wachsenden Bedeutung von Electronic Commerce wird auch die Nachfrage nach sicherer Informationstechnik zunehmen und damit einen Markt für IT-Sicherheitslösungen konstituieren. Die Spanne der in diesem Marktsegment angebotenen Produkte und Dienstleistungen reicht von einzelnen Produkten, wie z. B. kryptografischer Software oder Firewall-Computer bis hin zum integrierten Systemschutz, bei dem spezialisierte Beratungsunternehmen umfassende Sicherheitslösungen anbieten.

Entwicklung des weltweiten Marktes für Internet Sicherheit nach Funktionsbereichen



Quelle: Datamonitor, ComputerZeitung

- Nach Einschätzung der Marktforscher von Datamonitor wird das Marktvolumen für Internet-Sicherheit von 908 Millionen Dollar im Jahr 1998 auf 7 Milliarden Dollar im Jahr 2001 wachsen. In 1998 hatte er noch ein Volumen von 908 Millionen Dollar.
- Weltweit wird das Segment IT-Sicherheitslösungen einen Marktwert von 16 Milliarden Dollar in 2001 erreichen. Europäische Firmen werden ihren weltweiten Anteil von 25 % in 1996 auf 34.

Deutsche Unternehmen haben auf diesem expandierenden Markt sehr gute Ausgangsvoraussetzungen, weil sowohl ein hochentwickeltes Know How als auch eine technologische Systemführerschaft zur Zeit noch vorhanden ist. Allerdings kann diese gute Ausgangslage dauerhaft nur gehalten werden, wenn die technologische Entwicklung nicht durch politisch induzierte Restriktionen behindert wird.[65])

1.4.6 „Digitales Geld"

Neben der Wertaufbewahrungs-, Wertmesser- und Tauschfunktion ist mit Geld der Vorteil anonymer wirtschaftlicher Transaktionen – zumindest für die alltäglichen Kaufakte – verbunden. Für den elektronischen Handel ist letztere Bedingung noch nicht gegeben. Das heute übliche Bezahlen mit den Daten der Kreditkarte ist weder sicher, noch anonym oder datensparsam. Auch wenn die Sicherheitslücken des Kreditkartenzahlungsverkehrs im Netz technisch überwunden werden können, bleibt der Nachteil, daß die Transaktionskosten beim Abbuchen kleiner und kleinster Beträge über Kreditkarten zu hoch sind. Einen möglichen Ausweg bietet hier „digitales Geld".

[65]) Vgl. hierzu die Abschnitte 2.3, 5.1.3, sowie die Handlungsempfehlungen im Kapitel 6.

„Digitales Geld" erfordert vergleichbare Bedingungen wie „reales Geld":

- *Zentrale Erzeugung:* Nur eine Bank[66]) darf in der Lage sein, digitale Münzen herzustellen.
- *Echtheit:* Alle Beteiligten müssen die Echtheit digitalen Geldes überprüfen können
- *Anonymität:* An der eingelösten (digitalen) Münze darf die Bank nicht erkennen können, an wen sie diese ausgegeben hat. Der Händler muß eine Münze akzeptieren, ohne daß der Kunde sich vorher ausweist.
- *Eindeutigkeit:* Es darf nicht möglich sein, digitale Münzen zu duplizieren, also dieselbe Münze zweimal einzureichen.[67])

Wir wollen an dieser Stelle beispielhaft ein mögliches Modell für „digitales Geld", das auf sogenannten „blinden Signaturen" basiert, diskutieren[68]). Erste Ansätze zur Realisierung dieses Modells gibt es u. a. seitens der Deutschen Bank, die in einem Pilotversuch das Konzept „Ecash" der Firma DigiCash testet.

In einem einfachen Kreislaufmodell digitalen Geldtransfers existiert zum einen die Bank, die elektronisches Geld an jene Kunden ausgibt, die bei ihr ein spezielles Bankkonto für digitales Geld eröffnet haben. Die Kunden können sich dieser (digitalen) Konten bedienen, um z. B. eine Online-Bestellung beim Händler zu bezahlen. Der Händler kann das digitale Geld bei der Bank wieder in reales Geld zurücktauschen.[69])

Digitales Geld besteht aus speziell gebildeten Zahlen, die mit sogenannten „blinden Signaturen" [70]) geschützt sind. Sie werden als digitale Geldwertäquivalente von Geldinstituten herausgegeben. Jede blinde Signatur legt einen bestimmten Geldbetrag fest.

1.4.6.1 Wie blinde Signaturen zu „digitalem Geld" werden

Blinde Signaturen sind spezielle Formen der digitalen Signatur.[71]) Wie digitale Signaturen entstehen

[66]) Anders als beim realen Geld, das nur von der Zentralbank herausgegeben werden darf, kann digitales Geld auch von privaten Geldinstituten emittiert werden. So erprobt die Deutsche Bank das von David Chaum entwickelte DigiCash zur Zeit in einer Pilotphase mit 1 000 Kunden.

[67]) Vgl. Beutelspacher, A. et al. Moderne Verfahren der Kryptographie (1998) S. 86–87

[68]) Einen sehr umfassenden Überblick über die zur Zeit existierenden digitalen Zahlungsmittelsysteme und damit zusammenhängenden Sicherheitsthemen gibt Wicke, G. Mehrseitig sicherer digitaler Zahlungsverkehr, in: Müller, G. et al. (Hrsg.) Zukunftsperspektiven der digitalen Vernetzung (1996) S. 169–208

[69]) Wie einfach dieser Vorgang funktioniert, kann in einem Ecash-Test auf der Homepage von Digicash (http://www.digicash.com) nachvollzogen werden.

[70]) Blinde Signaturen sind von David Chaum entwickelt worden. David Chaum ist Eigentümer und Geschäftsführer der Firma DigiCash

[71]) Vgl. hierzu den Abschnitt 5.1.2

„blinde Signaturen" auf der Grundlage von asymmetrischen (RSA) softwarebasierten Verschlüsselungsverfahren, bei dem ein privater (geheimer) Schlüssel und ein öffentlicher Schlüssel (secret/public keys) generiert wird. Entsprechend dem Anwendungsmodus von digitalen Signaturen kann auch bei blinden Signaturen nur derjenige eine Signatur erzeugen, der im Besitz des privaten – geheimen – Schlüssels ist. In diesem Modell ist dies ausschließlich die digitales Geld emittierende Bank.

Im Unterschied zu herkömmlichen digitalen Signaturen kennt die Bank bei der blinden Signatur den zu signierenden Inhalt nicht.

Der erste Schritt im blinden Signaturverfahren ist die Erzeugung eines „digitalen Münzrohlings" im PC des Kunden. Der digitale Münzrohling ist eine Zufallszahl (mit nachprüfbarer spezieller Gestalt), die mit spezieller Software im Computer des Kunden erzeugt wird. Dieser Münzrohling wird in einen digitalen Briefumschlag gesteckt. Der digitale Briefumschlag ist eine andere Zahl, die mit der Zufallszahl multipliziert wird. Der digitale Münzrohling wird verschlossen im digitalen Briefumschlag vom Kunden zu seiner kontoführenden Bank geschickt. Mit anderen Worten: Das Produkt von Zufalls- und Briefumschlagszahl, welches, symbolisch gesprochen, der digitale Münzrohling im digitalen Briefumschlag ist – wird an die Bank geschickt. Die Bank prägt den digitalen Münzrohling mit einem Geldwert **durch den digitalen Briefumschlag hindurch.** Dieser Wert wird vom Konto des Kunden abgebucht.

Für jeden Wert verfügt die Bank über einen (geheimen) Schlüssel. 10 Pfennig entsprechen z.B. dem geheimen Schlüssel S(1), 1 DM dem Schlüssel (S2) usw. Nachdem der Kunde die nunmehr geprägten Geldmünzen zurückerhalten hat, entfernt spezielle Software im PC des Kunden den digitalen Briefumschlag; d.h. die Software rechnet die Faktorzahl des digitalen Briefumschlages heraus – übrig bleibt die mit einem Wert geprägte digitale Münze. Der Wert dieser Münze ist durch die mit dem geheimen Schlüssel der Bank (blind) erzeugte digitale Signatur festgelegt. Der Kunde kann nun mit diesen digitalen Münzen Waren im Internet bezahlen. Der Händler überprüft die Echtheit der Münzen mit dem öffentlichen Schlüssel der Bank. Dieser Vorgang entspricht der normalen Verifikation im digitalen Signaturverfahren. Außerdem findet anhand von Verzeichnissen der Seriennummern bereits eingelöster digitaler Münzen eine Überprüfung in Hinblick auf Kopien statt, so daß jede digitale Münzen nur einmal ausgegeben werden kann.

Wichtig ist, daß die Bank in diesem Kreislauf des digitalen Geldes nicht mehr nachvollziehen kann, wie der Kunde sein digitales Geld ausgegeben hat, denn die Bank konnte nur den digitalen Geldumschlag sehen, aber nicht die digitale Geldmünze selbst, die der Händler am Ende der Kette bei der Bank gegen reales Geld eintauscht.

Digitales Geld kann auch zwischen zwei Personen transferiert werden. Person A zahlt einen bestimmten (digitalen) Betrag an Person B. Diese zahlt diesen Betrag auf das Konto für digitales Geld an ihrer Bank ein. Diese Bank überpüft das Geld bei der Bank von Person A. Ist das Geld in Ordnung sendet die Bank von Person B diesen Betrag in Form neu geprägter digitaler Münzen zu dem PC von Person B.[72])

1.4.6.2 Wie sicher ist digitales Geld?

Die technische Grundlage für digitales Geld sind digitale Signaturen, die über Software für asymmetrische Verschlüsselungsverfahren gewonnen werden. Da die heute auf dem Markt befindlichen anerkannten Verschlüsselungsverfahren hohe Sicherheit gewährleisten, ist von dieser Seite her digitales Geld als sicher einzustufen.[73]) Allerdings ist hier einschränkend anzumerken, daß in einer IT-Systemwelt mit unsicherer Basistechnologie – wie z.B. nicht sichere und fehlerbehaftete Betriebssysteme – jede nachgeordnete Sicherheitsmaßnahme ihre Grenzen bei den Sicherheitslücken und Fehlern der grundlegenden Technik findet.[74])

Die Sicherheit von digitalem Geld wird in Fachkreisen insbesondere in Hinblick auf „Eindeutigkeit" bzw. Mängel beim Kopierschutz kritisch diskutiert. So geben zum Beispiel Albrecht Beutelspacher et al. zu bedenken: „Dieses elektronische Zahlungsmittel hat, wie viele andere auch, das Problem der Eindeutigkeit im Grunde nicht gelöst. Es gibt eine Reihe von Lösungsvorschlägen kryptographischer und nicht kryptographischer Natur, die das doppelte Ausgeben einer Münze riskant machen. Unter die nichtkryptographischen Lösungsmöglichkeiten fällt dabei der Vorschlag, elektronische Münzen immer sofort online bei der Bank einzulösen, was natürlich für den Händler mit hohen Kosten verbunden sein kann. [...] Neuere Untersuchungen zu diesem Thema befassen sich mit der Frage, ob elektronische Münzen genau wie echtes Geld einfach weitergegeben werden können, anstatt sie immer gleich wieder bei der Bank einzulösen. Das große Problem scheint dabei zu sein, im Falle des doppelten Ausgebens einer Münze den Schuldigen in der Kette derjenigen zu finden, durch deren Hände die Münze gegangen ist."[75])

Eine abschließende Bewertung der Sicherheit ist zur Zeit nicht möglich. Grundsätzlich kann der Ansatz, ein digitales Zahlungsmittelsystem auf kryptographische Verfahren (Digitalen Signaturen)aufzubauen in Hinblick auf eine systematische Berücksichtigung von IT-Sicherheit als zukunftsweisender Weg bewertet werden. Dies gilt insbesondere in Hinblick auf die Umsetzung der IT-Sicherheitsziele Anonymität, Vertraulichkeit und Beweissicherheit.

Bei allen derzeit angebotenen digitalen Zahlungsmittelsystemen ist in Hinblick auf die Ausbildung eines umfassenden und nachhaltigen Sicherheitsstandards wissenschaftliche Begleitforschung notwendig.

---

[72]) Vgl. How ecash works inside, in: http://www.digicash.com/ecash/docs/works/index.htm

[73]) Vgl. Wicke, G. Mehrseitig sicherer digitaler Zahlungsverkehr, in: Müller, G. et al. (Hrsg.) „Zukunftsperspektiven der digitalen Vernetzung" (1996) S. 169–208

[74]) Vgl. hierzu die Ausführungen im Kapitel 4.

[75]) Beutelspacher, A. et al. Moderne Verfahren der Kryptographie (1998) S. 88

1.5 Rechtliche und organisatorische Rahmenbedingungen der IT-Sicherheit

Die Frage rechtlicher Regelungen zur sicheren Nutzung elektronischer Netze hatte solange keine Bedeutung, wie der darauf ablaufende Datenverkehr dem freiwilligen Austausch rechtlich und ökonomisch unerheblicher Daten diente. In dem Maße, wie der Geschäftsverkehr zwischen Unternehmen und ihren Kundinnen und Kunden über offene Netze zunimmt und dabei Daten auch hoher Sensitivität anfallen, entsteht nun die Notwendigkeit, diesen Datenverkehr in einer Weise rechtlich zu schützen, wie sie aus der Rechtssphäre nichtelektronischer Interaktion bekannt ist. Dies ist der Hintergrund für die vielfach geäußerte Aussage, daß ein hohes Datensicherheits- und Datenschutzniveau die Voraussetzung für die Akzeptanz der elektronischen Märkte bei den Verbrauchern ist. Hinzu kommt, daß die Nutzung elektronischer Netze zu neuen rechtlich relevanten Problemen führen kann, die nicht nur die Übertragung bekannter Rechtsnormen auf die Welt des Internets, sondern möglicherweise neue rechtliche Möglichkeiten erfordern.

Mit diesem Thema hat sich der Berichtsteil *Strafrecht* dieses Zwischenberichts ausführlicher auseinandergesetzt. Gegenstand der Betrachtung soll daher in diesem Teil der rechtliche Rahmen sein, der für die Gewährleistung von IT-Sicherheit heranzuziehen ist. Auch hier erweist sich, daß IT-Sicherheit nicht allein technisch gesehen werden kann. Neben technischen Schutzmaßnahmen zur Erhöhung der IT-Sicherheit ist ein ergänzender rechtlicher Schutz unerläßlich, da solche Schutztechnologien weder absoluten Schutz gewährleisten und damit auch der Umgang mit Schäden und Schadensverursachern zu klären ist, sind noch viele dieser Maßnahmen – die beispielsweise durchaus mit dem informationellen Selbstbestimmungsrecht konfligieren können – ohne eine rechtliche Grundlage einsetzbar. Die rechtliche Definitionsnotwendigkeit resultiert also einerseits aus dem Schutzgegenstand, andererseits aus der Abwägung der Schutzinteressen und Rechte aller Beteiligten.

1.5.1 Notwendigkeit einer rechtlichen Regulierung

Die Notwendigkeit eines rechtlichen Schutzes ergibt sich auch aus der verfassungsrechtlichen Lage:

- Sofern Grundrechte der Bürger wie etwa das vom BVerfG in seinem Volkszählungsurteil im Jahre 1983[76]) entwickelte Recht auf informationelle Selbstbestimmung (Art. 2 I, 1 I GG) und das Fernmeldegeheimnis (Art. 10 GG) durch unzureichende Sicherungsmaßnahmen in der Informationstechnik berührt werden, trifft den Staat eine *Schutzpflicht* für die Unversehrtheit dieser Grundrechte.
- Da die Menschen in einer hochzivilisierten, hoch arbeitsteiligen Gesellschaft nur zusammen leben können, wenn Infrastrukturen einen intensiven Austausch von Energie, Gütern und Informationen ermöglichen, ist der Staat im verpflichtet, für seine Bürger das Funktionieren dieser Infrastrukturen sicherzustellen.
- Zur Erfüllung vieler Aufgaben bedient sich der Staat der Informationstechnik. In seiner Verantwortung für die *Funktionsfähigkeit staatlicher Aufgabenerfüllung* trifft ihn die Verpflichtung, die Verfügbarkeit der verwendeten Techniksysteme und Informationen, deren Unversehrtheit und Vertraulichkeit herzustellen.

Dennoch dürfen die rechtlichen Rahmenbedingungen nicht zu restriktiv sein. Eine liberale Informationsgesellschaft muß versuchen, einerseits den größtmöglichen Schutz der Grundrechte zu gewährleisten, andererseits den freien Informationsfluß möglichst wenig zu beeinträchtigen.

Auch unter ökonomischen Gesichtspunkten erscheint ein bestimmtes Maß an IT-Sicherheit gerechtfertigt[77]). In unregulierten Informations- und Telekommunikationsmärkten besteht auf Seiten der Nachfrager von Kommunikationsdiensten ein Informationsdefizit gegenüber der Anbieterseite: Da die Nachfrager die Effektivität der vom Netzbetreiber installierten IT-Sicherheitsmaßnahmen nicht beurteilen können, unterschätzen sie meist die Wahrscheinlichkeit eines Schadenseintritts (*sog. Informationsasymmetrie*). Daraus folgt einerseits, daß die Benutzer über eine zu geringe Zahlungsbereitschaft für Sicherheitsmaßnahmen verfügen; andererseits fehlen auf Anbieterseite Anreize, ein hohes (und damit kostenintensives) IT-Sicherheitsniveau zu gewährleisten.

Weiterhin können durch eine fehlerhafte Datenübermittlung außenstehende Dritte, auf die sich die Daten beziehen, geschädigt werden: Entsteht beispielsweise bei der Datenübermittlung zwischen zwei Behörden ein Übertragungsfehler, so kann dies den betroffenen Bürger u. U. empfindlich schädigen (sog. *negative Externalitäten*).

Durch die asymmetrische Informationsverteilung und die negativen Externalitäten werden in einem unregulierten Kommunikationsmarkt IT-Sicherheitsmaßnahmen ergriffen, die nicht dem volkswirtschaftlich optimalen Niveau entsprechen. Für den dadurch notwendigen staatlichen regulierenden Eingriff bieten sich auf rechtlichem Gebiet mehrere Möglichkeiten an, wobei nur eine Kombination der folgenden Instrumente eine befriedigende IT-Sicherheit gewährleisten kann:

- *Information:* Die Betreiber von IT-Anlagen können verpflichtet werden, die Benutzer ihrer Anlagen über mögliche Sicherheitsrisiken und die ergriffenen Gegenmaßnahmen aufzuklären oder ihnen über den Zugriff zu entsprechenden Informationen über Risiken und Sicherheitsmaßnahmen eine Information ermöglichen. Dadurch wird die Stellung der Benutzer im Marktprozeß gestärkt. Weiterhin könnte die freiwillige Einführung eines sog. IT-Sicherheitsaudits – eines Gütesiegels für ein hohes IT- Sicherheitsniveau – bei den Betreibern von In-

[76]) Vgl. BVerfGE 65, 1.

[77]) Vgl. zum Ganzen: Francke/Blind, Informationssicherheit in offenen Kommunikationssystemen, it+ti Heft 4/1996.

formations- und Kommunikationsdiensten einen zusätzlichen Anreiz zur Schaffung höherer Sicherheitsstandards schaffen: IT-Sicherheit als Marktfaktor. Dieses marktwirtschaftliche Instrument würde mittelbar auch eine Entlastung der rechtlichen Datenschutzkontrolle bewirken.[78])

- *Haftungsrecht:* Durch entsprechende haftungsrechtliche Regelungen entsteht für die Betreiber von IT-Anlagen der Anreiz und damit für deren Lieferanten von Informationstechnologie der Druck, mit Hilfe von Präventionsmaßnahmen den Eintritt von Schadensfällen zu vermeiden.
- *Mindestsicherheitsstandards:* Durch die Festlegung gewisser Sicherheitskriterien, die Betreiber offener Kommunikationssysteme erfüllen müssen, um von einer staatlichen Regulierungsbehörde eine Zulassung zu erhalten, steigt der objektive Sicherheitsstandard und damit das Vertrauen der Benutzer in die bereitgestellten Kommunikationsnetze.

Es sind aber auch die Grenzen rechtlicher Regulierung in einer globalen Informationsgesellschaft zu beachten: In einem weltweiten Informations- und Telekommunikationsmarkt können gezielt steuernde Eingriffe eines Nationalstaates nur von beschränktem Erfolg gekrönt sein[79]). Vielmehr werden internationale Kooperationen und Abkommen eine immer größere Bedeutung erlangen. Dennoch kann eine vorauseilende nationale Gesetzgebung durchaus sinnvoll zu sein, da einerseits die Internationalisierung der IT-Sicherheit und des Datenschutzes aufgrund unterschiedlicher Regelungsansätze in den Staaten zeitaufwendig ist, andererseits dadurch im internationalen Kontext eine Vorreiterrolle eingenommen und ein Anreiz für die Entwicklung exportfähiger Produkte der IT-Sicherheit geschaffen werden kann.

1.5.2 Derzeitige Rechtslage

Als bestimmend für die rechtliche Fundierung der IT-Sicherheit wird das Datenschutzrecht gesehen, das auch grundlegende Anforderungen an die technische Sicherheitsbelange stellt. Von Bedeutung sind jedoch darüber hinaus gesonderte IT-Sicherheits-relevante Strafrechts-, sowie einschlägige Spezialnormen. Zwar existieren einige rechtliche Regelungen zur Gewährleistung von IT-Sicherheit, aus dem gesamten Problembereich regeln diese jedoch nur punktuell einzelne Problemausschnitte und stellen keine systematische Kodifizierung der IT-Sicherheit dar:

- An erster Stelle ist das *Bundesdatenschutzgesetz* (BDSG) zu nennen. Im Zusammenhang mit der IT-Sicherheit sind insbesondere die „Zehn Goldenen Regeln der Datensicherung" in der Anlage zu § 9 BDSG bedeutsam: Danach ist die speichernde Stelle verpflichtet, bei der Verarbeitung personenbezogener Daten bestimmte Kontrollen durchzuführen, um sicherzustellen, daß Unberechtigte beispielsweise keinen Zugang, keinen Zugriff und keine Kenntnis erhalten oder keine Daten eingeben, verändern, löschen, mitnehmen oder vermitteln können. Zur Zeit wird eine Novellierung des BDSG vorbereitet.[80]) Im einzelnen ist noch umstritten, insbesondere ob das BDSG nur in einzelnen Bereichen angepaßt oder grundlegend novelliert werden sollte.[81]) Den Anstoß zu dieser Novelle gab die EU-Datenschutzrichtlinie vom 24. 10. 1995.[82]) In Bezug auf die IT-Sicherheit findet sich eine Regelung in Art. 17 der Richtlinie, die inhaltlich weitgehend § 9 BDSG und der dazugehörenden Anlage[83]) entspricht. Lediglich in bezug auf die zufällige Zerstörung und den zufälligen Verlust von personenbezogenen Daten geht die EU-Richtlinie weiter. Die Regelungen über die IT-Sicherheit im BDSG und in der EU-Richtlinie gelten jedoch nur für den Umgang mit personenbezogenen Daten, nicht für andere IT-Anwendungen.
- Daneben ist auf die *Datenschutzgesetze der Länder,* die *Landesmediengesetze* sowie die staatsvertraglichen Regelwerke der Bundesländer im Rundfunkbereich hinzuweisen, die teilweise bereichsspezifische Sonderregelungen beinhalten.
- Im Bereich des *Telekommunikationsrechts* wurden in der Vergangenheit Sicherheitsanforderungen durch verwaltungsinterne Vorgaben des Bundespostministeriums aufgestellt. Seit der Privatisierung der Telekommunikation durch die Postreform II müssen Sicherheitsanforderungen durch Gesetz oder Verordnung als Außenrecht formuliert werden. Daher verpflichtet § 87 TKG die Betreiber von Telekommunikationsanlagen, angemessene technische Vorkehrungen oder sonstige Maßnahmen zu treffen, um das in §§ 85f. TKG einfachgesetzlich geregelte Fernmeldegeheimnis und den Datenschutz zu gewährleisten. Dabei erstellt die Regulierungsbehörde für Telekommunikation und Post im Benehmen mit dem BSI nach Anhörung beteiligter Verbände und dem Bundesbeauftragten für Datenschutz einen Katalog von Sicherheitsanforderungen (§ 87 I 3, 4 TKG). Lizenzpflichtige Betreiber von Telekommunikationsanlagen müssen ein Sicherheitskonzept erstellen (§ 87 II TKG). Die Regulierungsbehörde verfügt über weitgehende Befugnisse (bis zur Untersagung des Betriebs des Telekommunikationsdienstes), um die Einhaltung dieser Bestimmungen zu gewährleisten (§ 91 TKG).
- Seit 1994 gilt das *Post- und Telekommunikationssicherstellungsgesetz* (PTSG). Es enthält eine Ermächtigungsgrundlage für Rechtsverordnungen, aufgrund derer Betreiber von Telekommunikationsdiensten zur Sicherstellung einer ausreichenden Versorgung von Telekommunikationsdienstleistungen bei einer Naturkatastrophe, einem

[78]) Vgl. Büllesbach, RDV 1997, S. 244; Lanfermann; RDV 1998, S. 5; Engel-Flechsig, RDV, 1997, S. 66; Stoll, RDV, 1997, S. 78.

[79]) Vgl. Rossnagel, ZRP, 1997, S. 27.

[80]) Vgl. dazu den Referentenentwurf vom 8. Dezember 1997 sowie den Gesetzentwurf von BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 13/9082.

[81]) Vgl. dazu: Brühann/Zerdick, CR, 1996, S. 430ff.; Werthebach, RDV, 1997, S. 1ff.; Jaspers, RDV, 1996, S. 18.

[82]) Vgl. RL 95/46/EG vom 24. 10. 1995, Abl. EG Nr. L 281/31.

[83]) Vgl. Anlage zu § 9, S. 1, Nr. 3.

besonders schweren Unglücksfall, im Rahmen von Bündnisverpflichtungen oder im Spannungs- und Verteidigungsfall verpflichtet sind. Ergangen ist u. a. eine Verordnung zur Sicherstellung der Telekommunikationsversorgung durch Schutzvorkehrungen und Maßnahmen des Zivilschutzes[84]) sowie eine Verordnung zur Sicherstellung von Telekommunikationsdienstleistungen[85]).

- Am 1. Januar 1998 ist das *Begleitgesetz zum TKG* in Kraft getreten[86]), das auch zu Änderungen beim Schutz der Vertraulichkeit in elektronischen Netzen geführt hat. Die Sicherheitsbehörden verfügen im wesentlichen über drei Rechtsgrundlagen, um im Telekommunikationsbereich Überwachungs- und Abhörmaßnahmen durchführen zu können: §§ 100a, 100b StPO, das Gesetz zu Artikel 10 GG (G 10) sowie § 39 Außenwirtschaftsgesetz (AWG). Durch das Begleitgesetz zum TKG wurden diese Vorschriften den Neuerungen des privaten Telekommunikationsmarktes angepaßt: Insbesondere wurde § 100b III StPO dahingehend geändert, daß nun jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen hat. Darunter fallen auch sog. Corporate Networks; gerade dort wurde ein unkontrollierbarer Informationsaustausch krimineller Organisationen befürchtet.[87]) Nach dem ebenfalls geänderten § 88 II 4 TKG n. F. darf der Betrieb der Anlage erst aufgenommen werden, wenn die technischen Überwachungseinrichtungen installiert sind und die Regulierungsbehörde (innerhalb von sechs Wochen) eine Genehmigung erteilt hat. Auch Betreiber von Nebenstellanlagen und Corporate Networks haben damit zuerst das langwierige Verfahren des § 88 TKG zu durchlaufen.[88]) Außer diesen Vorschriften enthält das Begleitgesetz zum TKG keine weiteren spezifischen Aussagen zur IT-Sicherheit.

- Im Rahmen des IuKDG wurde als Art. 2 im Juli 1997 das *Teledienstedatenschutzgesetz* (TDDSG) erlassen. Nach § 3 IV TDDSG sind die technischen Einrichtungen für Teledienste so auszugestalten, daß möglichst wenig personenbezogene Daten erhoben werden müssen, nach § 4 I TDDSG müssen die Systeme auch die anonyme Benutzung ermöglichen. Weiterhin hat der Dienstanbieter durch technische und organisatorische Vorkehrungen sicherzustellen, daß personenbezogene Daten über die Nutzung verschiedener Teledienste getrennt verarbeitet und nicht zusammengeführt werden (§ 4 II Nr. 2 TDDSG). Hier zeigt sich das Bemühen des Gesetzgebers, schon auf die technische Ausgestaltung der IT-Einrichtungen einzuwirken, damit negative Technikfolgen erst gar nicht entstehen (Systemdatenschutz, Schutz der Vertraulichkeit).[89])

- Der *Mediendienste-Staatsvertrag,* der zum 1. 8. 1997 in Kraft trat, enthält in §§ 12 V, 13 I und § 13 II Nr. 4 Regelungen, die weitgehend identisch mit denen des TDDSG sind, sich jedoch darin unterscheidet, ein im TDDSG gestrichenes Datenschutzaudit vorzusehen.

- Eine ähnliche Vorschrift findet sich auch in der neuen *EU-Telekommunikations-Datenschutzrichtlinie* vom 15. Dezember 1997[90]): Nach Art. 4 I müssen die Betreiber eines öffentlich zugänglichen Telekommunikationsdienstes geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten.

- Aus dem Schutzgedanken von Kernzielen der IT-Sicherheit heraus entwickelt wurden schon 1986 verschiedene *Strafrechtsnormen.* Für die IT-Sicherheitsschutzziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit bestehen damit seit dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität[91]) im Strafrecht die folgenden Schutznormen:

  1. Den Schutz der *Integrität* von Daten zum Gegenstand haben die Strafgesetzbuch-Normen §§ 263a (Computerbetrug), 269 (Fälschung beweiserheblicher Daten) und 303a (Datenveränderung), die dem Datenhalter Schutz vor unbefugter Datenmanipulation gewähren.

  2. Dem Schutz der *Authentizität* von Daten dienen in unterschiedlicher Weise zum einen der § 303a StGB insofern, als hier jedwede Form der Veränderung von in besonderer Weise geschützten Daten unter Strafe gestellt wird, wodurch auch Manipulationen an Authentizität schaffenden Daten strafbar sind. Sofern solche Manipulationen dem Erringen von Vermögensvorteilen dienen, ist zusätzlich noch § 263a StGB (Computerbetrug) einschlägig.

  3. Den Schutz der *Verfügbarkeit* von IT-Systemen zum Gegenstand hat der § 303b StGB (Computersabotage). Die Verfügbarkeit ist danach nicht mehr gegeben, wenn der „reibungslose Ablauf der Datenverarbeitung nicht unerheblich beeinträchtigt" ist[92]) und dies durch Manipulationen an Daten oder IT-Systemen verursacht wurde[93]).

  4. Dem Schutz der *Vertraulichkeit* dient der § 202a StGB, der das Ausspähen von Daten unter Strafe stellt, mit dem zugleich der Straftatbestand des Verrats von Geschäfts- und Betriebsgeheimnissen (§ 17 des Gesetzes gegen den unlauteren Wettbewerb) verschärft wurde.

  Voraussetzung für einen Rechtsschutz ist die besondere Sicherung der Daten und IT-Systeme ge-

[84]) Vgl. PTZSV, BGBl., 1996, Teil I, S. 1539ff.
[85]) Vgl. TKSiV, BGBl., 1997, Teil I, S. 2751ff.
[86]) Vgl. BGBl., 1997, Teil I, S. 3108ff.
[87]) Vgl. Begründung zum TKG-Begleitgesetz, BT-Drs. 13/8016, S. 26.
[88]) An der Verfassungsmäßigkeit der Vorschrift aus diesem Grund zweifelnd Gundermann, K&R, 1998, S. 52.
[89]) Vgl. Lanfermann, RDV, 1998, S. 4; s. a. Engel-Flechsig, RDV, 1997, S. 61f.
[90]) Vgl. RL 97/66/EG vom 15. Dezember 1997, Abl. EG L 24/1 vom 30. Januar 1998.
[91]) Vgl. BGBl. I, 1986, S. 721.
[92]) So die Begründung in Bt.-Drs 10/5058, S. 35
[93]) Vgl. Volesky, K.-H.; Scholten, H.; Computersabotage – Sabotageprogramme – Computerviren; in: iur, Heft 7–8, 1987, S. 280–289

gen unberechtigten Zugang (§ 202a StGB und darauf aufbauend § 303a und b StGB) oder ein unbefugter Eingriff in ein IT-System (§ 263a StGB) und damit dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen[94]). Dieser Schutz ist allerdings recht weitgehend. So läßt sich bereits eine Installation von Software, die durch nutzerseitig unkontrollierbare und irreversible Veränderungen in den Systemeinstellungen ein IT-System ganz oder in wichtigen Teilen unbrauchbar macht, als Straftat nach § 303b StGB werten.

- Einen expliziten Bezug zu IT-Sicherheitsanforderungen stellt das *Gesetz zur digitalen Signatur* (Signaturgesetz, SigG) im Rahmen des IuKDG her. Nach § 13 SigG sind technische Komponenten zur sicheren Erzeugung der Signatur und auf der Grundlage der Signaturverordnung gemäß § 15 SigG sind detaillierte und für die Zulassung einer Zertifizierungsstelle bindende Durchführungsvorschriften zur sicheren Erzeugung, Verwaltung und Verteilung digitaler Signaturen zu erstellen (§§ 16 und 17 SigVo). Diese Vorschriften lassen sich in einigen ihrer Aspekte als ein Grundstein für eine IT-Sicherheitsinfrastruktur begreifen. Ungeklärt blieb beim SigG allerdings die Frage der Haftung nach Schäden durch Fehler der Zertifizierungsstellen. Allenfalls ist denkbar, die Regulierungsbehörde für Telekommunikation und Post als Wurzel-Zertifizierungsinstanz auf dem Wege der Amtshaftung für Versäumnisse bei der Zulassung einer Zertifizierungsstelle in Regreß zu nehmen[95]).
- Einzelheiten einer Normierung von Aspekten der IT-Sicherheit sind schließlich im *BSI-Errichtungsgesetz* (BSIG) festgelegt[96]). Gemäß § 3 BSIG hat das BSI die Aufgabe, für Stellen des Bundes IT-Sicherheitsrisiken zu untersuchen, sichere IT-Systeme zuzulassen und die Arbeit einerseits des Bundesbeauftragten für den Datenschutz, andererseits die Sicherheitsbehörden zu unterstützen sowie für die Allgemeinheit IT-Sicherheitskriterien zu entwickeln und diese über Folgen mangelhafter IT-Sicherheit zu beraten. Für sichere Produkte kann zudem ein Sicherheitszertifikat erteilt werden.

Für die Konkretisierung von IT-Sicherheit spielt in der Praxis die Bewertung sicherer IT-Systeme und deren Gestaltung anhand der zuerst national – gemäß § 3 (1) Nr. 2 BSIG – vom BSI entwickelten und nun auch international abgestimmten IT-Sicherheitskriterien die zentrale Rolle. Eine Beteiligung des BSI an der Zulassung und Einführung von IT-Systemen, deren Ausfall erhebliche Schadenspotentiale hat, wurde dagegen abgelehnt[97]).

Während somit für die Verarbeitung personenbezogener Daten und Telekommunikationsdienstleistungen rudimentäre rechtliche Sicherheitsanforderungen oder Ermächtigungen zum Erlaß solcher Anforderungen bestehen, fehlt für andere IT-Anwendungen eine rechtliche Regulierung der IT-Sicherheit. Rechtliche Anforderungen an die IT-Sicherheit können sich in diesen Bereichen nur bedingt und im Rahmen der begrenzten strafrechtlichen Schutznormen oder darüber hinaus durch – für die IT-Sicherheit völlig unspezifische – Rechtsregeln des Vertrags- und das Versicherungsrecht ergeben. Die IT-Sicherheitskriterien dienen lediglich als allgemeiner, rechtlich jedoch in der Regel unverbindlicher Maßstab der IT-Sicherheit. Soweit sich Verträge auf diese Sicherheitskriterien oder auf BSI-Zertifikate beziehen, können diese rechtliche Relevanz zwischen den Vertragspartnern gewinnen. Die öffentliche Hand als Nachfrager nach Informationstechnik kann Sicherheitsanforderungen auch über die Vorgaben für das Beschaffungswesen einfordern und – wo dies nach dem BSIG erforderlich und zulässig ist – auch vorschreiben. Neben dem BSI ist auch der Bundesrechnungshof mit der Überprüfung der IT-Sicherheit bei IT-Systemen des Bundes betraut und erarbeitet in diesem Rahmen auch Vorschläge für IT-Sicherheitsmaßnahmen. Daneben kann auch das Versicherungsrecht Einfluß auf die IT-Sicherheit gewinnen. Hersteller, Anbieter und Nutzer von Informationstechnik versuchen, sich gegen mögliche Schäden durch den Abschluß von Versicherungen zu schützen. Um das Risiko überschaubar zu halten, fordern manche Versicherungen in ihren Versicherungsbedingungen, gewisse Maßnahmen zur Sicherung der Informationstechnik einzuhalten. Die Ausgestaltung der – in welcher Weise auch letztlich rechtlich Wirksamkeit entfaltenden – IT-Sicherheitsanforderungen obliegt jedoch einerseits – durch die Erarbeitung von grundlegenden IT-Sicherheits- und Bewertungskriterien – dem BSI bzw. den mit dem BSI kooperierenden nationalen und internationalen Institutionen und andererseits den spezifischen Schutzinteressen der Anwender und jeweils spezifischer Datenschutzkontrollinstanzen.

Jenseits dessen verfügt das moderne Datenschutzrecht neben dem klassischen Instrumentarium (Grundsatz der Zweckbindung und Erforderlichkeit der Datenerhebung, Erforderlichkeit der Einwilligung des Betroffenen sowie dessen Auskunftsrecht etc.) über neue Instrumente, die die IT-Sicherheit erhöhen können[98]):

- *Selbstdatenschutz:* Mit technischen Verfahren kann der Nutzer seine Daten unabhängig vom Netz- oder Systembetreiber schützen (z. B. Verschlüsselung, digitale Signatur, Anonymität).
- *Systemdatenschutz:* Bereits durch die Gestaltung der Systemstrukturen, in denen personenbezogene Daten erhoben und verarbeitet werden, soll einer unzulässigen Datenverwendung vorgebeugt und die Selbstbestimmung der Nutzer sichergestellt werden, negative Technikfolgen sollen erst

94) Vgl. dazu: Möhrenschlager, M., Reform des Computerstrafrechts, in: Die Polizei, Heft 2, 1987, S. 44–49

95) So A. Rossnagel in seiner Stellungnahme zum SigG vor dem Bundestagsausschuß für Bildung, Wissenschaft, Forschung und Technologie, 14. Mai 1997, A-Drs., S. 615f

96) Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz – BSIG) vom 17. Dezember 1990, BGBl. I, Nr. 71, 1990, S. 2834–2836

97) So der Änderungsantrag von BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 11/8197; Vgl. auch Plenarprotokoll vom 24. Oktober 1990, 11. Wahlperiode, S. 18247–18254

98) Vgl. Lanfermann, RDV, 1998, S. 4; Engel-Flechsig, DuD 1997, S. 13f.

gar nicht entstehen. Dies kann durch eine entsprechende technisch-organisatorische Ausgestaltung der Netze wie z. B. durch dateneinsparende Organisation der Übermittlung, der Abrechnung und Bezahlung, durch Abschottung von Verarbeitungsbereichen sowie durch Vermeidung von Machtkonzentration erreicht werden."[99])

Mit solchen Regelungsansätzen wandeln sich auch die Aufgaben des Staates: Er muß nicht mehr alle Funktionen, die ihm historisch zugewachsen sind, selbst erfüllen. Vielmehr liegt seine entscheidende Aufgabe darin, einen rechtlichen Rahmen für die Technikgestaltung zu liefern[100]), in dem der Bürger selbst durch die Verwendung technischer Schutzmechanismen zur IT-Sicherheit beitragen kann. Es fehlt die Möglichkeit der Bürger, sich angemessen von unabhängiger Seite in der schwierigen Materie IT-Sicherheit beraten zu lassen. Grundsätzlich müssen dafür die vorhandenen Netzinfrastrukturen allerdings ihrerseits freiheitstauglich sein, Systemschutz muß den Selbstschutz ergänzen.

Zusammengefaßt betrachtet bestehen in bestimmten Bereichen rechtliche Regelungen der IT-Sicherheit, ein einheitliches Regelungskonzept läßt sich jedoch vermissen. Die zergliederten bereichsspezifischen Regelungen in der Telekommunikation, bei den Telediensten und den Mediendiensten schaffen für IT-Sicherheit und Datenschutz teilweise eine überschneidende Überregulierung und eine strukturelle Unübersichtlichkeit für Nutzer, Verbraucher und Normadressaten[101]). Weitergehende IT-Sicherheitsanforderungen sind aus dem BSI-Gesetz ableitbar, aber auf wenige Bereiche bei Bundesbehörden beschränkt.

Die Legislative sollte bei der Ausgestaltung des Rahmens von IT-Sicherheit sich stärker beteiligen. So könnte das Datenschutzrecht um Bestimmungen ergänzt werden, die einen Grundstandard an organisatorischer und technischer IT-Sicherheit gewährleisten[102]). Eine stärkere Betonung dieses Systemdatenschutzes könnte insgesamt zu einer Vereinfachung des Datenschutzrechts und gleichzeitig zu einer Erhöhung der IT-Sicherheit führen. Die Vielfalt der Regelungsinhalte und der vom Datenschutz deutlich zu trennende Regelungszweck der IT-Sicherheit legen es jedoch eher nahe, einen eigenen gesetzlichen Rahmen der IT-Sicherheit zu schaffen.

[99]) Vgl. Engel-Flechsig, RDV, 1997, S. 64.
[100]) Vgl. Rossnagel, ZRP, 1997, S. 28ff.
[101]) Vgl. Büllesbach, A. Datenschutz bei Informations- und Kommunikationsdiensten: Gutachten. Bonn, Friedrich-Ebert-Stiftung 1998, S. 3
[102]) Vgl. Der Rat für Forschung, Technologie und Innovation: Informationsgesellschaft, Chancen, Innovationen und Herausforderungen, Bonn, Dez. 1995, S. 31f.
[103]) Die Zentralstelle für das Chiffrierwesen wurde 1989 zur Zentralstelle für Sicherheit in der Informationstechnik, aus der dann 1991 das BSI entstand. Zur Entstehungsgeschichte vgl. Bernhardt U.; Ruhmann, I.: ZSI: Die Bundesregierung will den Bock zum Gärtner machen, in: Computerwoche, Nr. 52, 22. Dezember 1989, S. 6–8; Bernhardt, U.; Ruhmann, I., Mutation einer Geheimdienststelle, in: Computerwoche, Nr. 12, 23. März 1990, S. 44–47

1.5.3 Organisatorischer Rahmen

Wie die dem BSI übergangsweise zugewiesene Bezeichnung „Zentralstelle für Sicherheit in der Informationstechnik"[103]) bereits nahelegte, ist in der Bundesrepublik das BSI die zentrale Stelle für alle mit der IT-Sicherheit zusammenhängenden Fragen beim Datenschutz ebenso wie in der Telekommunikation, der digitalen Signatur und der Prüfung und Evaluation von IT-Systemen, gleich, ob es sich dabei um die Prüfung von Systemen des Bundes handelt oder um die Prüfung zur Vergabe eines IT-Sicherheitszertifikats. Das BSI unterstützt die Arbeit der Sicherheitsbehörden und bewertet sogar die Zulässigkeit von Exporten von IT-Systemen, die der Ausfuhrkontrolle unterliegen. Wo das BSI selbst nicht tätig ist, kann eine gleichwertige Leistung nur aufgrund der Akkreditierung einer Prüfeinrichtung beim BSI erbracht werden. Derartige Leistungen sind möglich bei einem IT-Sicherheitszertifikat, das ebenso von akkreditierten Prüfstellen wie dem TÜV-IT vergeben werden kann. Bei der digitalen Signatur wiederum ist das BSI nicht für die Zertifizierung der Signatur selbst, sondern nur die Zertifizierung und Zulassung der Zertifizierungsstellen zuständig. Eine Ausnahme von dieser singulären Stellung besteht nur bei der Prüfung von IT-Systemen des Bundes, bei der das BSI beratend, evaluierend und unterstützend zuständig ist, der Bundesrechnungshof jedoch als Prüfungsinstanz, die die Sicherheit von IT-Systemen von Bundesbehörden umfassenden Prüfungen unterzieht.

Bei der Beratung der Öffentlichkeit bestehen keine weiteren dem BSI vergleichbaren Einrichtungen. Die Datenschutzbeauftragten des Bundes und der Länder informieren die Öffentlichkeit über besonders schwerwiegende Gefahren für die IT-Sicherheit. Bei der Aufklärung über spezifische Fragen des Virenschutzes und IT-Sicherheit hat sich neben dem BSI das Viren-Testcenter von Prof. Brunnstein an der Universität Hamburg etabliert. Für andere spezifische Probleme stehen Unternehmen heute jeweils eine Reihe kommerzieller Beratungsangebote zur Verfügung. Für die breite Öffentlichkeit und damit den Großteil der Nutzer elektronischer Netze stehen damit allerdings nur sehr wenige kompetente und unabhängige Informationsangebote zur Verfügung. Das Internet bietet zwar eine Vielfalt von Informationen zu global genutzten Systemen. Diese Informationen werden jedoch vor allem für Fachleute angeboten, kaum aber für Nutzer ohne Fachkenntnisse. Fragen der Sicherheit beispielsweise des spezifisch bundesdeutschen T-Online-Systems sind dort kaum zu finden.

Insgesamt läßt sich die Organisation von IT-Sicherheitsfragen dadurch kennzeichnen, daß sie nur wenig durch Vorschriften, sondern in hohem Maße von der Nachfrageseite her strukturiert ist. So findet eine für ein Sicherheitszertifikat erforderliche Prüfung eines IT-Systems auf Antrag des Herstellers bei einer der Zertifizierungsstellen statt. Im Gegensatz zu anderen technischen Geräten wie beispielsweise selbst Steckdosen findet außerhalb von Bundesbehörden keine systematische Prüfung sicherheitsempfindlicher IT-Systeme statt – es existiert überdies nicht

einmal eine rechtlich relevante Definition derartiger IT-Systeme. Keinerlei Prüfung oder Zertifizierung der IT-Komponenten gibt es dagegen beispielsweise bei Medizinprodukten wie etwa Implantaten. Herzschrittmacher werden zwar gemäß der Regelungen zur CE-Kennzeichnung auf ihre technische Funktion intensiv geprüft, diese Regelungen beinhalten jedoch bislang keinerlei Kriterien zur Evaluierung und Zertifizierung der in diesen Geräten eingesetzten Software.

Diese Organisation hat auch dort Folgen, wo schärfere Vorschriften bestehen. Trotz der Möglichkeit zu bindenden IT-Sicherheitsvorschriften für den Einsatz von IT-Systemen zumindest bei einigen Bundesbehörden setzt die Bundesverwaltung laut Auskunft der Bundesregierung mangels verfügbarer Alternativen über 65 000 Computer mit dem nicht sicherheitszertifizierten Betriebssystem MS-DOS ein[104]). Damit zeigt sich, daß eine solche Organisation von geprüfter IT-Sicherheit nicht notwendigerweise zu einem ausreichenden Angebot sicherer IT-Systeme führt. Betroffen sind davon auch Nutzer, die ihre IT-Systeme – auch ohne durch gesetzliche Normen dazu verpflichtet zu sein – in besonderem Maße mit technischen Mitteln schützen möchten. Der in Unternehmen nur im Zusammenhang mit Datenschutzauflagen oder dem Eigeninteresse an der Sicherheit der Daten bestehende organisatorische Rahmen der IT-Sicherheit sieht sich daher vielfach vor die Wahl gestellt, auf sehr restriktive Lösungen zurückzugreifen oder IT-Sicherheitsprobleme in Kauf zu nehmen. Ohne eine unabhängige Evaluation von IT-Sicherheitsstandards der Anbieter schließlich sind Nutzer elektronischer Netze nicht in der Lage, die Sicherheit der an diese Anbieter übermittelten Daten abzuschätzen. Damit verzichtet dieser Teil der Wirtschaft auf die in anderen technischen Gebieten absatzfördernd wirkende Prüfung technischer Sicherheit und damit auf die Entfaltung ökonomischer Perspektiven in Bereichen elektronischer Interaktion mit höherer Sicherheitsempfindlichkeit.

2. Ziele der IT-Sicherheit

2.1 Verfügbarkeit von Daten und Informationen, Sicherung vom Datenbestand, Datenverkehr und Datenzugang

Die große Abhängigkeit der Gesellschaft, ihrer Institutionen und infrastrukturellen Einrichtungen von funktionierenden Datenverarbeitungsprozessen bedeutet, daß der *Verfügbarkeit* von Daten als IT-Sicherheitsziel eine grundlegende Bedeutung zukommt.

Bei Daten ist Verfügbarkeit im Sinne von *„Zugriff ist in akzeptabler Zeit möglich"* gemeint. Dienstleistungen sind dann verfügbar, wenn sie abrufbar sind und in akzeptabler Zeit ausgeführt werden. Maschinen sind dann verfügbar, wenn ihre Funktion aufrechterhalten bleibt oder nur in akzeptablem Rahmen verzögert ist.

Die Verfügbarkeit kann durch mehr zufällige Faktoren wie Katastrophen (Feuer, Wasser usw.), technisches Versagen (durch schlechte Qualität, Alterung, ungeeignete Umweltbedingungen usw.), unbeabsichtigte Aktionen von Personen (Bedienungsfehler, Fehler bei der Wartung usw.) beeinträchtigt werden.

Aber auch absichtliche Aktionen (Manipulation, Sabotage) mindern die Verfügbarkeit: Zerstörung von Daten, Beeinträchtigung der Zugriffsmöglichkeiten auf Daten, absichtliche Zerstörung von Hardware-Komponenten, Einbau von Software-Fehlern und Einbringen von Schadensprogrammen.

Beispiel: Die klassische Dienstleistung im Bereich der Netzwerke ist der Datentransport, dessen Verfügbarkeit betriebsbedingt durch hohes Datenaufkommen oder durch technische Defekte vermindert werden kann. Eine andere Gefahr liegt etwa darin, ein Netzwerk absichtlich so mit Datenpaketen „vollzupumpen", daß andere Benutzer lange Wartezeiten in Kauf nehmen müssen oder überhaupt keinen Zugriff mehr auf die Netz-Ressourcen haben.

Ein IT-System, das solchen Bedrohungen gegen die Verfügbarkeit widerstehen soll, benötigt zuverlässige Hard- und Software-Komponenten mit einem angemessenen Grad an Korrektheit, Methoden der Fehlererkennung und Fehlerüberbrückung, eine Zugriffskontrolle zur Abwehr von illegalen Aktionen und zur Begrenzung von Betriebsmitteln.

Aus diesen Ausführungen resultiert vor allem eine andere Auffassung von Verfügbarkeit als Handlungsfehler. Da davon auszugehen ist, daß *unerwartete, nicht-intendierte Ereignisse* – also Fehler – eintreten werden, ist es notwendig, neben dem präventiven Fehlervermeidungskonzept eine operative *Fehlerbewältigungsstrategie* zu vermitteln und zu erwerben.

So die Handlungsfehler *Erstmaligkeit* (Neuigkeit und hohe Überraschung) besitzen, kann davon ausgegangen werden, daß Erfahrungsbildung und Kompetenzerweiterung eingeleitet werden, die letztlich eine erweiterte Bewußtseinsstruktur hinterlassen. Damit wird deutlich, daß nur aus dem gelungenen Fehlermanagement auch antizipative Komponenten für zukünftige Fehlervermeidung resultieren.

Nicht ein Zustand der Fehlerlosigkeit ist erstrebenswert, es geht eher darum, daß Fehlerkonsequenzen

[104]) So die Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Dr. Manuel Kiper und Manfred Such Das Bundesamt für Sicherheit in der Informationstechnik, Bt.-Drs 13/3408, Frage 7

harmlos gehalten werden müssen, so daß individuelle und kollektive Bewußtseinsbildung möglich wird und daraus letztlich die Überwindung bekannter Fehlhandlungsbedingungen resultiert.

2.2 Integrität der Information und Kommunikation

Die Problematik der unerwünschten Änderung von Daten und Systemen hat zur Folge, daß Daten inhaltlich inkorrekt sind, darauf aufbauende Schlußfolgerungen unzutreffend sind oder Dienstleistungen falsch oder unvollständig erbracht oder nur vorgetäuscht werden, Zeitbedingungen nicht mehr eingehalten werden können, Steuerungen inkorrekt ablaufen.

Die Integrität kann durch Bedienungsfehler, Fahrlässigkeit oder technischen Defekt (einschließlich inkorrekt funktionierender Hard- und Software) verletzt werden. Dies kann zu einem anderen technischen Verhalten, Funktionsausfällen oder inkonsistenten Daten führen.

Integritätsverletzungen können aber auch beabsichtigt sein (Manipulation, Sabotage). Viele Programme mit Schadenfunktionen (z. B. Viren) verletzen die Integrität der Programme und Prozesse.

Die Zielrichtung, dies zu verhindern oder zumindest zu entdecken, wird bei der IT-Sicherheit verfolgt.

Gegen Integritätsverlust wirken Plausibilitätskontrollen (z. B. bei der Dateneingabe), fehlerkorrigierende Codes (bei der Datenübertragung und -speicherung), Integritäts- und Signaturprüfungen (z. B. bei Datenbanken, Betriebssystemen und wichtigen Programmen – auch im Kontext von Viren), aber auch die Zugriffskontrolle und damit zusammenhängende Funktionen.

2.3. Vertraulichkeit von Information und Kommunikation

Der Schutz von Daten gegen unbefugte Einsichtnahme durch Dritte ist für die Nutzung von IT-Systemen von hoher Bedeutung. Der in der IT-Sicherheit dafür geprägte Begriff ist der Schutz der *Vertraulichkeit*. Im Unterschied zu anderen Aspekten der IT-Sicherheit ist dieser Schutz jedoch nicht allein technisches Gestaltungsziel, sondern war bereits 1986 Gegenstand einer gesetzlichen Regelung. Danach ist im § 202a StGB das Ausspähen von Daten unter Strafe gestellt.

Zweck der Vertraulichkeit ist die Durchsetzung der Schutzinteressen der Person oder Organisation mit Verfügungsgewalt über spezifische Daten mit dem Ziel eines Schutzes vor Nachteilen, die durch Einblick Dritter entstehen können. Die in IT-Sicherheitsmaßnahmen umzusetzenden Schutzpflichten beruhen auf Rechten und Pflichten wie dem Schutz von Betriebsgeheimnissen, der Wahrung des Arzt- oder Beichtgeheimnisses oder anderen Regelungen zur Vertraulichkeit von Daten und Informationen. Das Fernmeldegeheimnis unterwirft zudem die Kommunikation diesen Schutzinteressen. Der Gesetzgeber hat den Schutz der Vertraulichkeit als Aufgabe der Anbieter von Telediensten in § 4 Abs 2 Nr. 3 des Teledienstedatenschutzgesetzes normiert.

Vertraulichkeit in Computersystemen und -netzen sicherzustellen, ist eine technische wie organisatorische Aufgabe, die zu den Angelegenheiten von IT-Verantwortlichen im privaten wie öffentlichen Sektor gehört und die erst nach und nach als Element privater IT-Nutzung gesehen wird. In einigen Sonderbereichen – wie etwa der Telekommunikation oder dem Bankenwesen – werden spezifische Sicherheitskriterien angelegt, deren Einhaltung teilweise Voraussetzung für eine Marktteilnahme ist.

Eine Gefährdung der Vertraulichkeit läßt sich mit Hilfe einer Bedrohungsanalyse untersuchen, aus der Abwehrmaßnahmen abgeleitet werden. Zu den Bedrohungen der Vertraulichkeit zählt, wenn durch Zugang zu einem Rechner beliebige Daten abgerufen werden können. Dies ist ebenso der Fall durch die unbefugte Einsichtnahme in Datenübermittlungen, die mangels geeigneter Schutzmaßnahmen auch zufällig sein kann. Schließlich sind vorsätzliche Angriffe auf Computersysteme oder Übermittlungskanäle zu beachten, die mit dem Ziel des Ausspähens von Daten unternommen werden. Darunter ist auch die Nutzung passiver Empfangseinrichtungen für kompromittierende Strahlung von IT-Systemen zu zählen.

Da prinzipiell alle Computersysteme gegen eine oder mehrere Bedrohungen der Vertraulichkeit anfällig sind, gilt es, den erkannten Bedrohungen durch Schutzmaßnahmen zu begegnen. Diese werden entsprechend der Schutzziele ausgelegt, die für den jeweiligen Anwendungsfall sinnvoll und notwendig sind. Sofern gesetzliche Vorschriften – die Datenschutzgesetze, das Bankgeheimnis, Regelungen zu beruflichen Schweigepflichten und anderen Verschwiegenheitspflichten – den Grad der Vertraulichkeit von Daten regeln, sind IT-Systeme diesen Vorschriften entsprechend technisch zu gestalten und organisatorisch einzubinden. Sofern weitergehende Schutzinteressen bestehen, ist der erforderliche Schutz individuellen Bedürfnissen anzupassen.

Die Grundlagen derartiger Sicherheitsmaßnahmen entstammen den Zeiten zentraler Großrechner, in denen Datenbestände entsprechend organisatorisch definierter Zugriffsrechte organisiert waren. Der durch Paßwort geschützte Zugang zu spezifischen Datenbeständen des Rechners erlaubt auch heute einen recht guten Schutz der Vertraulichkeit innerhalb des organisatorischen Rahmens.

Neue Probleme beim Schutz der Vertraulichkeit erwachsen durch die Vernetzung von Computern. Für die Betrachtung der Sicherheitsaspekte beginnt dies nicht erst bei der Vernetzung per Internet, sondern bereits bei der Nutzung von In-House-Systemen. Schon hier gilt, daß etwa ein lokales Netzwerk auf Ethernet-Basis prinzipiell Daten im Klartext an alle Computer übermittelt, die zwischen Sender und Empfänger liegen. Erst mit zusätzlichen Systemen läßt sich eine Vertraulichkeit wieder herstellen.

Als Mittel zum Schutz der Vertraulichkeit ist allein eine effektive Verschlüsselung von Daten nutzbar.

Die von den Herstellern von WWW-Browser-Software aufgrund der gesetzlichen Exportbestimmungen der USA genutzten Verschlüsselungsverfahren sind allerdings so schwach, daß eine Gruppe von Studenten mit Universitäts-Ressourcen verschlüsselte Nachrichten innerhalb weniger Wochen knackten, so daß die verwendeten Verschlüsselungsverfahren kompromittiert wurden.

Die Anbindung von Computern ans Internet führt auch dazu, daß die Vertraulichkeit der Daten auf dem eigenen Computersystem durch Angriffe kompromittiert werden kann. Neben der Manipulation und der Zerstörung ist hauptsächlich das Ausspähen von Daten Ziel derartiger Angriffe. Ein unberechtigter Zugang zu Computern und deren Daten läßt sich entweder über bekannte Schwachstellen oder über das Ausspähen von Zugangsdaten im Internet erreichen, wobei Paßwörter und andere Zugangsinformationen abgefangen werden. Die Vehemenz von Angriffen steigt dabei mit der Bedeutung der Daten, die auf einem ans Internet angeschlossenen Computer vermutet werden. Allein die Computersysteme des U. S. Department of Defense waren 1995 über 250000 Angriffen ausgesetzt.

Derartige Angriffe auf Behördencomputer gewinnen an erheblicher Bedeutung, wenn – wie schon heute in den USA – viele Behördengänge per Internet erledigt werden und damit vertrauliche Daten von Bürgern auf Behördencomputern liegen. Bei der Vernetzung der staatlichen Verwaltung ist wesentlich stärker das Problem der Vertraulichkeit zu beachten, wenn es nicht zu gravierenden Mißbräuchen kommen soll. In den USA beispielsweise hatte eine Studie des General Accounting Office 1996 als Ergebnis, daß die Steuerbehörde IRS nicht für die Vertraulichkeit der Daten garantieren kann, die ihr die Bürger bei der per Internet möglichen Steuererklärung anvertraut haben.

Neben dem Ausspähen von Daten entstehen durch neue Softwaretechnologien im Internet weitere Risiken. Die vor allem durch die Nutzung von Web-Browsern verbreiteten neuen Softwarekonzepte Java und Active-X bedeuten beim Surfen im Internet und dem Betrachten einer Internet-Seite das Laden und Ausführen von Programmen. Derartige Programme können nicht nur Schäden wie die komplette Zerstörung von Festplatten-Daten verursachen. Sie können auch zum Ausspähen der Daten auf Rechnern genutzt werden. Ein Beispielprogramm für die Nutzung von Active-X zur Kompromittierung und Manipulation von Online-Banking-Transaktionen ging vor wenigen Monaten durch bundesdeutsche Newsgruppen. Sichere Abhilfe schafft hier derzeit nur das vollständige Unterdrücken jedweder Softwareübermittlung, was jedoch die Funktionalität einer Nutzung von Web-Seiten stark einschränken kann. Nutzer sind daher gezwungen, auf die Nutzung zu verzichten oder unkalkulierbare Risiken einzugehen. Dies ist typischerweise auch der Effekt von Firewalls mit hoher Schutzwirkung, bei denen Software den Datenstrom zwischen externem Netz und zu schützendem Computer filtert, um unzulässige Daten nicht weiterzuleiten.

Die hier möglichen, derzeit aber nicht verfügbaren Lösungen – wie beispielsweise ein Katalog sicherer und zertifizierter Software, die von sicheren Servern bezogen und in Web-Angebote eingebunden werden kann – haben gemeinsam, daß sie aus Gründen der Herstellerunabhängigkeit und der Evaluation durch unabhängige Dritte zwar privatwirtschaftlich organisiert sein können, dabei aber die Einhaltung nichtdiskriminierender Prinzipien und die Bewertung nach allgemeingültigen Kriterien sicherzustellen sind.

Der Schutz der Vertraulichkeit ist vor diesem Hintergrund nicht allein ein Mittel zur Sicherung vor unbefugter Einsichtnahme. Im Geschäftsverkehr ist das Wahren von Vertraulichkeit vielfach Voraussetzung für Geschäftsvorgänge, unabhängig davon, ob diese durch gesetzliche Regelungen Verschwiegenheitspflichten unterliegen oder nicht. Kunden bauen zudem zu Recht darauf, daß ihre sensitiven Daten in ausreichendem Maße geschützt werden.

Ein Verlust der Vertraulichkeit von Kreditkarten-Daten, medizinischen Daten und vielen anderen Bereichen zerstört das Vertrauen in einen Anbieter und kann Schadensersatzansprüche gegen diesen nach sich ziehen.

Zur unkontrollierten kommt unwillentliche Datenweitergabe hinzu. Diese Form der Gefährdung von Vertraulichkeit wurde in der letzten Zeit durch neue Technologien ohne ausreichende Schutzmechanismen deutlich erhöht. Ein Schutz der Vertraulichkeit ist dabei nur durch eine Kontrolle der für einen Abruf verfügbaren Daten oder den vollständigen Verzicht auf die entsprechende Technik leistbar. Hier sind vielfach noch Entwicklungsarbeiten zu leisten, um die Vertraulichkeit in verschiedenen technischen Anwendungen zu schützen. Gerade die Aufdeckung von Sicherheitsmängeln bei der Vertraulichkeit von Daten gilt als einer der Mängel bei IT-Anwendungen, der die Verbreitung nachhaltig behindern kann.

Der Schutz der Vertraulichkeit ist daher ein wichtiger Faktor für den Erfolg oder Mißerfolg von IT-Anwendungen. Dies trifft gleichermaßen für abgeschottete wie offene Anwendungen zu.

Die Entwicklung hin zu ubiquitären Systemen,[105]) die Daten sammeln und weitergeben, führt zu neuen Gefährdungen der Vertraulichkeit. Mittel und Wege, die Kontrolle über diese Datenverarbeitung und den Schutz vertraulicher Daten zu behalten, sind zum Teil nicht einmal in Ansätzen erkennbar. Wie bei der Einführung von PCs, die eine Schwächung des Sicherheitsniveaus mit sich brachten, liegen auch hier Quellen für neue Gefährdungen der Vertraulichkeit.

Das Ziel eines Schutzes der Vertraulichkeit bedingt, eine Kontrolle über die Einsichtnahme und Weitergabe von Daten zu gewährleisten. Dies bedeutet sowohl Mechanismen zur Unterdrückung einer Datenweitergabe wie auch solche zur Auswahl der Daten zur Verfügung zu haben, die Dritten überlassen werden. Zur Erreichung dieses Ziels ist nicht nur entsprechende Entwicklungsarbeit notwendig, vielmehr kann auch von staatlicher Seite eine Verbesserung der Rahmenbedingungen erreicht werden.

2.4. Unbeobachtbarkeit

Im Unterschied zur Vertraulichkeit gehört der Schutz der Unbeobachtbarkeit nicht zu den international einheitlich definierten Zielen der IT-Sicherheit. Dies ist insofern nicht verwunderlich, da diese auf die Trusted Computer System Evaluation Criteria des U. S.-Verteidigungsministeriums aus dem Jahr 1983 zurückgehen, deren Ziele am sicheren Transport von Daten und der zuverlässigen Verfügung über Computerresourcen ausgerichtet waren. Die Weiterentwicklung der Informations- und Kommunikationstechnologie hat zu einer erheblichen Ausweitung der Dienste geführt, die elektronisch abgewickelt werden. Erst in einem Umfeld, in dem eine breite Palette auch solcher Aktivitäten über elektronische Netze abgewickelt werden kann, bei denen vorher das Hinterlassen von Datenspuren nicht denkbar war, gewinnt das Ziel der Unbeobachtbarkeit an Bedeutung. Die technische Entwicklung und ihre Nutzung macht hier auch die Anpassung und Weiterentwicklung der IT-Sicherheitskriterien notwendig.

Unbeobachtbarkeit läßt sich als Variante der Vertraulichkeit interpretieren. Bei einer unbeobachteten elektronischen Aktivität soll Vertraulichkeit über die Identität der agierenden Person gewahrt bleiben. Das generelle Schutzziel der Vertraulichkeit, dem „Herren der Daten" die alleinige Kenntnis der Daten zu sichern, wird dabei eingeengt auf die Herrschaft über identifizierende Daten. Die Einsichtnahme Dritter in Identifikationsdaten ist zu unterbinden. Dabei ist es das Ziel, auch in elektronischen Netzen solche Handlungen unbeobachtet ausführen zu können, die in der realen Welt anonym bleiben. Neue Nutzungsformen solcher Netze können aber auch zu neuen Anwendungen von und Notwendigkeiten für unbeobachtete Interaktionsformen führen.

Der Gesetzgeber hat dies zum Anlaß genommen, in § 3 Abs. 4 des Teledienstedatenschutzgesetzes ein generelles Daten-Minimierungsgebot festzuschreiben und in § 4 Abs 1 des Gesetzes eine anonyme oder pseudonyme Nutzung elektronischer Netze zu ermöglichen. Artikel 2 (13) Nr. 6 des Begleitgesetz zum Telekommunikationsgesetz führt mit der Erweiterung des Fernmeldegeheimnisses auf die näheren Umstände der Telekommunikation ebenfalls zu einer rechtlichen Stärkung unbeobachteter Nutzung von Informations- und Kommunikationstechnologie. Der Gesetzgeber berücksichtigt damit die Gefahren, die von der Erstellung von Kommunikationsprofilen in Telekommunikationsnetzen ausgehen.

Die Funktion der Unbeobachtbarkeit von Handlungen für den Schutz der Privatsphäre, den Schutz der Menschenwürde und die freie Entfaltung der Persönlichkeit wurde vom Bundesverfassungsgericht in verschiedenen Entscheidungen hervorgehoben. Dabei ging es jedoch nicht allein um den Schutz der Privatsphäre, sondern auch um den Schutz von Handlungen in der Öffentlichkeit, die anonym vollzogen werden. Das Bundesverfassungsgericht befaßte sich vor allem mit der zwangsweisen Offenbarung von Lebensumständen und deren Daten entweder im Zusammenhang mit staatlichen Aufgaben (Volkszählungs-, Brokdorf-, Mikrozensus-Urteil) oder der Presse (Soraya-Urteil). Viele der mit neuen Nutzungsformen von Informations- und Kommunikationstechnologie verbundenen Fragen sind daher noch keiner abschließenden rechtlichen Klärung unterzogen worden. Der Schutz der Unbeobachtbarkeit bei der Nutzung der Informations- und Kommunikationstechnologie setzt zudem die freiwillige Teilnahme an Diensten voraus, bei der Daten gesammelt werden. Doch auch dies läßt sich nicht zum Anlaß nehmen, die Erbringung von Diensten von der beliebigen Sammlung von Daten abhängig zu machen (§ 3 Abs. 3 Teledienstedatenschutzgesetz). Vor diesem rechtlichen Hintergrund ist Unbeobachtbarkeit als Ziel einer Systemgestaltung zu beachten.

Bei der Nutzung von Telekommunikationsnetzen als physikalischer Grundlage elektronischer Vernetzung spielte die Kontrolle über die Identität der Teilnehmer von Beginn der technischen Entwicklung an eine Rolle. Schon die Listen, auf denen zur Zeit der Handvermittlung Verbindungen festgehalten wurden, waren für die Sicherheitsbehörden von Interesse. Die im Fernmeldeanlagengesetz geregelte Wei-

---

[105]) *Ubiquitär* bedeutet „überall verbreitet". Mit ubiquitären IT-Systemen ist eine Entwicklungsrichtung der IT-Forschung gemeint, die informationstechnische Systeme auf die Bedürfnisse des Anwenders hin in die alltägliche Lebenswelt einbindet. Führend in diesem Forschungsbereich ist das MIT. Es hat eine interdisziplinäre Forschungsgruppe gegründet, die den programmatischen Titel *Things That Think* trägt. In ihrem Things That Think Vision Statement beschreibt diese Forschungsgruppe ihren Auftrag und ihre Vision von ubiquitären Systemen wie folgt: „... We live in a world cluttered with buttons, batteries, wires, and userids that are simultaneously demanding and helpless. The solution to this problem ist that more is less: more capable devices, more pervasively embedded into the environment, linked more widely into robust distributed networks, can finally become less obstrusive. **Technology can not truly be helpful unless it can provide the information that you need where you want it, when you want it, and without you needing to mange it.** [...] The future of the computer is to be blown to bits, unchaining information from the cumbersome boxes that it currently inhabits. But ubiquitous computing must not become oppressive computing; true intelligence comes from building balanced systems that seamlessly merge together the many required levels of description." in: http://www.media.mit.edu/ttt

tergabe dieser Daten basiert auch heute noch fast unverändert auf den entsprechenden Paragraphen der Fernmeldeanlagenordnung aus den zwanziger Jahren dieses Jahrhunderts. Was damals die Suche in handschriftlichen Aufzeichnungen war, ist in den heute genutzten fast vollständig digitalisierten Telekommunikationsnetzen die automatisierte Suche in Datenbeständen. Sie kann anhand der Zuordnung von Telefonnummer und Anschlußinhaber in kurzer Zeit zusammenstellen, wer wie lang mit wem kommuniziert hat. Klarheit läßt sich nicht nur darüber herstellen, wer wen angerufen hat, sondern auch, von wem jemand angerufen wurde. Die Brisanz solcher Daten erschließt sich dann, wenn etwa das Kommunikationsprofil von Journalisten, Anwälten oder Ärzten erstellt wird, um an die Identität ihrer Informanten, Mandanten oder Patienten zu gelangen.

Aus diesen Gründen kam es in den letzten Jahren durch gerichtliche Schritte und den Erlaß der Telekommunikationsunternehmens-Datenschutzverordnung sowohl zu einer klareren Regelung des Umfangs der Daten, einer Verkürzung der Aufbewahrungsdauer der Daten als auch zur Verpflichtung von Telekommunikationsunternehmen, Kunden die sofortige Löschung der Verbindungsdaten anzubieten[106]).

Kommunikationsprofile durch Telekommunikationsunternehmen sind jedoch nur ein Teil des Problems. In digitalen Nebenstellenanlagen laufen in Unternehmen und Behörden weitgehend dieselben Daten über das Kommunikationsverhalten auf wie in den Vermittlungsstellen von Telekommunikationsnetzen. Im Gegensatz zu öffentlichen Netzen gelten hier jedoch nur in eingeschränktem Maße Schutzrechte. Digitale Telekommunikationsnetze übertragen außerdem die Teilnehmerdaten des Anrufenden an den Angerufenen. Bei einer Verbindung ins Ausland verlassen derartige Daten den Geltungsbereich deutschen Rechts und damit zugleich das hier erreichte Schutzniveau. Abhilfe kann hier die Nutzung von Vermittlungsoptionen in digitalen Netzen bieten.

Die international von der International Telecommunications Union (ITU) festgelegten Optionen erlauben das selektive Unterdrücken der Anrufer-Nummer und andere Schutzmechanismen. Voraussetzung ist allerdings, daß sie auch vom jeweiligen Telekommunikations-Anbieter zur Verfügung gestellt werden. Hier bietet sich die Möglichkeit, zur Durchsetzung bestehender technischer Standards beizutragen und auf ihre Weiterentwicklung zum Schutz der Unbeobachtbarkeit Einfluß zu nehmen.

Die technische Entwicklung führt auch hier zu neuen Problemen. Die mögliche Einführung einer Seriennummer in heute noch anonymen vorausbezahlten Telefonkarten kann den Betrug durch gefälschte Karten erschweren. Eine solche Maßnahme würde jedoch die Möglichkeit eröffnen, personenbeziehbare Daten in ein bis dahin zuverlässig anonymes Verfahren einzuführen. Auch die Weiterentwicklung des GSM-Standards sieht derzeit eine Ausweitung personenbeziehbarer Daten für viele zusätzliche Dienste vor und führt damit zu neuen Gefährdungen unbeobachtbarer Telekommunikation.

Vor der Vernetzung von Computern stand deren unbeobachtete Nutzung in aller Regel im Widerspruch zu IT-Sicherheitszielen, die sicherstellen sollten, daß nur Befugte einen Datenzugriff erhielten. In elektronischen Netzen werden Computer dagegen in Formen genutzt, die eine anonyme Nutzung erlauben. So werden zum einen Daten durchgeleitet, was keine Identitätskontrolle notwendig macht. Zum anderen werden auf Computern Daten für die Allgemeinheit zum kostenfreien Abruf bereitgestellt, wozu ebenfalls keine Identifikation des Nutzers erforderlich ist. Bei der Unbeobachtbarkeit stehen jedoch die Interessen der Nutzer und der Anbieter von Diensten in elektronischen Netzen in Widerstreit.

In elektronischen Kaufhäusern ist erstmals die genaue Beobachtung des Kundenverhaltens auf Angebote registrierbar. Von dem Moment an, in dem ein solches Angebot aufgesucht wird, kann jede Aktivität protokolliert werden. Der Kunde erzeugt beim Anbieter Daten über seine Präferenzen, Suchanlässe, Reaktionen auf spezielle Werbeangebote, die Verweilzeit bei einzelnen Angeboten usw. Der Anbieter kann auch versuchen, zu diesen Verhaltensdaten weitere identifizierende Informationen vom Kunden abzurufen. Damit sind nicht nur abstrakte, sondern für jeden Kunden spezifische Kundenprofile möglich.

Während die aus einer größeren Zahl von Kunden aggregierten Kundenprofile erlaubten, das eigene Angebot bestimmten Verhaltensmustern anzupassen, ermöglichen individuelle Kundenprofile, Angebote auf die spezifischen Präferenzen des einzelnen Kunden abzustimmen; jeder Kunde erhält damit einen spezifischen Angebotsausschnitt. Kundenprofile sind nicht allein für das eigene Angebot nutzbar, sondern ihrerseits wiederum ein Wirtschaftsgut. Anbieter verwenden Daten nicht nur aus eigenen Quellen. Verschiedene Anbieter durchsuchen elektronische Netze nach Mailadressen und bieten das Verschikken von elektronischer Werbepost an.

Problematischer als elektronische Massenwerbung sind jedoch Erstellung und Verkauf von Kundenprofilen. Bei derartigen Profilen ist nicht allein die zielgerichtete Ansprache von Kunden das Ziel, damit ist auch der selektive Zugang oder Ausschluß von Kunden zu Angeboten realisierbar. Weltweit operierende Unternehmen aus der Kreditwirtschaft zeigen, in welcher Form solche Daten ausgewertet und genutzt werden können. Wenn Nutzern allein aufgrund ihrer Identität der Zugang zu elektronischen Angeboten verwehrt wird, stellt dies eine unzulässige Diskriminierung dar, die durch den Verlust der Unbeobachtbarkeit hervorgerufen wird. Die Regelungen im Teledienstedatenschutzgesetz, die Nutzerprofile bei Nutzung von Pseudonymen erlauben, sind in internationalen Netzen kein ausreichender Schutz gegen solche Auswüchse.

Unbeobachtbarkeit spielt auch eine Rolle beim Zahlungsverkehr. Unser Wirtschaftssystem basiert darauf, unabhängig von der Vorlage einer Berechtigungskarte oder Identifikation Ware gegen Geld erstehen zu können. Dies soll sich nach dem Willen

[106]) Gem. § 6 (4) TDSV

einiger Systemanbieter ändern. Elektronische Zahlungssysteme (electronic cash; e-cash) basieren derzeit zumeist darauf, Daten über Transaktionen aus Sicherheits- wie aus Marketinggründen zu sammeln und auswertbar zu machen. Dieser Verlust der Unbeobachtbarkeit gilt sowohl für realweltliche e-cash-Systeme, wie das in der Bundesrepublik von der Gesellschaft für Zahlungssysteme eingeführte System oder das in Großbritannien genutzte Mondex, als auch für Internet-basierte Zahlungssysteme. Lediglich das derzeit in der Pilotphase befindliche System *digicash* verspricht anonyme Zahlungen, sofern sich „alle Beteiligten an die Spielregeln" halten. In diesem Zusammenhang muß allerdings auch beachtet werden, daß Anonymität in Verbindung mit der „Körperlosigkeit" digitalen Geldes auch neue Formen der Kriminalität, zumindest neue Begehungsformen, nach sich ziehen kann.[107])

Nicht-anonyme Zahlungen führen nicht nur zu den bereits beschriebenen Problemen bei Kundenprofilen schon bei kleinsten Käufen. Die Möglichkeit, elektronisches Taschengeld mit solchen Daten zu versehen, die Kindern das Erstehen jugendgefährdender Inhalte im Internet unmöglich machen, ist ebenso geeignet für jedwede gruppenspezifische Selektion, sei dies aus religiösen, rassischen, politischen oder anderen Gründen. Identifizierbare Zahlungsmittel bergen – unabhängig von allen ökonomischen Gefahren – die Gefahr, daß bestimmten Kunden und Kundengruppen der Kauf spezifischer Waren unmöglich gemacht werden kann.

Angeführt wird auch, daß elektronische Zahlungsmittel – ob Internet-basiert oder nicht – besondere Anforderungen an die Wahrung der Unbeobachtbarkeit stellen. Mit dem Signaturgesetz wurde in der Bundesrepublik auch eine rechtliche Grundlage für elektronische Zahlungsmittel geschaffen, ohne jedoch auf neue Bedrohungsformen der Unbeobachtbarkeit einzugehen. Jede Form von Zahlungsmittel, das auch bei kleinsten Transaktionen eine Identifikation und damit Klassifikation des Zahlenden erlaubt, lege den technischen Grundstein zu diskriminierenden Transaktionspraktiken. Dabei gingen die Möglichkeiten deutlich über die bei der Debatte um ein Recht auf ein Girokonto behandelten Fragen hinaus. Die verdeckte Anwendbarkeit solcher Eingriffe machten sie für den Gesetzgeber zwar regulierbar, aber kaum kontrollierbar. Allein die Wahrung der Unbeobachtbarkeit in elektronischen Zahlungsmitteln stellt aber sicher, daß ein freier elektronischer Handelsverkehr entsteht und erhalten bleibt.

Unbeobachtbarkeit basiert auf Datenvermeidung. Eine Umsetzung dieses Grundgedankens bedeute aus der Perspektive der IT-Sicherheit eine entsprechende technische und organisatorische Gestaltung von IT-Systemen. Bei der Nutzung entgeltpflichtiger Angebote läßt sich dies typischerweise durch Vorauszahlung ermöglichen, bei unentgeltlichen Angeboten ist dies noch einfacher durch die Nichterhebung identifizierender Daten möglich. Das Problem, im Internet nach Daten wie Mailnummern zu suchen, läßt sich jedoch nur durch die konsequente Umsetzung von Techniken zur Vermeidung einer Archivierung von Daten gegen den Willen des Betroffenen und die Entwicklung neuer technischer Lösungsansätze angehen.

2.5 Transparenz und Interoperabilität

Was bis vor einiger Zeit noch als *Protokollierung* bezeichnet wurde, wird heute *Beweissicherung* genannt, und dient durch die Aufzeichung aller ausgeübten Rechte, insbesondere auch aller sicherheitsrelevanten Ereignisse, letztlich dem Zweck zur Herstellung von *Transparenz*.

Der Zweck besteht also in der *nachträglichen* Entdeckung von Ereignissen und damit unter anderem der Beweisführung bei Manipulationen.

Es ist klar, daß die Herstellung von Transparenz den Namen nur verdient, wenn lückenlos aufgezeichnet und alle zur Beweisführung notwendigen Informationen (zumindest Benutzer, Uhrzeit, Datum, Art der Aktion) gespeichert werden. Das Ziel der Transparenz, also der Beweissicherung, bestimmt, was im Detail zu erfassen ist.

Wenn Benutzer oder Prozesse in der Lage sind, den Umfang der Protokollierung selbst festzulegen, die Protokollierung ganz auszuschalten oder selbst beliebige Einträge in der Protokolldatei zu erzeugen, ist die Beweissicherung täuschbar und erfüllt somit nicht ihren Zweck. Aktionen des System-Verwalters und anderer privilegierter Personen sollten sicher protokolliert werden können – was aber in der Praxis vielfach nicht geschieht oder technisch nicht möglich ist.

Andererseits müssen in einem IT-System privilegierte Rollen eingerichtet werden können, denen das Recht zur Bearbeitung von Protokollaufzeichnungen, zum Löschen nicht mehr aktueller Aufzeichnungen, zum Einsatz der Protokollparameter und zur Auswahl aufzeichnungswürdiger Aktionen übertragen wird. Sinnvoll ist Transparenz letztlich nur dann, wenn Auswertungsprozeduren vorhanden sind, mit denen die gesamten Aufzeichnungen nach sicherheitskritischen Ereignissen durchsucht und damit manipulative Aktionen entdeckt werden können. Diese Prozeduren müssen natürlich auch regelmäßig angewendet werden. Die Zeiten, in denen viele Magnetbänder mit Protokollierungsdaten unbearbeitet irgendwo im Archiv verstauben, sollten für sensitive IT-Systeme vorbei sein.

Eine eher präventive Methode der Entdeckung sicherheitsrelevanter Vorkommnisse besteht darin, typische Verhaltensweisen der Benutzer zu erfassen und bei signifikantem Abweichen von diesem Normalprofil entweder Alarm zu schlagen, oder diese „Datenspuren" durch Methoden des „data-mining" zu kommerziell verwertbaren Adressen- bzw. Kunden- und deren Verhaltensprofilen zu verdichten.

Grundsätzlich ist es mit Hilfe der elektronischen Beweissicherung im Prinzip technisch möglich, Manipulationen zu entdecken, herauszufinden, wer sich Paßwörter illegal verschafft hat, auch wenn er aus

[107]) Vgl. hierzu den Abschnitt 5.4 im Berichtsteil Strafrecht.

Systemsicht formal autorisiert ist. Dies wirft datenschutz- wie arbeitsrechtliche Fragen auf.

Einen ganz anderen Aspekt spricht die dringend erforderliche *Interoperabilität* vor allem der verschiedenen Verschlüsselungs- und digitalen Signaturanwendungen und Signatursysteme an. Interoperabilität bedeutet, da? Anwendungsmöglichkeiten von einer Software- und Hardwareumgebung in eine andersartige übertragen werden können (Übertragbarkeit), und daß Benutzer ortsunabhängig, beispielsweise mit dem gleichen „Trust-Center", arbeiten können (Mobilität).

Um den Bedürfnissen des Marktes nachzukommen, sind im Hinblick auf die Interoperabilität technische Standards notwendig, die in offenen und marktorientierten Verfahren ausgearbeitet werden müssen. Technische Standards werden für die Formate digitaler Signaturen und von Zertifikaten, aber auch für die Definition von Lizenzierungskriterien zur Abnahme und Überprüfung von Trust-Centern benötigt.

2.6 Zuordenbarkeit

Eine zentrale Grundlage der Informationssicherheit ist die zuverlässige Authentisierung – auch Zuordenbarkeit – des Benutzers eines IT-Systems durch den Rechner selber. Nur Berechtigte dürfen Zugriff auf die Daten etwa eines Unternehmens haben. Die Authentisierung stellt die zentrale Funktion der Zugriffskontrolle dar und beinhaltet die Identifikation, die Authorisierung und die Protokollierung, mit der Ereignisse in IT-Systemen beweissicher dokumentiert werden können.[108])

In allen erhältlichen Netzwerkbetriebssystemen (z. B. Novell IntranetWare, Windows NT und UNIX) ist heute standardmäßig ein Paßwortmechanismus zur Authentisierung implementiert. Für die Paßwörter können bestimmte Eigenschaften festgelegt bzw. erzwungen werden. Hierzu gehören insbesondere Mindestlänge und Gültigkeitsdauer. Das Paßwort ist (im Idealfall) nur dem Benutzer und dem Rechner bekannt. Damit das Paßwort von anderen Benutzern nicht direkt ausgespäht werden kann, darf es zudem am Bildschirm nicht im Klartext bzw. in der Länge dargestellt werden. Es hat sich in der Praxis allerdings gezeigt, daß die Bequemlichkeit und Vergeßlichkeit des Benutzers das schwächste Glied bei der Paßwortauthentisierung ist.

Die Möglichkeiten der Beeinträchtigung der Sicherheit des Paßwortverfahrens von der Benutzerseite zeigen, daß es für sensitive Anwendungen keinesfalls ausreichend ist, sie mittels eines Paßwortmechanismus zu schützen. Dies beweisen immer wieder Fälle des erfolgreichen Hackings und der Computerkriminalität,[109]) die letztlich durch das ungerechtfertigte Vertrauen der Betreiber in die Wirksamkeit von Paßwörtern ermöglichst werden.

Meldungen über erfolgreiche Einbrüche in Rechner sind immer wieder mit dem Internet verbunden. Die dortigen Sicherheitsprobleme lassen sich zu zwei Kernpunkten zusammenfassen. Es fehlt allgemein ein Authentisierungsmechanismus, der feststellt, mit welcher Gegenseite man Kontakt hat. Fast alle spektakulären Hacker-Erfolge beim Eindringen in fremde Rechnersysteme lassen sich auf erhebliche Defizite der Sicherheit auf der Protokollebene und den Schwächen des Paßwortverfahrens zurückführen. Ob ein 16jähriger Schüler in einen Pentagonrechner eindringt oder die Webseite des CIA manipuliert wird, die Faktoren des Erfolges sind immer gleich: Öffentlicher Zugang, Möglichkeit des Rechnerzugriffes mit einem erratenen oder abgehörten Paßwort, Angriff auf Paßwortdateien des Rechners bzw. der mit ihm verbundenen Rechner, Erweiterung der Zugriffsrechte bis zum Supervisor. Entsprechende Meldungen wird es solange geben, wie diese Schwächen existieren.

Als Alternative zu Paßwort-gestützten Verfahren bieten sich heute mehrere Techniken an, die allein allerdings nur bedingt höhere Sicherheit bieten und daher in Kombination genutzt werden. Als erstes zu nennen sind dabei *biometrische Verfahren,* die unveränderliche Eigenschaften des Menschen zur Identifikation nutzen[110]). Neben dem Fingerabdruck[111]) und der Handgeometrie[112]) werden dabei die Blutgefäße des Auges oder die Retina genutzt, die zur Identifikation ebenso nutzbar sind[113]) wie das Muster der vaskularen Blutgefäße im Gesicht, die sich mit Infrarotgeräten auch aus der Ferne und damit unbemerkt erfassen lassen[114]). Durch verbesserte Mustererkennungssysteme wird auch die Sprechererkennung

---

[108]) Vgl. hierzu auch den Berichtsteil Strafrecht, Abschnitt 10 „Außerrechtliche Lösungsansätze"

[109]) Vgl. Ausführungen zur Computerkriminalität im einleitenden Kapitel und im Berichtsteil Strafrecht.

[110]) Einen Überblick von Einsatzbeispielen liefert, Putting the Finger on Security, in: Time, 3. April 1989, S. 46 oder Zugangsverfahren zu Computersystemen, in: Sicherheits-Report, Nr. 3, 1986, S. 25–26

[111]) Zugangskontrollsysteme auf unterschiedlicher technischer Basis sind etwa TouchSafe von Identix (Scanning Fingers, Newsweek, 26. September 88, S. 3), Fingerscan (Öffentliche Sicherheit, Nr. 3, 1997) DermoPrint (Öffentliche Sicherheit, Nr. 10, 1995, S. 34), aber auch ein Pilotsystem des BGS zur automatisierten Grenzkontrolle an Flughäfen.

[112]) Systeme zur Messung der Handgeometrie nutzt die US-Einwanderungebehörde als automatisierte Grenzkontrolle an Flughäfen seit 1992 (Erleichterte US-Einreise; in: Der Spiegel, Nr. 31, 1992, S. 123)

[113]) Systeme hierzu sind Eye Dentifcation, Produktbeschreibung der NUCLETRON GmbH, München, 1985. Für Geldautomaten in den USA, Großbritannien und Japan liefert die Sensar Incorp. ein Iris-Erkennungssystem (Schau mir in die Augen, Kleines; in: Süddeutsche Zeitung, 14. Mai 97, S. 12)

[114]) Ein derartiges System wurde entwickelt von Technology Recognition Systems (Safe Face; in: Newsweek, 16. Oktober 1995, S. 5). Zur Technologie vgl. Paul Robinson: We will find You; in RISKS-Forum Digest Vol 15 Nr. 62, 3. März 1994. Auf der Infrarot-Erkennung von Blutgefäßen des Fingers beruht ein System von M. Willmore (Aviation Week & Space Technology, Jan 9, 1995, S. 15)

und die Gesichtserkennung[115]) zur Identifikation genutzt.

Biometrische Verfahren erfordern oft jedoch zusätzliche Sicherungen, da sie nur einen zugangsberechtigenden Besitz nachweisen. Damit unterscheiden sie sich im Prinzip nicht von anderen besitzbasierten Verfahren wie Chipkarten. Da Besitztümer jedoch auch unrechtmäßig – bei Chipkarten durch Diebstahl, bei Fingerabdruckverfahren durch Abtrennen eines Fingers, bei Sprechererkennung durch Abspielen eines Tonbands, Ausnahme ist das vaskulare Gefäßsystem des Gesichts – in Besitz gebracht worden sein können, ist zusätzlich noch die Identifikation durch Wissen oder den Nachweis des Seins erforderlich. Besser als Paßwortverfahren sind – als wissensbasierte Verfahren – dazu psychometrische Methoden, die typische motorische Leistungen der Person messen.[116])

Vielen dieser Verfahren ist jedoch als gravierende Schwäche gemein, daß dabei eine Speicherung von Zugangsberechtigungs-Daten auf dem IT-System erfolgt, womit diese Daten für ein Ausspähen anfällig sind. Gelöst wird dies einerseits dadurch, daß etwa Fingerabdruckleser als autonome Geräte realisiert sind oder durch die Verschlüsselung von etwa von Paßworten oder anderen Berechtigungsdaten, durch die ein Ausspähen erfolglos bleiben muß. Je komplexer jedoch die Erkennungsprozedur, um so schwieriger ist eine Realisierung in autonomen Geräten.

Das Übermitteln authentisierender Daten über ein Netz birgt jedoch wieder Risiken der Kompromittierung dieser Daten. Um solcher Übermittlungsprobleme zu vermeiden, wurden Zero-Knowledge-Protokolle entwickelt, die eine Authentisierung durch schrittweisen Austausch von Wissen – vergleichbar einem Stellen und Lösen zufälliger Aufgaben, deren Ergebnis nur durch das Wissen um keinem Dritten bekannte Parameter zu bestimmen ist – leisten, ohne dabei verräterische Informationen preiszugeben.

Eine Kombination verschiedener Verfahren erscheint aus heutiger Sicht die beste Alternative, um die Sicherheit der Authentisierung auf ein hohes Niveau zu bringen. Dieser Überlegung entspricht die Idee einer Sicherheitstastatur, welche Wissen, Haben und Sein einer Person integriert überprüfen kann.

- Das Wissen einer Person kann wie bisher zur Authentisierung mittels der Eingabe eines Paßwortes genutzt werden.
- Das Haben wird durch eine Chipkarte realisiert, welche zugleich die psycho- oder biometrischen Merkmalen der Person als Referenzwert speichert.
- Das Sein bzw. personenspezifische Verhalten wird durch einen physiometrischen Controller in der Sicherheitstastatur überprüft. Tastaturen mit integrierten Chipkarten-Lesern und zugehörigen Kontrollsystemen, die für die Implementation physiometrischer Verfahren geeignet sind, befinden sich bereits auf dem Markt.

So hat der Wirtschaftsinformatiker Dieter Bartmann an der Universität ein Progamm namens *Psylock* entwickelt, das den individuellen Tastenanschlag einer Person ermittelt und damit die Zugangsberechtigung feststellt. Bei diesem Verfahren vergleicht die Software, wieviel Zeit zwischen dem Anschlag eines A und dem danebenliegenden S vergeht, wie schnell die Wörter aufeinander folgen oder wie der Gesamtrythmus des Tippens ist. Die Wahrscheinlichkeit, daß ein Hacker *Psylock* durch Probieren überlisten kann, liegt nach Auskunft des Wissenschaftlers bei einem Treffer auf rund tausend Versuche und ist damit vergleichbar mit der Fehlermenge anderer Kontrollsysteme.[117])

---

[115]) Einen Überblick gibt: Eberl, U., Das enttarnte Gesicht; in: Bild der Wissenschaft, Nr. 12, 1995, S. 16–20. Für 60 US-$ bietet die Firme Visionics die PC-Version des Produkts Facelt an, das auch am Langkawi Airport (Malaysia) für die Boarding-Zutrittskontrolle per Gesichtserkennung genutzt wird (Gesichtserkennung statt Paßwort; in: c't, Nr. 8, 1997) Neuronale Netze zur Erkennung setzt das System ZN-Face ein, das auch Gesichtsmasken von Originalen unterscheiden soll (Gesicht in der Chipkarte; Wirtschaftswoche, Nr. 5, 1997, S. 50–51). Von der Nielsen Media Research wurde ein System entwickelt, das eine Testfamilie an ihren Gesichtern erkennt, so: Brother Nielsen Is Watching, in: Time, 12. Juni 1989, S. 45. Leistungsfähige Systeme zur Zutrittskontrolle auf der Basis von Gesichtserkennung wurden seit den 80er Jahren vermarktet von den Firmen Borer Communications, Inform und Siemens, (RZ-Zutrittskontrolle: Keine Chance für die Diebe, in: online, Nr. 8, 1988, S. 30–31).

[116]) Hierzu gehört derzeit vor allem die Messung der Handschrift und ihrer Dynamik, aber auch die Messung charakteristischer Merkmale des Tippverhaltens an der Computertastatur; Vgl. Am Tippen erkannt; in: c't, Nr. 13, 1997, S. 66. Hierzu gehört derzeit vor allem die Messung der Handschrift und ihrer Dynamik, aber auch die Messung charakteristischer Merkmale des Tippverhaltens an der Computertastatur.

[117]) Vgl. Aschbrenner, N., Mit Psylock sind Paßwörter passé, in: Berliner Morgenpost vom 14. September 1997

3. Möglichkeiten der Technik

Die Betrachtung von technischen Möglichkeiten in Hinblick auf IT-Sicherheitsprobleme erfordert zwei unterschiedliche Perspektiven.

Zum einen werden zahlreiche Sicherheitsprobleme erst durch Technik hervorgerufen. Hier stellt sich deshalb die Frage, welche Risiken durch diese Techniken erzeugt werden und welche Möglichkeiten der Technikgestaltung existieren, die systematisch IT-Sicherheit im Interaktionsmodus von Mensch und Maschine berücksichtigen.[118])

Zum anderen sind es Sicherheitstechnologien, wie z.B. Firewalls oder kryptographische Systeme, mit denen überhaupt erst adäquate Lösungen für bestimmte Sicherheitsprobleme möglich werden.

Obwohl diese beiden Seiten von Technik auf dem ersten Blick ambivalent erscheinen, entfalten sich die Möglichkeiten der Technik gerade in der Verbindung von einer systematischern Berücksichtigung sicherheitsrelevanter Aspekte bei der Technikentwicklung bzw. Technikgestaltung und dem Einsatz technischer Werkzeuge zur Lösung von IT-Sicherheitsproblemen. Dieser Ansatz einer alle (auch technischen) Ebenen berücksichtigenden IT-Sicherheit spiegelt sich im Begriff der mehrseitigen Sicherheit wider. Die Existenz dieses Begriffes bedeutet allerdings nicht, daß die Probleme, die sich in diesem Spannungsfeld darstellen, wissenschaftlich und konzeptionell gelöst sind. Vielmehr dokumentiert dieser Begriff wissenschaftliche und konzeptionelle Defizite in Hinblick auf eine umfassende IT-Sicherheitsarchitektur. Deshalb muß dieser Begriff auch als Aufruf an die Politik verstanden werden, wissenschaftlich ausgerichtete Schwerpunkte zu fördern, die sich verstärkt mit den Fragen einer umfassenden IT-Sicherheitsarchitektur befassen. Die bisher existierende Forschung auf diesem Gebiet erlaubt keine umfassende Abklärung der Risikopotentiale bestehender, neu entwickelter oder kombinierter Technik.

Deshalb können im Rahmen dieses Abschnitts diese Themen nur rudimentär und keineswegs abschließend behandelt werden.

In Hinblick auf technische Werkzeuge zur Lösung bestimmter IT-Sicherheitsprobleme sind die derzeitigen Möglichkeiten umfassend dokumentiert, so daß die wichtigsten technischen Werkzeuge und Schutzstrategien in diesem Abschnitt dargestellt werden können.

[118]) Dieser Ansatz korrespondiert mit dem Abschnitt 1.2.

3.1 IT-Sicherheitsprobleme angewandter Informationstechnologie

3.1.1 Probleme aus technologischer Abhängigkeit

In Deutschland und Europa besteht eine weitgehende Abhängigkeit von der Soft- und Hardware großer ausländischer Hersteller. Diese technologische Abhängigkeit ist problematisch, weil mangelnder Wettbewerb die Herausbildung von Technologien mit besseren Sicherheitseigenschaften behindert. Der Umstand, daß Software fehlerbehaftet und mit zahlreichen Sicherheitslücken an den Verbraucher für teures Geld verkauft wird, damit dieser Fehler und Qualitätsmängel in seinen täglichen Anwendungen aufdeckt, ist nicht nur Ausdruck einer mangelnden Haftungsregulierung in diesem Bereich, sondern auch der Ausdruck einer verzerrten Wettbewerbssituation.

Bei Beachtung der Gefahrenpotentiale, die von Nachrichtendiensten und industriellen Angreifern für die nationale Informations- und Kommunikationsstruktur ausgehen, ist es mit den Anforderungen an eine nationale Sicherheitsinfrastruktur im Bereich der IT-Infrastuktur als nicht vereinbar anzusehen, daß derzeit eine weitreichende und nicht ohne weiteres entfernbare Abhängigkeit von der Soft- und Hardwarebelieferung durch Firmen vorliegt, aus deren Heimatstaaten potentielle Angriffe erwartet werden können.

Dieses Abhängigkeitsproblem nimmt in erheblicher Weise Einfluß auf die Möglichkeiten der Gestaltung einer besseren und sicheren Technik, denn die technische Dominanz eines Herstellers – etwa im Bereich von Betriebssystemen – erzeugt Referenzzwang bei der Entwicklung von Anwendungsprogrammen und anderen nachgelagerten Programmen.

Im folgenden werden einige der wichtigsten sicherheitsrelevanten Probleme weit verbreiteter Informationstechnik angesprochen.

3.1.2 Betriebssysteme als entscheidende IT-Sicherheitsgröße

Eine Sonderstellung im Bereich der Software nehmen die Betriebssysteme ein. Sie sollen u.a. die Hardwareressourcen des Rechners verwalten und deren Verfügbarkeit sowie den ordnungsgemäßen Betrieb aufrechterhalten, durch Abstraktion von der konkreten Hardware eine plattformunabhängige Schnittstelle für Anwenderprogramme bieten, für den allgemeinen Betrieb des Rechners notwendige Funktionen bündeln usw. Das Betriebssystem sollte die ständige Kontrolle über die Hardware des Rechners haben, also auch den Prozessor, den Hauptspeicher und die Peripherie.

Daraus ergeben sich zwei für die Sicherheit sehr bedeutsame Eigenschaften des Betriebssystems:

1.) Das Betriebssystem hat zweckbedingt jederzeit Zugriff auf die gesamte Hardware, insbesondere den Prozessor, den Hauptspeicher und die Peripherie.

2.) Sicherheitsprobleme des Betriebssystems sind nicht durch Gegenmaßnahmen in der Anwendungssoftware abzufangen.

Sicherheitsprobleme des Betriebssystems bedeuten die Unsicherheit des Gesamtsystems. Die Sicherheitsanforderungen an das Betriebssystem müssen daher kompromißlos und mit höchster Priorität erfüllt werden.

Ein Betriebssystem mit entsprechenden Eigenschaften kann aber – unter Ausnutzung entsprechender Hardwarefunktionen[119]) – den Zugriff von Anwendungs- und anderen Programmen auf die Hardware einschränken oder unterbinden bzw. den Zugriff nur indirekt über Dateisysteme usw. ermöglichen und darüber hinaus bei jedem Zugriff eine regelbasierte Prüfung der Plausibilität und der Berechtigung durchführen und den Zugriff dementsprechend zulassen oder verwehren.

Dadurch entsteht ein überaus mächtiges und wichtiges Werkzeug, das es erlaubt, sicherheitsrelevante Programmteile aus dem Anwendungsprogramm in das Betriebssystem zu verlagern, und damit die Anwendungsprogramme bezüglich der Sicherheitsanforderungen nachhaltig zu entlasten.

Die dazu notwendigen Eigenschaften hat ein Betriebssystem jedoch nicht bereits aufgrund seiner Eigenschaften als Betriebssystem. Vielmehr muß das Betriebssystem für diese Aufgabe entworfen sein und höchsten Anforderungen an Sicherheit und Qualität standhalten.

3.1.2.1 Optionen einer sicheren Gestaltung von Betriebssystmen

Die Konsequenz daraus ist, daß eine strikte und technisch durchgesetzte Trennung zwischen Betriebssystemfunktionen einerseits und Anwendungsfunktionen andererseits besteht oder hergestellt wird. Dazu gehört auch, daß graphische Benutzeroberflächen, Web-Browser usw. nicht zum Betriebssystem gehören. Nur dann ist eine Beeinträchtigung des Betriebssystems durch zweckfremde Funktionen ausgeschlossen und gleichzeitig die zuverlässige Sicherungswirkung des Betriebssystems auf diese Anwendung gewährleistet.

Damit sind die wesentlichen Voraussetzungen für eine effiziente Sicherung gegeben, die auch unter den durch die Realität vorgegebenen Randbedingungen umsetzbar ist.

[119]) Hierzu gehören u. a. zeitgesteuerte Interruptschaltungen, Speicherverwaltungen und Prozessoren mit Supervisormodus o. ä. Heutige Rechnerarchitekturen verfügen über diese Ausstattung. Deren Zuverlässigkeit ist aber von der Qualität der Hardware abhängig.

Eine Vielzahl von Anwendungen ist aufgrund ihrer Komplexität, aufgrund der Vielfalt und aufgrund der Distributionsformen nicht unmittelbar mit den Sicherheitsanforderungen vereinbar. Dies muß und kann aber in großem Umfang durch eine entsprechend starke Auslegung des Betriebssystems ausgeglichen werden. Dadurch kann erreicht werden, daß eine für sich betrachtet als riskant einzuschätzende Anwendung bei Verwendung unter einem sicheren Betriebssystem und Beachtung geeigneter Regeln als akzeptabel eingestuft werden kann.

Damit erweist sich das Betriebssystem als das für die Gesamtsicherheit des Systems bedeutsamste Element, an das die höchsten Sicherheitsanforderungen zu stellen sind. Hier kann auch sehr viel mehr Aufwand betrieben werden, da hier nicht eine Vielzahl verschiedener Programme zu verschiedenen Anwendungen betrachtet werden muß, sondern nur ein universelles Programm(-paket) Gegenstand der Betrachtung sein muß.

Vor diesem Hintergrund ist es nicht zu verantworten, daß in nahezu allen Bereichen Betriebssysteme, die nicht im Quelltext vorliegen und die schon von ihrer Struktur her den Sicherheitsanforderungen widersprechen, eine so weite Verbreitung erreicht haben[120]). Während bei allen anderen Industrieprodukten eklatante Fehler zu entsprechenden Reaktionen der Presse und der Verbraucherführen (Beschwerde, Umtausch, Rückgabe usw.), herrscht im Softwarebereich ein gewisser Verbraucherfatalismus gegenüber der unübersichtlichen Technik, der Produkte zusammen mit ihren bekannten Fehlern zum De-facto-Standard werden läßt.

An dieser Stelle besteht dringender Handlungsbedarf für Politik, Verwaltung, Wirtschaft, Forschung und Entwicklung.

Die Verfügbarkeit und der weitgehende Einsatz eines universell einsetzbaren, plattformunabhängigen, im Quelltext verfügbaren, auf Sicherheit ausgelegten, zunächst nicht kommerzielle und in allen Einsatzbereichen akzeptierten Betriebssystems müssen vorrangiges Ziel einer auf Sicherheit ausgerichteten Strategie sein.

3.1.3 Anwendungsprogramme: Small is beautiful

Die Realität und die nötige allgemeine Akzeptanz von Sicherungsmaßnahmen machen es notwendig, Anwendungsprogramme einzusetzen, die nicht als sicher oder nicht als überprüfbar angesehen werden können, und eine ausreichende Sicherungswirkung des Betriebssystems vorauszusetzen.

Hier müssen andere spezifische Forderungen erhoben werden:

[120]) Zur Problematik der an Firmenstrategien statt an Spezifikationen und Sicherheitsanforderungen orientierten Betriebssystemwahl siehe z. B. Microsoft und Siemens erweitern Zusammenarbeit, in: Die Welt, 7. Februar 1998, Seite 17; Bayard, B. Aus dem Untergrund – Kommerzielle Anwendungen eines freien Betriebssystems, in: iX 10/97, Seite 44

- Die Einhaltung gewisser Randbedingungen soll während der Laufzeit durch das Betriebssystem überwacht und durchgesetzt werden. Dies setzt voraus, daß das als korrekt angesehene Laufzeitverhalten des Programmes so genau durch Regeln beschrieben werden kann, daß jede Abweichung von der korrekten Funktion vom Betriebssystem als Regelverstoß erkannt und verhindert werden kann; so zum Beispiel, wenn ein Textverarbeitungsprogramm schreibend auf eine Programmdatei zugreift oder eine Netzwerkverbindung zu einer fremden Maschine aufzubauen versucht. Dazu muß die Beschreibung möglichst eng gefaßt sein.

  Das setzt aber voraus, daß die Spezifikation und die Funktionsweise des Programmes bekannt und ausreichend genau dokumentiert sind.

- Weiterhin setzt es voraus, daß es überhaupt eine enge Beschreibung gibt. Derzeit ist ein Trend zu integrierten Officeumgebungen, die alle Funktionen in einem Programm bieten wollen, wie Textverbeitung, Grafikprogramm, Tabellenkalkulation, WWW-Browser, Telebankingclient, Kontenverwaltung, Sprachinterpreter, Multimediabasis, Betriebssystemerweiterung oder -ersatz, usw., und ähnlichen „Universalprogrammen" zu beobachten.

  Das Laufzeitverhalten einer solche Anwendung ist nicht exakt und schon gar nicht eng zu beschreiben. Wer etwa mit ein und demselben Programm in ein und derselben Instanz seine Geschäftspost schreibt, sein Konto verwaltet und im Internet „surft", kann auf Betriebssystemebene nicht regelbasiert die Offenlegung dieser Geheimnisse über das Internet verhindern.

  Notwendig sind also schlanke und genau auf eine Aufgabenstellung spezialisierte Programme, deren Laufzeitverhalten einfach, exakt und eng zu beschrieben ist.

Eine sichere Betriebssystemumgebung kann erheblich zur Erhaltung der Vertraulichkeit und der Integrität beitragen, indem es Aktionen verhindert, die mit der Beschreibung des Laufzeitverhaltens im Widerspruch stehen.

Die ordnungsgemäße Funktion des Programmes läßt sich jedoch nicht erzwingen. Ein Programm, das seine Funktion nicht erfüllt, kann normalerweise auch nicht mit Hilfe des Betriebssystems zur ordentlichen Funktion gebracht werden. Genauso wenig kann es dadurch an neue Betriebssystemversionen oder Laufzeitbibliotheken angepaßt oder zur Kooperation mit neuen Versionen anderer Programme gebracht werden.

Erfahrungsgemäß kommt es in der Praxis immer wieder vor, daß durch eine Aktualisierung von Teilen der Hard- oder Software eines funktionsfähigen Systems Anwendungsprogramme funktionsunfähig werden und ein Update nicht verfügbar oder zu teuer ist. Damit ist die Verfügbarkeitsbedingung verletzt.

Oft ist auch zu beobachten, daß zur Vermeidung dieses Effektes eine Aktualisierung unterlassen und das System um seiner Funktionsfähigkeit willen in einem bestimmten Zustand ‚eingefroren' wird. Dies birgt die Gefahr, daß entdeckte oder neu entstandene Lücken nicht geschlossen werden und die Sicherheit des Gesamtsystems nicht mehr gewährleistet ist.

Programme, bei denen die schnelle und billige Verfügbarkeit aktualisierter Versionen nicht gewährleistet ist, sind inakzeptabel, wenn nicht Wartungsverträge existieren, ausreichend Redundanz durch voll kompatible Konkurrenzprodukte besteht oder der Quelltext für eigene Änderungen und Neukompilierungen vorliegt.

3.1.4 Datenformate: Mehr Transparenz und Verfügbarkeit!

Bei praktisch jeder größeren Anwendung besteht das Bedürfnis der Datenübertragung – entweder zeitlich (Datenspeicherung) oder räumlich (Telekommunikation). Das bedeutet aber, daß es auch zeitlich oder räumlich getrennte Empfänger gibt. Ist der Empfänger nicht in der Lage, die Daten ihrem Sinn und Zweck entsprechend zu interpretieren, ist die Verfügbarkeit beeinträchtigt. Aufgrund der fehlenden unmittelbaren Wahrnehmbarkeit mit menschlichen Sinnen muß der Empfänger Syntax und Semantik der Daten kennen. Er muß das Datenformat lesen und interpretieren können. Kann er das nicht, sind die Daten nicht verfügbar, auch deren Authentizität und Integrität nicht mehr prüfbar.

Es muß also stets die Ausweichmöglichkeit auf ein verfügbares, voll kompatibles Alternativprogramm bestehen, damit eine verlustfreie Datenkonvertierung durchgeführt werden kann (was eine Standardisierung des Datenformates voraussetzt) oder aber das Datenformat muß so genau bekannt sein, daß man selbst ein Anwendungs- oder Konvertierungsprogramm anfertigen kann.

Dazu gehört auch, daß Konfigurationsdateien u. ä. im Klartext gespeichert sind und mit jedem gewöhnlichen Texteditor gelesen und geändert werden können.

Die Verwendung proprietärer undokumentierter Dateiformate ist vom Standpunkt der Sicherheit, der Qualitätskontrolle, der Wartbarkeit und der Datenpersistenz aus betrachtet höchst fragwürdig und bedenklich, denn sie gefährdet die Verfügbarkeit und erschwert die notwendige enge Beschreibung des Laufzeitverhaltens und der ein- und ausgehenden Informationen sowie die Einschätzung des Gefährdungspotential.

Im Gegensatz zu Maschinen und Geräten stellen Daten Werte von zeitlich nahezu unbegrenztem Charakter dar. Ihre Nutzung ist aber nicht nur an die Haltung der Daten selbst, sondern auch an die Haltung der syntaktischen und semantischen Interpretationsvorschriften gebunden.

Bereits die Notwendigkeit, zum Schreiben oder Lesen eigener Daten unter Kostenaufwand ein Programm kaufen zu müssen, kann als erfolgreicher Angriff gegen die Verfügbarkeit verstanden werden.

Insbesondere bieten undokumentierte Dateiformate den idealen Nährboden für „ Subliminal Channels"[121]), da sie die Überprüfung der Informationen und die Simulation der Schreib- und Lesevorgänge im Rahmen einer Überprüfung massiv erschweren, was in Bereichen, die Vertraulichkeit erfordern, eine hohe Gefahr darstellt.

Höchste Vorsicht ist geboten, wenn Datenformate zur Bindung an bestimmte Hersteller oder als Zwang zum „Upgrade" mißbraucht werden. Bestehen Hinweise darauf, daß Datenformate gezielt nicht offengelegt werden, um den Benutzer an ein bestimmtes Produkt zu binden, oder daß zwischen Programmversionen die Datenformate ohne plausiblen Grund und ohne befriedigende Konvertierungsmöglichkeit geändert werden um Benutzer zum Erwerb einer neuen Programmversion zu „nötigen", **ist von der Verwendung dieses Produktes dringend abzuraten.** Die Verfügbarkeit und die Kontrollierbarkeit des Laufzeitverhaltens sind so massiv gefährdet.[122])

3.1.5 Risikopotentiale aus der Kombination bestehender Technik

Die Kopplung verschiedener digitaler Techniken führt auch dazu, daß Sicherheitsprobleme in bisher abgeschotteten Bereichen nun Wirkung in anderen entfalten können. Ein Beispiel dafür sind computergesteuerte Telefonanlagen. Der damit verbundene Zuwachs an Funktionsvielfalt und deren auf spezifische Kundenbedürfnisse zugeschnittene Konfiguration wird durch eine softwarebasierte Steuerung ermöglicht, die ihrerseits zum Teil auf PCs realisiert wird. Damit eröffnen sich jedoch auch alle für solche Systeme typischen Manipulationsmöglichkeiten. Zusätzliches Sicherheitsproblem sind die softwaregesteuerten Endgeräte der Telefonanlage: Alle Leistungen solcher Telefone lassen sich von der Telefonzentrale aus fernsteuern, sogar auch durch Manipulationen von außen, sofern die Fernwartungszugänge zur Anlage nicht abgeschaltet oder auf sichere Weise konfiguriert sind. Hinzu kommt die Nutzung des D-Kanals in ISDN-Netzen zur Übermittlung illegaler Befehlsfolgen, mit denen der Prozessor der Telekommunikationsanlage manipulierbar ist[123]). Derartige Manipulationsmöglichkeiten führen dazu, daß beispielsweise durch von außen gesteuertes Anschalten des Freisprech-Mikrofons eines Telefons eine Raumüberwachung ebenso möglich wird wie ein Telefonieren unbefugter außenstehender Dritter auf Kosten des Anlagenbetreibers[124]). Die Kommunikation von PCs mit Hilfe eingebauter ISDN-Karten kann diese zusätzlich gegen Angriffe auf Datenbestände anfällig machen, die Schwächen der ISDN-Technik und in den Schutzsystemen der betroffenen Rechner ausnutzen.[125])

Ähnliche Probleme drohen auch durch digitale Vermittlungsstellen in öffentlichen Telekommunikationsnetzen. Bedeutsam ist, daß für derartige Kopplungsrisiken herkömmliche IT-Sicherheitsmaßnahmen nicht ausreichen. So hat die Bundesregierung hierzu erklärt, daß im Telekommunikationssektor „wegen der vermittlungsspezifischen Prozesse die in der Informationstechnik sonst üblichen Sicherheitsstandards nicht ausreichen. Von Anbeginn wurde daher die in den telekommunikationsspezifischen internationalen Standardisierungsgremien erarbeiteten Sicherheitsstandards [...] angewandt"[126]).

Die Entwicklung multimedialer Systeme hat zur Kombination einer Vielzahl bisher getrennter Geräte in einem unspezifisch als Multimedia-PC bezeichneten Gerät geführt. Dieser vereint heute vom Telefon bis zum Fernseher verschiedene Funktionen. Computer dienen im Gegensatz zu Radio, Telefon oder TV-Gerät aber keineswegs allein dem Empfang oder der Umwandlung von Signalen, sondern auch deren Speicherung und Veränderung. Ein multimedia-fähiger PC ist daher gleichzeitig ein digitales Sprachaufzeichnungsgerät, mit einer Kamera verbunden auch ein Videorecorder. Ist ein solcher PC mit einem Computernetz verkoppelt, werden derartige Aufzeichnungsmöglichkeiten vielfach von außenstehenden Dritten – und zudem unbemerkt – steuerbar. Damit führen solche und andere Einsatzmöglichkeiten zur Kompromittierung der Vertraulichkeit.

3.1.6 Risikopotentiale aus neu entwickelter Technik

Jenseits von herkömmlichen Computersystemen und deren Vernetzung führen noch stärker miniaturisierte Computer zu neuen Problemen. Während bislang sensitive Daten noch in Computersystemen gespeichert wurden, die wenigstens Buchgröße hatten, machen die Einsatzzwecke von Datenspeichern mit und ohne Prozessor bis hinunter zur Größe von wenigen Millimetern neue Ansätze zum Schutz der Vertraulichkeit notwendig. Die hierbei zu betrachtenden Technologien reichen von miniaturisierten PCs über Chipkarten und Smart-House-Systemen bis hin zu miniaturisierten Identifikations-Chips.

Chipkarten sind eine Form der Datenhaltung, die eigentlich für den Schutz der Vertraulichkeit vorteilhaft sind. Vordergründig bestimmt der Chipkarteninhaber über die Nutzung der Daten auf seiner Chipkarte – ohne sein Zutun scheint keine Datenübermittlung stattzufinden. Doch diese für die Sicherheit jener Technologie vorgebrachten Argumente sind nur begrenzt zutreffend. Den Besitzern von Chipkarten ist zumeist nicht möglich, die auf ihren Karten gespeicherten Inhalte selbst zu lesen. Sie transportieren auf diese Weise Daten über sich zu den Lesestationen im Vertrauen darauf, daß ihre Daten vertraulich behan-

---

[121]) Das bedeutet, daß Informationen durch geschicktes „Verstecken" in Datenströmen unbemerkt transportiert werden können.

[122]) Siehe auch: Web-Ärgernis: proprietäre Sites, in: c't 14/97, Seite 34

[123]) Fink, M. ISDN – Im Sinne der Nachrichtendienste?, in: CD Sicherheits-Management Nr 6/97, S. 52–59, (54))

[124]) Vgl. Schwarz, H. Der Spion, der durch das Telefon kommt, in: Süddeutsche Zeitung vom 23. Dezember 96, S. 16

[125]) Fink, a. a. O., S. 58

[126]) Antwort der Bundesregierung auf die Kleine Anfrage des Abg. Dr. Manuel Kiper „Sicherheit von digitalen Vermittlungsstellen der Telekom AG", Drs. 13/1110, Frage 5

delt werden. Monofunktionale Chipkarten lassen sich organisatorisch und technisch so gestalten, daß der Schutz der Vertraulichkeit in hohem Maße gewährleistet werden kann. Ein Schutz setzt bei multifunktionalen Chipkarten zum Schutz der Vertraulichkeit aber voraus, daß mit unterschiedlichen Zugriffsrechten versehene Datenbereiche strikt voneinander abgetrennt sind. Schon im Kartendesign ist somit darauf zu achten, welche Daten welchen Nutzergruppen bekannt werden dürfen. Bleibt dies unvollständig oder nicht angemessen, ist eine solche Chipkartennutzung mit einem nicht zu behebenden Systemfehler behaftet.

In allen Fällen aber muß der Karteninhaber darauf vertrauen, daß die Vertraulichkeit der ausgelesenen Daten bei ihrer Weiterverarbeitung beachtet wird. Der Chipkarteninhaber hat somit lediglich die Wahl, den Schutz der Vertraulichkeit seiner Daten durch die Auswahl derjenigen zu gewährleisten, denen er die Chipkarte zum Lesen gibt. Die Entwicklung eines kulturellen Bewertungsrahmens und Erfahrungsschatzes ist hier ein Element höherer IT-Sicherheit.

Der Vertraulichkeitsgewinn besteht also darin, daß durch das Auslesen einer Chipkarte die Gelegenheiten des Datentransfers transparent werden. Dem steht gegenüber, daß der Umfang der gespeicherten Daten, deren Nutzung und Weiterverarbeitung jedoch für den Karteninhaber nicht nachvollziehbarer wird wie bei herkömmlichen Systemen. Als zusätzliches Problem für die Vertraulichkeit kommt hinzu, daß die Chipkarte als Datenträger nicht länger organisatorisch geschützt und daher ein totaler Vertraulichkeitsverlust durch den Verlust der Chipkarte möglich ist. Diese Gefahr läßt sich nur durch geeignete Schutzvorkehrungen auf der Chipkarte mindern.

Die Fortentwicklung der Chipkartentechnologie, die die Leistung von PCs auf einer Chipkarte verfügbar machen kann, eröffnet potentiell weitgehende technische Lösungsansätze. Die Entwicklungspfade sind derzeit offen. Die Kopplung von Chipkarten und Java-Software kann dazu genutzt werden, zusätzliche Sicherheitsmechanismen einzusetzen. Sie kann aber auch dazu führen, daß Chipkarten zu einem zusätzlichen Einfallstor für manipulative Software werden.

Der Sicherheitsgewinn, der durch den bewußten Vorgang des Kartenaushändigens zum Auslesen von Daten erzielt werden kann, wird außerdem konterkariert durch die zur schnelleren und bequemeren Datenerfassung genutzten berührungslosen Lesegeräte. Diese Geräte aktivieren die Chipkarte, die für Markierungszwecke Tieren, Kleidungsstücken und Waren aller Art, versuchsweise auch Personen implantiert werden sollen, durch ein Hochfrequenz-Feld, mit dem ein ebenso schnelles Auslesen möglich ist wie bei einem herkömmlichen Lesegerät. Dabei wird weder transparent, welche Daten übermittelt werden, noch, wann dies geschieht. Überdies lassen sich entsprechend ausgestattete Chipkarten nicht gegen berührungsloses Auslesen schützen, da die verfügbare Technologie keine nutzerseitigen Inaktivierungsmeachanismen bietet.

Ähnliche Probleme folgen auch aus dem Einsatz von körperbasierten Datenübermittlungssystemen, sogenannten Body-LANs oder Personal Area Networks, die die Leitfähigkeit des Körpers zur Datenübermittlung nutzen und etwa bei einer Begrüßung per Handschlag Daten austauschen. Was als elektronischer Austausch von Visitenkarten-Daten heute vorgestellt wird, gefährdet in weiteren Ausbaustufen die Vertraulichkeit, wenn auf diese Weise Daten über Konsumbedürfnisse, aber auch die physische Befindlichkeit übermittelt werden.

Aus der Sicht der IT-Sicherheit ist dies zum Schutz der Vertraulichkeit dann nicht hinnehmbar, wenn die genutzten Chipkarten und andere genannte Systeme sensitive Daten enthalten und zur Verfügung stellen. Sensitive Daten von Chipkarten oder ID-Tags können sowohl personenbeziehbare, als auch produktions- und herstellerspezifische Daten sein. Implantierbare Blutwertanalysatoren können Diabetes-Patienten helfen, aber auch vertrauliche medizinische Daten unkontrolliert zugreifbar machen.

Gefahren für die Vertraulichkeit ergeben sich schließlich aus dem als Endpunkt vernetzten Computereinsatzes gesehenen ubiquitären Computing, dem Einsatz von kleinsten Computern, die in fast allen Gegenständen des täglichen Lebens eingebaut sind. Die Gefährdungspotentiale werden deutlich bei „Intelligenten Häusern", die in ihrer Nutzung von Computern und Sensoren für die Steuerung aller Funktionen eines Hauses als heute bereits verfügbares Beispiel für Gefahren des ubiquitären Computing allgemein dienen können.

Die vollautomatisierte Steuerung von Heizung, Licht und anderen Versorgungsleistungen, der Zugangskontrolle und der Haussicherheit in „Intelligenten Häusern" machen von Seiten der IT-Sicherheit Vorkehrungen gegen einen Systemausfall vordringlich. Derartige Installationen sind jedoch mit Anbindungen an die Außenwelt ausgestattet, um Bewohnern oder Nutzern wie Technikern aus unterschiedlichen Gründen ein Fernwirken und -warten, aber auch Energieversorgungsunternehmen eine Verbrauchsmessung und voraussichtliche -abschätzung zu ermöglichen. Für den Schutz der Vertraulichkeit ist daher bedeutsam, daß nicht anhand der Daten über den Energieverbrauch in Labors und viele ähnliche Parameter Daten offenbart werden, die beispielsweise der Industriespionage wesentliche neue Mittel in die Hand geben können oder die Lebensgewohnheiten und Details des Privatlebens der Bewohner unzulässigen Einblicken öffnet. Mit globalen Ortungssystemen einerseits und der Ausweitung der Internetkompatiblen Anbindung von Geräten an Rechnernetze andererseits erhält dieses Problem eine zusätzliche Dimension. Zum Schutz der Vertraulichkeit wären hier schon auf unterster technischer Ebene Maßnahmen ebenso notwendig wie umfassende Schutzkonzepte.

3.2 Schutzstrategien als „Möglichkeiten der Technik"

Wird die Frage nach den „Möglichkeiten der Technik" notwendigerweise und konsequent dahinge-

hend verstanden, daß nach den heutigen, im Alltag der IT-Sicherheitspraxis verwendeten technischen Ansätzen zur Reduktion von Schadensmöglichkeiten gefragt wird, so hat sich dieses vorrangig am Profil alltäglicher Schadensfälle auszurichten. Da es nicht angemessen erscheint, die Frage nach den „Möglichkeiten der Technik" zum Abbau von Schadenspotential allein an technischen Vermeidungsstrategien festzumachen – die so isoliert zwar definierbar sind, aber der Komplexität der Risiken nicht gewachsen sind – werden im folgenden schwerpunktmäßig und beispielhaft jene Sicherheitsmaßnahmen skizziert, die, auch in ihrer wechselseitigen Verstärkung, in der heutigen IT-Sicherheitspraxis – trotz unterschiedlichen Grades der Ausgestaltung – zunehmend anzutreffen sind:

3.2.1 Geprüfte IT-Sicherheit

Es ist zunehmend unverzichtbar, die technische Sicherheit von IT-Systemen von unabhängigen und fachkundigen Dritten prüfen und zertifizieren zu lassen.

„Evaluation" ist zum wichtigen Baustein beim Aufbau und Betrieb von Infrastruktur-Einrichtungen der Informationsgesellschaft geworden. Längst gibt es eine Reihe von Instituten und Firmen, die Sicherheitsevaluation als Dienstleistung anbieten. Immer mehr Hersteller lassen ihre Systeme – ob Chipkartenbetriebssystem oder PC-Sicherheitssoftware – nach anerkannten Kriterien wie den im Sicherheitsbereich wichtigen ITSEC, den im Finanzbereich relevanten ZKA-Kriterien („Zentraler Kreditausschuß") oder nach anderen Kriterienwerken evaluieren. Die Hersteller nehmen die Zertifizierung als Chance einer zusätzlichen Qualitätskontrolle wahr, sie erhoffen sich dadurch einen Marktvorteil gegenüber den Konkurrenten und überhaupt dem Marktzugang beim Kunden. Viele Anwendungsanbieter wie Banken oder große Telekommunikationsunternehmen verlangen von ihren Betrieben die unabhängige Evaluation ihrer Produkte. Keine Bank würde mittlerweile einem Chipkartenhersteller für eine Geldkartenanwendung auch nur eine Chipkarte ohne unabhängige Prüfung abnehmen.

Die Evaluation bietet ein Maß, inwieweit der versprochenen IT-Sicherheit getraut werden kann, beispielsweise um Fehlfunktionen zu entdecken.

Kriteriengestützte Evaluationen von IT-Sicherheit geben Auskunft über die Vertrauenswürdigkeit, die man „objektiv" in die technische Sicherheit eines konkreten Produktes haben kann. Sie versprechen die Meßbarkeit von IT-Sicherheit. Das europäische Kriterienwerk, das diese Prüfung erlaubt, ist die 1991 vorgelegte ITSEC, die „Information Technology Security Evaluation Criteria" – *„Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik"*.

Sie bieten sieben Stufen der Vertrauenswirklichkeit: Je höher diese Stufe ist, um so tiefer gehende und höherwertige Dokumente muß der Hersteller für die Evaluation bereitstellen.

Die meisten zertifizierten Produkte pendeln momentan bei E2/E3 – eine langsame Verschiebung nach E4/E5 wird erwartet. Nach E6 wurde in Europa noch kein Produkt evaluiert- Bislang wurde in Deutschland und Europa vorwiegend nach ITSEC evaluiert und vom BSI zertifiziert.

Die ITSEC gilt allerdings als abstrakt und bürokratisch. Sie sind jetzt von den CC, den „Common Criteria for IT-Security Evaluation" abgelöst worden.[127])

Die ITSEC umfaßt vorrangig die Bewertung technischer Sicherheitsmaßnahmen. Organisatorische, personelle, administrative Maßnahmen stehen nicht im Mittelpunkt der Analyse, werden aber berücksichtigt. Das Kriterienwerk ist so allgemein gehalten, daß sowohl Hardware als auch Software evaluierbar ist. Jede ITSEC-Evaluation soll objektiv und unvoreingenommen sein – darauf sind die deutschen vom BSI akkreditierten Prüfstellen geprüft und verpflichtet.

Die konkrete Prüfung eines Produktes (oder eines Systems) nach ITSEC erfolgt auf Initiative des Hersteller bzw. eines seiner (potentiellen) Kunden – auf jeden Fall freiwillig.

Die Grenzen des Zertifikats sind deutlich: Es wird bescheinigt, daß die vom Hersteller definierten Sicherheitsziele mit der zur Verfügung gestellten Sicherheitsfunktionalität erreicht werden. Ob die Vertrauenswürdigkeit für konkrete Einsatzgebiete ausreicht oder nicht, muß in jedem Einzelfall vom Kunden geprüft werden. Es ist auch stets zu prüfen, wie alt das Zertifikat ist – bei zu alten Produkten haben es Angreifer vielleicht in der Zwischenzeit gelernt, die Sicherheitsbarrieren zu umgehen.

Das (BSI-)Zertifikat gilt nur für die „eine" evaluierte Version der Software. Bei Versionsänderungen des Produktes gilt das Zertifikat nicht mehr – es muß eine Re-Evaluation durchgeführt werden.

3.2.2 IT-Grundschutz als Bestandteil eines IT-Sicherheitskonzeptes

Ziel des Grundschutzes im Rahmen eines IT-Sicherheitskonzeptes ist es, durch die Anwendung von geeigneten infrastrukturellen, organisatorischen, personellen und technischen Standardsicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den mittleren Schutzbedarf angemessen und ausreichend ist und als Grundlage für hochschutzbedürftige IT-Systeme bieten kann.

Kernidee des IT-Grundschutzes ist die Anwendung eines auf typische IT-Konfigurationen mit mittlerem Schutzbedarf zugeschnittenen Katalogs administrativer und technischer IT-Sicherheitsmaßnahmen. Die Standardsicherheitsmaßnahmen des IT-Grundschutzes bilden die Mindestanforderungen für den Betrieb typischer IT-Systeme. Sind sie nicht realisiert, so ist davon auszugehen, daß das betroffene System meist fundamentale Schwachstellen besitzt. Für IT-Systeme, die einen höheren Schutzbedarf besitzen, sollten allerdings mittels detaillierter Analysen die über den IT-Grundschutz hinaus notwendigen wirkungs-

[127]) Vgl. hierzu den Abschnitt 4.1.4.1

volleren IT-Sicherheitsmaßnahmen individuell ermittelt werden.

Entwicklungsgrundlage des IT-Grundschutzes ist eine pauschalisierte Gefährdungslage. Bei der Formalisierung der Maßnahmenempfehlungen zu bestimmten Komponenten werden die typischerweise auftretenden Gefährdungen und deren Eintrittswahrscheinlichkeiten berücksichtigt. Gleichzeitig wird versucht, mit standardmäßig vorhandenen oder leicht umsetzbaren Maßnahmen dieser Pauschalgefährdung zu begegnen. Dabei wird zugrunde gelegt, daß das betrachtete IT-System einen mittleren Schutzbedarf hat – was für etwa 80 Prozent der IT-Anwendungen ausreicht.

3.2.3 IT-Sicherheitsausbildung

Das Gebiet der IT-Sicherheit (und des Datenschutzes) als Studienschwerpunkt für Informatik-Studenten wird in Deutschland nicht obligatorisch angeboten; es kann aber davon ausgegangen werden, daß es ein hohes Interesse an Datenschutzfragen und IT-Sicherheitsthemen gibt. Dies wohl auch, weil in der Berufspraxis und in der Forschung ein steigender Bedarf an IT-Sicherheitsfachleuten zu verzeichnen ist. Um beispielsweise Sicherheitsinfrastrukturen kompetent gestalten und aufbauen zu können, sind Sicherheitsexperten mit einer soliden Ausbildung in den technischen, organisatorischen, aber auch den rechtlichen und sozialen Aspekten der IT-Sicherheit erforderlich.

Aufgrund der Vielfältigkeit der Anforderungen zur Ausbildung von Sicherheitsexperten einerseits und zur Sensibilisierung im Thema IT-Sicherheit andererseits ist ein eigenständiges IT-Sicherheitscurriculum erforderlich. Dieses hätte neben der Vermittlung von Kompetenzen etwa auf dem Gebiet der Risikoanalyse und Sicherheitsplanung, der Unfallaufklärung, dem Entwurf sicherer Systeme und dem Datenschutz auch die Entwicklung eines IT-Sicherheits-Managements, sowie die Fertigkeit zur Definition spezifischer Gefährdungsszenarien zu vermitteln. Damit wären dann auch Kenntnisse zu vermitteln zur Festlegung einer (institutions-)spezifischen IT-Sicherheitspolitik sowie zur Definition verbindlicher IT-Sicherheitsziele.

3.2.4 Schutz vor Angriffen aus dem Internet

Das Problem des Schutzes vor Angriffen oder der Abwehr von Bedrohungen aus offenen Netzen – wie dem Internet – ist im Prinzip nicht gelöst, was aber der wachsenden Begeisterung der Menschen in der Benutzung des Internet offenbar nicht schadet.

Die Nutzung des Internets wächst rasant. Ein Briefgeheimnis ist im Netz völlig unbekannt und es kann allenfalls von einem Postkartengeheimnis gesprochen werden.

Durch die zunehmende Kommerzialisierung wird der herkömmliche Hacker, dessen Motivation in erster Linie Neugierde ist, durch professionelle Angreifer ersetzt.

Den wichtigsten Schutz gegen Angriffe bieten die umfassende Information über Gefährdungen und die Aufnahme von Sicherheit als gleichrangiges Ziel neben Funktionalität und Leistungsfähigkeit bei der Entwicklung und beim Kauf eines Rechnersystems.

Firewall-Computer

Firewalls sind Computer, die den Datentransfer zwischen zwei Netzen kontrollieren. Durch technische und administrative Maßnahmen wird dafür gesorgt, daß jede Kommunikation zwischen den beiden Netzen über den Firewall geführt werden muß. Auf dem Firewall sorgen Zugriffsrechte und Protokollauswertungen dafür, daß das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt werden. Ein Angreifer muß also den elektronischen Kontrollposten „Firewall" unerkannt überwinden, um etwa über das Internet in ein Intranet einzudringen, um dort an die IT-Systeme und deren Daten heranzukommen.

3.2.5 Schutz digitalisierten geistigen Eigentums

Die Enquete-Kommission hat sich in ihrem Zwischenbericht „Neue Medien und Urheberrecht" eingehend mit den Fragen zum Schutz digitalisierten geistigen Eigentums beschäftigt und Empflehlungen hierzu ausgesprochen.

Ohne die Möglichkeit der Kontrolle über den Zugriff auf Informationen, die Art der Verwendung von wertvollen, schützenswerten Daten und die Möglichkeit des Urheberrechtnachweises sowie des damit verbundenen Rückfluß von Tantiemen bestehen von Seiten der Informationsanbieter berechtigte Bedenken, ihre wertvollen Informationen über Netzwerke anzubieten. Es liegt in der Natur der digitalen Daten und Datenübertragung, daß sich das Anfertigen von Kopien nur schwer oder fast gar nicht verhindern läßt.

Als das eleganteste und sicherste technische Verfahren zum Schutz digitalisierten geistigen Eigentums wird das *Watermarketing* als Markierungsverfahren angesehen. Hier wird ein digitales Wasserzeichen in die Daten integriert. Diese Markierung ist visuell und auch mit Hilfe statistischer Tests nicht wahrnehmbar, kann jedoch von einer autorisierten Person mit Hilfe eines geheimen Schlüssels gelesen oder verändert werden. Das digitale Wasserzeichen kann jede beliebige Information enthalten, z. B. den Namen des Urhebers, den Zeitpunkt der Erstellung der Daten oder den Namen des Käufers.[128])

3.2.6 Technische Schutzstrategie: Kryptographie

Mit Hilfe kryptografischer Verfahren werden Inhalte von Dokumenten so verschlüsselt, daß sie von Seiten eines unberechtigten Dritten nicht erkannt werden können. Nur wer im Besitz eines passenden Schlüssels ist, kann den verschlüsselten Text wieder entschlüsseln. Damit wird mit Hilfe von Verschlüsselungsverfahren das IT-Sicherheitsziel „Vertraulichkeit" erreicht.

[128]) Vgl. hierzu Enquete-Kommission „Neue Medien in Wirtschaft und Gesellschaft" (Hrsg.) „Neue Medien und Urheberrecht" (1997)

Die Methodenlehre zur Geheimhaltung von Nachrichten ist nicht neu; sie hat eine jahrtausendelange Tradition.[129]) Allerdings wurde die über lange Zeiten bei symmetrischen Verschlüsselungsverfahren vorherrschende Vorstellung, daß Sender und Empfänger im Besitz desselben Schlüssels sein müßten, seit Mitte der 1970er-Jahre durch einen Paradigmenwechsel abgelöst. Die Mathematiker M. Diffie und M. Hellman stellten ihr sogenanntes asymmetrisches Verschlüsselungsverfahren vor, bei dem ein *öffentlicher* und ein *privater* Schlüssel erzeugt und verwendet wird.[130])

Bei diesem Verfahren verwendet der Sender A den öffentlichen Schlüssel vom Empfänger B, um seine Nachricht zu verschlüsseln.

Der Empfänger B empfängt die vom Sender A verschlüsselte Nachricht und entschlüsselt diese mit seinem privaten Schlüssel.

„In einem asymmetrischen Verschlüsselungsschema kann jeder einem Empfänger eine verschlüsselte Nachricht schicken – ohne irgendeine Geheiminformation zu besitzen. Aber nur der Empfänger kann die Verschlüsselung rückgängig machen. Mann kann sich vorstellen, daß der Sender die Nachricht in den „Briefkasten" des Empfängers wirft. Das Einwerfen der Nachricht in den Briefkasten entspricht der Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers: Jeder Teilnehmer kann das machen. Nur der Empfänger ist aber in der Lage, mit seinem geheimen Schlüssel den Briefkasten zu öffnen und die Nachricht zu lesen."[131])

Ein mit PGP verschlüsseltes Dokument

-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 5.0i for non-commercial use
MessageID: H7oZLwStxV7Z1d6Vkk49KaiFNEgbp6mQ
ANQR1DBwU4DYtTYsQ0jiZ0QCACz4cK+mYaaHjV2d0XjY0PoKfFTiGmyO
HPhhyJbbCT6kVP1dmqADufu30cTH95mdyeLe4ajp6uqhsmEXBNERqqc6UlP
n0nznxPtm2/IsD1+GXQnLAURm8AtG+DaZHJdYv1CKPH5ZbzJwAXiXyBcU
rUkuBU2LivDRysJ1k1QQcJmF9eC1n3nb1dgsWp9oER9xnZrh5XIkq8BxL9pmv
ItCCrX9C1ej13+xFlvyNG
rJdF67k0UsQF4RoGKfj78mFz56H/M/TyD/i5A76dEEdcleaz5J5eo2GVxIKJxwK
Op7PXnk3PC+018yA9Zl+JRgAwyOVel4mtbeKG+h51BEPIRVRrB/9AmRjFdJi
EjgUp6X3+PNTWdFYKO7qa0a23Tpa6/r1gFio8ezi0TodOcTQwI8fo4MwxEk+L
3XJvsKHtTVdgKhiVvoTvT2eo5mOSTAJTut7jxS5fh2b02lLTZx+JLfd5hkrhON

Das asymmetrische Verschlüsselungsverfahren hat gegenüber dem symmetrischen Verschlüsselungsverfahren den offensichtlichen Vorteil, daß nur noch der private Schlüssel vom Inhaber geheimgehalten werden muß und das Problem einer vertraulichen Schlüsselverteilung zwischen den Teilnehmern entfällt.

Auf der Grundlage dieses technischen Verfahrens ist der Aufbau eines öffentlichen Schlüsselsystems (Public-Key-Verfahren) möglich, bei der z. B. eine bundesbehördlich lizensierte dritte Partei – die sogenannte *Trusted Third Party* (TTP) – die öffentlichen Schlüssel lizensiert[132]) und registriert. Die Nutzer können dann in einem von der TTP herausgegebenen „elektronischen Schlüsselbuch" die öffentlichen Schlüssel anderer Netznutzer abfragen. Private Schlüssel werden entweder als passwortgeschützte Datei auf der Festplatte des Computers oder auf einer ebenfalls passwortgeschützten Chipkarte gespeichert.

Der Nachteil asymmetrischer Verschlüsselungsverfahren ist, daß sie bei großen Datenmengen und Datenübertragungsgeschwindigkeiten – etwa umfangreichen Bilddokumenten oder Videokonferenzen – zu langsam sind. Die Lösung ist eine Kombination von Public-Key- und Private-Key-Verfahren. Dabei generiert Teilnehmer A einen privaten Schlüssel exklusiv für einen anwendungsbezogenen Fall – den sogenannten Session-Key. Dieser Session-Key wird vom Teilnehmer A mit dem öffentlichen Schlüssel vom Teilnehmer B verschlüsselt und dann an Teilnehmer B geschickt. Dieser entschlüsselt mit seinem privaten Schlüssel den Session-Key und ist somit im Besitz desselben Schlüssels wie Teilnehmer A.[133])

„Die sichere und schnelle Ver- und Entschlüsselung wird durch die Kombination von RSA[134]) und DES (**D**ata **E**ncryption **S**tandard)[135]) Verfahren erreicht. Das DES Verfahren entspricht dabei einem 1977 von der US-Regierung definierten ANSI Standard und eignet sich aufgrund der hohen Verarbeitungsgeschwindigkeit besonders für die Ver- und Entschlüsselung von großen Dateien. Die Verbindung mit dem RSA Verfahren garantiert, daß verschlüsselte Dateien nicht von unberechtigten Dritten, sondern nur vom berechtigten Empfänger entschlüsselt werden können."[136])

Die auf mathematischen Algorithmen aufbauenden und in Softwareform angebotenen anerkannten Ver-

---

[129]) Vgl. Beutelspacher, A. et al., Moderne Verfahren der Kryptographie, Braunschweig, 1998 S. 10

[130]) ebenda, außerdem vgl. Diffie, W.; Hellmann, M. E., New Dirctions in Cryptogphy, in: IEEE Transactions on Information Theory (6. November 1976) S. 644–655;

[131]) Beutelspacher, A. et al., Moderne Verfahren der Kryptographie, Braunschweig, 1998 S. 10

[132]) „Lizensieren" bedeutet, daß die TTP die registrierten öffentlichen Schlüssel mit ihrem privatem Schlüssel signiert.

[133]) Vgl. Asymmetrische Kryptosysteme, in: http://www.ix.de/ix/9512132/asym.html

[134]) Weit verbreitetes algorithmenbasiertes asymmetrisches Verschlüsselungsverfahren nach Rivest, Shamir und Adleman. Dieses Verfahren gilt bis heute als nicht korrumpierbar, d. h. es garantiert eine sichere Authentifizierung von Kommunkationspartner, die untereinander vertrauliche Daten transferieren.

[135]) Beim DES-Verfahren verfügen Absender und Empfänger einer Datei über denselben Schlüssel zur Ver- und Entschlüsselung. Es handelt sich dabei um ein symmetrisches Konzept.

[136]) Hähn, H.-J., Sicherheit bei der DFÜ im Gesundheitswesen, in: Glade, Reimer, H., Struif, B. Digitale Signaturen & Sicherheitssensitive Anwendungen. Wiesbaden, 1995, S. 40

schlüsselungsverfahren bieten einen verhältnismäßig sicheren[137]) und effizienten Weg zur Erreichung des IT-Sicherheitsziels „Vertraulichkeit". Die entsprechende Software ist im Internet weit verbreitet. So kann beispielsweise die neuste Version (5.0) der bekannten **P**retty-**G**ood-**P**rivacy-Software über die internationale Homepage von PGP bei kommerzieller Nutzung gegen einen geringen Preis bzw. bei privater Nutzung kostenlos bezogen werden.[138]) Für die öffentlichen PGP-Schlüssel existiert eine weltweit verteilte Key-Server-Infrastruktur, über die öffentliche Schlüssel andere Teilnehmer abgefragt werden können.[139])

3.2.6.1 Steganographie

Der Begriff *Steganografie* bedeutet entsprechend seines griechischen Ursprungs *verdecktes Schreiben.*[140]) Steganographische Verfahren verstecken Nachrichten in Bild- oder Textdateien.[141]) Eine so verschlüsselte Nachricht kann nicht als verschlüsselt erkannt werden.

Steganographische Verfahren arbeiten mit „unterschwelligen Kanälen" *(subliminal channels).* So kann in den niederwertigsten Bits der Farbe Rot/Grün/Blau eines Bildes ein verborgener Kanal untergebracht werden.[142])

Beispiel: Gegeben ist ein 24-bit Bild mit 1024 × 768 Pixel. Dies entspricht einem üblichen Format von Satelliten-Bilder und anderen hoch auflösenden Bildformaten. Diese Bild produziert eine Datei mit über 2 Mbyte Größe. (1024 × 768 × 24/8=2359296 Bytes) Alle Farbvariationen dieses Bildes leiten sich von den Primärfarben Rot, Grün und Blau ab. Jede Primärfarbe repräsentiert 1 Byte (8 Bits). 24-Bit- Bilder nutzen 3 Bytes in jedem Pixel. Wenn Information im niederwertigsten Bit (last significant Bit) eines jeden Bytes gespeichert wird, können 3 Bits Information in jedem Pixel des Bildes gespeichert werden.[143]) Dies bedeutet, daß in diesem Bild eine Nachricht mit einer Größe von circa 290 Kbyte versteckt werden kann. ([1024 × 768 × 3]/8)

Steganographische Verschlüsselungsverfahren[144]) sind eine wichtige ergänzende Option zu symmetrischen und asymmetrischen Kryptoverfahren. So kann etwa in einem symmetrischen Verfahren der geheime Schlüssel in einer steganografisch verschlüsselten Datei zwischen den Kommuniaktionspartnern ausgetauscht werden.

3.2.7 Technische Schutzstrategie: Digitale Signatur

Im vorausgegangenen Abschnitt ist dargestellt worden, wie auf der Basis eines asymmetrischen Verschlüsselungsverfahrens mit dem öffentlichen Schlüssel verschlüsselt und mit dem privaten Schlüssel entschlüsselt wird. Die Funktion des privaten Schlüssels beschränkt sich aber nicht nur auf das Entschlüsseln. Vielmehr kann mit ihm auch ein digitales Dokument elektronisch signiert werden. Eine mit dem privaten Schlüssel ausgeführte digitale Signatur sichert die Authentizität und Integrität des digitalen Dokuments. Obwohl Verschlüsselung und Digitale Signatur auf derselben technischen Plattform beruhen, erfüllen sie verschiedene Sicherheitsfunktionen. Ein digital signiertes Dokument ist nicht verschlüsselt, sondern in Hinblick auf seine Integrität und die Authentizität seines Unterzeichners gesichert und dokumentiert.

Digital signiertes Dokument

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Sehr geehrter Herr Müller,

unter Bezugnahme auf unser letztes Telefongespräch möchte ich Ihnen
folgendes Angebot vorlegen.

12 PCs der Kategorie A, incl. Installierung

45.200 DM.

Bei Abnahme von mehr als 12 PCs der Kategorie wird ein Rabatt von
2,75 % auf die Endsumme gewährt.

Mit freundlichen Grüßen

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 5.0i for non-commercial use
Charset: noconv

iQA/AwUBNS+LDqDUIu1CCBD+EQKHHQCfe3Br+
NW/bOGSyuwB9GFflS8/JrcAn3dG
ahRx1ZsjrHOuptlP6NLrapfX
=gpMI
-----END PGP SIGNATURE-----

Dabei kann die Digitale Signatur mit einem gläsernen Tresor verglichen werden. „Nur der Eigentümer des Tresors besitzt den Schlüssel zum Öffnen, nur er kann also Nachrichten im Tresor deponieren. Daher

---

[137]) Die Sicherheit kryptographischer Verfahren, wie z. B. beim weitverbreiteten RSA-Verschlüsselungsverfahren, ist relativ zur Rechnerleistung, die einem Angreifer im Verhältnis zur verwendeten Schlüssellänge zur Verfügung steht. Im Jahr 1992 wurde der Aufwand für Hardware zum Knacken eines 512-Bit-Schlüssel auf 8,2 Millionen Dollar geschätzt. Bedingt durch den Preisverfall für Rechnerleistung würden die Kosten heute wesentlich geringer sein. (Vgl. „Asymmetrische Kryptosysteme" in http://www.ix.de/ix/9512132/asym.html). Dieser Entwicklung steht gegenüber, daß in dieser Zeit sowohl die zur Verfügung stehenden Schlüsselängen gewachsen sind als auch verbesserte Algorithmen entwickelt worden sind. So bietet die 5.0-Version von PGP die Generierung von 512-Bit-Schlüsseln aufwärts an, wobei auch Schlüssellängen von mehr als 1000 Bit zur Verfügung stehen, die als sehr sicher gelten.

[138]) Siehe: http://www.pgpi.com

[139]) Siehe: http://www.pgp.net/pgpnet/

[140]) Vgl. Johnson, N. F. Steganography, in: http://patriot.net/~johnson/html/neil/stegdoc/sec201.html

[141]) Das Verstecken einer Nachricht in einer Text- bzw. Bilddatei ist das übliche Verfahren der Steganographie. Allerdings muß beachtet werden, daß auch alle anderen digtalen Dateiformate – wie z. B. Sound-Dateien – sich grundsätzlich für steganographische Verfahren eignen.

[142]) Beth, T. Schriftliche Stellungnahme zur Öffentlichen Anhörung der Enquete-Kommission „Neue Medien in Wirtschaft und Gesellschaft" am 12. Mai 1997

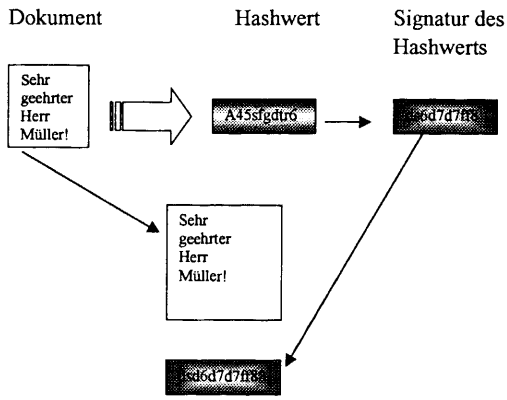
[143]) Vgl. Johnson, N. F. Steganography, in: http://patriot.net/~johnson/html/neil/stegdoc/sec201.html

[144]) Einen guten Überblick über existierende Verfahren gibt http://isse.gmu.edu/~njohnson/Security/stegtools.html

muß man davon ausgehen, daß jede Nachricht im Tresor nur von dessen Eigentümer stammen kann. Eine Nachricht wird also durch Einschließen in den gläsernen Tresor signiert und kann dann von jedem anderen Teilnehmer verifiziert werden."[145])

Die Verifikation einer digitalen Signatur ist mit dem öffentlichen Schlüssel des Anwenders möglich, ohne daß von dem öffentlichen Schlüssel auf den privaten Schlüssel geschlossen werden könnte.[146])

Die Digitale Signatur arbeitet mit der sogenannten Hash-Funktion, bei dem aus dem Inhalt eines Dokuments mit Hilfe eines Komprimierungsalgorithmus eine Liste von Buchstaben und Zahlen – der sogenannte Hashwert – gewonnen wird. Diese Liste ist eine Kurzkennung des Dokuments. Mit dem privaten Schlüssel wird dieser Hashwert signiert und diese Signatur des Hashwertes dem Dokument hinzugefügt. Der Empfänger des so signierten Dokuments kann nun diese digitale Signatur mit dem öffentlich Schlüssel verifizieren.



Quelle: Beutelspacher, A. et al. (1998) S. 18

Kryptographische Verschlüsselungsverfahren und Digitale Signaturen sind heute die wichtigsten Instrumente des IT-Selbstschutzes in Bezug auf die Sicherheitsziele Vertraulichkeit, Integrität und Authentizität.

4. Bausteine einer modernen Sicherheitsinfrastruktur

4.1 Leitgedanke: Abwägung von Schutzwürdigkeit, Gefährdungspotential und Aufwand

IT-Sicherheit ist vergleichbar mit der der Bedeutung, die der Sicherheit und Verfügbarkeit anderer infrastruktureller Ressourcen, wie etwa Elektrizität oder Telekommunikationsverbindungen, in unserer technisierten Gesellschaft beigemessen wird. Mit der Breite der Anwendungen weitet sich das Verständnis von IT-Sicherheit aus.

Unter der Annahme, daß Anbieter und Nutzer gleichermaßen die Sicherheitsinvestitionen ihren wachsenden Sicherheitsbedürfnissen anpassen, ist die Rolle des Staates in IT-Sicherheitsfragen auf Kerngebiete beschränkt. Ihm kommt die Aufgabe zu, den rechtlichen Rahmen zu setzen und auf internationaler Ebene eine Koordinierung von Sicherheitsbemühungen zu unterstützen. Durch geeignete Mittel zur unabhängigen Beratung der Allgemeinheit, zur Erforschung sicherer IT-Systeme und zur frühzeitigen Abschätzung gesellschaftlicher Auswirkungen hat er außerdem die Möglichkeit, das Vertrauen in die IT und deren Sicherheit zu erhöhen. Auf der normativen Ebene kann sich der Staat dann darauf beschränken, notwendige Anpassungen der technischen Überwachung an die Bedingungen der Informationstechnik vorzunehmen, aber auch durch IT-Einsatz entstehende Lücken in Haftungsregelungen zu schließen sowie den Verbraucherschutz informationstechnisch weiterzuentwickeln.

Bei der technischen Überwachung von Anlagen mit hohen Sicherheitsanforderungen, wie Kernreaktoren und Flugzeugen, zeigt sich die Herausforderung zur Lösung IT-spezifischer Probleme sehr deutlich. Die für die Steuerung der Anlagen nunmehr als Hard-/Softwaresysteme ausgebildeten Steuerungen müssen hinsichtlich der Sicherheit den gleichen Maßstäben unterworfen werden wie die bisher eingesetzten elektronischen Geräte und Systeme. Für die Sicherheitsüberprüfung sind naturgemäß andere Verfahren einzusetzen, insbesondere sind für die Prüfung sicherheitsrelevanter Software (auch High-Integrity-Software) rigorose Prüfungen anzusetzen. Hervorzuheben ist jedoch, daß hochsichere Software entsprechend dem heutigen Stand von Wissenschaft und Technik nach strengen formalen Vorgaben entwikkelt wird und ebenso geprüft wird. Bisherige Erfahrungen in der Luft- und Raumfahrt zeigen, daß es definitiv möglich ist, Hard-/Softwaresysteme zu entwickeln, die den bisherigen elektronischen Systemen in der Sicherheit mindestens ebenbürtig, wenn nicht überlegen sind. In der Tat sind etwa die in der Flugzeugindustrie aufgetretenen Fehler zum weitaus überwiegenden Teil darauf zurückzuführen, daß die Spezifikation mangelhaft war, d.h. das Steuerungssystem hat versagt, weil es für eine spezielle Situation nicht ausgelegt war (z.B. Mangel in der Landeklappensteuerung bei glitschiger Fahrbahn). Insoweit sind z.B. in der Kerntechnik die Auslegungsprinzipien und Sicherheitsanforderungen auch für softwaregetragene Systeme durch bestehende Regeln und Richtlinien, (z.B. Leitlinien der Reaktor-

[145]) Vgl. Beutelspacher, A. et al. Moderne Verfahren der Kryptographie. Braunschweig, 1998, S. 17
[146]) ebenda, S. 16

Sicherheitskommission, KTA-Regeln) festgelegt. Spezifische Prüfmethoden für Hard-/Softwaresysteme sind ausreichend vorhanden, allerdings haben sich feste Regeln für den Umfang ihrer Anwendung in den Prüfverfahren national und international noch nicht etabliert. Eine den herkömmlichen Prüfregularien vergleichbare verbindliche Prüfung von Software ist daher anzustreben.

Ein ganz generelles Problem ist der zweckmäßige Umfang des Einsatzes automatischer Steuerungssysteme. Dazu wird in zum Teil sehr umfangreichen Untersuchungen in der Planungsphase, die insbesondere Fragen des menschlichen Potentials für die Führung von Prozessen einschließt, untersucht, welche Aufgaben man besser den Menschen überläßt und welche Aufgaben besser durch Automatiken bewältigt worden. Diese Frage ist jedoch völlig unabhängig davon zu lösen, ob man herkömmliche Steuerungssysteme oder komplexe Hard-/Softwaresysteme einsetzt.

Wenn die Funktionsweise einer wachsenden Zahl technischer Produkte immer stärker vom Funktionieren der darin genutzten Computersysteme abhängig ist, so hat der Gesetzgeber die Aufgabe, solche Systeme in einer Art und Weise in die Überwachung der technischen Funktionstüchtigkeit miteinzubeziehen, die für herkömmliche Technologien erprobt ist.

Bisher sind nur wenige Kriterien dafür entwickelt, welche Produkte dies umfassen sollte und welche Maßstäbe notwendigerweise in eine solche technische Überwachung einzubeziehen sind. Ob etwa auch die Funktionstüchtigkeit des Bordcomputers eines Kraftfahrzeugs in die technische Überwachung einzubeziehen ist, wird davon abhängen, welche Funktionen des Fahrzeugs davon gesteuert werden und in welchem Maß dieses IT-System manipulierbar ist. Eine kosteneffektive Kontrolle der Funktionalität von Software etwa setzt vereinheitlichte Spezifikationsstandards voraus, die eine zuverlässigere und schnellere Evaluation erlaubt, als bei der heute für die Bewertung sicherheits-zertifizierter Produkte geleistete Arbeit.

In Bezug auf globale Datennetze bestehen für den Staat nur begrenzte Kontroll- und Regulierungsmöglichkeiten. Globale Datennetze mit offener Netzwerkarchitektur wie beispielsweise das Internet, konstituieren einen körperlosen Sozialraum, in dem die Flüchtigkeit der Daten und Ereignisse Programm ist. Diese Morphologie virtueller Räume steht konträr zu einem Rechtssystem, das auf materiellen Beweisen, rekonstruierbaren Vorgängen und identifizierbaren Zeugen und Tätern baut. Hinzu kommt, daß Recht sich auf definierte Territorien bzw. Hoheitsgebiete (Territorialitätsprinzip) bezieht. Welches Recht aber gilt für das globale Internet? Deutsches Recht? EU-Recht? Amerikanisches Recht?

Zwar ist die Etablierung von allgemeinen Standards, etwa zu zentralen Themen der IT-Sicherheit oder der Strafverfolgung durch internationale Vereinbarungen, möglich. Dadurch verändern sich aber nicht die spezifischen Bedingungen der virtuellen Netzwelt. So kann der Staat Strafverstöße im Cyberspace oft gar nicht mehr erkennen. Zielsetzungen, etwa der Außenhandelskontrolle oder des Datenschutzes, werden bei länderübergreifender Datenübermittlung ausgehebelt, denn Grenzkontrollen gibt es im Netz nicht. Netzteilnehmer können ihre Identitäten über Anonymisierungsserver verschleiern und ihre Nachrichten mit kryptografischen Verfahren sicher verschlüsseln. Niemand weiß, wer und wie viele Nutzer mit welchen Aktionen am Internet teilnehmen – auch kein Nachrichtendienst und keine Polizei.

Damit verlagern sich Belange zur Herstellung von Sicherheit und Schutz im Netz vom Staat auf den einzelnen Netzteilnehmer selbst sowie auf Mechanismen der Selbstregulierung.

Wenn also der demokratische Rechtsstaat seine Bürger im neuen Sozialraum der Netze nicht mehr zuverlässig schützen kann, muß er sie zum Ausgleich zum Selbstschutz befähigen. Er muß ihnen ermöglichen, vorhandene Instrumente zu ihrer Sicherheit und ihrem Schutz eigenverantwortlich einzusetzen.

In Hinblick auf einen IT- Basisschutz, der die IT-Sicherheitsziele Vertraulichkeit, Integrität und Authentizität umfaßt, existieren kostengünstige und effiziente Verschlüsselungssysteme, die einen solchen Selbstschutz ermöglichen können.

Diese Verschlüsselungssysteme sind in technischer Hinsicht bereits vorgestellt worden. Im folgenden wird es um die politischen, rechtlichen und weitergehenden gesellschaftlichen Implikationen dieser Sicherheitsmittel gehen. Dabei werden auch die Interessengegensätze im Hinblick auf eine freie Verwendung starker Verschlüsselungssysteme, wie sie in der sogenannten Kryptokontroverse zum Ausdruck kommen, dargestellt und erörtert.

4.1.1 Die digitale Signatur

In dem Kapitel „Möglichkeiten der Technik" ist die digitale Signatur von ihrer technischen Seite dargestellt worden. In diesem Abschnitt wird die Digitale Signatur in ihrer Bedeutung für eine moderne Sicherheitsinfrastruktur betrachtet. Dabei steht die Frage, inwieweit die Digitale Signatur ein Äquivalent zur natürlichen Unterschrift ist, im Mittelpunkt der Betrachtung.

Ein besonders großes Problem des digitalen Handels ist der Mangel an Rechtssicherheit. Dies liegt u. a. an dem bereits angesprochenen flüchtigen und immateriellen Charakter digitaler Transaktionen, die den herkömmlichen Anforderungen an Beweissicherheit entgegen laufen.

In der „realen Welt" hat sich seit Jahrhunderten die natürliche Unterschrift, die auf ein aus Papier bestehendes Dokument gesetzt wird, als Mittel zur Herstellung von Rechtssicherheit bewährt. In der virtuellen Welt gibt es kein „materielles" Papier, das unterzeichnet und in einem Safe aufbewahrt werden könnte, um es im Falle eines Rechtstreites als sicheres Beweismittel dem Gericht vorlegen zu können.

Dieses Defizit soll mit der Digitalen Signatur überwunden werden. Um die Digitale Signatur als mögliches elektronisches Äquivalent zur natürlichen Unterschrift erörtern zu können, ist eine kurze

Betrachtung der Leistungsfunktionen natürlicher Unterschriften notwendig:

Echtheitseigenschaft: Diese stellt sicher, daß das Dokument wirklich vom Unterschreibenden stammt. Hier wird gefordert, daß ein enger Zusammenhang zwischen Dokument und Unterschrift besteht. Dies wird dadurch erreicht, daß die Unterschrift und die unterschriebene Erklärung auf demselben Blatt stehen.

Identitätseigenschaft: Jede natürliche Unterschrift verkörpert die Identität des jeweils Unterschreibenden, d. h., die Unterschrift kann einer und nur dieser Person zugeordnet werden.

Abschlußeigenschaft: Dies wird dadurch ausgedrückt, daß die Unterschrift am Ende des Dokuments steht. Damit wird das Dokument abgeschlossen, so daß nachfolgende, nicht unterschriebene Äußerungen, keine Rechtsgültigkeit haben.

Warneigenschaft: Dies soll den Unterzeichnenden vor einer Übereilung bewahren. Der Akt des handschriftlichen Unterschreibens ist in der Regel ein auch in Hinblick auf rechtliche Konsequenzen bewußter Akt.

Verifikationseigenschaft: Jeder Empfänger eines unterschriebenen Dokuments kann die Unterschrift verifizieren, etwa durch einen Unterschriftenvergleich.[147])

Die Schriftform mit natürlicher Unterschrift wird in vielen Rechtsbereichen für verschiedenartigste Willenserklärungen vorgeschrieben. Mindestens 3907 Regelungen in 908 rechtlichen Vorschriften verlangen heute die Schriftform mit eigenhändiger Unterschrift auf einer Papierurkunde. Der Formzwang dient jeweils unterschiedlichen Zwecken, die sich aus dem spezifischen rechtlichen Kontext der Willenserklärung ergeben[148]). So stehen neben den bekannten Funktionen der privatrechtlichen Willenserklärungen wie Abschluß-, Identitäts-, oder Echtheitsfunktion für Bürgschaften der Übereilungsschutz, für Grundbucheinträge die Publizitätswirkung, für Rechtsnormen, Verwaltungsvorschriften und bestimmte Verwaltungsakte die Verbreitungswirkung, für die Begründung von Verwaltungsakten die Rechtsschutzerleichterung, für die schriftliche Fassung von Technikzulassungen deren Vollziehbarkeit, für Testamente die Beweissicherheit[149]) und für schriftliche Akten der Verwaltungsbehörden die Kontrollfunktion im Vordergrund.[150])

Abgesehen von den rechtlich definierten Urkundenformaten, bei denen natürliche Vorschriften zwingend vorgeschrieben sind, gibt es zahlreiche rechtlich verbindliche Willenserklärungen, bei denen eine Unterschrift nicht vorgeschrieben wird, aber dennoch häufig freiwillig geleistet wird. Denn der Akt des Unterschreibens signalisiert immer Einverständnis, Verbindlichkeit, Ernsthaftigkeit, weil die Unterschrift eine hohe beweissichernde Kraft hat. Damit erfüllt die Unterschrift aber auch eine soziale Funktion, die sich durch einen langen Zeitraum praktischer Ausübung und Bewährung im Bewußtsein der Bevölkerung verankert hat.

Für die Entfaltung eines nach heutigen Maßstäben gesicherten Rechtsverkehrs im Netzraum ist deshalb ein Äquivalent zur natürlichen Unterschrift unabdingbar. Dies gilt im besonderen für die Entfaltung einer digitalen Ökonomie.

„In der Praxis besteht ein [...] hoher Bedarf nach einer gesetzlichen Regelung, die einem elektronischen Dokument (etwa einer UN/EDIFACT-Nachricht über eine Bestellung oder eine Steuererklärung) denselben Stellenwert zuordnet wie einem Papierdokument. Dies haben meine empirischen Untersuchungen im Bereich deutscher Speditionen, Banken und in der Automobilindustrie ergeben.[151]) Knapp ein Drittel aller Unternehmen verfährt deshalb derzeit zweigleisig und übermittelt wichtige Nachrichten nicht elektronisch, sondern auch auf Papier. Dies erhöht die Transaktionskosten und führt zu Wettbewerbsnachteilen.[152])

Ein Ausweg besteht gegenwärtig nur dann, wenn die Beteiligten für Streitigkeiten, die sich aus der Nichtanerkennung elektronischer Dokumente ergeben, statt eines staatlichen Gerichts die Anrufung eines Schiedsgerichts vereinbaren. (§ 1025ff. ZPO). Ein solches Gericht wäre an die Vereinbarung der Parteien gebunden, den Beweiswert übermittelter elektronischer Dokumente nicht angreifen zu wollen."[153])

Ausgehend von der Prämisse, daß der Übergang vom Medium Papier zum elektronischen Dateidokument die Bedürfnisse in Bezug auf die Leistungsfunktionen der Unterschrift nicht verändert hat, muß die Behandlung der Frage, inwieweit eine Digitale Signatur funktionsäquivalent zur natürlichen Unterschrift ist, anhand der oben aufgeführten Leistungsfunktionen beantwortet werden.

- **Echtheitseigenschaft:** Die Digitale Signatur kann in einer Umgebung erzeugt worden sein, die nicht vertrauenswürdig ist, was z. B. bedeuten kann, daß der Signierende nicht den Text signiert hat, den er auf dem Bildschirm gesehen hat. [154])
- **Identitäteigenschaft:** Jede natürliche Unterschrift verkörpert die Identität des jeweils Unterschrei-

[147]) Vgl. Beutelspacher, A. et al., Moderne Verfahren der Kryptographie, 1998, S. 16; Goebel, J. W.; Scheller, J., Elektronische Unterschriftenverfahren in der Telekommunikation, 1991

[148]) Vgl. Rossnagel, A., Die Infrastruktur sicherer und verbindlicher Telekooperation Gutachten für die Friedrich-Ebert-Stiftung, Darmstadt, 1996

[149]) Für Testamente gelten besonders strenge Formvorschriften: Sie müssen nicht nur unterschrieben, sondern müssen als ganzes handschriftlich verfertigt sein.

[150]) Vgl. Rossnagel, A., Die Infrastruktur sicherer und verbindlicher Telekooperation Gutachten für die Friedrich-Ebert-Stiftung, Darmstadt, 1996

[151]) Vgl. Kilian, W.; Picot, A., Electronic Data Interchange, 1994, S. 109, 201ff.

[152]) Vgl. hierzu auch den Abschnitt 1.4

[153]) Schriftliche Stellungnahme von Prof. Dr. Kilian, Leiter des Instituts für Rechtsinformatik an der Universität Hannover zur Öffentlichen Anhörung Datensicherheit der Enquete Kommission: Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft am 12. Mai 1998.

[154]) Vgl. Glade, A. et al., Digitale Signatur & Sicherheitssensitive Anwendungen, 1995, S. 123

benden – bei der Person des elektronisch Signierenden kann dies technisch nie positiv nachgewiesen werden.[155]) Denn es ist möglich, daß der Paßwortzugang zur Digitalen Signatur erspäht bzw. geknackt worden ist. Außerdem kann der Signaturinhaber z. B. seine Mitarbeiter zur Nutzung der Digitalen Signatur ermächtigen. Dies entspricht aber Blankounterschriften bei natürlichen Unterschriften.

- **Abschlußeigenschaft:** In dieser Beziehung ist die Digitale Signatur funktionsäquivalent zur natürlichen Unterschrift. Über ihre integritätssichernde Funktion dokumentiert sie darüber hinaus, daß das elektronische Dokument während seiner Datenreise nicht verletzt worden ist.

- **Warneigenschaft:** Natürliche Unterschriften haben sich in den sozialen Verhaltenskodex der Bevölkerung über einen langen Zeitraum verankert. Im allgemeinen gehen Bürgerinnen und Bürger verantwortungsvoll mit ihrer Unterschrift um. Die digitalen Signaturverfahren hingegen sind technisch neue Sachverhalte. Ihre Bedeutung als Unterschriftenersatz ist weder deutlich erkennbar noch praktisch erprobt. Sie kann auch kaum verstanden und nachvollzogen werden.

Versuche mit solchen Verfahren[156]) und auch der oft wenig sicherheitsbewußte Umgang mit Magnetstreifen im Bankverkehr lassen vermuten, daß ein entsprechendes soziales Bewußtsein für die Rechtserheblichkeit solcher neuen Tatbestände in der Bevölkerung noch keineswegs verbreitet ist. Vielmehr reicht die Bandbreite an Reaktionen von Ablehnung der als unpersönlich empfundenen Technik bis zum unreflektierten Spieltrieb. Um einer Erfüllung der Warnfunktion wenigsten nahe zu kommen, wären daher im Rahmen der jeweiligen konkreten Applikationen der digitalen Signatur bis auf weiteres zusätzliche Maßnahmen erforderlich, z. B. ausdrückliche Warnhinweise („Vorsicht! Sie signieren jetzt und erzeugen dieselben Rechtswirkungen wie im Fall einer handschriftlichen Unterschrift; das bedeutet, daß Sie an ihre Erklärung gebunden sind.")[157])

Verifikationseigenschaft: Hier schneidet die Digitale Signatur gut ab, weil mit dem öffentlichen Schlüssel des Unterzeichners dessen Digitale Signatur verifiziert werden kann.[158])

Diese knappe Erörterung der Funktionsäquivalenz der Digitalen Signatur zur natürlichen Unterschrift hat bereits gezeigt, daß nur sehr eingeschränkt von einer Funktionsgleichheit der Digitalen Signatur im Vergleich zur natürlichen Unterschrift ausgegangen werden kann.

Allerdings muß beachtet werden, daß im Zeitalter der Neuen Medien auch Papierdokumente, die mit einer natürliche Unterschrift versehen sind, neuen Kopier- und Manipulationsmöglichkeiten – etwa durch Scannen und digitaler Bildbearbeitung – ausgesetzt sind.

Dies ändert nichts daran, daß ein digital signiertes Dokument nicht die Beweiskraft wie die vom Aussteller unterschriebene Privaturkunde erreichen kann, die nach § 416 ZPO den vollen Beweis dafür erbringt, daß die in Ihnen enthaltenen Erklärungen vom Aussteller abgegeben sind.[159]).

In Hinblick auf den dringenden Bedarf eines den elektronischen Rechtsverkehr sichernden Instruments – das bisher ohne Alternative die Digitale Signatur ist – besteht dringender Handlungsbedarf beim Gesetzgeber, die Digitale Signatur als beweissicherndes Instrument im elektronischen Rechtsverkehr rechtlich zu fundieren.

In diesem Zusammenhang ist zu beachten, daß im bereits existierenden Signaturgesetz die Frage der Beweissicherheit ausdrücklich ausgeklammert wird. Mit dem Signaturgesetz ist die rechtliche Voraussetzung für die Schaffung einer institutionellen Infrastruktur zur sicheren Erzeugung, Verbreitung und Verifikation der Digitalen Signatur geschaffen worden. Damit ist aber nicht die rechtliche Stellung der Digitalen Signatur im elektronischen Rechtsverkehr geregelt worden.

Wie gezeigt worden ist, bietet die Digitale Signatur eine spezifische Sicherungsmöglichkeit des elektronischen Rechtsverkehrs, die dazu beitragen kann, bestimmte Risiken zu vermindern, ebenso wie die handschriftliche Unterschrift dies im schriftlichen Rechtsverkehr tut.

Da eine einfache Funktionsgleichheit zur natürlichen Unterschrift aber nicht festgestellt werden kann, erfordert die Einführung einer elektronischen signierten Urkunde eine politische Entscheidung, die aus einer Abwägung des Nutzens, der Wesensmerkmale sowie der Risiken Digitaler Signaturen getroffen werden muß.

Das Ziel ist dabei, die Digitale Signatur neben der natürlichen Unterschrift als starkes beweissicherndes Instrument mit einer sich der natürlichen Unterschrift annähernden Funktionsäqivalenz zu etablieren.

Zu der Frage notwendiger gesetzlicher Anpassungsmaßnahmen für die Einführung der Digitalen Signatur hat eine Arbeitsgruppe „Elektronischer Rechtsverkehr" der Bundesnotarkammer einen umfassenden Vorschlag vorgelegt.[160])

Abgesehen von den notwendigen rechtlichen Schritten, die unternommen werden müssen, um die Digitale Signatur als Rechtssicherheit herstellendes Instrument zu etablieren, ist auch zu beachten, daß

---

[155]) Vgl. ebenda

[156]) Vgl. provet/GMD, Die Simultationsstudie Rechtspflege, Berlin, 1994; Rossnagel, A. CR 1994, S. 498

[157]) Glade, A. et al., Digitale Signatur & Sichersensitive Anwendungen, 1995, S. 122

[158]) Diese Aussage geht von der Annahme aus, daß die Digitale Signatur mit dem privaten Schlüssel eines öffentlichen Schlüsselsystems ausgeübt wurde und der öffentliche Schlüssel von einer anerkannten TTP zertifiziert worden ist.

[159]) Vgl. Kilian, W., Schriftlichen Stellungnahme zur Öffentlichen Anhörung der Enquete-Kommission: Neue Medien in Wirtschaft und Gesellschaft – Deutschland Weg in die Informationsgesellschaft am 12. Mai 1997

[160]) Vgl. hierzu Glade, A. et al., Digitale Signatur & Sichersensitive Anwendungen, 1995, S. 126–130

eine umfassende Strategie zur sozialen Etablierung der Digitalen Signatur notwendig ist. Wie unter dem Stichwort „Warnfunktion" bereits ausgeführt worden ist, wird die Digitale Signatur nicht schon deshalb genutzt, weil sie eben da ist. Ohne eine breit angelegte Kampagne zur Einführung der Digitalen Signatur, die Aufklärungs-, Beratungs- und Schulungsmaßnahmen – aber auch die frühe verbindliche Einführung in die Organisationen des Öffentlichen Dienstes – umfassen muß, ist zu befürchten, daß die Digitale Signatur irgendwann rechtlich abgesichert zwar besteht, aber auf nicht absehbare Zeit von breiten Bevölkerungsschichten nicht akzeptiert werden wird.

4.1.2 Die Kryptographie

Der Mangel an Vertraulichkeit beim Datenaustausch über elektronische Netzwerke ist eines der grundlegenden Probleme, die alle Anwendungen in Datennetzwerken betreffen. Die Dimension dieses Problems und die Bedeutung eines vertraulichen Datenaustausches für die Entwicklung der Informationsgesellschaft sind an verschiedenen Stellen dieses Berichtsteils bereits ausführlich dargestellt worden. Dabei ist die Bedeutung des IT-Sicherheitszieles „Vertraulichkeit" auch in Hinblick auf das dem Datenschutz zugrunde liegende informationelle Selbstbestimmungsrecht betont worden.[161]) In dem Kapitel „Möglichkeiten der Technik" wurden „harte" softwarebasierte Verschlüsselungstechniken vorgestellt, mit denen Vertraulichkeit technisch hergestellt werden kann.

Es ist heute unumstritten, daß moderne Verschlüsselungstechnologien unverzichtbare Instrumente zur Herstellung von Vertraulichkeit und damit des IT-Selbstschutzes sind. Allerdings existieren unterschiedliche Vorstellungen und Interessen in Hinblick auf die gesellschaftlichen und rechtlichen Rahmenbedingungen, in denen technische Verschlüsselungsmethoden eingesetzt werden. Damit ist die sogenannte „Kryptokontroverse" angesprochen: Auf der einen Seite stehen die Befürworter einer gesetzlichen Regulierung, die nur solche Verschlüsselungssoftware zulassen wollen[162]), die den Sicherheitsbehörden die Möglichkeit eröffnet, mit starker Kryptosoftware verschlüsselte Dokumente bei gesetzlich definierter Sachlage entweder mit einem hinterlegten Schlüssel (Key Escrow) oder einer Rekonstruktion des privaten Schlüssels als Nachschlüssel (Key-Recovery) zu entschlüsseln.

Key-Recovery und Key-Escrow

„Key-Recovery-Verschlüsselungssysteme erlauben einen Zugang zum Orginaltext außerhalb der normalen Ver- und Entschlüsselung. Key-Recovery wird auch manchmal Key-Escrow genannt.

Der Ausdruck Key-Escrow wurde in Verbindung mit der Clipper-Chip-Initiative der US-Regierung bekannt, nach der ein Nachschlüssel zu jeder Verschlüsselungseinrichtung zugänglich für die Sicherheitsbehörden hinterlegt werden sollte. Heute wird der Ausdruck „Key-Recovery" stellvertretend für all die verschiedenen „Key-Escrow"-, „Trusted Third Party!"- „Exceptional Access"-, „Data Recovery"- und „Key-recovery"-Systeme benutzt, die in den letzten Jahren vorgestellt wurden. [...]

Key-Recovery-Verschlüsselungssysteme arbeiten auf unterschiedliche Art und Weise. Erste Key-Escrow-Verschlüsselungssysteme beruhten auf der Speicherung privater Schlüssel durch die U.S.-Regierung oder, etwas später, durch private Gesellschaften. Andere Systeme benutzen „escrow agents" oder „Key-recovery agents", die gewährleisten, daß die Schlüssel für eine bestimmte verschlüsselte Sitzung oder eine gespeicherte Datei zurückgewonnen werden können. Derartige Systeme verlangen, daß solche Sitzungsschlüssel wiederum mit einem Schlüssel des jeweiligen Agenten verschlüsselt werden und als Teil der eigentlichen Daten verschickt werden müssen. Einige Systeme teilen die Fähigkeit der Schlüsselwiedergewinnung unter mehreren Agenten auf. [...]

So sind zweifellos verschiedene neue Key-Recovery-Systeme entstanden, die sich vom orginalen „Clipper"-Vorschlag in der Art unterscheiden, wie sie Schlüssel speichern und wiedererlangen.

Alle diese Systeme haben zwei Wesenseigenschaften gemein:

- einen Mechanismus, jenseits der eigentlichen Aufgabe von Ver- und Entschlüsselung, durch den ein Dritter unbemerkt Zugriff auf den Klartext einer verschlüsselten Nachricht erhalten kann, und
- die Existenz eines hochsensiblen, geheimen Schlüssels (oder einer Sammlung von Schlüsseln), der (die) über eine sehr lange Zeit geheim gehalten werden muß (müssen).

Zusammengenommen ergeben diese Elemente ein „allgegenwärtiges Key-Recovery-System, das die Spezifikationen der Sicherheitsbehörden erfüllt. Einige spezielle Details mögen sich vielleicht noch ändern, die grundlegenden Anforderungen jedoch höchstwahrscheinlich nicht: Es sind die essentiellen Forderungen an jedes System, welches das erklärte Ziel der Sicherheitsbehörden erfüllt, zeitnah und ohne Kenntnis der Nutzer Zugang zu den Klartexten verschlüsselter Kommunikation zu erhalten."[163])

Die Rechtskonformität von Key-Recovery-Systemen ist überdies in zwei Punkten unklar. Erstens ist fraglich, in welcher Weise die zeitliche Beschränkung einer Überwachungsmaßnahme auch technisch nachgebildet wird. Findet keine automatische Veränderung der genutzten Verschlüsselung in bestimmten Zeitintervallen statt, ist eine Offenlegung des Schlüssels gleichbedeutend mit der dauerhaften Möglichkeit zur Entschlüsselung der betroffenen Kommunikation. Zweitens erzwingt die Eigenart asymmetrischer Verschlüsselungsverfahren eine rechtlich problematische Ausweitung der aufzudeckenden Schlüssel. Bei diesen Verfahren macht die Kenntnis des privaten

[161]) Vgl. hierzu auch den Berichtsteil Datenschutz, Abschnitt 3.5.1.

[162]) Die Vorschläge der Regulierungsbefürworter variieren hierzu: Während die „harten" Regulierungsbefürworter nur solche Verschlüsselungssoftware zulassen wollen, die von staatlicher Seite lizensiert und mit einem Key-Recovery-Mechanismus ausgestattet sind, schlagen die moderaten Regulierungsbefürworter vor, die Nutzung von Verschlüsselungssoftware grundsätzlich frei zu stellen, allerdings von staatlicher Seite sehr starke Anreize zur Nutzung von lizensierter und mit einem Key-Recovery-Mechanismus ausgestatteten Verschlüsselungssoftware zu setzen. Dazu zählt z.B., daß von staatlicher Seite eine sehr komfortable und kostengünstige Verschlüsselung angeboten wird und das Unternehmen beim Datenverkehr mit Behörden ein bestimmter Verschlüsselungsstandard (mit Key-Recovery-Mechanismus) vorgeschrieben wird.

[163]) Abelson, H.; Anderson, R.; Bellovin, S. et. al., Risiken von Key-Recovery, Key-Escrow und Trusted Third Party-Verschlüsselung, in: DuD 22, 1998 1, S. 16

Schlüssels einer überwachten Person nur ihren eingehenden Verkehr lesbar. Erst die Kenntnis der privaten Schlüssel aller der von der überwachten Person adressierten Kommunikationspartner ermöglicht das Mitlesen des ausgegehenden Verkehrs. Da gegen diese Vielzahl von Personen jedoch nur in Ausnahmefällen ein Ermittlungsverfahren möglich ist, muß entweder der Erfolg der Überwachung auch von Key-Escrow geschützten Datenverkehr begrenzt bleiben oder zu einer Freigabe privater Schlüssel in großer Zahl führen. Alternativ dazu wäre nur noch die generelle Einigung auf Kryptosysteme möglich, die schwach genug sind, um auch ohne Kenntnis der privaten Schüssel leicht zu entschlüsseln sind.

Auf der anderen Seite argumentieren die Gegner einer gesetzlichen Regulierung, daß zum einen jede Form von Krypto-Regulierung leicht und kaum nachvollziehbar umgangen werden könne, daß zum anderen der politische und wirtschaftliche Schaden die etwaigen Vorteile einer gesetzlichen Regulierung bei weitem aufheben würde. Der Bedeutung dieses Themas entsprechend, wird die Kryptokontroverse in diesem Abschnitt ausführlich dargestellt.[164])

Bedingt durch die weltumspannende Dimension von Datennetzwerken ist das Thema ‚Vertraulichkeit durch Verschlüssselung' sui generis transnational angelegt. So gibt es sowohl bei unseren europäischen Nachbarn unterschiedliche Kryptoregulierungen als auch eine unterschiedliche Behandlung des Themas auf Ebene der Europäischen Union.

Ob und wie bei unseren europäischen Nachbarn Kryptographie reguliert wird und wie sich die Europäische Kommission zu dieser Frage verhält, wird in knapper Form ein weiteres Thema dieses Abschnitts sein. Über die europäische Perspektive hinaus wird hierzu auch die Position der OECD als bedeutende internationale Organisation referiert.

Von außerordentlicher Bedeutung für deutsche und europäische Interessen sind die politischen Initiativen der USA zur Kryptographie.

Dies gilt insbesondere für das Bemühen der amerikanischen Regierung, ein weltweites Key-Recovery-System zu etablieren, das für Deutschland und seine europäischen Nachbarn weitreichende Konsequenzen hätte.

4.1.2.1 Der Streit um die Kryptographie

Unter dem Begriff der „Kryptokontroverse" wird die Auseinandersetzung um das Für und Wider einer Einschränkung der Verwendung von starken kryptographischen Verfahren (Verschlüsselungsverfahren) verstanden. Auf Seiten des Innenministeriums und der Sicherheitsbehörden wird die Auffassung vertreten, die Verwendung von Verschlüsselungsverfahren müsse unter staatlichem Genehmigungsvorbehalt gestellt werden.

Demnach sollen nur jene kryptografischen Produkte zur Verfügung stehen, die durch staatliche Stellen bzw. durch staatlich akkreditierte Privatinstitutionen zugelassen sind. Das entscheidende Merkmal dieser lizensierten Kryptosoftware wäre, daß entweder Nachschlüssel in einem Trust Center hinterlegt würden, auf die unter bestimmten gesetzlichen Bedingungen Sicherheitsbehörden einen Zugriff hätten oder daß die privaten Schlüssel rekonstruierbar wären.

Begründet wird diese Forderung im Kern mit der Feststellung, daß starke Verschlüsselungsverfahren auch einen Kommunikationsschutz für Kriminelle bieten würden, der durch die technischen Möglichkeiten der Ermittlungsbehörden nicht mehr aufhebbar wäre. Dadurch würde, so die Sicherheitsbehörden, die gesetzlich bereits eng definierte Möglichkeit der Überwachung des Fernmeldeverkehrs vollends ausgehebelt und damit den Strafverfolgungsbehörden ein wichtiges Ermittlungsinstrument entzogen.

Die Gegner einer gesetzlichen Kryptoregulierung argumentieren dagegen, daß starke kryptographische Verfahren weit verbreitet wären und sehr einfach über das Internet bezogen werden könnten. Hinzu kämen Verschlüsselungsverfahren, wie die Steganografie, bei der nicht mehr erkennbar sei, daß verschlüsselt wurde. Kriminelle, so die Gegner einer Regulierung kryptographischer Verfahren, würden sich nicht der Verschlüsselungsmethoden bedienen, von denen bekannt sei, daß sie vom Staat entschlüsselt werden könnten. Ein Nachweis der Nutzung ungesetzlicher Kryptographie sei schwierig. Hinzu komme, daß aus politischen Gründen viele Internetnutzer sich nicht autorisierter Kryptosoftware bedienen könnten, so daß selbst ein Differenzierungsschema „Nutzung legaler vs. illegaler Kryptographie" keinen Erkenntnisgewinn mehr für die Ermittlungsbehörden bringen würde. Betont wird auch, daß Verschlüsselung ein effizientes und kostengünstiges Mittel sei, um die bisher nicht existierende Vertraulichkeit in offenen Netzen herzustellen. Dieses diene auch der Abwehr krimineller Angriffe auf IT-Systeme und ihrer Daten. Eine gesetzlich Einschränkung der Nutzung von kryptographischen Methoden könne Bürger und Unternehmen hindern, sich im Netzverkehr zu schützen. Es würde ferner den Wettbewerb zwischen den Anbietern von kryptrographischen Lösungen behindern und damit einer Entwicklung zu immer besseren Verschlüsselungsmethoden entgegen stehen.[165])

4.1.2.2 Krypto-Politik in Europa, den USA und Japan

Die in Deutschland stattfindende Kontroverse um eine gesetzliche Regulierung von Kryptographie muß über den nationalen Rahmen hinaus im europäischen und weltweiten Zusammenhang betrachtet werden. Dies ist u.a. deshalb notwendig, weil die Realisierung von Vertraulichkeit durch kryptographische Verschlüsselung wesentliche Voraussetzung für die Entfaltung einer „digitalen Ökonomie" im europäischen Wirtschaftsraum sowie zwischen Europa und anderen Wirtschaftsräumen in der Welt ist.

[164]) Beachte hierzu auch die Handlungsempfehlung im Kapitel 5

[165]) Vgl. hierzu die schriftlichen Ausführungen der Sachverständigen zu der Anhörung Datensicherheit am 12. Mai 1997.

Die folgende Tabelle gibt eine Übersicht zu den gesetzlichen Kryptoregulierungen in einer Auswahl europäischer Länder sowie Japan und den USA als wichtigste europäische Handelspartner. Dabei wird unterschieden zwischen gesetzlichen Nutzungseinschränkungen kryptographischer Systeme, ob ein Key-Recovery -System existiert und wie der Export bzw. Import kryptographischer Produkte geregelt ist.

	Gesetzliche Einschränkung der Nutzung von Kryptographie	**Key-Recovery/Key Escrow**	**Import-/Exportbeschränkungen**
Deutschland	Bisher gibt es keine gesetzliche Grundlage, die eine freie Nutzung kryptographischer Systeme einschränkt. Allerdings gibt es Bemühungen von Seiten des Innenministeriums und der Sicherheitsbehörden, die Verwendung kryptographischer Produkte unter behördlichen Genehmigungsvorbehalt zu stellen. Diese Initiative wird in Politik, Wirtschaft und Wissenschaft kontrovers diskutiert.	Das Innenministerium und die Sicherheitsdienste machen sich für eine gesetzlich verankerte Key-Recovery-Lösung stark. Vorhaben wird in Politik, Wirtschaft und Wissenschaft kontrovers diskutiert. Es gibt derzeit kein Gesetzesvorhaben, das auf die Einführung eines Key-Rcovery-Systems abzielt.	Import Es gibt keine Importbeschränkungen Export Ja – Deutschland folgt den Europaratsdokumenten 3381/94 und 94/942/CFSP, wonach der Export von Kryptographie lizensierungspflichtig ist.
Europäische Länder	Nein – mit Ausnahme von Frankreich[166]), wo Verschlüsselung genehmigungspflichtg ist. Unklare Rechtslage in Belgien.[167])	Mit Ausnahme von Frankreich gibt es in keinem Mitgliedsstaat ein gesetzlich verankertes Key-Recovery -System. Die britische Regierung plant mit Blick auf die Gefahren einer Nutzung der Kryptographie durch Kriminelle die Einführung eines Key Recovery-Systems.[168])	Import Mit Ausnahme von Frankreich gibt es in den Mitgliedsstaaten der EU keine Importrestriktionen Export Unterschiedlich – Die meisten Mitgliedsstaaten folgt dem COCOM-bzw. Wassenaar-Abkommen. Kryptosoftware kann demnach nicht nach Iran, Irak, Lybien und Nordkorea exportiert werden. Frankreich hat eigene Exportrestriktionen im nationalen Recht verankert.
Europäische Kommission	Die Generaldirektion XIII der Europäischen Kommission[169]) bezieht in ihrer Mitteilung *„Sicherheit und Vertrauen in elektronische Kommunikation/Ein europäischer Rahmen für digitale Signaturen und Verschlüsselung"* [KOM (97)503] Stellung zu den Fragen einer gesetzlichen Regulierung von Verschlüsselungsprodukten. Eine gesetzliche Regulierung des Gebrauchs kryptographischer Systeme wird in diesem Dokument kritisch gesehen. Als Begründung dieser in der Tendenz ablehnenden Haltung werden die Argumente gegen eine gesetzliche Kryptoregulierung, wie sie oben bereits genannt worden sind, angeführt. Insbesondere wird befürchtet, daß unterschiedliche nationale Regelungsansätze innerhalb der EU zu einer Behinderung des Binnenmarktes führten. Mehrfach wird in diesem Dokument darauf hingewiesen, daß ein Eingriff in die Verschlüsselung gesetzestreuen Unternehmen und Bürgern durchaus unmöglich machen könne, sich vor kriminellen Angriffen zu schützen, aber Kriminelle nicht davon abhielte, diese Verfahren zu nützen. Auch die Forderung der Sicherheits- und Strafverfolgungsbehörden nach einem rechtlichen Zugriff (lawful access) auf private Schlüssel wird in der Tendenz ablehnend betrachtet. Insgesamt werden von der Direk-		

[166]) Frankreich hat eine umfassende Kontrolle kryptographischer Produkte in seinen Gesetzen verankert. Kein anderes europäisches Land verfügt über eine vergleichbar umfassende Krypto-Regulierung. Allerdings zeichnen sich Liberalisierungstendenzen ab. Nicht nur bestätigte der französische Industrieminister Christian Pierret das Communique der European Ministerial Conference on Global Information Networks, welches eine freie Nutzung kryptographischer Produkte vorsieht, sondern erklärte, daß eine Liberalisierung der Verschlüsselungstechnologie französischen Unternehmen den vollen Eintritt in elektronischen Handel erlauben würde, der zur Zeit noch von US-Unternehmen dominiert würde. Vgl. hierzu: http://www.gilc.org/gilc/crypto/crypto-results.html

[167]) Im Dezember 1994 verabschiedete das belgische Parlament ein Gesetz, das ein Key-Escrow-System für Krypto-Schlüssel vorschreibt. In diesem Gesetz wird die Belgacom und die belgische Post- und Telekommunikationsgesellschaft ermächtigt „to disconnect a phone that used unescrowed encryption." Bisher ist das Gesetz nicht umgesetzt worden. Außerdem existiert eine parlamentarische Gesetzesinitiative für eine Lockerung der Restriktionen in Bezug auf eine freie Nutzung kryptografischer Produkte. Vgl. hierzu: http://www.gilc.org/gilc/crypto/crypto-results.html

[168]) „In developing ist policy on encryption, the Government has given serious consideration to the risk that criminals and terrorists will exploit strong encryption techniques to protect their activities from detection by law enforcement agencies. Encryption might be used to prevent law enforcement agencies from understanding electronic data seized as the result of a search warrant or communications intercepted under a warrant issued by a Secretary of State. This would have particularly serious implications for the fight against serious crime and terrorism. [...] **In response to these concerns, the Government intends to introduce legislation to enable law enforcement agencies to obtain a warrant for lawful access to information necessary to decrypt the content of communications or stored data (in effect, the encryption key).**; Vgl. hierzu: http://dtiinfo1.dti.gov.uk/CII/ana27p.htm

[169]) Die Generaldirektion XIII ist zuständig für Telekommunikation, Informationsmarkt und Nutzung der Forschungsergebnisse.

	tion in ihrer Bewertung acht Argumente gegen eine gesetzliche Regulierung der Kryptographie angeführt.[170] In Hinblick auf Ausfuhrkontrollen wird auf das Wassenaar-Übereinkommen über die Kontrolle der Weitergabe von konventionellen Waffen und Gütern und Technologien mit doppelten Verwendungszweck (19. Dezember 1995), in deren Rahmen 28 Staaten Ausfuhrkontrollen für Verschlüsselungsprodukte vereinbart haben sowie auf die Dual-Use-Verordnung vom Dezember 1994 verwiesen, wonach bestimmte Verschlüsselungsprodukte nur mit Genehmigung exportiert werden können. Die Generaldirektion XIII sieht dringenden Handlungsbedarf für eine europäische Rahmenordnung im Bereich der Kryptografie. Bis zum Jahre 2000 soll ein entsprechender Rahmen geschaffen worden sein.		
Rat der Europäischen Union	Der Rat der Europäischen Union empfiehlt in seinen *Recommendation No. R (95) 13,* Maßnahmen zu ergreifen, die die negativen Effekte einer Nutzung kryptografischer Mittel auf die Aufklärung krimineller Delikte minimieren, wobei die rechtmäßige Nutzung nur soweit betroffen sein sollte, wie dies unbedingt nötig ist.[171]		
USA	*Gesetzliche Einschränkung der Nutzung von Kryptophrafie* **Nein – die Nutzung kryptografischer Produkte ist nicht reglementiert.** *Key-Recovery-Systeme* Während die US-Regierung 1993 eindeutig den Aspekten der inneren Sicherheit Vorrang gab und sich bemühte, einen bestimmten Hardwarestandard („Clipper Chip") durchzusetzen, setzt sie sich seit etwa 1995 viel stärker um einen Interessenausgleich ein. Ein Verbot oder eine rechtliche Einschränkung der Nutzung von Kryptographie in den USA ist nicht geplant. Kernstück der US-Politik ist die Einführung von „Key-Recovery" „KR)-Technologie durch Anreize (erleichterte Exportkontrollen, Staatsaufträge). In der „Interim Rule" über die Erleichterung der Exportkontrollen sind KR-Systeme definiert: – bei jeder Verschlüsselung muß automatisch ein Doppel des Schlüssels an einen „Recovery Agent" übersandt und bei diesem hinterlegt werden; – der verschlüsselte Datensatz muß die unverschlüsselte Information enthalten, bei welchem Agent das Schlüsseldoppel hinterlegt ist; – der Nutzer darf nicht die Möglichkeit haben, diese Funktion abzustellen. Damit können Strafverfolgungsbehörden mit entsprechenden Durchsuchungsbefehl von dem Recovery Agent ein Schlüsseldoppel erhalten. Außerdem hat der Nutzer selbst – im Fall, daß der Schlüssel verlorengeht – jederzeit Zugang zu einem Doppel. Die Voraussetzungen für die Zulassung als Recovery Agent müssen noch gesetzlich festgelegt werden. Größere Firmen sollen interne Recovery Agents benennen können. Die US-Regierung geht davon aus, daß KR-Technologien auch ohne spezielle Förderung einen gewissen Anteil am Kryptographiemarkt gewinnen werden. Indem sie die Exportkontrollen für KR-Technik erleichtert und zudem selbst als Nachfrager auftritt, will sie einen hohen Marktanteil durchsetzen, so daß die Strafverfolgungsbehörden in einem Großteil der Fälle Zugriff auf die Schlüssel hätten. Sie rechnet dabei mit dem intensiven Wettbewerb zwischen den Herstellern von Kryptotechnik – erleichterte Exportkontrollen stellen einen Wettbewerbsvorteil dar, den sich so leicht kein Hersteller entgehen lassen wird. Weiter geht sie davon aus, daß die Hersteller auf Dauer nicht zweigleisig fahren werden, indem sie KR- und andere Technologien nebeneinander anbieten und unter hohen Aufwand weiterentwickeln. Bei der Industrie stößt die KR-Politik auf wenig Verständnis. Viele Hersteller machen zwar von den Regierungsanreizen Gebrauch und entwickeln dazu KR-Lösungen. Zugleich aber lobbyiert[172] die Industrie im Kongreß nachdrücklich für eine völlige Aufhebung der Exportkontrollen. Der Ausgang dieser Debatte – und damit die innenpolitische Durchsetzbarkeit der KR-Politik – ist noch völlig ungewiß.[173] *Import-/Export-Beschränkungen* *Import* Keine Importbeschränkungen *Export* Ja – nur lizensierte Kryptosoftware mit beschränkter Schlüssellänge und Key-Recovery- Mechanismus wird auf Antrag zum Export zugelassen. Aufgrund der Wettbewerbsnachteile für die amerikanische Wirtschaft, die mit dieser Regelung verbunden sind, lassen sich deutlich Liberalisierungs-tendenzen beobachten. So hat es bereits Gesetzesinitiaiven gegeben, die auf eine Liberalisierung der Exportbeschränkungen abzielt.		
Japan	Nein – die Nutzung kryptographischer Produkte ist nicht reglementiert.	Das Post- und Telekommunikationsministerium ist verantwortlich für die Regulierung privater und commerzieller Nutzung von Verschlüsselung im nationalen Telekommunikationsnetz.[174]	Import Keine Importrestriktionen Export Japan folgt dem Wassenaar-Abkommen, außerdem kontrolliert und lizensiert das MITI den Export kryptographischer Produkte.

[170] Vgl. die Mitteilung der Europäischen Kommission (Generaldirektion XIII) KOM(97)503, S. 17 – 18

[171] „V. Use of Encryption: 14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting ist legimate use more than strictly necessary."; Vgl. http://www.privacy.org./pi/intl_orgs/coe/info_tech_1995.htm

[172]

[173] Stellungnahme der Deutschen Botschaft in Washington vom 23. Januar 1998 zur US-Kryptoplitik. Vgl. auch: Kuner, C., Die Kryptodebatte in den USA, in: DuD 22, 1998 1, S. 5–7; Cryptography and Liberty: An international survey of encryption policy, in: http://www.gilc/crypto/crypto-survey.html

[174] Vgl. Cryptography and Liberty: An international survey of encryption policy, in: http://www.gilc/crypto/crypto-survey.html

4.1.2.3 Kryptopolitik international: Die US-Key-Recovery Initiative

Erhebliche Auswirkungen auf die internationalen Perspektiven der Kryptographie (politisch, technisch und wirtschaftlich) sind auch durch die jüngsten Entwicklungen in den USA zu erwarten. Seit dem 30. Dezember 1996 gilt dort eine neue Exportregulierung (Interim Rule), die das vorherige Ausfuhrregime, das Kryptoprodukte ab einer bestimmten Schlüssellänge (40 Bits) als Kriegswaffen einstufte (International Traffic of Arms Regulation), ablöste.[175])

Im wesentlichen sehen die neuen Regeln folgende Punkte vor:

- Exportfähig sind starke Verschlüsselungsprodukte (Schlüssellänge über 56 Bits) nur, wenn sie Key-Recovery-Funktionen besitzen. Unterhalb dieser Grenze muß der Exporteur der Exportgenehmigungsinstanz einen Plan vorlegen, der die Einrichtung von Key-Recovery-Funktionen für das Produkt bis zum 31. 12. 1998 vorsieht. Einzige Ausnahme: Verschlüsselungsprodukte zur Nutzung im Finanzsektor.

- Key-Recovery bedeutet, daß US-Sicherheitsdienste innerhalb von zwei Stunden Zugriff auf den Klartext der verschlüsselten Nachrichten haben müssen.

- Der Zugriff soll durch sog. Key-Recovery-Agenten ermöglicht werden. Eine Zulassung der Key-Recovery-Agenten erfolgt durch die zuständige US-Exportgenehmigungsinstanz – auch wenn sie sich im Ausland befinden (dann in „Abstimmung" mit der jeweiligen Gastregierung).

- Key-Recovery Produkte dürfen nicht mit Non-Key-Recovery-Produkten kompatibel sein.

Mit diesem Exportregime geht es der US-Regierung im Ergebnis vor allem darum, einen weltweiten Standard für Kryptoverfahren zu etablieren, der – unabhängig von der technischen Ausgestaltung im einzelnen – den unbemerkten Zugriff von US-Regierungsstellen auf den Klartext verschlüsselter Informationen auch ausländischer Nutzer von US-Produkten erlaubt. Zur Begründung erklärte Präsident Bill Clinton in der entsprechenden Executive Order vom 15. November 1996:

„Encryption products, when used outside the United States, can jeopardize our foreign policy and national security interests. Moreover, such products, when used by international criminal organizations, can threaten the safety of U.S. citizens here and abroad, as well as the safety of the citizens of other countries."

Obwohl die US-Kryptohersteller über ein beträchtliches Marktpotential verfügen,[176]) fehlt es bislang allerdings an der erforderlichen „kritischen Masse", um einen solchen Standard „am Markt" zu erzeugen. Flankiert wird deshalb die US-Initiative

- auf unternehmerischer Ebene durch die sog. „Key-Recovery-Alliance" unter Federführung von IBM, der inzwischen bereits 60 Unternehmen aus aller Welt angehören und die sich mit der technisch-wirtschaftlichen Umsetzung der politischen Vorgaben befaßt, sowie

- auf politischer Ebene durch die Aktivitäten eines US-Sonderbotschafters, der die Regierungen anderer Staaten zu bewegen versucht, durch Anpassungen der nationalen und internationalen rechtlichen Rahmenbedingungen (z. B. im Exportbereich) an der US-Initiative teilzunehmen.

Innenpolitisch ist der derzeitige Kurs der US-Regierung äußerst umstritten. So brachte Rep. Bob Goodlatte den sog. SAFE-Bill (H. R. 695), der die Kopplung zwischen der Erteilung von Exportlizenzen und Key-Recovery-Funktionionalität aufhebt, in das US-Repräsentantenhaus ein. Im Zuge des Gesetzgebungsverfahrens wurde dieser Entwurf im Ausschuß für das geheime Nachrichtenwesen zwar noch erheblich verschärft, mit dem Ziel eine Nutzungsbeschränkung für Kryptoprodukte im Inland einzuführen; diese Verschärfung wurde allerdings vom Wirtschaftsausschuß des Repräsentantenhauses wieder aufgehoben. Mit dem Abschluß der Gesetzesarbeiten wird nicht vor Mitte 1998 gerechnet. Auch andere Gesetzesinitiativen zielen – mit unterschiedlichen Schwerpunkten – auf eine Liberalisierung der US-Kryptopolitik, so der Pro-CODE Bill (S. 377) und der Encrypted Communications Privacy Act (S. 376) des US-Senats. Für eine Erleichterung bzw. Abschaffung der Exportbeschränkung tritt auch eine mächtige Allianz der US-Industrie ein, u. a. die Business Software Alliance, der Information Technology Council sowie die Software Publishers Association.

Die US-Initiative zur Förderung eines globalen Key-Recovery-Standards wird von verschiedenen Seiten im Ausland höchst kritisch beurteilt. So erhob die US- und europäische Wirtschaft im Rahmen des Transatlantic Business Dialogue kürzlich u. a. die Forderung, daß die Standardisierung von Key-Recovery keinesfalls seitens der Regierungen vorangetrieben werden solle. Ebenso hat auch Japan große Probleme mit dieser Initiative, da es dort verfassungsrechtlich nur in einem sehr beschränktem Maße möglich ist, Abhörmaßnahmen durchzuführen. Auch die Bundesrepublik Deutschland hat bereits auf verschiedenen Ebenen deutlich gemacht, daß die Key-Recovery-Initiative als ein Versuch, US-Politik in das Ausland zu exportieren, nicht akzeptabel sei. Vor allem scheint dieses Initiative nach Abwägung aller Faktoren zu einseitig auf die Erreichung von US-Regierungsinteressen zugeschnitten und es kann nur schwerlich hingenommen werden, daß die vertrauliche Datenkommunikation deutscher Nutzer dem Zugriff ausländischer Instanzen außerhalb des Geltungsbereichs deutscher Gesetze und unkontrolliert durch deutsche Gerichte ausgesetzt ist. Hier wird mit gro-

[175]) Eine gemeinsame Studie des US-Handelsministeriums und der NSA stellten 1995 fest, daß die damalige restriktive US-Exportpolitik die US-Wirtschaft, bei 60 Mrd. Dollar Umsatzverlust, 200000 hochqualifizierte Arbeitsplätze bis in Jahr 2000 kosten werde.

[176]) Heute werden rund 1400 Verschlüsselungsprodukte von 862 Unternehmen in 68 Staaten hergestellt; über die Hälfte dieser Unternehmen befinden sich in den USA; Vgl. Dennings D., Markettrends, 1997, S. 3

ßer Besorgnis zur Kenntnis genommen, daß mit der Key-Recovery-Initiative auch die erforderlichen Spielräume anderer Regierungen zur Gestaltung einer eigenen Kryptopolitik beschränkt werden. Neben diesen politischen Bedenken bestehen begründete Zweifel, daß die aufgrund der einschlägigen US-Vorschriften nach Deutschland exportierten Key-Recovery-Produkte in Einklang mit deutschem Recht stehen (vor allem mit dem GG, StGB, BDSG, TKG).

Das manchmal vorgebrachte Argument, gerade wegen der US-Key-Recovery-Initiative müßten auch die anderen Staaten den Aufbau eigener Schlüsselhinterlegungs-Infrastrukturen vorantreiben, um zu verhindern, daß die Schlüssel ihrer Nutzer unter der Kontrolle von US-Behörden aufbewahrt werden, ist sicher nicht zwingend. Im Gegenteil: Gerade Staaten ohne eine solche Infrastruktur sollten sich überlegen, welche Vorkehrungen möglich und nötig sind, um die nichtautonome Entschlüsselung chiffrierter Nachrichten ihrer Bürger durch unbefugte Dritte im Geltungsbereich einer fremden Jurisdiktion zu verhindern, denn für den einzelnen Betroffenen kann es einen empfindlichen Unterschied machen, unter welchem Rechtsregime ein Strafverfahren gegen ihn eröffnet wird. Selbst wenn sich Deutschland – theoretisch – der US-Initiative anschlösse, dürfte damit faktisch nichts gewonnen sein, denn angesichts der Marktmacht der US-Hersteller würde sich dann das Key-Recovery nach US-Regeln, d.h. mit Key-Recovery-Agenten, die US-Kontrolle unterworfen sind, auf breiter Front durchsetzen. Dieser Effekt würde noch verstärkt, wenn sich auch die Produzenten von PC-Betriebssystemen und Anwendungssoftware den staatlichen Vorgaben beugen müßten, da auf diesen Ebenen die „Schnittstellen" für den Einsatz anderer Systemkomponenten, also auch für Verschlüsselungsprogramme anderer Hersteller, definiert werden.[177]) Um einen fairen Interessenausgleich herbeizuführen, ist es erforderlich, daß sich die verschiedenen Verschlüsselungsverfahren – einschließlich der Schlüsselverwaltungssysteme – im freien Wettbewerb entwickeln. Dazu muß allerdings darauf gedrungen werden, daß die Interoperabilität zwischen den verschiedenen Verfahren gewährleistet ist und die Nutzer über die Möglichkeiten des Zugriffs Dritter auf ihre vertrauliche Kommunikation aufgeklärt werden. Für beide Voraussetzungen enthalten die OECD-Guidelines, die von den USA mitunterzeichnet wurden, die notwendige „Legitimationsbasis".

4.1.2.4 Guidelines for cryptography policy – Die Position der OECD

Ein sehr wichtiges internationales Referenzdokument in der internationalen Krypto-Diskussion sind die „Guidelines for cryptography policy" der OECD. Auch wenn diese Richtlinien für die Mitgliedsstaaten nicht verbindlich sind, dienen sie häufig als Referenzrahmen für die Formulierung und Begründung nationaler Kryptopolitiken sowie internationaler Vereinbarungen.

Der mit diesen Richtlinien aufgespannte Rahmen für Krypto-Politiken basiert auf Grundsätzen, die Interpretations- und damit politische Gestaltungsspielräume offen lassen.

So besagt ein Grundsatz, daß die Nutzer ein Recht zur freien Wahl der Verschlüsselungsmethode haben: „Users should have a right to choose any cryptographic method, subject to applicable law."[178])

Der Anhang nach dem Komma ... „subject to applicable law" ... hat weitreichende Konsequenzen dahingehend, daß kryptographische Methoden, die nicht mit bestehenden Gesetzen übereinstimmen, auch nicht der freien Wahl des Nutzers zur Verfügung stehen. Ausdrücklich verweist aber die OECD im Kommentar darauf, daß sie dies nicht als Aufforderung einer Gesetzgebung verstanden haben möchte, die die freie Wahl des Nutzers einschränkt: „Governments control on cryptographic metods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible. **This principle should not be interpreted as implying that governments should initiate legislation which limits user choice.**"[179])

Die OECD-Richtlinien lassen Raum für eine nationale Gesetzgebung, die dem Staat und seine Sicherheitsbehörden einen gesetzlich definierten Zugang zu verschlüsselten Daten bei Berücksichtigung der anderen OECD-Grundsätze erlaubt. Auch hier gilt wieder: Wenn die OECD-Richtlinien die Möglichkeit eines Zugriffs auf verschlüsselte Daten durch staatliche Behörden offenhalten, so möchte die OECD sich nicht so verstanden wissen, daß sie zu einer entsprechenden Gesetzgebung auffordert. Unmißverständlich deutlich wird diese Politik der OECD im Grundsatz „Lawful Access": „ National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible." Im Kommentar heißt es dann: „If considering policies on cryptographic methods that provide lawful access, governments should carefully weigh the benefits, including the benefits for public safety, law enforcement and national security, as well as the risks of misuse, the additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. **This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.**"

Es folgen weitere Erläuterungen und Bestimmungen zum „lawful access". Demnach soll der rechtmäßige Zugriff auf private Schlüssel und verschlüsselte Daten folgende Bedingungen erfüllen:

– Das Verfahren des rechtmäßigen Zugriffs soll dokumentiert werden, damit die Rechtmäßigkeit der

[177]) So besitzen US-Hersteller bei PC-Betriebssystemen einen weltweiten Marktanteil von insgesamt rd. 90 % und bei Anwendungssoftware von ungefähr 80 %.

[178]) Vgl. Guidelines für cryptography policy, in: http://www.oecd.org/dsti/sti/it/secur/prod/crypto2.htm

[179]) Vgl. ebenda

Entschlüsselung nachträglich geprüft werden kann.

- Jedes Verfahren des rechtmäßigen Zugriffs soll entsprechend der jeweiligen Umstände immer zeitlich begrenzt sein.

- Beim Zugriff auf geheime Kryptoschlüssel sollte unterschieden werden, ob diese Schlüssel der Geheimhaltung oder anderen Funktionen dienen; bei Kryptoschlüsseln, deren Funktion der Erzeugung von Integrität und Authentizität dienen, sollte ein Zugriff nicht ohne die Einwilligung des Schlüsselinhabers erfolgen. [180])

Ausdrücklich hat sich die Europäische Ministerkonferenz über Global Information Networks, die im Juli 1997 in Bonn stattfand, auf die OECD Krypto-Guidelines bezogen. In der Erklärung der Minister heißt es: „They [the ministers] will work to achieve international avialbility and free choice of cryptography products and interoperable services, subject to applicable law, thus effectively contrbuting to data security and the confdentiality of personal and business information. If countries take measures in order to protect legitimate needs of lawful access, they should be propotionate and effective and respect applicable provisions relating to privay. Ministers take note of the recently agreed OECD Guidelines on Cryptography Policy as a basis for national policies and international co-operation." [181])

4.1.2.5 Zusammenfassung und Bewertung

Die Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft" hat in verschiedenen Anhörungen und Sitzungen betroffene und engagierte Institutionen und Gruppen zum Thema „Kryptographie und gesetzliche Regulierung" gehört. Nach vorsichtiger Abwägung aller Argumente ist die Enquete-Kommission zu dem Schluß gekommen, daß zum derzeitigen Zeitpunkt eine gesetzliche Regulierung der Kryptographie nicht geboten ist.

Es ist derzeit nicht erkennbar, daß eine gesetzliche Einschränkung der freien Wahl kryptographischer Methoden in Verbindung mit der Etablierung eines Key-Recovery-Mechanismus die Ermittlungsarbeit der Sicherungsbehörden erleichtern und unterstützen könnte, da für Kriminelle zahlreiche Ausweichmöglichkeiten existieren. Abgesehen von dem zweifelhaften Erfolg einer gesetzlichen Krypto-Regulierung existieren bei jedem Key-Recovery-System erhebliche Sicherheitsprobleme und Kostenrisiken, die sich gegen eine rasche und flächendeckende Verbreitung kryptographischer Systeme auswirken könnten.[182]) In diesem Zusammenhang vertritt die Enquete-Kommission die Auffassung, daß alle Maßnahmen und Hemmnisse, die einer breiten Nutzung von Verschlüsselungsverfahren entgegenwirken, vermieden und abgebaut werden müssen. Darüber hinaus sollte die breite Nutzung kryptographischer Verschlüssekungsmethoden aktiv unterstützt und gefördert werden. In diesem Zusammenhang sind Bund und Länder aufgefordert, geeignete Verschlüsselungsmethoden systematisch in ihrem elektronischen Datenverkehr einzusetzen.

Dabei erkennt die Enquete-Kommission an, daß durch die neuen Verschlüsselungsmethoden auch neuartige Gefährdungsformen entstehen und die Ermittlungsarbeit der Sicherheitsbehörden erschwert werden kann. Sie fordert deshalb die zuständigen Behörden auf, zu klären, welcher spezifische neue Sicherheitsbedarf durch Informationstechnologien entsteht und durch bestehende Gesetze nicht abgedeckt werden kann. Auf der Grundlage dieser Defizitermittlung ist zu klären, ob und welcher Handlungsbedarf beim Gesetzgeber existiert.

Die Enquete-Kommission sieht in Hinblick auf die Gestaltung der rechtlichen, technischen und gesellschaftlichen Rahmenbedingungen zur Nutzung der Kryptographie einen weitgehenden Abstimmungsbedarf innerhalb der Europäischen Union. Sie unterstützt deshalb das Vorhaben der Europäischen Kommission, bis zum Jahr 2000 eine europäische Rahmenordnung zur Kryptographie vorzulegen.

Die Entwicklung und der Einsatz eines weltweiten Key-Recovery-Systems ist mit nationalen Sicherheitsinteressen nicht vereinbar und wird deshalb von der Enquete-Kommission abgelehnt.

4.1.3 Abgrenzung zwischen Selbstregulierung, privater und staatlicher Verantwortung (Kompetenz des Regulierers)

Durch das anhaltend hohe Wachstum der Internetnutzung ist innerhalb von wenigen Jahren ein neuer – virtueller – Sozialraum entstanden. Darin ist der Mangel an IT-Sicherheit und Datenschutz ein grundlegendes Problem, dessen mögliche Lösungsansätze bereits ausführlich beschrieben wurden.

In diesem Abschnitt soll erörtert werden, welche Rolle der Staat im Verhältnis zur individuellen Selbstverantwortung und Institutionen der Selbstregulierung übernehmen kann, denn die Erzeugung von Sicherheit und Schutz im globalen Netzraum verlangt die Verantwortungsübernahme und Kooperation aller beteiligten Akteure und Organisationen.

Der Entwicklungsprozeß des Internet wurde von Beginn an von nichtstaatlichen, häufig dem Wissenschaftssystem zugehörigen Institutionen gestaltet und gesteuert. Zwar hat insbesondere die amerikanische Regierung durch den Ausbau der Datennetzinfrastruktur und Maßnahmen der Forschungsförderung den Entwicklungsprozeß des Internet

[180]) Vgl. ebenda
[181]) Global Information Networks 1997: Minsterial declaration, in: http://193.91.44.33/bonn/final.htm
[182]) Vgl. Abelson, H.; Anderson, R.; Bellovin, S. et. al., Risiken von Key-Recovery, Key-Escrow und Trusted Third Party-Verschlüsselung, in: DuD 22, 1998 1

unterstützt, aber eine Regulierung der inneren Netzwelt hat es von staatlicher Seite nicht gegeben[183]). Durch den Verzicht des Staates, über Nutzungsformen des Netzes zu entscheiden, konnte erst ein wirklich offenes Datennetzwerk entstehen. Diese Offenheit des Internet für Personen, Inhalte und neue technische Anwendungen hat allerdings auch vielfältige Probleme erzeugt, denen im Internet mit Mechanismen der Selbstregulierung als Möglichkeit der Problemlösung begegnet wurde und wird. Bevor die Selbstregulierung als konstituierendes Merkmal des Internet erörtert wird, soll zunächst nach der individuellen Verantwortung des Netznutzers gefragt werden und wie diese vom Staat gefördert werden kann.

4.1.3.1 Befähigung zum Selbstschutz als staatliche Aufgabe

Aus den nur sehr eingeschränkten Möglichkeiten des Staates seine Bürger im neuen Sozialraum der Netze effektiv zu schützen, erwächst für den Netznutzer die Notwendigkeit des Selbstschutzes. Weil der Staat keinen direkten Schutz mehr garantieren kann, obliegt ihm die Verpflichtung, den Netznutzer zum Selbstschutz zu befähigen[184]). Hierzu gehört zunächst, daß der Staat auf allen möglichen Ebenen über Risiken der Netznutzung und mögliche Gegenmaßnahmen aufgeklärt wird. Ergänzt werden muß dieses Aufklärungs- und Schulungsangebot durch die Förderung und Verbreitung geeigneter technischer Hilfsmittel des Selbstschutzes, die dem Netznutzer zu vertretbaren Kosten zugänglich gemacht werden müssen. Als Instrumente eines Basisselbstschutzes gelten „harte" Verschlüsselungssoftware und Digitale Signaturen. Hier ist der Staat gefordert, zum einen den Netznutzer zum kompetenten Umgang mit Selbstschutzinstrumenten, z. B. kryptographischerer Software, zu befähigen, zum anderen die Rahmenbedingungen für eine öffentliche Sicherungsinfrastruktur zu schaffen. Mit dem Gesetz zur Digitalen Signatur, das seit August 1997 in Kraft ist, hat die Bundesrepublik Deutschland erste wichtige Rahmenbedingungen für den Aufbau einer Sicherungsinfrastruktur geschaffen, ohne die eine abgesicherte breite Nutzung der Digitalen Signatur nicht möglich wäre.[185]) Damit ist eine andere wichtige Aufgabe des Staates angesprochen: Die Erzeugung von Rahmenbedingungen für die Umsetzung informationstechnischer Sicherheitsziele.

[183]) Diese Aussage darf nicht dahingehend mißverstanden werden, daß Gesetze, wie etwa das Strafrecht, nicht für das Internet gelten. Insofern gilt die soziale Regulierungsfunktion von Gesetzen natürlich auch für das Internet und ein Rechtsbruch, der im Internet verübt wird, zieht dieselben Strafverfolgungs- und Verurteilungsmechanismen nach sich wie Delikte außerhalb des Internet.

[184]) Vgl. Rossnagel, Alexander

[185]) Mit diesem Gesetz hat Deutschland eine Vorreiterrolle auch mit Blick auf eine entsprechende EU-weite Richtlinie für elektronische Signaturen übernommen. Am 13. Mai 1998 hat die Europäische Kommission einen „Vorschlag für Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen" [KOM(1998)297end] vorgelegt.

4.1.3.2 Staatlich geförderte Rahmenbedingungen für Sicherheit und Schutz im Netz

Eine Form der institutionellen Verbreitungsförderung kryptografischer Systeme ist der rasche und breit angelegte Einsatz von Verschlüsselungssoftware und digitaler Signaturen in öffentlichen Institutionen des Landes und des Bundes. Durch die systematische Anwendung von Verschlüsselung und digitaler Signatur beim elektronischen Datenaustausch sowohl zwischen den Behörden als auch zwischen Behörden und Wirtschaftsunternehmen könnte ein positiver Effekt für die weitere Verbreitung und Akzeptanz dieser Sicherheitswerkzeuge entstehen.

Bis heute bringen Softwarehersteller fehlerhafte und mit Sicherheitslücken versehene Software auf den Markt. Mögliche Schäden hat zunächst der Kunde. In diesem Zusammenhang muß die Eigenverantwortlichkeit der Hersteller bei der Lösung von IT-Sicherheitsproblemen stärker betont werden. Darüber hinaus sollte auch eine Überprüfung des Haftungsrechts erfolgen.

Zudem könnte der Aufbau eines Zertifizierungswesens überlegt werden, bei dem staatlich anerkannte Prüfstellen die Sicherheit von Soft- und Hardware nach gesicherten Kriterien und Verfahren prüfen. In vergleichbarer Weise könnte eine „Stiftung Softwaretest" eine bessere Sicherheits- und Funktionsfähigkeit von Softwareprodukten fördern.

Darüber hinaus kann der Staat die Entwicklung einer hinreichend flexiblen allgemeinen IT-Sicherheitsinfrastruktur initiieren, die zum einen unterschiedliche Sicherheitsniveaus, zum anderen der technischen Entwicklung Rechnung tragen kann.

Als Träger staatlicher Bildungs- und Forschungseinrichtungen sind Bund und Länder gefordert, Belange der IT-Sicherheit sowohl verstärkt in der Ausbildung als auch in der Forschung zu verankern. Nur eine systematische Verankerung von IT-Sicherheitsthemen in der Ausbildung und Forschung schafft die Voraussetzung für eine dynamisch sich entwickelnde IT-Sicherheit, die der hohen Innovationsdynamik im Bereich der Informationstechnologie gewachsen ist.

Und schließlich kann der Staat einen breit angelegten Dialog zwischen Politik und Bürgern, der Wissenschaft, der Wirtschaft, Institutionen der Selbstregulierung initiieren und moderieren, um zum einen das Bewußtsein für Belange der IT-Sicherheit – insbesondere des IT-Selbstschutzes – zu erhöhen, zum anderen aber auch, um ein Bild über die unterschiedlichen Bedürfnisse verschiedener Gruppen und der Entwicklungsdynamik informationstechnischer Sicherheitsthemen zu gewinnen.

4.1.3.3 Selbstregulierung als konstituierender Faktor des Internet

Dieser Dialog muß insbesondere mit jenen Institutionen geführt werden, die für Selbstregulierung im Internet stehen. Denn die eingangs dargestellte eingeschränkte Regulierungs-, Kontroll- und Schutzfunktion des Staates im digitalen Netzraum hinterläßt nicht notwendigerweise ein Vakuum. Die Entwick-

lungsgeschichte des Internets war und ist geprägt durch die Herausbildung nichtstaatlicher Selbstregulierungs-mechanismen. Der Begriff „Selbstregulierung" wirft allerdings die Frage nach den Regulierungsinstitutionen des Internet auf. Zunächst kann gesagt werden, daß diese Institutionen immer nichtstaatliche Stellen, sogenannte *Non Governmental Organisations* (NGO's), sind. Unterschieden werden muß aber zwischen NGO's, die im Sinne des Begriffes „Regulierung" tätig sind und jenen NGO's, die sich als politische oder anderweitige Initiative in das Internet einbringen, aber keinen direkten regulierenden Einfluß haben. Letztere gibt es in großer Zahl im Internet. Eine kleine Auswahl dieser NGO's wird im folgenden Abschnitt vorgestellt. In diesem Abschnitt liegt der Fokus auf jenen NGO's, die durch ihre Arbeit maßgeblichen Einfluß auf die Gestalt und die Entwicklung des Internet nehmen.

Hier können als wichtigste Regulierungsinstitutionen für das Internet die *Internet Society*[186]) und für das World Wide Web das am Massachusetts Institute of Technology (MIT) beheimatete *W3-Konsortium*[187]) genannt werden. [188])

4.1.3.3.1 Die Internet Society (ISOC)

wurde 1992 gegründet und umfaßt mehr als 100 Mitgliedsorganisationen und 7 000 individuelle Mitglieder aus mehr als 150 Nationen. ISOC verfügt über weltweit verteilte Zweigstellen – so auch in Deutschland.[189])

Sie beschreibt sich selbst als „non-governmental International organization for global cooperation and coordination for the Internet and its internetworking technologies and applications."[190])

Ihr *mission statement* lautet: „To assure the beneficial, open evolution of the global Internet and its related internetworking technologies through leadership in standards, issues, and education."

Unter dem Dach der Internet Society arbeiten der Internet Architecture Board (IAB), die Internet Engineering Steering Group (IESG) und die Internet Engineering Task Force (IETF) an der technischen Weiterentwicklung des Internet. Die ISOC engagiert sich auch bei allen politischen Belangen des Internet. So ist z. B. im Arbeitsprogramm der ISOC der Punkt „Schutz gegen Überregulierung" verzeichnet. Hierzu zählt u. a. das Engagement der ISOC gegen eine exzessive Kontrolle der Kryptografie durch Regierungen und gegen die Einführung von Key Recovery.[191]) Darüber hinaus betreibt die ISOC umfangreiche Bildungsarbeit. Und schließlich zählt auch das Thema „Sicherheit im Internet" zu ihren Aufgabenfeldern. Die ISOC sponsert hierzu das jährlich stattfindende Symposium Network and Distributed System Security [192]).

4.1.3.3.2 Das W3-Consortium

hat für die Weiterentwicklung des World Wide Webs eine ähnlich zentrale Bedeutung wie die ISOC für das Internet. Gegründet wurde das W3-Konsortium 1994. Seine Hauptstandorte sind das Massachusetts Institute of Technology/Laboratory for Computer Science (MIT/LCS) in den USA, das Institut National de Recherche en Informatique et en Automatique (INRIA) in Europa und die Keio University Sonan Fujisawa Campus in Japan. Außerdem unterhält das W3-Consortium seit März 1998 eine deutsche Zweigstelle bei der GMD-Forschungszentrum Informationstechnik GmbH, um die Kontakte zu Unternehmen im deutschsprachigen Raum auszubauen. Anders als die ISOC nimmt das W3-Consortium keine individuellen Personen, sondern nur Organisationen und Unternehmen auf. Es versteht sich selbst als Industriekonsortium, dem 220 wissenschaftliche und wirtschaftliche Organisationen aus der ganzen Welt angehören. Zu diesen Mitgliedern zählen große Softwareunternehmen, Telekommunikationsgesellschaften, Content Provider, staatliche und akademische Organisationen. Geleitet wird es von Tim Berners-Lee, der das World Wide Web Anfang der 1990er-Jahre am Genfer CERN maßgeblich mitentwickelt hatte.

Das Motiv für die Gründung des W3-Konsortiums wird so beschrieben: „The W3C was found to develop common protocols to enhance the interoperability and lead the evolution of the World Wide Web."

Diese allgemeine Aufgabendefinition des W3C mündet in ein umfassendes Arbeitsprogramm, in dessen Zentrum die Weiterentwicklung der Internet-Protokolle und der HTML-Sprache steht.

Für den thematischen Zusammenhang dieses Zwischenberichtes ist es wichtig darauf hinzuweisen, daß das W3C sehr umfangreiche Forschungsarbeiten und Projekte zur IT-Sicherheit und dem Datenschutz durchführt. So gibt es z. B. die Projekte „Digital Si-

---

[186]) http://www.isoc.org/iso

[187]) http://www.w3.org

[188]) Die hier gemachte Unterscheidung zwischen NGO's mit und ohne Regulierungskompetenz dient in erster Linie einer besseren Beschreibbarkeit ohne für sich in Anspruch zu nehmen, die Wirklichkeit des Internet objektiv abzubilden. Ohne Zweifel sind ISOC und das W3C Organisationen mit zentraler Bedeutung für das Internet. Beachtet werden muß aber, daß diese Organisationen in erster Linie an der technischen Entwicklung des Internet arbeiten. In Hinblick auf die Regulierung des körperlosen Sozialraumes repräsentieren das „Selbst" des Internet über diese beide großen Instituionen hinaus zahlreiche andere NGOs, die sich z. B. aktiv gegen Kinderpornografie, Netzkriminalität, für Datenschutz und IT-Sicherheit, gegen Key Recovery, gegen Zensur, für Bildung, für ethische Verhaltensregeln etc. einsetzen. In diesem Sinne findet die Regulierung des Internet nicht durch statische Institutionen statt, sondern ist ein dynamischer Prozeß kommunikativ gewonnener Übereinstimmungen von Netzteilnehmern.

[189]) Siehe: http://www.isoc.de/isoc/presse.html

[190]) Vgl. http://www.isoc.org/iso

[191]) Vgl. http://www.isoc.org/isoc/mission/program; http://www.isoc.org/isoc/media/releases/cryptography_release.sht.

[192]) Vgl. http://www.isoc.org/isoc/mission/program

gnature Initiative", „Platform for Privacy Preferences"[193]) und „Platform for Internet Content Selection (PICS)[194])." Im Rahmen der Electronic Commerce Initiatives beteiligt sich W3C an der Entwicklung sicherer Zahlungsmittel.

Auf europäischer Seite ist RIPE (Réseaux IP Européens) zu nennen, die die adminstrative und technische Koordination der europäischen IP-basierten Datennetzwerke übernommen hat.[195])

4.1.3.4 Berührungspunkte zwischen Selbstregulierung und staatlichem Handlungsauftrag

Die entwickelten demokratischen Staaten, Staatenbündnisse und zahlreiche internationalen Organisationen haben sich die Förderung und den Ausbau des Internet zum Wohle der Wissenschaft, der Wirtschaft und des Bürgers zur Aufgabe gemacht. Dieser politische Wille ist in zahllosen Deklarationen, Programmen und Studien zum Ausdruck gebracht und mit erheblichen staatlichen Investitionen in den Ausbau der Netzinfrastruktur und in neue Technologien praktisch umgesetzt worden. Es existiert auch ein weitgehend geteiltes Verständnis darüber, daß die weitere Entwicklung des Internet sich aus der freien Kraft seiner Institutionen und Akteure entfalten und dabei nicht durch staatliche Überregulierung behindert werden sollte.

Die Einsicht demokratischer Rechtsstaaten in ihre nur noch beschränkt gegebenen Regulierungsmöglichkeiten bei gleichzeitiger Bereitschaft, die weitere Entwicklung des Internet aktiv zu fördern, korrespondiert im Grundsatz mit den Interessen und der Arbeit der Selbstregulierungsinstanzen des Internet.

Zwischen staatlichen Regulierungsinstanzen und Institutionen der Internet-Selbstregulierung besteht bislang ein übereinstimmendes Interesse an einer Selbstregulierung des Netzes. Erleichtert wird dies durch zahlreiche Ziel- und Interessenübereinstimmungen beider Seiten, wie etwa:

- Herstellung und Verbesserung von IT-Sicherheit und Datenschutz im Netz
- Befähigung des Netznutzers zum Selbstschutz
- Entwicklung organisatorischer und technischer Maßnahmen zur Bekämpfung von Netzkriminalität
- Entwicklung organisatorischer und technischer Maßnahmen zu einem verbesserten Kinder- und Jugendschutz im Netz
- Entwicklung organisatorischer und technischer Maßnahmen für den Urheberschutz im Netz
- Nutzung des Internet zur Aufklärungs- und Bildungsarbeit
- Weiterentwicklung der kommerziellen Nutzungsmöglichkeiten des Internet und sicherer elektronischer Zahlungsmittel

Diese Themenfelder zeigen beispielhaft Berührungspunkte und sich ergänzende Interessen zwischen staatlichem Handlungsauftrag und der Arbeit von Selbstregulierungsinstitutionen auf. Der Staat kann hier fördernd wirken, indem er Rahmenordnungen schafft, in denen sich die gemeinsamen Ziele gut entfalten können. Hierzu ist ein intensiver und kontinuierlicher Dialog zwischen Staat und Selbstregulierungsinstanzen notwendig. Außerdem kann der Staat Initiativen ergreifen, um die gemeinsamen Ziele zu unterstützen.

Grundsätzlich können entsprechende staatliche Organisationen sich aber auch direkt an der Arbeit von Selbstregulierungsinstanzen, wie der ISOC und dem W3-Consortium beteiligen. Eine Mitgliedschaft staatlicher Organisationen ist in beiden Institutionen möglich.

Insgesamt muß die Rollenverteilung zwischen Staat und Selbstregulierungsinstitutionen mit Blick auf die weiteren Entwicklungmöglichkeiten des Internet als effizient und sich gegenseitig ergänzend betrachtet werden. Die zurückhaltende Rolle des Staates schafft den notwendigen Freiraum, damit sich der konzentrierte Sachverstand der Selbstregulierungsinstitutionen im Entwicklungsprozeß des Internet positiv entfalten kann, und umgekehrt: Durch den intensiven Dialog zwischen Selbstregulierern und dem Staat werden wichtige Impulse für eine sinnvolle Ausgestaltung der staatlichen Rahmenordnung gegeben.

Abschließend kann festgestellt werden, daß die Perspektive des Verhältnisses von Staat und Selbstregulierungsinstitutionen in einer sich ergänzenden produktiven Gemeinschaft liegt und der einzelne Staat nur mäßige Chancen hat, Regulierungsvorhaben durchzusetzen.

Die Einschränkung einzelstaatlicher Regulierungsmöglichkeiten kann potentiell über Staatenbündnisse – wie die Europäische Union – oder internationale Verträge und Vereinbarungen aufgehoben werden, weil internationale Regeln und Standards der globalen Flächenausdehnung des Internet eher gerecht werden als vergleichbare Aktivitäten von Einzelstaaten. Welche Möglichkeiten hierzu existieren wird u. a. das Thema des nächsten Abschnitts sein.

4.1.4 Nationale und internationale Aufgaben

Die globale Dimension des Internet schränkt die Regulierungsmöglichkeiten des Netzraumes durch einzelne Staaten erheblich ein. In den Abschnitten 4.1.3ff. sind die verbleibenden Handlungsmöglichkeiten des einzelnen Staates und die Bedeutung von Selbstregulierungsinstitutionen für das Internet dargestellt und erörtert worden. In diesem Abschnitt liegt der Schwerpunkt in der Bedeutung internationaler Institutionen, Vereinbarungen, Standards und

[193]) Vgl. hierzu http://www.w3c.org/securit

[194]) PICS ist ein Protokoll zur Beschreibung der Inhalte von Internet-Dokumenten. Mit Hilfe dieses Protokolls können Internet-Dokumente nach bestimmten Kriterien gefiltert, aber auch mit Meta-Informationen, wie z. B. Urheberrecht-Erläuterungen und Nutzungsinformationen ausgestattet werden; vgl. hierzu http://www.w3c.org/securit

[195]) Vgl. http://info.ripe.net/info/ripe/ripe.htm

Verträge für die Verbesserung der IT-Sicherheit im globalen Netzraum. In einem zweiten Teil wird die Bedeutung von *Non Governmental Organisations* (NGOs) in diesem Prozeß betrachtet.

Für die Durchsetzung internationaler IT-Sicherheitsstandards sind die *Common Criteria for Information Technology Security Evaluation (CC)* von zentraler Bedeutung. Sie stellen in der internationalen Diskussion um IT-Sicherheit ein zentrales Referenzdokument dar und können als ernsthafter Versuch gesehen werden, einen Rahmen für internationale IT-Sicherheitsstandards zu schaffen. Entsprechend ihrer Bedeutung leiten Sie die Übersicht zu internationalen Institutionen im Bereich der IT-Sicherheit ein. Vergleichbares gilt für die *OECD Guidelines for the Security of Information Systems,* die von allen 24 Mitgliedstaaten der OECD angenommen wurden.

Der Entfaltung einer digitalen Ökonomie wird international große Bedeutung zugemessen. In Hinblick auf die Herstellung von Rechtssicherheit beim Electronic Commerce ist die digitale Signatur unverzichtbares und bisher nicht ersetzbares Instrument.[196]) Die Gewinnung von Rechtssicherheit durch die digitale Signatur verlangt die rechtliche Abstützung dieses Instruments. Deshalb sind sowohl auf nationaler und mit Blick auf die globale Dimension des digitalen Handels auch auf internationaler Ebene Regulierungsinitiativen zur digitalen Signatur entstanden. In diesem Zusammenhang wird auch ein kurzer Blick auf die Initiativen zum *Electronic Data Interchange* geworfen.

4.1.4.1 Die Common Criteria[197])

Die Common Criteria repräsentieren die Ergebisse einer Initiative der EU, der USA und Kanada, allgemeine Kriterien für die Evaluation von IT-Sicherheit in der internationalen Gemeinschaft zu entwickeln. Dieser Initiative vorausgegangen waren die Entwicklungen von jeweils eigenen Evaluierungskriterien in den beiden Ländern und der EU. In den frühen 1980er-Jahre hatten die USA als erstes Land die *Trusted Computer System Evaluation Criteria (TCSEC)* entwickelt, die zahlreichen anderen Ländern bei der Entwicklung ihrer Evaluationskriterien als Referenzrahmen dienten. Die Europäische Kommission gab die gemeinsam von Frankreich, Deutschland, die Niederlande und Großbritannien entwickelten *Information Technology Security Evaluation Criteria (ITSEC)* im Jahre 1991 heraus. Von Kanada wurden 1993 die *Canadian Trusted Computer Product Evaluation Criteria (CTCPEC, Version 3.1)* mit dem Ziel entwickelt, die US- und EU-Kriterien zu kombinieren. Auch die zweite im Jahre 1993 herausgegebene Vorlage der USA – die *Federal Citeria for Information Security (FC)* war von dem Bemühen gekennzeichnet, das europäische mit dem amerikanischen Konzept zu kombinieren.

Den Versuch, einen von vornherein international angelegten Standard für die Evaluierung der Sicherheit von IT-Systemen zu entwickeln, wurde 1990 von der International Organisation for Standardisation (ISO) gestartet. Schließlich begannen 1993 die Akteure von CTCPEC, FC, TCSEC und ITSEC, ihre jeweiligen Kriterien auf eine Linie zu bringen und ein gemeinsames Dokument – *die Common Criteria* – bei der ISO als Beitrag zu deren Standardisierungsbemühungen vorzulegen.

Die Träger der Entwicklungsarbeit an den Common Criteria sind die Europäische Union (EU), die U. S. National Security Agency (NSA), das U. S. Nationale Institute of Standards and Technology (NIST) und das Canadian Communications Security Establishment (CSE). In enger Kooperation mit dem Common Criteria Implemention Board (CCIB) arbeitet die ISO Working Group (WG3) an der Entwicklung internationaler Sicherheitsstandards. Die Perspektive der Arbeit dieser beiden Organisationen ist die Herausgabe gemeinsamer IT-Sicherheitskriterien.

Mit den Common Criteria ist ein umfassender Katalog von Evaluierungskriterien für IT-Sicherheit vorgelegt worden, in dessen Rahmen international vergleichbare Prüfkriterien entwickelt werden können und auf dessen Grundlage die sicherheitstechnische Ausstattung von IT-Systemen vergleichbar wird.

Die CC unterscheiden auf der einen Seite zwischen drei Zielgruppen – den Konsumenten, den Entwicklern von IT-Systemen und den Prüfern von IT-Sicherheit; auf der anderen Seite existieren fünf thematische Hauptgruppen, die die inhaltliche Struktur der CC abbilden. Daraus ergibt sich folgende Funktionsübersicht der CC:

---

[196]) Vgl. hierzu den Abschnitt 2.4 dieses Zwischenberichtsteils

[197]) Das vollständige Dokument kann z. B. über http://cse.dnd.ca/cse/english/cc.htm oder auch über http://www.nist.gov/cgi-bin/swish-query.pl Unter dieser Internetadresse kann auch die Kurzfassung der CC bezogen werden.

Roadmap of Common Criteria[198])

	Consumers	Developers	Evaluators
Part 1 Introduction and general model. Defines general concepts and principles of IT-security evaluation and presents a general model of evaluation.	Use for background information and reference purposes.	Use for background information and reference for the development of requirements and formulating security specifications for TOEs.	Use for background information and reference purposes. Guidance structure for PPs and STs.
Part 2 Security functional requirements for TOEs[199])	Use for guidance and reference when formulating statements of requirements for security functions.	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Mandatory statement of evaluation criteria when determining whether TOE effectively meets claimed security functions.
Part 3 Security assurance requirements presents evaluation assurance levels that define the CC scale for rating assurance for TOEs	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.
Part 4 Predefined Protection Profiles initially contains examples of PPs[200]) that represent functional and assurance requirements which have been identified in source criteria. Part 4 will ultimately become the registry for PPs which have completed the registration process.	Use for guidance and reference when formulating requirements.	Use for reference when interpreting statements of requirements and formulating security specifications for TOEs.	Mandatory reference base when determining claimed conformance of TOEs to PPs.
Part 5 Registration procedures will define the procedures necessary to register additional PPs and to maintain them in an international registry	Use for guidance when offering PPs for registration	Use for guidance when offering PPs for registration	Use for guidance when determining whether PPs are eligible for registration

198) Vgl. CCEB-96/011, Textmarke 24
199) TOE: Technical-Organisational-Entity
200) PP: Protection Profile

Mit Blick auf die globale Dimension des Marktes für Informationstechnologie und der weltweiten Daten- und Telekommunikationsinfrastruktur können die CC als Ausgangsplattform für die Entwicklung einer weltweiten IT-Sicherheitsinfrastruktur betrachtet werden. Durch die CC werden nationale, mit IT-Sicherheit betraute Organisationen, wie z.B. das Bundesamt für Sicherheit in der Informationstechnik, in die Lage versetzt, Sicherheitsanforderungen für IT-Systeme so zu definieren, daß sie mit jenen anderer Länder weitgehend kompatibel sind. Der Wert solcher internationaler Standards für IT-Sicherheit kann gar nicht hoch genug eingeschätzt werden. Dies gilt insbesondere für global tätige Wirtschaftsunternehmen, die auf der Grundlage internationaler Sicherheitsstandards für ihre über mehrere Länder hinweg verteilte elektronische Informations- und Kommunikationsinfrastruktur einheitliche Sicherheitsstandards auf hohem Niveau etablieren können.[201])

Den Herstellern von IT-Systemen und den Dienstleitern in diesem Bereich dienen Standards für die sicherheitstechnische Auslegung ihrer IT-Systeme. Und schließlich werden durch internationale Sicherheitsstandards die Transaktionskosten bei der Zusammenarbeit mehrerer Hersteller und Dienstleister gesenkt, denn etwaige IT-Sicherheitsnachrüstungen wegen unterschiedlicher nationaler Sicherheitsniveaus könnten entfallen.

4.1.4.2 Die OECD Guidelines for the Security of Information Systems

Im Abschnitt 4.1.2.4 sind die OECD Guidelines on Cryptography Policy als Referenzdokument in der internationalen Kryptodebatte vorgestellt worden. Über Politikempfehlungen zu einem partiellem Thema der IT-Sicherheit hinaus, hat die OECD 1992 erstmalig Richtlinien für die Sicherheit von Informationssystemen herausgegeben, die in einer revidierten Form 1997 wieder erschienen sind.

Als Ziele dieser Richtlinien werden angegeben:

- Das Bewußtsein für die Risiken von Informationssystemen sowie für entsprechende Schutzmöglichkeiten zu stärken;
- Einen allgemeinen Bezugsrahmen für jene zu schaffen, die im öffentlichen und privaten Sektor für die Entwicklung und Umsetzung von kohärenten Konzepten, Maßnahmen und Verfahrensweisen zur Erzeugung von IT-Sicherheit zuständig sind;
- Die Zusammenarbeit zwischen dem privaten und öffentlichen Sektor bei der Entwicklung und beim Einsatz dieser Konzepte, Maßnahmen und Verfahrensweisen zu stärken;
- Das Vertrauen in Informationssysteme zu stärken;
- Die Entwicklung und Nutzung national und international zu erleichtern; und
- Die internationale Zusammenarbeit bei der Erzeugung von IT-Sicherheit zu unterstützen.[202])

Die Mitgliedsländer der OECD umfassen Nordamerika, die pazifische Region und Europa. Dieser weite geopolitische Radius schafft gute Voraussetzungen für eine weitreichende internationale Resonanz der OECD-Richtlinien bezüglich der Entwicklung und Umsetzung von IT-Sicherheitskriterien. Die Richtlinien umfassen Gesetze, Verhaltensrichtlinien, technische Maßnahmen, Gebote für IT-Adminstratoren und Nutzer sowie Vorschläge für öffentliche Schulungsmaßnahmen. Diese Richtlinien sind in ihrer Gestalt wesentlich offener und unspezifizierter als die Common Criteria.

Sie stehen damit nicht in einem Widerspruch zu diesen, sondern bilden den deutlich weiteren Rahmen. Sie tragen damit entscheidend zu einer Schärfung des Bewußtseins über mögliche Risiken und möglicher Schutzstrategien auf internationaler Ebene bei, auch wenn davon ausgegangen werden kann, daß für die weitere konkrete Ausgestaltung einer globalen IT-Sicherheitsstruktur die Common Criteria entscheidender sind.

4.1.4.3 Electronic Commerce, nationale und internationale Initiativen zur digitalen Signatur

Die digitale Signatur eignet sich in hervorragender Weise zur exemplarischen Darstellung nationaler und internationaler Regulierungsinititiativen zu einem Teilproblem der IT-Sicherheit.

Die bereits weit fortgeschrittenen Bemühungen, die digitale Signatur sowohl auf nationaler als auch auf internationaler Ebene als ein Instrument zur Erzeugung von IT-Sicherheit rechtlich abzustützen, erklärt sich aus der hohen Bedeutung, die dem Electronic Commerce für die weitere wirtschaftliche Entwicklung beigemessen wird. Wie in diesem Zwischenberichtsteil bereits mehrfach gezeigt wurde, kann Rechtssicherheit derzeit nicht ohne digitale Signatur hergestellt werden. Dieser Umstand bedeutet aber auch, daß ohne Rechtssicherheit Electronic Commerce sein Potential nicht entfalten kann. Diese Ausgangslage beschreibt nationalen und internationalen politischen Handlungsbedarf dergestalt, daß zunächst der Aufbau einer organisatorischen und technischen Infrastruktur zur Erzeugung und Verwaltung der digitalen Signatur geschaffen werden muß, um in einem zweiten Schritt die digitale Signatur einer natürlichen Unterschrift rechtlich gleichzustellen. Im Hinblick auf die Regulierung der organisatorischen und infrastrukturellen Voraussetzungen war die Bundesrepublik Deutschland mit dem im August 1997 in Kraft getretenen Gesetz zur Digitalen Signatur im Rahmen des Informations- und Kommunikationsdienstegesetzes (IuKDG) Vorreiter einer Entwicklung, die ihre transnationalen und internationalen Entsprechungen in Initiativen der EU bis hin zur UN-Kommission für internationales Handelsrecht (UNCITRAL) hat.

[201]) Vgl. hierzu den Abschnitt 1.4

[202]) Vgl. http://oecd.org./dsti/sti/it/secur/prod/e_secur.htm

4.1.4.3.1 Die Initiativen der Europäischen Kommission zur digitalen Signatur

In einem ersten Schritt unterbreitete die europäische Kommission dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuß und dem Ausschuß der Regionen 1997 eine Mitteilung über „Sicherheit und Vertrauen in elektronische Kommunikation – ein europäischer Rahmen für digitale Signaturen und Verschlüsselung"[203]) Der Rat der Europäischen Union begrüßte die Mitteilung und forderte die Kommission auf, einen Vorschlag für eine entsprechende Richtlinie vorzulegen. Dieser Aufforderung folgte die Kommission im Mai 1998 mit einem „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen".[204]) Damit ist ein weiterer wichtiger Schritt für die europaweite Schaffung eines einheitlichen Rechtsrahmen für digitale Signaturen getan.

Dieser Aspekt wird auch als zentrale Begründung für den Richtlinienvorschlag angeführt: „Die Sicherstellung der – insbesondere grenzüberschreitenden – rechtlichen Anerkennung elektronischer Signaturen und von Zertifizierungsdiensten gilt als wichtigste Aufgabe in diesem Bereich."[205]) Hinzu kommt eine Vielzahl von Regulierungsinitiativen in den Mitgliedsländern, die sich im Kern zwar auf dieselben Konzepte konzentrieren, aber im Ergebnis dann doch zu voneinander abweichenden Rechtslagen führen.[206])

Die Regulierungsbandbreite des Richtlinienvorschlages entspricht in etwa dem des deutschen Gesetzes. Hinzu kommt aber im Artikel 5 Abs. 2 des Vorschlages die Aufforderung an die Mitgliedsländer, die rechtlichen Voraussetzungen für eine Gleichstellung der digitalen Signatur zu einer natürlichen Unterschrift zu schaffen und als Beweismittel vor Gericht zuzulassen.[207]) Dies bedeutet, daß auch für die Bundesrepublik Deutschland über das IuKDG hinaus weiterer gesetzgeberischer Handlungsbedarf besteht, denn das Gesetz zur digitalen Signatur schafft noch nicht die rechtlichen Voraussetzungen für eine Gleichstellung der digitalen Signatur zur natürlichen Unterschrift.

Mit Blick auf den globalen Anwendungszusammenhang digitaler Signaturen hat die Kommission in ihrem Regulierungsvorschlag im Artikel 7 Voraussetzungen für die Anerkennung von Zertifikaten aus Drittländern festgelegt.[208]) Die Positionierung der digitalen Signatur als Gegenstand internationaler Vereinbarungen und gegenseitiger Anerkennung reflektiert auch die zahlreichen Aktivitäten und Diskussionen auf internationaler Ebene.

Unter anderem wird Bezug genommen auf die Initiativen der UNCITRAL und der OECD. Ausdrücklich wird festgestellt, daß die laufenden Entwicklungen auf internationaler Ebene bei der Einführung europäischer Richtlinien zu berücksichtigen sind.[209])

4.1.4.3.2 Die Initiative der United Nations Commission on International Trade Law (UNCITRAL)

Die UNCITRAL hat im Januar 1998 einen Vorschlag für einheitliche Regeln zur digitalen Signatur (Draft Uniform Rules on Electronic Signatures)[210]) vorgelegt. Mit der Erarbeitung dieser Regeln war 1996 die Arbeitsgruppe „Electronic Commerce" beauftragt worden. Diese Arbeitsgruppe hatte ein Modellgesetz zum Electronic Commerce vorgelegt, zu dem die Signaturregeln als konsistente Ergänzung erarbeitet worden sind. Die Zielsetzung dieser Regeln ist die Harmonisierung der länderspezifischen Regulierungsinitiativen, um damit günstige Voraussetzung für den Einsatz digitaler Signaturen bei internationalen Geschäftstransaktionen zu erzeugen. Die Arbeit der UNCITRAL-Arbeistgruppe konzentriert sich auf die privatrechtlichen Aspekte des Electronic Commerce. Ein besonderer Schwerpunkt der UNCITRAL-Regeln ist die Etablierung notwendiger Standards für Zertifizierungsinstanzen bei besonderer Berücksichtigung transnationaler Zertifizierungsprozesse. Mit den „Einheitlichen Regeln" versucht UNCITRAL nicht alle Fragen, die mit der Nutzung digitaler Signaturen entstehen, zu lösen. „In particular, the Uniform Rules do not deal with aspects of public policy, administrative law, consumer law or criminal law that may need to be taken into account by national legislators when establishing a comprehensive legal framework for electronic signatures."[211])

Die Regulierungstatbestände der UNICITRAL-Regeln entsprechen weitgehend denen der Europäischen Kommission.

Die rechtlichen Entwicklungen und die damit einhergehenden Standardisierungsprozesse zur digitalen Signatur illustrieren deutlich, wie nationale und internationale Institutionen mit ihren Initiativen ineinandergreifen, um für ein Teilproblem der IT-Sicherheit harmonisierte Rechtsbedingungen zu schaffen. Es darf dabei nicht verkannt werden, daß die fortgeschrittene Entwicklung bei der internationalen Regulierung digitaler Signaturen sich durch die große Bedeutung dieses IT-Sicherheitsinstruments für die Gewinnung von Rechtssicherheit beim elektronischen Handel erklärt.

Aus der Perspektive von IT-Sicherheitszielen erweist sich Electronic Commerce als ein kraftvolles Vehikel für die internationale, rechtlich abgesicherte Etablierung digitaler Signaturen. Es darf erwartet werden, daß die Telemedizin mit ihren sehr hohen IT-Sicherheits – und Datenschutzanforderungen – eine ver-

[203]) KOM (97) 503 endgültig vom 8. Oktober 97
[204]) Vgl. KOM(1998)297end S. 2–3
[205]) ebenda, S. 3
[206]) ebenda, S. 5
[207]) ebenda, S. 13–14
[208]) ebenda, S. 15
[209]) ebenda, S. 4
[210]) UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW/Working Group on Electronic Commerce; Thirty-second session, Vienna, 19–30 January 1998 DRAFT UNIFORM RULES ON ELECTRONIC COMMERCE, in: http://www.un.or.at/uncitral/sessions/wg_ec/wp-73.html
[211]) ebenda (I. General Remarks)

gleichbare Funktion in Hinblick auch auf andere IT-Sicherheitsziele übernimmt.

Allgemein kann gefolgert werden, daß die Chancen bestimmter IT-Sicherheitsziele Objekte internationaler Regulierungsinitiativen zu werden, von deren Bedeutung für übergeordnete Ziele abhängen.

4.1.4.4 Electronic Data Interchange

Ein anderes Beispiel weitreichender internationaler Standardisierung ist Electronic Data Interchange (EDI). EDI steht für einen plattformunabhängigen elektronischen Datenaustausch strukturierter Geschäftsinformationen zwischen Computersystemen.[212]) Es ist ganz besonders nützlich bei dem Austausch großer Datenvolumen, die in standardisierter Form vorliegen.[213]) Beispiele hierfür sind

- Finanzielle Transaktionen,
- Bestellungen und Rechnungen,
- Statistische Daten,
- Personendaten und Patientenakten.

Es gibt standardisierte EDI-Formulare sowie Programme, die eine automatische Übersetzung in das EDI-Format vornehmen.

In der Gruppe der EDI-Anwendungen ist EDIFACT (EDI For Adminsitration Commerce and Trade) besonders bedeutsam, weil es zwei weit verbreite Standards – das amerikanische JEDI und den Standard der Vereinten Nationen für Europa – miteinander verbindet.

Seine Definition lautet: „The agreed representation of information (what items and how they are individualy structured and put together) to be sent from one computer application to another."[214]) Der EDIFACT-Standard bezieht sich auf Datenelemente (Wörter), Segmente (Sätze) und Syntax (Grammatik).

Grundsätzlich sind mit EDI dieselben IT-Sicherheitsprobleme verbunden wie mit anderen Formen der Datenübertragung in offenen elektronischen Netzwerken. EDI unterscheidet sich aber insofern, als daß bei den internationalen Vereinbarungen, die die Entwicklung dieses Kommunaktionssystems begleiteten, Belange der IT-Sicherheit früh systematisch mitberücksichtigt wurden und sich in standardisierten Sicherheitsparametern niedergeschlagen haben.

Als Beispiele hierfür können die *Uniform rules of conduct for interchange of trade data by teletransmission* (UNICID)[215]) der International Chamber of Commerce (ICC) aus dem Jahre 1987 und die Europäische EDI-Mustervereinbarung von 1994 angeführt werden.

In den UNICID gibt es zahlreiche Regeln, die auf IT-Sicherheitsaspekte abzielen: So heißt es im Artikel 6 (Messages and transfers): "A transfer should identify the sender and the recipient; it should include means of verifying, either trough the technique used in the transfer itself or by some other manner provided by the TDI-AP[216]) concerned, the formal completeness and authentication of the transfer.[217])

Und im Artikel 9 (Protection of trade data) werden die am Datenaustausch beteiligten Parteien zu Schutzmaßnahmen aufgefordert: „The parties may agree to apply special protection, where permissible, by encryption or by other means, to some or all data exchanged between them."[218])

In ähnlicher Weise ist im Artikel 6 (Sicherheit von EDI-Nachrichten) der Europäischen EDI-Mustervereinbarung zu lesen:

„6.1 Die Parteien verpflichten sich, Sicherheitsverfahren und -maßnahmen durchzuführen und aufrechtzuerhalten, um EDI-Nachrichten vor unbefugtem Zugriff, Veränderungen, Verzögerung, Zerstörung oder Verlust zu schützen.

6.2 Zu den Sicherheitsverfahren und -maßnahmen gehören die Überprüfung des Ursprungs, die Überprüfung der Integrität, die Nichtabstreitbarkeit von Ursprung und Empfang sowie die Gewährleistung der Vertraulichkeit von EDI-Nachrichten.

Sicherheitsverfahren und -maßnahmen zur Überprüfung des Ursprungs und der Integrität, um den Sender einer EDI-Nachricht zu identifizieren und sicherzustellen, daß jede empfangene EDI-Nachricht vollständig ist und nicht verstümmelt wurde, sind für alle Nachrichten obligatorisch. Bei Bedarf können im Technischen Anhang zusätzliche Sicherheitsverfahren und – maßnahmen festgelegt werden."[219])

In den USA sind IT-Sicherheitsparameter in EDI-Standards verankert worden: So hat eine Arbeitsgruppe des American National Institute of Standards (ANSI) zur Verschlüsselung, zu Sicherheitsstrukturen und zu einem Dateiformat für kryptografisches Schlüsselmanagement entwickelt. Diese Standards schließen die Funktionen Schlüsselerzeugung, Schlüsselverteilung und Schlüsselinstallation (einschließlich automatische Verteilung und Austausch von Schlüsseln) ein. [220])

EDI ist ein gutes Beispiel dafür, wie bei der Entwicklung eines internationalen Informations- und Kommunikationsstandards Belange der IT-Sicherheit systematisch mitberücksichtigt werden. Bei der weiteren Entwicklung internationaler Vereinbarungen

---

212) „E.D.I. is defined as the transfer of structured data by agreed message standards from computer to computer by electronic means" in http://ganges.cs.tcd.ie/4ba2/ed

213) Vgl. Electronic Data Interchnage, in: http://www.ewos.be/edi/gtop.htm

214) Vgl. „Introduction to EDIFACT in http://ganges.cs.tcd.ie/4ba2/edi/intro.htm

215) ICC publication No. 452

216) Trade data interchange application protocol: Eine akzeptierte Methode für den Austausch von Handelsdaten (trade data messages), die auf internationalen Standards für die Präsentation und Strukturierung von Handelsdaten beruht, die über Telekommunikationsnetze befördert werden.

217) UNCID/ICC publication No. 452

218) ebenda

219) Europäische EDI-Mustervereinbarung und Kommentar vom 19. Oktober 1994 (94/820/EG)

220) Vgl. Electronic Commerce World Institute. A road map to EDI, Chapter 10, in: http://www.ecworld.org/Resource_Center/Agora/Roadmap/chapt10.htm

und Standards muß geprüft werden, inwieweit sich die EDI-Regeln und Standards bewährt haben und in modifizierter Form auf andere Telekommunikations- und Datennetze übertragen werden können.

Die bisher in diesem Abschnitt aufgezeigten internationalen Initiativen zu einer harmonisierten Regulierung von IT-Sicherheit beziehen sich auf große, von der Völkergemeinschaft getragenen Institutionen bzw. auf Staatenbündnisse. Dieses System kann, bildhaft gesprochen, als die großen Netzknoten in einem globalen Institutionennetzwerk betrachtet werden, dessen Aufgabe die Erzeugung einer globalen IT-Sicherheitsinfrastruktur durch Regulierungsinitiativen ist. Die mittleren und kleineren Knotenpunkte dieses Netzwerkes werden von zahlreichen, global verteilten NGOs gebildet.

4.1.4.5 NGOs und IT-Sicherheit in Netzen

Darauf, daß das Internet einerseits keine zentrale Steuerungsinstanz kenne und IT-Sicherheit nicht zu den Entwicklungszielen der dem Netz zugrundeliegenden Verfahrensweisen gehöre, wurde bereits mehrfach eingegangen. Auch die engen Grenzen staatlicher Normsetzung wurden mit Blick auf die globale Dimension des Internet gezeigt, so daß die Etablierung von stärkeren IT-Sicherheitsmechanismen im Internet und anderen gleichartigen elektronischen Netzen kaum realisierbar erscheint. Diese Schlußfolgerung würde deswegen zu kurz greifen, weil die Organisation des Internets und die an der Entwicklung der dort genutzten Mechanismen beteiligten Gruppen und Institutionen sehr wohl über Verfahren verfügen, für höchst unterschiedliche Ziele technische Dienste zu schaffen. Diese Verfahren bieten einen Ansatz zur Realisierung einheitlicher IT-Sicherheitsstandards auch im Internet. Ein heterogenes Netz wie das Internet muß zur eigenen Funktionsfähigkeit über robuste IT-Sicherheitsmechanismen zumindest für die Verfügbarkeit seiner Netzressourcen verfügen. Damit zeigt sich, daß aus dem Kreis der bisher das Internet tragenden Organisationen und den daran Beteiligten selbst Wege zur Verbesserung der Sicherheit in elektronischen Netzen erwachsen können.

Die Verfügbarkeit wird vor allem durch die Nutzung eines einheitlichen Übertragungsprotokolls und der Verfügung über Adressressourcen realisiert, um die Weiterleitung einer elektronischen Nachricht zu ermöglichen. Die Verfügbarkeit über diese Adressressourcen ist ein Beispiel für die Beachtung von IT-Sicherheitsgesichtspunkten im Internet, da zur Sicherung eines Zugriffs für jeden Domainnamen zumindest zwei Namensserver anzugeben sind. Hier führt Redundanz auch bei Ausfall eines Servers nicht zum Verlust der Verfügbarkeit des Dienstes. Darüber hinaus entsprechen die etablierten Mechanismen dieses Beispiels allerdings nur begrenzt den IT-Sicherheitsgedanken. Für die Integrität der Datenbank eines Namensservers ist der jeweilige Administrator zuständig, auch die Integrität der für die jeweiligen zentralen Namensserver – die die Internet-Domänen wie. de,. com oder. edu verwalten – ist uneinheitlich und teilweise nur in gewissem Rahmen gegen Manipulationen geschützt geregelt. Die Authentizität dieser Daten wird zum Teil mit Hilfe, zum Teil ohne die Nutzung digitaler Signaturen geschützt. Die geringe Zahl von Problemen zeigt aber die Zuverlässigkeit dieses pragmatischen und historisch gewachsenen Verfahrens.

Bedeutsam für IT-Sicherheit in elektronischen Netzen ist, daß die zur Verwaltung des Internets gebildeten Verfahren zugleich Wege anbieten, neue Sicherheitsmechanismen zu etablieren. Die von der ursprünglichen Organisationsstruktur des Internet Activities Boards (IAB) – entsprechend heute der Internet Society (ISOC) – her entwickelten Koordinationsgremien mit ihren jeweils mehr oder minder weitentwickelten regionalen und nationalen Entsprechungen bilden eine weltweit anerkannte Struktur von Non-Government-Organisationen, die bisher die Entwicklung des Internets vorangetrieben haben. Die Gründung des World Wide Web Consortiums (W3C), das der Koordination eines einzelnen Dienstes auf dem Internet dient, zeigt zusätzliche Möglichkeiten zur Koordinierung auch von IT-Sicherheitsmaßnahmen, soweit sie nicht in das herkömmliche Raster der Aktivitäten von Internet-spezifischen NGOs fallen[221]).

Außerhalb der Koordination und Verwaltung elektronischer Netze haben sich seit den 80er Jahren Organisationen gebildet, die sich in stärkerer Weise der IT-Sicherheit widmen. Von Bedeutung sind hier zunächst die in ihrer Struktur höchst unterschiedlichen Computer Emergency Response Teams (CERTs) als Gruppen von Personen mit spezifischem Fachwissen bei IT-Sicherheitsproblemen, beispielsweise bei Computerviren, Hackern oder anderen Anomalien und Störungen beim Betrieb von Computern. Die starken Unterschiede in Organisationsgrad, Zielen und Struktur dieser Gruppen machen sie eher zu einer Kommunikations- und Koordinationsinstanz bei der Vermeidung und Beseitigung von Lücken in der IT-Sicherheit, weniger aber zu einer Form von Organisation zur strukturellen Verbesserung der IT-Sicherheit in elektronischen Netzen. Vor dem Hintergrund der Entwicklung des WWW bis zur Gründung des W3C ist es allerdings auch nicht auszuschließen, daß CERTs eine stärkere Rolle in der IT-Sicherheit einnehmen werden.

In den USA spielt die IT-Sicherheit auch für Berufsorganisationen in der Informatik eine Rolle. So fördert die älteste und größte derartige Organisation, die Association for Computing Machinery(ACM), seit fast 20 Jahren den systematischen Austausch über Risiken, Sicherheit und Zuverlässigkeit von IT-Systemen. Vor allem der Vertraulichkeit in Netzen, aber auch der Zuverlässigkeit, Authentizität und Integrität widmen sich im klassischen Sinne als NGOs zu verstehende Gruppen wie die aus den USA stammenden computer professionals for social responsibility (cpsr),

[221]) Ein Überblick über die Historie der Internet-Organisation ist zu finden unter http://www.isoc.org/internet/history/index.shtml. Einen Vergleich mit der Bundesrepublik liefert: Volker Leib, Raymund Werle: Wissenschaftsnetze in Europa und den USA – Die Rolle staatlicher Akteure bei ihrer Bereitstellung; in: Raymund Werle, Christa Lang (Hg.): Modell Internet? München, 1997, S. 157–185

das Electronic Privacy Information Center (EPIC) oder die Electronic Frontier Foundation(EFF)[222]). Diese Gruppen widmen sich mit ihren technischen Expertisen den unterschiedlichen Formen von Sicherheitsdefiziten in elektronischen Netzen. Aufgrund ihrer Arbeit haben diese Gruppen eine hohe Bedeutung dabei, der Öffentlichkeit bestimmte IT-Sicherheitsrisiken bei der Nutzung elektronischer Netze zu vermitteln und Lösungsansätze vorzuschlagen.

Auch auf nationaler Ebene sind Institutionen vertreten, die den als Promotoren von IT-Sicherheit genannten Organisation und Gruppen vergleichbar sind. Der naheliegendste Vergleich bietet sich natürlich bei den zur nationalen Organisationsstruktur des Internets gehörenden Einrichtungen wie der zentralen Internet-Namensverwaltung DE-NIC in Karlsruhe, dem bei Aufbau des Internets in der Bundesrepublik und heute dem Betrieb des Wissenschaftsnetzes bedeutsamen Deutschen Forschungsnetz e.V. (DFN) und der seit 1998 bestehenden Dependance des W3C in dem GMD -Forschungszentrum Informationstechnik. Diese Einrichtungen sind zwar in der Lage, hierzulande für bedeutsam und erforderlich gehaltene IT-Sicherheitsmaßnahmen in internationalen Gremien zu vertreten. Sie sind jedoch nicht in der Lage, derartige Maßnahmen in einem nationalen Alleingang technisch umzusetzen. Gleichwohl ist die hohe Bedeutung einer Mitsprache an der Entwicklung neuer Standards nicht zu unterschätzen, die auf dem Internet zwar in einem offenen Prozeß entstehen, deren Umsetzung aber der Koordinierung und Organisation bedarf.

Darüber hinaus bestehen verschiedene wissenschaftlich oder kommerziell orientierte Institutionen, die die Verbesserung der IT-Sicherheit zum Ziel haben. Anders als für die ACM spielt IT-Sicherheit für die bundesdeutsche Gesellschaft für Informatik nur im Rahmen zuverlässiger Systeme und gesellschaftlicher Folgen eine Rolle. IT-Sicherheit in elektronischen Netzen und Transaktionsverfahren ist dagegen Ziel des TeleTrust e.V., an dem sich auch das BSI beteiligt. Die in der Bundesrepublik angesiedelten CERTs*) sind von einer so informellen Struktur, daß hier keine Vorgehensweise im Sinne einer organisierten Verbesserung von IT-Sicherheit zu beobachten ist.

Spezifisch für die Bundesrepublik sind dagegen einige wenige Gruppen, die auf unterschiedliche Weise zur Verbesserung von IT-Sicherheit beitragen. Die bekannteste und besonders auf IT-Sicherheitsfragen ausgerichtete Organisation in der Bundesrepublik ist dabei der Chaos Computer Club (CCC)[223]), dessen wiederholte Aktivitäten zur Aufdeckung von IT-Sicherheitslöchern in nationalen wie internationalen IT-Systemen und -Netzen die Sicherheit von Systemen in einer Reihe von Fällen erhöht haben. Ziele des CCC sind dabei sowohl die Aufdeckung von Schwachstellen und Risiken in IT-Systemen als auch der Schutz der Vertraulichkeit. Eher akademisch geprägt ist dagegen das Gegenstück zu den cpsr aus den USA, das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung(FIfF)[224]), das sich mit der Zuverlässigkeit von Systemen und Risiken, dem Schutz der Vertraulichkeit und neuartigen Bedrohungen (Information Warfare) beschäftigt. Aus einem juristischen Blickwinkel heraus arbeitet die Deutsche Vereinigung für den Datenschutz (DVD) im Bereich IT-Sicherheit an Themen zum Schutz der Vertraulichkeit. Wie ihre Gegenstücke in den USA[225]), dienen CCC, FIfF und DVD der Aufklärung der Öffentlichkeit, stellen ihre Expertise zunehmend aber auch parlamentarischer Beratung zur Verfügung. Diese Gruppen sind darüber hinaus auch international vernetzt und unterstützen in unterschiedlicher Weise Arbeiten zur Erhöhung von IT-Sicherheit.

Dieser Überblick zeigt, daß jenseits staatlicher Normsetzung oder des Einsatzes der mit Aufgaben der IT-Sicherheit betrauten Exekutive eine Vielzahl von Institutionen und Organisationen existiert, die sich in sehr unterschiedlicher Weise mit der Sicherheit in elektronischen Netzen beschäftigen. Die Spanne der allein in der Bundesrepublik vertretenen Gruppen reicht von der Koordination von Netzen bis zu Wissenschaftsorganisationen und NGOs im bereits klassischen Sinne. Zweifellos ist in diesen Gruppen die Kompetenz vorhanden, Fragen der IT-Sicherheit umfassend zu behandeln. Es fehlt jedoch bislang an einem genügend hohen gemeinsamen Interesse, derartige Probleme auch umzusetzen. Hinzu kommt, daß die genannten NGOs nur unsystematisch mit den für Fragen der Netzorganisation zuständigen Organisationen Erfahrungen über IT-Sicherheitsprobleme austauschen. Die Aktivitäten etwa des CCC oder Warnungen des FIfF bei IT-Sicherheitsmängeln in Netzen verweisen auf die vorhandenen unterschiedlichen Problemsichten. Eine Stärkung der IT-Sicherheit könnte jenseits von Eingriffen des Staates dadurch gefördert werden, alle auf IT-Sicherheitsfragen stark orientierten Organisationen in einen intensiveren Dialog über Sicherheitsprobleme zu bringen. So könnte mit geringem Aufwand fachlich hochqualifizierter Rat versammelt werden, der sich zu einer selbsttragenden Struktur zur Erhöhung der IT-Sicherheit entwickeln könnte.

---

[222]) Weitere Informationen sind im einzelnen zu finden unter: http://www.cprs.org, http://www.eff.org, http://www. epic.org

*) CERTs: Computer Emergeney Response Teams

[223]) http://www.ccc.org

[224]) http://www.fiff.de

[225]) Zum Vergleich der USA mit der Bundesrepublik siehe: Bernhardt, U.; Ruhmann, I. Technische Experten und die Gestaltung der Informationsgesellschaft, in: Forschungsjournal Neue Soziale Bewegungen, Heft 4, 1997, S. 94–98

5. Handlungsempfehlungen

Die Möglichkeiten der Nutzer zum Selbstschutz durch kryptografische Verfahren sollten nach dem derzeitigen Erkenntnisstand rechtlich nicht eingeschränkt werden. Eine Einschränkung der freien Verwendung solcher Verfahren kann bei einer Abwägung von Nutzen und Schaden nach diesem Erkenntnisstand nicht gerechtfertigt werden. Die Enquete-Kommission empfiehlt, die Nutzung von Systemen zur Verschlüsselung von Daten nur insofern gesetzlich zu regulieren, als daß europäische Richtlinien dies für nationales Recht vorschreiben. Dabei soll die Position der Europäischen Kommission zur Verschlüsselung auf internationaler Ebene nachhaltig unterstützt werden. Ergänzend hierzu empfiehlt die Enquete-Kommission, die uneingeschränkte Nutzung von Verschlüsselungsmethoden auf europäischer und internationaler Ebene – wie z. B. G8 und OECD – zu fördern und zu unterstützen. Verschlüsselungsprogramme, die eine Entschlüsselung verschlüsselter Inhalte durch Dritte ermöglichen, sollten als solche gekennzeichnet werden.

Die Enquete-Kommission empfiehlt, daß die jeweils zuständigen Behörden die sicherheitspolitischen Anliegen im Zusammenhang mit den neuen Informationstechnologien aufmerksam verfolgen. Hierbei ist zu klägen, ob Handlungsbedarf beim Gesetzgeber besteht. Hierbei sind neuen Formen der interdisziplinären Zusammenarbeit und einer Netzwerkbildung von Wissenschaft, Politik und Wirtschaft ein besonderer Stellenwert zu verleihen. Bei der Entwicklung von Rahmenbedingungen für eine Sicherungsinfrastruktur ist die Dynamik des Veränderungsprozesses der Informations- und Kommunikationstechnik zu berücksichtigen und der gesetzliche Anpassungsbedarf regelmäßig darzustellen.

Die Enquete-Kommission empfiehlt zu prüfen, ob und inwieweit durch Pilotprojekte und gesetzliche Experimentierklauseln die Erprobung neuer technischer und organisatorischer Sicherheitsvorkehrungen für genau umrissene Anwendungsbereiche und für einen klar umrissenen Zeitraum zugelassen werden sollte.

Die Enquete-Kommission beobachtet mit Besorgnis die Bemühungen, ein weltweites „Key-Recovery" – System einzuführen, das den Zugriff von ausländischen Regierungsstellen auf die vertraulichen Informationen auch deutscher Nutzer ermöglicht. Nicht akzeptabel wäre es und ein Eingriff in die Souveränität der Bundesrepublik Deutschland, daß solche Zugriffe außerhalb des Geltungsbereiches deutscher Gesetze und der Kontrolle deutscher Gerichte erfolgen können. Die Bundesregierung empfiehlt, die Auswirkungen der US – „Key Recovery" Initiative in Deutschland umfassend zu untersuchen und einen Bericht mit Handlungsempfehlungen vorzulegen. Zu prüfen ist darüber hinaus, ob und inwieweit auf europäischer Ebene, im Rahmen der OECD oder der G-8 Vereinbarungen getroffen werden müßten.

Die Enquete-Kommission empfiehlt, die Voraussetzungen für den Aufbau einer nationalen Sicherheitsinfrastruktur zu schaffen, die den vielfältigen Bedrohungsformen, wie sie mit dem Begriff des Information Warfare zum Ausdruck kommen, geeignete Schutz- und Abwehrstrategien entgegenzusetzen.

Die Enquete-Kommission empfiehlt, die internationale Zusammenarbeit zu intensivieren und auf der Grundlage der bereits existierenden Übereinkünfte zur IT-Sicherheit (Common Criteria, etc.) zu verstärken. Im Kern einer verstärkten internationalen Zusammenarbeit sollte das Bemühen um die Standardisierung von technischen Komponenten – insbesondere von Kryptoschnittstellen – Dienstleistungen und Verfahren des Electronic Commerce stehen, um die Vergleichbarkeit des Sicherheitsniveaus zu gewährleisten und um die Kompatibilität der Verfahren und die Qualität auf einem angemessenen Niveau sicherzustellen. Die Enquete-Kommission empfiehlt insbesondere, sich für die Offenlegung von Standards einzusetzen. Große Bedeutung kommt dabei multi- und bilateralen Vereinbarungen um die gegenseitige Anerkennung dieser Verfahren zu.

Die Enquete-Kommission empfiehlt, da sich IT-Sicherheitsmängel des Betriebssystems nicht auf den Ebenen nachgeordneter Funktions- und Anwendungsbereiche beheben lassen und damit zum Sicherheitsrisiko des gesamten IT-Systems werden,

- die Weiterentwicklung von Sicherheitsanforderungen zu unterstützen,
- deren Umsetzung intensiv zu verfolgen und dazu Sicherheitsanforderungen in Begutachtungs- und Zertifizierungsvorgängen als Beurteilungsgrundlage zu verankern.

Das Paradigma dieser Sicherheitsanforderungen sollte die strikte Trennung zwischen Betriebssystemfunktionen einerseits und Anwendungsfunktionen andererseits sein. Die Überprüfung der Sicherheitskriterien für Betriebssysteme sollte in regelmäßigen Abständen stattfinden.

Die Enquete-Kommission empfiehlt, die Forschungsförderung zur IT-Sicherheit auf breiter Ebene zu verstärken.

Die Prinzipien der IT-Sicherheit der Informationsverarbeitung müssen schon bei der Forschung und Fortentwicklung von Dienstleistungen und Produkten systematisch mitberücksichtigt werden, um sie so zum integralen Bestandteil der Produkte, Dienstleistungen und Beratungen zu machen. Besondere Bedeutung kommt dabei der Förderung von Forschung und Entwicklung bei folgenden IT-Sicherheitsfeldern zu:

- Förderung der Möglichkeiten des Selbstschutzes für IT-Anwender, wie sie beispielsweise kryptographische Verfahren darstellen. Dabei gilt es

auch, anwendungsspezifische Fragestellungen zu berücksichtigen.

- Förderung von Forschung und Entwicklung von sicherer Software und IT-Sicherheit als inhärentem Baustein von IT-Systemen.
- Entwicklung einer angemessenen Sicherungsinfrastruktur, die neben den gesetzlichen Maßnahmen (z. B. Signaturgesetz) aus der Definition von Prüfkriterien und -verfahren, Evaluierungsverfahren, Begleitforschung, etc. bestehen sollte.
- IT-Sicherheit sollte anwendungsbezogen präzisiert werden. Dies bedeutet, ihre Funktion und ihr Anforderungsprofil im jeweiligen Anwendungskontext und seinen organisatorisch-rechtichen Umgebungsbedingungen zu verstehen. Untersuchungen für exemplarische Handlungsfelder mit Vorbildcharakter, die auch die Durchsetzung von IT-Sicherheitsstandarads vereinfachen könnten, sollten forciert werden.
- Förderung einer interdisziplinären Technikfolgenabschätzung im Bereich der IT-Sicherheit, um mögliche Risiken und Gefährdungen rechtzeitig erkennen und möglichen Gegenmaßnahmen organisieren bzw. entwickeln zu können.

Die Enquete-Kommission empfiehlt als Ziel die Entwicklung neuartiger Sicherheitsstrategien, die das „Machen von Fehlern" nicht ausschließen und das „Lernen aus Fehlern" zuläßt, sich also systematisch an den Möglichkeiten und Fähigkeiten der IT- Nutzer orientiert.

Das komplexe Gebiet der IT-Sicherheit (wie auch des Datenschutzes) muß entsprechend seiner grundlegenden Bedeutung eine angemessene Berücksichtigung in der Informatik-Ausbildung erfahren.

Dabei ist vor allem die Bedeutung einer „mehrseitigen" Sicherheit zu erkennen.

Notwendig sind interdisziplinäre Konzepte, die die Erfahrungen der IT-Sicherheit, der Technik- und Risikobeurteilung, der Technikfolgenabschätzung, der Ökonomie, der Staatswissenschaft, der Sozialwissenschaft und der jeweiligen Fachdisziplinen, beispielsweise der Medizin, bündeln – um nur einige zu nennen. Die Enquete-Kommission empfiehlt, in Abstimmung mit den Ländern den Umbau der Informatik-Ausbildung zu einer derartigen interdisziplinären Ausrichtung zu intensivieren.

Die Enquete-Kommission empfiehlt, einen Maßnahmenkatalog zu entwickeln und umzusetzen, um den Schutz von vertraulichen Informationen deutscher Nutzer in den weltweiten Informationsnetzen zu verbessern. Vor allem die privaten Haushalte und die vielen mittelständischen Unternehmen fühlen sich durch die rasante Entwicklung sowie die zunehmende Intransparenz der Kryptomärkte in zunehmenden Maße verunsichert. Notwendig dazu ist nicht zuletzt eine breit angelegte gesellschaftliche Debatte und eine allgemein verständliche Aufklärungskampagne über die tatsächlichen Risiken dieser Netze und über die Möglichkeiten sich mit technisch Mitteln hiergegen zu schützen. Ziel ist, die Eigenverantwortung der Bürger für die Sicherheit und den Schutz ihrer Daten zu fördern und das Bewußtsein für den eigenen Systemschutz und Selbstdatenschutz zu stärken. Um die erforderliche Transparenz zu schaffen, sollte gemeinsam mit den beteiligten Kreisen (z. B. Wirtschafts-, Verbraucherschutzverbände, Datenschützern) geprüft werden, ob und inwieweit sich ein „Kryto-TÜV", der unterschiedliche Sicherheitsebenen unterscheidet, auf breiter Front und auf freiwilliger Basis einführen läßt.

Bund und Länder sind aufgefordert, den Einsatz digitaler Signaturen zum Schutz der Integrität und der Authentizität von Daten und der Verschlüsselung zum Schutz der Vertraulichkeit in der elektronischen Kommunikation mit den Bürgern und Unternehmen zu fördern und zu forcieren. Zu denken ist beispielsweise an Anwendungen oder Dienstleistungen gegenüber dem Finanzämtern, Meldeämtern und in der Beratung. Auch die Ermöglichung einer informationstechnisch sicheren elektronischen Wahl neben der heutigen Urnen- und Briefwahl könnte einen großen Beitrag zur besseren Akzeptanz leisten.

Die Enquete-Kommission empfiehlt die rechtlichen Voraussetzungen für die Gleichstellung der digitalen Signatur zur natürlichen Unterschrift zu prüfen und solche Bereiche zu schaffen, die für eine Gleichstellung ein angemessenes Experimentierfeld bieten.

Die Enquete-Kommission empfiehlt, einen angemessen flexiblen Kriterienrahmen für eine IT- Sicherungsinfrastruktur zu formulieren.

Die Enquete-Kommission empfiehlt, für besonders sensitive IT-Systeme Sicherheitsanforderungen zu formulieren, um auch für diese zu einem herkömmlichen Techniken mit hohen Gefährdungspotentialen vergleichbaren Sicherheitsniveau zu gelangen. Auch gilt es zu prüfen, inwieweit bei Teilen von IT-Systemen mit besonders hoher Bedeutung für die IT-Sicherheit – wie etwa Betriebssystemen – Maßnahmen zur Hinterlegung des Quellcodes oder andere Mittel zur Prüfung für eine Verbesserung der IT-Sicherheit notwendig sind.

Die Enquete-Kommission empfiehlt, den Aufbau eines Zertifizierungswesens für IT-Systeme zu prüfen. Eine erste Voraussetzung dafür kann durch eine Produktzertifizierung nach anerkannten Kriterien und anerkannten Verfahren durch anerkannte Prüfstellen erfolgen.

Die Enquete-Kommission empfiehlt, den Aufbau einer Stiftung „Software-Test" zu prüfen. In Analogie zur Stiftung Warentest würde eine Stiftung „Software-Test" auch die Sicherheit von Software testen. Dabei werden Softwareprodukte im Zentrum der Tests stehen. Soweit wie möglich sollten auch die sicherheitsrelevanten Aspekte berücksichtigt werden, die aus dem Umfeld der betreffenden Produkte, ihrer jeweiligen Hardware- und Softwareumgebung, den Schnittstellen und dem komplexen Zusammenwirken mit anderen Komponenten resultieren.

Die Enquete-Kommission empfiehlt, die Eigenverantwortlichkeit der Hersteller bei der Lösung von IT-Sicherheitsproblemen stärker zu betonen. In diesem Sinne sollte auch eine Überprüfung des Haftungsrechts erfolgen.

Die Enquete-Kommission empfiehlt, durch die Förderung des gesellschaftlichen Dialogs über die zur Sicherung und Schutz von persönlichen Daten notwendige Selbstverantwortung das Bewußtsein der Bürger für den eigenen Systemschutz und den Selbstdatenschutz zu stärken. Dabei sollte in einem solchen Dialog IT-Sicherheit nicht nur als Kostenfaktor dargestellt werden. Vielmehr ist die zunehmende Bedeutung von IT-Sicherheit als Leistungsmerkmal von IT-Systemen und in ihrer Bedeutung als Wettbewerbsfaktor zu betonen.

Die Enquete-Kommission empfiehlt, die bislang organisatorisch auf wenige Institutionen konzentrierten Bemühungen zur IT-Sicherheit auf eine breitere Basis zu stellen und schlägt vor, die in diesem Bereich arbeitenden Organisationen und Institutionen mit unterschiedlichsten Hintergründen zu einem intensiven IT-Sicherheitsdialog anzuregen.

Anhang

Auszug aus dem

Gutachten
über

Künftige Anforderungen an die Kommunikationssicherheit in der Medizin

Europäisches Institut für Systemsicherheit
Universität Karlsruhe

10. Februar 1998

2 Sicherheitsprobleme und Risiken in spezifischen Bereichen

2.1 Gesundheitswesen

Die Betrachtungen zur Bedeutung der Sicherheitstechnik in der Medizin beruhen u.a. auf den Erfahrungen und Erkenntnissen aus der Zusammenarbeit mit Ärzten, sowie den Erfahrungen aus dem DFG-Sonderforschungsbereich 414 „Informationstechnik in der Medizin – Rechner- und sensorgestützte Chirurgie" der Universitäten Karlsruhe und Heidelberg.

Wurde die EDV früher praktisch nur zu Verwaltungs- und Abrechnungsarbeiten genutzt, wird sie nun zum integralen Bestandteil der Diagnose und Therapie, bzw. ist es bereits geworden.

Es ist davon auszugehen, daß die Führung der Patientenakte auf rechnergestützten Datenbanken statt auf Papier und Film auch in Kliniken in absehbarer Zeit zum Normalfall wird.

Die Sicherheitsanforderungen haben sich damit grundlegend verändert. Waren bisher vornehmlich finanzielle, verwaltungstechnische und in gewissem Umfang datenschutzrechtliche Aspekte relevant, sind und werden nunmehr auch die Gewährleistung der ärztlichen Schweigepflicht und die Gesundheit des Patienten in zunehmendem Maße von der fehlerfreien und nachweislich nicht manipulierbaren und nicht manipulierten Funktion der in stark zunehmendem Umfang eingesetzten Rechner und Telekommunikationseinrichtungen abhängig.

Ein Nebeneffekt des EDV-Einsatzes und der Vernetzung ist, daß dadurch auch Fremdeinflüsse wie die Fernwartung auf den Ablauf der medizinischen Behandlung einwirken können, daß also nicht mehr nur der behandelnde Arzt den entscheidenden Faktor bei Erfolg oder Mißerfolg der Behandlung repräsentiert.

2.1.1 Erhöhte Bedeutung der Datenverarbeitung

Die Entwicklung der Medizintechnik in den letzten Jahren zeigt vor allem in den Kliniken eine massive Zunahme der Verwendung und Abhängigkeit von Rechnern und Telekommunikationsgeräten.

Dies ist einerseits auf die Entwicklung und Nutzung von neuen medizinischen Geräten, wie z.B. Computertomographen, Kernspintomographen, Operationsrobotern oder Geräten zur maßgenauen Einzelanfertigung von Prothesen, zurückzuführen, die ohne Computertechnik gar nicht denkbar wären. Andererseits sind inzwischen auch Diagnose- und Therapieeinrichtungen „computerisiert", die nicht notwendigerweise der Rechnerunterstützung bedürfen, wie Röntgen- und Bestrahlungsgeräte, EKG und EEG.

Der verstärkte Einsatz von EDV bedingt und wird bedingt durch die sich zeitgleich entwickelnde Verwendung von Telekommunikationseinrichtungen, die zur einfachen und schnellen Datenübermittlung, aber auch zur Ferndiagnose und Telemedizin genutzt werden.

Damit hat die Datenverarbeitung in der Medizin eine neue Qualität erlangt.

Zur Verdeutlichung werden einige fiktive (aber durchaus realistische und von realen Gegebenheiten ausgehende!) Szenarios dargestellt:

Szenario 2.1
„Datarazzi" und Krankenakten

Eine prominente Person befindet sich nach einem schweren Autounfall in Folge von Alkoholproblemen in stationärer Behandlung. Weil die Regenbogenpresse massiv versucht, an medizinische und sonstige Informationen zu gelangen, wird der Patient physisch abgeschirmt.

- Statt diesen Schutzwall zu durchdringen läßt man Hacker auf der Suche nach personenspezifischen Informationen („Datarazzi" in das mangelhaft geschützte Kliniknetz eindringen. Sie gelangen dabei an die Pa-

tientenakte und die Laborwerte von Blutuntersuchungen.

Der Skandal nimmt seinen Lauf.

- Der Hersteller des Computertomographen dieser Klinik hat Sicherungsmaßnahmen ebenfalls vernachlässigt und verwendet einfache und leicht zu merkende Paßworte für den Steuerungsrechner. Der Hacker dringt so auch in den Tomographen vor. Weil zu jeder Untersuchung zwecks Einblendung in die Röntgenbilder der Name des Patienten eingegeben und in den Tomographiedateien abgelegt wird, findet der Hacker sofort die gesuchten Daten aus der Vielzahl der gespeicherten Tomographien.

Der Angreifer zieht alle diese Daten vom Personal völlig unbemerkt über das Internet oder einen ISDN-Wartungszugang ab. Am nächsten Tag werden alle Informationen wie die Leberwerte, die bestehenden Infektionen und die Tomographien samt Befundung der Verletzung in der Regenbogenpresse wiedergegeben, was fatale Auswirkungen für die Person hat.

Szenario 2.2
Sicherheitsproblem mit tödlichem Ausgang

Ein durch einen anderen Staat verfolgter Dissident liegt nach einer Routineoperation auf der Intensivstation. Er ist gegen bestimmte in seiner Situation indizierte Medikamente allergisch.

Ein gedungener und medizinisch versierter Hacker dringt in das Kliniknetz ein und entfernt den Hinweis auf die Allergie aus der Datenbank. Dem Patienten wird infolge dessen ein unverträgliches Medikament verabreicht. Er erleidet wenig später einen anaphylaktischen Schock mit terminalem Kreislaufkollaps. Die Patienten der Station sind zwar an ein Meldesystem angeschlossen, das alle Vitalfunktionen überwacht, in das Zimmer des diensthabenden Personals überträgt und dort gegebenenfalls Alarm auslöst. Der Hakker modifiziert aber das System über einen Fernwartungszugang und sorgt dafür, daß die Anzeigen mehrerer Patienten vertauscht oder durch Kopien und Simulationen ersetzt werden. Bei Eintritt des Kreislaufversagens schlägt das System Alarm, zeigt die kritische Situation jedoch nicht für den betroffenen, sondern in kurzen Abständen für drei andere Patienten an. Das Personal ist dadurch für längere Zeit abgelenkt und mit den anderen Patienten beschäftigt.

Der Dissident verstirbt planmäßig und unbemerkt.

Szenario 2.3
Gesundheitsschäden durch Softwaremängel

Auf verschiedenen Rechnern in einem Klinikum wird eine neue Software installiert. Die Installation wird dabei durch eine nichtssagende graphische Benutzeroberfläche gesteuert, die keinerlei Aufschluß darüber gibt, daß nicht nur das Softwarepaket einkopiert wird, sondern auch an verschiedenen Stellen des Betriebssystems Konfigurationsdaten verändert werden. Außerdem ersetzt die Installationssoftware einige der Programmbibliotheken durch andere Versionen, die der Autor der Software für neuer oder wichtiger hält.

Zunächst erscheinen alle Funktionen einwandfrei. Tatsächlich aber unterscheiden sich die Datenstrukturen der neuen Bibliotheken geringfügig von denen der alten Versionen. Die anderen Programme funktionieren zwar augenscheinlich, unter bestimmten Umständen werden während des Programmlaufs aber falsche Speicherbereiche beschrieben, Array-Grenzen überschritten, Texte als Gleitkommazahlen interpretiert usw.

Diese Fehlfunktionen fallen nicht weiter auf. Es kommt zwar in seltenen Fällen zum Absturz einiger Rechner oder zu Meldungen über „Allgemeine Rechteverletzungen", aber da dies ohnehin als normal angesehen wird, wird dem keine Beachtung geschenkt.

Im Laufe des Betriebs treten dann unbemerkte Fehler auf:

- In der Medikamentenliste eines Patienten mit hohem Blutdruck und altersbedingten Gefäßveränderungen fehlt plötzlich ein blutdrucksenkendes Präparat, weil während des fehlerhaften Programmlaufes der Text mit Nullen überschrieben wurde.

  Der Patient erleidet einen Schlaganfall.

- Ein anderer Patient mit einem Hirntumor wird mit Bestrahlungen behandelt. Dazu wird mit einer rechnergesteuerten Fräse eine Maske hergestellt, die die Bestrahlung auf das befallene Gewebe beschränkt. Bei der Berechnung der Steuerdaten für die Fräse wurden zwei Gleitkommazahlen mit Text überschrieben und erhielten dadurch unsinnige Werte. Der Ausschnitt der Maske wurde dadurch geringfügig verschoben und deformiert. Außer dem Tumor wird deshalb mehrfach auch angrenzendes gesundes Gewebe bestrahlt. Zwar stellen Patient und Arzt daraufhin bald Beschwerden fest, die auf eine Beeinträchtigung der Hirnfunktionen zurückzuführen sind, als Ursache wird aber der vermeintlich wachsende Tumor angesehen und die Behandlung fortgesetzt.

- Der Patient erleidet eine irreversible Hirnschädigung.

2.1.2 Zugriffsrechte und Sicherheitsanforderungen

Im Rahmen des Entwurfs einer medizinischen Datenbank sollten die Zugriffsberechtigungen auf konventionell gespeicherte Patientendaten (Papier, Filme usw.) erfaßt werden, um diese durch Modellbildung organisatorisch und kryptographisch nachzubilden.

Bei Sicherheitsuntersuchungen in Kliniken stellte sich jedoch heraus, daß es kein allgemeingültiges Sicherheitsmodell und keine Methodologie gibt und daß Lese-, Schreib- und Löschzugriffe sicherheitstechnisch normalerweise weder erfaßt, noch kontrolliert werden. Ausnahmen sind einige lokale Regelungen, die aber nicht mit voller Konsequenz durchgehalten werden und nicht die anzustrebende Wirkung erzielen. Integrität, Authentizität, Vertraulichkeit und Nachweisbarkeit der Datenhaltung sind nicht gewährleistet; dem ist gegenüberzustellen, daß eine erhebliche Steigerung der Sicherheit im Bereich konventionell gespeicherter Daten mit vernünftigem Aufwand auch nicht zu erreichen wäre.

In der Realität wird bezüglich der Vertraulichkeit die Stellung der Mitarbeiter einer Abteilung – Ärzte, Pfleger, Sekretärin usw. – praktisch nicht differenziert. Herkunft und Echtheit von Daten werden praktisch nie explizit überprüft.

Szenario 2.4
Aktenanforderung durch falschen Arzt

Es ist durchaus möglich, daß ein Unbefugter sich durch entsprechendes Auftreten in einer Klinik als behandelnder Arzt eines Patienten ausgibt und unter Angabe einer Briefkastenadresse um künftige Zusendung der Befunde usw. bittet und so an Patientendaten gelangt, die der Schweigepflicht unterliegen.

Ebenso könnte ein Unbefugter mit entsprechendem Auftreten und entsprechender Kleidung unrichtige Patientendaten über die Stationsrechner oder auf konventionelle Weise einschleusen und auf Fehlbehandlung etc. „hoffen".

Durch den verstärkten Einsatz von EDV und Telekommunikation, und damit auch automatisierbarer

Vorgänge, würde zwar einerseits die Gefährdung erheblich erhöht, wenn hier kein explizites Rechtemodell geschaffen und technisch durchgesetzt wird, andererseits bieten EDV und Telekommunikation aber auch erst die organisatorischen und kryptographischen Mittel zum Einsatz eines solchen Rechtemodells.

Parallel zum zunehmenden Einsatz der Computertechnik muß daher vom Gesetzgeber ein restriktives Zugriffsrechtemodell entworfen und durchgesetzt werden.

2.1.3 Besonderheit Notfall

Der medizinische Bereich ist durch eine Besonderheit gekennzeichnet, nämlich das mögliche Vorliegen eines Notfalls, der die plötzliche Anforderung höchster Verfügbarkeit mit sich bringt.

Sicherheitsanforderungen wie Vertraulichkeit, Authentizität und Integrität haben jedoch zum Ziel, die Verfügbarkeit für den Angreifer zu minimieren und können sich dann als gefährlich erweisen, wenn sie der im Notfall benötigten Verfügbarkeit entgegenstehen, weil der behandelnde Arzt nicht oder nicht schnell genug als befugter Benutzer erkannt werden kann und ihm der möglicherweise dringend notwendige Zugang verweigert wird.

Daher ist durch geeignete Maßnahmen sicherzustellen, daß im Notfall

- durch den Einsatz der Computertechnik keine Nachteile entstehen und
- daß Vorteile, die die Computertechnik bieten kann, auch tatsächlich gewährleistet werden.

Ein Problem stellt in dieser Situation die Unterscheidung zwischen befugtem und unbefugtem Benutzer dar, weil Notfälle nicht vorhersagbar sind, prinzipiell jeder Arzt der behandelnde Arzt sein kann und die personenspezifische Befugnisse eines bestimmten Arztes im Notfall möglicherweise nicht überprüft werden können[226])

Es ist daher ein Rechtemodell zu entwickeln, das im Notfall die Verfügbarkeit nicht einschränkt und trotzdem hinreichenden Schutz bietet, auch bei einem fingierten Notfall.

Auch hier besteht dringender Handlungsbedarf bei Forschung, Entwicklung und Gesetzgebung.

2.1.4 Beweisbare Dokumentation

Verstärkte Beachtung muß – gerade mit Hinblick auf datenschutzrechtliche Belange – auch der Zugriffsmöglichkeit des Patienten auf seine Daten geschenkt werden.

Dabei ist zu unterscheiden zwischen der Akteneinsicht und der Aktenveränderung, etwa die Entfernung von Einträgen, die dem Patienten peinlich sein könnten.

Der Patient hat ein Interesse, die Akte auf Vollständigkeit (Integrität der Gesamtakte), Integrität der Einzeleinträge und Authentizität prüfen zu können, außerdem in Erfahrung zu bringen, wer wann worauf Einblick genommen hat. Außerdem will er im Streitfall den Inhalt der Patientenakte einem Dritten resp. einem Gericht gegenüber beweisen können.

Auch der Arzt muß im Streitfall beweisen können, welche Einträge er wann vorgenommen hat, um sich z. B. vom Vorwurf einer Fehlbehandlung befreien zu können. Ebenso muß er auch aktive und passive Zugriffe des Patienten beweisen können, nämlich wenn es um Behandlungsfehler aufgrund vom Patienten entnommener (d. h. gegen Zugriff gesperrter) Daten oder den Vorwurf mangelnder Aufklärung geht.

Damit werden ganz erhebliche Anforderungen an die Integrität, Authentizität, Vertraulichkeit und Beweisbarkeit von Patientenakten gestellt.

2.1.5 Abrechnungswesen

Die Gefahr der Verletzung der Schweigepflicht und des Datenschutzes, aber auch der Fälschung sind durch die neue Art der detaillierten digitalen Abrechnung offensichtlich. Zu Ungereimtheiten bei der Abrechnung medizinischer Leistungen wird auf die Veröffentlichungen in der Presse, und zu Verletzungen des Datenschutzes auf die Berichte der Datenschutzbeauftragten ergänzend verwiesen.

Hier muß ein Modell erstellt werden, das bei Wahrung der Vertraulichkeit Gesetzesverstöße unterbindet und u. a. die Konsistenz zwischen Patientenakten und Abrechnungen sicherstellt.

2.1.6 Gerätespezifische Probleme

Durch den hohen Grad der Technisierung und der Komplexität, sowie die im Medizinbereich übliche Art der Gerätewartung und -betreuung ergeben sich im klinischen Umfeld weitere Besonderheiten.

Fern- und Fremdwartung

Als erhebliche Gefahrenquelle anzusehen ist die große Zahl von Geräten, die der Fremd- oder Fernwartung durch die Hersteller- oder eine Wartungsfirma unterliegen, wie z. B. Computertomographen und ähnliche Geräte.

Diese Geräte stehen nicht unter der Kontrolle des Klinikpersonals, das häufig nicht einmal das Paßwort der steuernden Workstation kennt. Fast immer liegt die volle Kontrolle beim Träger des Wartungsdienstes, der, wie die Erfahrung zeigt, mitunter nahezu täglich zum Einsatz kommt. Es wird kaum versucht, Sicherheit durch echte Sicherheitsmaßnahmen zu erreichen, sondern vornehmlich dadurch, daß das befugte Bedienungspersonal gerade soweit in die Maschine eingewiesen wird, wie es zum Betrieb nötig ist, etwa in die Benutzeroberfläche des Hauptprogrammes.

Der Wartungsdienst kann hier alle (!) regulär oder versteckt auf dem Gerät liegenden Patientendaten

[226]) Beispielsweise weil der Arzt seinen Berechtigungsnachweis in der Eile nicht bei sich hat.

einsehen. Er kann überdies Software installieren oder einschleppen, die das – häufig an das Kliniknetz angeschlossene – Gerät mißbraucht, um etwa Paßworte aus dem Netz zu sammeln, andere Maschinen anzugreifen und dergleichen mehr.

Die Sicherheit des Kliniknetzes hängt damit von der Zuverlässigkeit der Software jedes solchen Gerätes ab. Die wiederum hängt von den Sicherheitsmaßnahmen beim Hersteller ab. Ein Angreifer kann so einen indirekten Angriff durchführen, indem er den Hersteller angreift und die Software modifiziert, die beim nächsten Wartungsbesuch installiert wird.

Sowohl bei Fernwartungszugängen, als auch bei Wartungsbesuchen vor Ort besteht außerdem die Gefahr, daß ein unbefugter Angreifer sich für den Wartungsdienst ausgibt.

In einem Fall wurden eine schier unglaubliche und unerträgliche Inkompetenz des vor Ort arbeitenden Wartungspersonals und an Schlamperei grenzende Nachlässigkeiten eines renommierten Medizingeräteherstellers bei Belangen der Sicherheit festgestellt. Das Wartungspersonal konnte u.a. selbst nicht mit dem Gerät umgehen, sondern nur hilflos Befehle buchstabenweise aus dem Handbuch abtippen, ohne dabei deren Bedeutung zu verstehen oder den Erfolg oder Nichterfolg der Aktion erkennen zu können. Die Wahl der Paßwörter war in diesem Fall so mangelhaft gestaltet, daß firmenweit ein bekanntes Paßwort benutzt wurde.

Aufgrund dieser Erfahrungen ist die Fremd- und Fernwartung deshalb als überaus problematisch anzusehen. Es besteht auch hier großer Handlungsbedarf.

Datenformate und Verfahren

Viele Geräte im medizinischen Bereich zeichnen sich durch proprietäre und undokumentierte Datenformate und eine nicht genau spezifizierte Verfahrensweise aus.

Die Haltung und Verarbeitung medizinischer Daten, deren genaue Syntax und Semantik nicht bekannt ist, und deren Verwendung an einen bestimmten Hersteller bindet, ist bedenklich und sollte – wenn möglich – durch bessere Alternativen ersetzt werden.

Arbeitsplatzrechner und Nutzung von Telekommunikation

Die zunehmende Nutzung von EDV und Telekommunikation im medizinischen Bereich zieht natürlich nicht nur die spezifisch medizinischen, sondern zwangsläufig auch die allgemein mit dieser Technik verbundenen Probleme und Risiken nach sich. Deshalb gelten die in Kapitel 3 aufgezeigten Probleme in vollem Umfang auch für den medizinischen Bereich, weshalb zur Vermeidung von Wiederholungen auf dieses Kapitel Bezug genommen wird.

2.1.7 Anwenderstruktur

Im klinischen Umfeld wurde eine Anwenderstruktur beobachtet, die als prototypisch für viele fachbezogene Einsatzgebiete der EDV und Telekommunikation angesehen werden kann.

Es liegt eine überwiegend homogene Anwenderstruktur aus sehr gut ausgebildeten und hochkompetenten medizinischen Fachleuten vor, die sehr gut befähigt sind, auch schwierige und komplexe Problemstellungen zu erfassen. Die Anwender sind überdies aufgrund ihrer Ausbildung und medizinischer Notwendigkeiten auf ständige Fortbildung vorbereitet und nehmen auch tatsächlich an berufsspezifischen Fortbildungen teil. Die Anwender sind mehrheitlich technischen Fragen aufgeschlossen und entwickeln eigenes Interesse am Umgang mit EDV und Telekommunikationstechniken, die auch auf freiwilliger Basis und im Privatbereich gern eingesetzt werden.

Trotz dieser überaus erfreulichen Rahmenbedingungen ist die tatsächliche Situation sehr unbefriedigend. Obwohl die Arbeit mit Rechnern und Netzwerken bzw. Diensten wie WWW, E-Mail usw. mittlerweile schon als unverzichtbar angesehen wird, besteht diesbezüglich im allgemeinen kein ausreichend tiefes technisches Fachwissen über die Systemaspekte, insbesondere bezüglich der Risiken und Gefahren, die sich aus den neuen Informationstechniken und ihrer rasanten Fortentwicklung ergeben. Die wesentlichen zugrundeliegenden Funktionen werden oft nicht erkannt oder verstanden. Die weit überwiegende Mehrzahl der Anwender ist allein schon durch die übermäßige zeitliche Auslastung in ihrem Fachgebiet objektiv überfordert, zusätzlich dazu noch mit der technischen Komplexität fertigzuwerden, die andernorts den Einsatz von Vollzeitbeschäftigten verlangt.

Die Ursache hierfür ist darin zu sehen, daß aufgrund der zugrundeliegenden Berufsethik das Sicherheitsdenken zwar grundsätzlich ausgeprägt ist, aber nur den Bereich „Safety" abdeckt. Mit großer krimineller Energie vorgetragene Angriffe fallen in den Bereich „Security" und bleiben in der medizinischen Ausbildung unberücksichtigt.

Dies zeigt sich beispielsweise darin, daß zwar in gewissem Umfang Bemühungen um die Systemsicherheit unternommen werden, diese aber meistens auf einfache Maßnahmen wie das An- und Abstecken von Fernwartungsleitungen und den massenhaften Einsatz von Virenschutzprogrammen beschränkt bleiben. Organisatorische Maßnahmen gegen Computer-Viren usw., wie z.B. die sichere Ablage von Programmen auf schreibgeschützten Fileservern, werden normalerweise nicht ergriffen.

Die Ursache hierfür ist darin zu sehen, daß diese Themen – zumindest im beobachteten Bereich – weder Gegenstand der Grundausbildung, noch der Fortbildung sind. Schulungen, Seminare usw. werden hierzu nicht angeboten; die Wissensaneignung bleibt der privaten Initiative überlassen.

Daher muß das medizinische Personal durch Informatik-Fachleute ergänzt werden, da häufig auch in

der Klinikverwaltung oder den teilweise bestehenden Klinikrechenzentren das in Bezug auf Sicherheit nötige Fachwissen nicht bzw. nicht zuverlässig vorhanden ist.

Diese Situation ist unbefriedigend; eine starke Verbesserung kann aber problemlos durch systematische Schulungen und Fortbildungsmaßnahmen, sowie eine entsprechende personelle Ergänzung erreicht werden.

Es besteht dringender Handlungsbedarf.

C. Zweiter Berichtsteil: Datenschutz

(Verabschiedet am 23. März 1998)

1. Bedeutung des Datenschutzes in Netzen

Mit der zunehmenden Durchdringung vieler Lebensbereiche durch die neuen Informations- und Kommunikationstechniken wächst auch das Bewußtsein um deren Gefahren. Immer wieder gibt es Nachrichten, die die Privatsphäre durch die neuen Techniken gefährdet erscheinen lassen – Nachrichten über unberechtigte Zugriffe auf scheinbar sichere Datenbestände[227]), über Programme, die in Telekommunikationsnetzen sensible Daten wie Kreditkartennummern abfangen, oder über Software, die über Datennetze unbemerkt auf der Festplatte des Nutzers installiert wird, um von dort aus Informationen in das weltweite Datennetz zu kopieren.[228]) Es kann der Eindruck entstehen, das Orwellsche Schreckensszenario vom „gläsernen Menschen" rücke mit dem Übergang von der Industrie- zur Informationsgesellschaft in bedrohliche Nähe.[229])

Dadurch ausgelöste Ängste können den weiteren Ausbau der Informationsgesellschaft und die Nutzung der durch die neuen Informations- und Kommunikationstechniken entstehenden Vorteile und Chancen ernsthaft behindern. Umfragen belegen eine nicht nur in Deutschland wachsende Sensibilität für den Schutz der Privatsphäre vor durch die neuen Medien bedingten Gefahren: Einer im Auftrag der Europäischen Kommission erstellten repräsentativen Untersuchung zufolge sind zwei Drittel der EU-Bürger über Datenspuren in Telekommunikationsnetzen besorgt; die weit überwiegende Mehrheit würde die neuen Technologien nicht oder nur mit Einschränkungen nutzen, wenn die Gefahr besteht, daß personenbezogene Daten ausgeforscht und zu Zwecken verwendet werden, mit denen sie nicht einverstanden sind.[230])

Eine aufgrund der Besorgnis um den Schutz der Privatsphäre ablehnende Haltung gegenüber den neuen Informations- und Kommunikationstechniken hätte möglicherweise auch große wirtschaftliche Konsequenzen: Schätzungen zufolge wird allein für Deutschland im Bereich des Online- und Teleshopping ein Umsatzpotential von bis zu 60 Milliarden Mark pro Jahr prognostiziert[231]), und es wird angenommen, daß eine rasche Verbreitung dieser Geschäftsformen erforderlich ist, damit deutsche Unternehmen im weltweiten Wettbewerb mithalten können.[232])

Insofern kann ein wirksamer Datenschutz auch ein wichtiger Wettbewerbsfaktor sein.[233]) Das ist auf nationaler wie auf internationaler Ebene anerkannt: Sowohl die G 7[234]), die OECD[235]) und die Europäische Kommission[236]) als auch die USA[237]) halten den Schutz der Privatsphäre in den weltumspannenden Datennetzen für eine der wichtigsten Voraussetzungen für die Nutzung der Chancen der neuen Informations- und Kommunikationstechniken. Ebenso geht der von der Bundesregierung eingesetzte Rat für Forschung, Technologie und Innovation davon aus, daß ein konsequenter Datenschutz zu den zentralen Akzeptanzvoraussetzungen der Informationsgesellschaft zählt.[238])

---

227) Vgl. z. B.: Die Welt vom 18. Dezember 1996: Datenklau hat Konjunktur. Gegen unerwünschtes Eindringen in Datennetze besteht kaum ein Schutz; Die Zeit vom 23. August 1997: Räuber im Netz. Das weltweite Internet öffnet dem Datenmißbrauch Tür und Tor – die nationalen Kontrolleure sind machtlos.

228) Vgl. Der Spiegel 7/1997: Schleusen geöffnet. Ein Bummel im Internet kann fatale Folgen haben. Software, die das World Wide Web attraktiver machen soll, ist für Mißbrauch anfällig.

229) Vgl. Der Spiegel 36/1996: Lauscher im Datenreich. Die Welt der Computer ist ein Paradies für Spione aller Art. PC verraten vertrauliche Daten durch hochfrequente Abstrahlung. Geheimdienste überwachen den internationalen Datenverkehr und unterhöhlen zielstrebig alle Schutzvorkehrungen. Selbst das gutgesicherte Netz der Banken haben Profi-Lauscher angezapft; Computer-Zeitung vom 3. Juli 1997: Das Data-Warehouse-Konzept schürt die Angst vor dem gläsernen Bürger.

230) Vgl. Eurobarometer 46.1: Information Technology and Data Privacy. Report produced for the European Commission, Directorate General „Internal Market and financial services", Brüssel 1997; zur Situation in den USA vgl. die unter http://www.etrust.com abrufbare Umfrage und U.S. Department of Commerce: Privacy and the NII: Safeguarding Telecommunications-Related Personal Information, http://www.ntia.doc.gov/ntiahome/policy/privwhitepaper.html, unter A; vgl. ferner Bäumler, H.: Eröffnungsrede, in DuD 1996, S. 647–649 (648).

231) Vgl. Bundesministerium für Wirtschaft: Elektronischer Geschäftsverkehr. Initiative der Bundesregierung, Stand: Oktober 1997, S. 59.

232) Vgl. ebd., Vorwort;

233) Vgl. Büllesbach, A.: Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor, Tagungsband 20. DAFTA (1996), Köln 1997; Hoeren, T.: Datenschutz als Wettbewerbsvorteil. Das ungarische Datenschutzgesetz unter der ökonomischen Lupe, in DuD 1996, S. 542–549.

234) Vgl. die Ergebnisse der G7-Ministerkonferenz über die Informationsgesellschaft am 25. und 26. Februar 1995 in Brüssel, abrufbar unter http://www.ispo.cec.be/g7/keydocs/G7en.html.

235) Vgl. Report of the Ad Hoc Meeting of Experts on Information Infrastructures. Issues Related to Security of Information Systems and Protection of Personal Data and Privacy, Paris 1996 (OECD/GD(96)74).

236) Vgl. Europäische Initiative für den elektronischen Geschäftsverkehr. Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Auschuß der Regionen vom 14. April 1997, KOM (97) 157, S. 21 f; zuvor schon: Europe and the Global Information Society. Recommendations to the European Council, Brüssel, 26. Mai 1994, Kapitel 3, unter Privacy, Europe's Way to the Information Society. An action plan, Luxemburg 1995, Kapitel I.6.

237) Vgl. die Erklärung des U.S.-Präsidenten Bill Clinton „A Framework for Global Electronic Commerce", abufbar unter http://www.whitehouse.gov

238) Vgl. Empfehlungen Nr. E 22 bis E 27. Die Empfehlungen des Rates wurden der Öffentlichkeit am 21. Dezember 1996 vorgestellt. Sie sind abrufbar unter http://www.iid.de.

Diese Übereinstimmung im Grundsatz führt nicht notwendig auch zu einem Konsens über die Konsequenzen im einzelnen. Für die neuen Informations- und Kommunikationsdienste müssen auch im Bereich des Datenschutzes Rahmenbedingungen gefunden werden, die einen Ausgleich zwischen den Interessen der Wirtschaft, den Interessen der einzelnen Nutzer und den vom Staat wahrgenommenen Interessen der Allgemeinheit herstellen. Das kann auf vielerlei Weise geschehen.[239]) Zu erfahren, wie solche Rahmenbedingungen beschaffen sein sollten, erfordert daher eine Auseinandersetzung auch mit dem Detail. Diese soll hier erfolgen, indem zunächst der Begriff des Datenschutzes geklärt (3.2.), die datenschutzrelevanten Merkmale der Kommunikation in Netzen (3.3.) sowie die Risiken und Chancen der neuen Informations- und Kommunikationstechnologien beschrieben (3.4.) und dann die grundsätzlichen Handlungsoptionen aufgezeigt werden (3.5.). Schließlich werden auf der Grundlage einer Analyse der bereits erfolgten und der bevorstehenden Anpassungen des Datenschutzes auf nationaler (3.6.), europäischer (3.7.) und internationaler Ebene (3.8.) Empfehlungen abgegeben. Eine Zusammenfassung dieser Empfehlungen bildet den Schluß der Darstellung (3.9.)

2. Der Begriff des Datenschutzes

2.1. Das Recht auf informationelle Selbstbestimmung

Unter dem Begriff des Datenschutzes versteht man entgegen seinem Wortsinn nicht den Schutz der Daten selbst, sondern vor allem den Schutz des Menschen und seines nach der Rechtsprechung des Bundesverfassungsgerichts im Grundgesetz verankerten Grundrechts auf informationelle Selbstbestimmung.[240]) Dieses Recht beinhaltet die Befugnis des Einzelnen, „grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[241]) Denn, so das Bundesverfassungsgericht:

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden. (...) Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen könnten, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[242])

Unmittelbares Schutzgut des Datenschutzes sind „personenbezogene Daten". Mit diesem Begriff werden nach § 3 Abs. 1 Bundesdatenschutzgesetz „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" beschrieben. Was darunter zu fassen ist, kann nur im Einzelfall bestimmt werden. Zumindest auf der Grundlage der verfassungsgerichtlichen Rechtsprechung kann jedoch die grundsätzliche Aussage gelten, daß eine Differenzierung in sensible und weniger sensible Daten für den Datenschutz wenig aussagekräftig ist: Im Volkszählungsurteil führt das Bundesverfassungsgericht aus, durch die der Informationstechnik eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten könne auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen. Insoweit gebe es unter den Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr. Wieweit Vorgänge sensibel seien, könne demzufolge nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Die Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums könne vielmehr erst dann getroffen werden, wenn klar sei, zu welchem Zweck die Angabe erhoben wird und welche Verknüpfungsmöglichkeiten bestehen.

Das Verhältnis des Datenschutzes zur Datensicherheit hat viele Facetten. Einerseits ist die Datensicherheit ein wichtiges und unverzichtbares Instrument eines wirksamen Datenschutzes.[243]) Andererseits ist der Schutz der im Mittelpunkt des Datenschutzes stehenden Vertraulichkeit von personenbezogener In-

[239]) Vgl. zu unterschiedlichen Optionen Lawson, I.: Privacy and the Information Highway. Regulatory Options for Canada, 1996, Kapitel 10 (abrufbar unter http://strategis.ic.gc.ca) sowie Bennett, C. J.: The Political Economy of Privacy: A Review of the Literature, 1995 (abrufbar unter http://www. cous.uvic.ca/poli/gnom.html.

[240]) Vgl. Gola, P.; Schomerus, R.: Bundesdatenschutzgesetz, 6. Aufl., München 1997, S. 47; Schneider, J.: Datenschutz und Datensicherheit, in: Schwarz, M.: Recht im Internet. Der Rechtsberater für Online-Anbieter und -Nutzer, Stand 21. Mai 1997, 11–2.1.

[241]) Vgl. BVerfGE 65, 1 (43).

[242]) Vgl. BVerfGE 65, 1 (42f).

[243]) Vgl. Bäumler, H.: Wie geht es weiter mit dem Datenschutz?, in DuD 1997, S. 446–452 (450).

formation und Kommunikation auch Ziel der Datensicherheit.[244]) Dabei ist der Begriff der „mehrseitigen Datensicherheit" zugrundezulegen, demzufolge die legitimen Sicherheitsinteressen aller Betroffenen, also auch der Verbraucher und Bürger, angemessen zu berücksichtigen sind und es ausgeschlossen ist, nur die Sicherheit eines Beteiligten in Rechnung zu stellen, etwa des Betreibers eines Verfahrens.[245])

Konkretisiert wird das Recht auf informationelle Selbstbestimmung durch allgemeines und bereichsspezifisches Datenschutzrecht des Bundes und der Länder. Im einzelnen wird auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts davon ausgegangen, Datenschutz müsse gewährleisten, daß

- der betroffene Bürger grundsätzlich die Entscheidungsfreiheit darüber hat, wer seine personenbezogenen Daten zu welchem Zweck verarbeiten darf,
- er wissen können muß, wer seine Daten zu welchem Zweck verarbeitet hat,
- Daten nur zu einem bestimmten, dem Bürger bekannten Zweck verarbeitet werden dürfen, und zwar auch innerhalb der datenverarbeitenden Stellen (informationelle Gewaltenteilung);
- technisch-organisatorische Vorkehrungen getroffen werden müssen, um dies zu gewährleisten,
- Daten nicht auf Vorrat gespeichert werden und keine Persönlichkeitsprofile gebildet werden,
- Vorschriften zur Löschung personenbezogener Daten bestehen, um ein „Recht auf Vergessen" zu gewähren, und
- Datenverarbeitung durch unabhängige Stellen kontrolliert wird.[246])

2.2 Das Fernmeldegeheimnis

Neben dem aus Art. 1 und 2 Grundgesetz abgeleiteten Recht auf informationelle Selbstbestimmung ist für den Datenschutz in Netzen das durch Art. 10 Grundgesetz geschützte Fernmeldegeheimnis von großer Bedeutung. Das Fernmeldegeheimnis schützt sowohl den Inhalt jeder Art von Fermeldeverkehr, d. h. auch zum Beispiel den Funkverkehr und die Datenfernübertragung, als auch sämtliche Umstände des Kommunikationsvorgangs, also dessen Art, Zeitpunkt, Dauer und dergleichen.[247]) Konkretisiert und auch für private Telekommunikationsanbieter verbindlich gemacht wird das Fernmeldegeheimnis unter anderem durch Bestimmungen im Telekommunikationsgesetz und im Strafgesetzbuch.

2.3 Einschränkungen

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis werden von der Verfassung nicht schrankenlos gewährleistet. Einschränkungen sind vielmehr im überwiegenden Allgemeininteresse hinzunehmen, etwa in dem vom Staat wahrgenommenen Interesse der Allgemeinheit an effektiver Gefahrenabwehr und Strafverfolgung. Auch im übrigen sind viele Konstellationen denkbar, in denen die Nachteile von Sammlungen und Übertragungen personenbezogener Daten deren Vorteile jedenfalls nicht von vornherein überwiegen müssen. Medizinische Datenbanken können helfen, Krankheiten zu bekämpfen, Informationen über die Kreditwürdigkeit eines Käufers reduzieren das Risiko des Verkäufers und damit möglicherweise auch den Preis seiner Produkte. Ob und inwieweit in solchen Fällen eine Einschränkung des Rechts auf informationelle Selbstbestimmung zulässig ist, hängt vom Ergebnis einer anzustellenden Güterabwägung ab. Sie bedürfen jedenfalls einer gesetzlichen Grundlage, die die Voraussetzungen und den Umfang der Beschränkungen klar erkennen läßt.[248])

Sowohl das Recht auf informationelle Selbstbestimmung als auch das Fernmeldegeheimnis gewährleisten Schutz grundsätzlich lediglich im Verhältnis des Bürgers zum Staat. Es ist jedoch allgemein anerkannt, daß Grundrechte nicht nur Abwehrrechte des Einzelnen gegen den Staat, sondern zudem auch Elemente einer objektiven Wertordnung sind und damit auch die Rechtsbeziehungen zwischen Privaten, etwa im Verhältnis eines Telekommunikationsunternehmens zu seinen Kunden, prägen können.

---

[244]) Unter dem Begriff der Daten- oder Informationssicherheit werden die Sicherung der Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen gefaßt. Vgl. z. B. die Legaldefinition in § 2 Abs. 2 des Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik, BGBl. 1990, Teil I, S. 2834–2836.

[245]) Vgl. Bäumler, H.: Wie geht es weiter mit dem Datenschutz?, in DuD 1997, S. 446–452 (450).

[246]) Vgl. Roßnagel, A.; Bizer, J.: Multimediadienste und Datenschutz, in DuD 1996, S. 209–217 (211f).

[247]) Vgl. *BVerfGE 85, 386 (396);* Schmitt Glaeser, W.: Schutz der Privatsphäre, in: Isensee, J.; Kirchhof, P.: Handbuch des Staatsrechts der Bundesrepublik Deutschland, Heidelberg 1989, Band IV, S. 41–108, Rn. 64f.

[248]) Vgl. BVerfGE 65, 1 (44, 48 ff).

3. Datenschutzrelevante Merkmale der Datenerhebung und -verarbeitung in Netzen

Die neuen Informations- und Kommunikationstechniken haben die Datenverarbeitung revolutioniert. Daten können um ein Vielfaches schneller und einfacher erhoben, verarbeitet und übermittelt werden als zuvor. Das gilt auch für personenbezogene Daten: Sie fließen auf den Datenautobahnen wie Wasser, das aus vielen unterschiedlichen Quellen in Bäche, Flüsse und Seen in Ozeane strömt, heißt es in einem kanadischen Bericht über den Datenschutz in der Informationsgesellschaft.[249]) Ursache sind einige besondere Merkmale der Datenverarbeitung in Netzen:

3.1. Gesteigerter Anfall personenbezogener Daten

Bei der Kommunikation in Netzen fällt eine ungleich größere Menge personenbezogener Daten an als bei anderen Kommunikationsformen: Jeder Anruf, jeder Tastendruck und jeder Mausklick hinterläßt eine Datenspur.[250]) Während beim Einkauf in einem Kaufhaus in der Regel jedenfalls dann keinerlei personenbezogene Daten entstehen, wenn keine Kredit- oder Euroscheckkarte benutzt wird, kann beim Teleshopping im Internet registriert werden, was der Einkäufer bestellt, welche Teile des Warenangebots er zuvor wie lange betrachtet hat und für welche Produkte er sich im Anschluß daran interessiert hat. Ebenso nachvollziehen lassen sich etwa die Lektüre einer elektronischen Zeitung, die Teilnahme an einer Online-Diskussion und die Wahrnehmung von neuartigen Fernsehangeboten wie „Teleshopping", „pay per view" oder Video auf Abruf.[251])

Hinzu kommt, daß Telekommunikationsnetze zunehmend auch außerhalb der neuen Dienste zur Datenerhebung und –verarbeitung genutzt werden: In fast allen Lebensbereichen werden bestehende Daten digitalisiert, in Computersystemen verarbeitet und über Telekommunikationsnetze transportiert.[252]) Ein sichtbares Zeichen dieser Entwicklung ist der zunehmende Einsatz von Chipkarten als Speichermedium. Nachdem Bank- und Kreditgeschäfte bereits seit geraumer Zeit mit EC- und Kreditkarten abgewickelt werden, die eine Kommunikation über Telekommunikationsnetze erlauben, wurden auch im Gesundheitswesen mit der Einführung der Patientenchipkarte[253]) und der Verwendung von digitaler Technik in immer mehr medizinischen Untersuchungsgeräten die Voraussetzungen für medizinische Betreuung, aber auch Kostenabrechnungen mittels Telekommunikation geschaffen.[254]) Weitere Anwendungen der Telekommunikation sind jetzt schon absehbar: Elektronische Mautsysteme ermöglichen die Erfassung von Verkehrsbewegungen, intelligente Navigationssysteme informieren über die Position eines bestimmten Fahrzeugs und zeigen die optimale Streckenführung an, biometrische Verfahren, mit denen unverwechselbare körperliche Kennzeichen eines Menschen registriert werden, erlauben sichere Zugangskontrollen auch über große Distanzen.[255])

Unabhängig von der jeweiligen Anwendung lassen sich die Arten der in Telekommunikationsnetzen entstehenden Daten wie folgt unterscheiden:[256])

Bestandsdaten (Stammdaten) sind Daten, die der Identifikation des Netznutzers dienen und daher dauerhaft gespeichert und bereitgehalten werden. Zu ihnen gehören in der Regel die Nutzernamen und -anschriften sowie Anschlußkennungen (Rufnummern, Domain-Namen). Hinzu kommen Daten, die für die Begründung, inhaltliche Ausgestaltung und Änderung des Vertragsverhältnisses erhoben werden, also etwa Angaben über die Bankverbindung, das Geburtsjahr und einen Status, der zu Preisermäßigungen führen kann.

Inhaltsdaten sind die eigentlichen Nachrichten, z. B. elektronische Briefe, übersandte Bilder und Musikstücke, Telefongespräche, Beiträge in Diskussionsforen, Bestellungen und weitere Angaben wie Bankverbindung und Adresse beim Telekauf.

Verbindungsdaten sind Angaben über die näheren Umstände eines Kommunikationsvorgangs. Dazu gehören etwa Daten über den Zeitpunkt und die Dauer der Verbindung, über die in Anspruch genommenen Leistungen (z. B. Telefon, Fax, Email), über die Kennungen des rufenden und angerufenen Anschlusses. Verbindungsdaten werden vor allem zur Abrechnung für Dienstleistungen in Telekommunikationsnetzen genutzt, sofern diese nicht vorab bezahlt werden oder nur pauschal abgerechnet wird. Die dazu notwendigen Daten werden zum Teil als gesonderte

[249]) Lawson, I.: Privacy and the Information Highway. Regulatory Options for Canada, abrufbar unter http://www.strategis.ic.gc.ca

[250]) Vgl. Simitis, S.: Daten- oder Tatenschutz – ein Streit ohne Ende?, in: NJW 1997, S. 1902f (1903).

[251]) Vgl. 15. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, Berichtsjahr 1996, unter 5.1.

[252]) Vgl. Kilian, W.: Möglichkeiten und zivilrechtliche Probleme eines rechtswirksamen elektronischen Datenaustauschs (EDI), in DuD 1993, S. 606–610.

[253]) Vgl. Alles, P.; Kraus, D.: IT-Sicherheitsmaßnahmen beim Einsatz der Krankenversichertenkarte, in DuD 1994, S. 141–145.

[254]) Vgl. Jacob, J.: Datenschutz – ärztliche Schweigepflicht – Telekommunikation, Vortrag am Institut für Medizinische Statistik, Dokumentation und Datenverarbeitung an der Universität Bonn am 13. Juni 1996, abrufbar unter http://imsdd.meb.uni-bonn.de/datenschutz/bfd.html

[255]) Vgl. Weichert, T.: Biometrie – Freund oder Feind des Datenschutzes, in: CR 1997, S. 369–375.

[256]) Vgl. z. B. Köhntopp, M.: Datenschutz in der Informationsgesellschaft, in: Buhlmann, E.; van Haaren, K.; Hensche, D.; Kiper, M.; Kubicek, H.; Rilling, R.; Schmiede, R. (Hrsg.): Informationsgesellschaft – Medien – Demokratie, Marburg 1996, S. 212–218 (219).

Kategorie, nämlich als Abrechnungsdaten aufgeführt.

3.2 Erleichterte Speicherung, Übermittlung, Verarbeitung und Zusammenführung personenbezogener Daten

Die neuen Informations- und Kommunikationstechnologien erleichtern die Datenverarbeitung ungemein. Verarbeitungsgeschwindigkeiten und Übertragungsraten werden kontinuierlich erhöht; die Speicherkapazitäten wachsen ins Unermeßliche. Die Unterlagen ganzer Unternehmen lassen sich auf Datenträgern speichern, die in jede Aktentasche passen,[257]) und selbst große Datenmengen können unabhängig von nationalen Grenzen in Sekundenschnelle rund um den Erdball geschickt werden. Auch kleine Kommunalverwaltungen verfügen heute über Rechnerkapazitäten, die Anfang der 70er Jahre lediglich für die Mondflüge der NASA bereitstanden.[258]) Computerprogramme mit Suchfunktionen machen es möglich, auch aus größten Datenbeständen die Daten einer einzelnen Person ohne nennenswerten Zeit- und Kostenaufwand herauszufiltern und zusammenzuführen. Die Auswertungsmöglichkeiten sind nahezu unbegrenzt und müssen nicht im voraus festgelegt werden.

3.3 Dezentraler und globaler Anfall personenbezogener Daten

Personenbezogene Daten fallen in Telekommunikationsnetzen nicht lediglich an einigen wenigen zentralen Stellen in einem überschaubaren und von bestimmten rechtlichen Regelungen bestimmten Gebiet an; sie entstehen vielmehr global und an einer Vielzahl unterschiedlicher Stellen.[259]) Der Nutzer des Internets hinterläßt mit den sogenannten LOG-Protokollen Daten auf jeder Netzseite, die er aufruft. Der Server, auf dem die Seite abgerufen wird, kann ebenso in Deutschland wie in der Karibik installiert sein, ohne daß dies zuverlässig festgestellt werden könnte.[260]) Auch elektronische Briefe gehen häufig weite und unbekannte Wege:[261]) Ein über den Service eines US-amerikanischen Anbieters von Bonn nach Brüssel über das Internet versandter elektronischer Brief wird stets über den zentralen Mailserver dieses Unternehmens in Ohio geschickt.[262]) Auf seinem Weg passiert er – neben dem Einwahlknoten des Providers – eine im Voraus nicht absehbare Anzahl von sogenannten Mail Transfer Agenten, d. h. Computerprogrammen auf Servern, die dafür sorgen, daß elektronische Briefe an den richtigen Empfänger weitergeleitet werden. An all diesen Stellen hinterläßt der elektronische Brief eine Datenspur, die zumindest aus den Verbindungsdaten besteht. Ähnliches gilt bei anderen Telekommunikationsdiensten. Wird bei Anbietern stationärer Telefonie lediglich gespeichert, zwischen welchen Apparaten eine Verbindung hergestellt und wie lange sie aufrecht erhalten wird, werden bei der Mobilkommunikation auch die Bewegungen des Teilnehmer erfaßt – und zwar auch dann, wenn er nicht telefoniert, das Gerät aber eingeschaltet ist.[263])

3.4 Privater Anfall von personenbezogenen Daten

Bis vor wenigen Jahren war es vor allem der Staat, der personenbezogene Daten für seine Zwecke erhob, sammelte und verarbeitete. Folge der Verbreitung von PCs, des Anstiegs der Speicherkapazitäten und Datenverarbeitungsgeschwindigkeiten, der Vernetzung von Computern und der Privatisierung der Telekommunikation ist, daß der Staat diese Vorherrschaft verliert und immer mehr privatwirtschaftliche Unternehmen und einzelne Bürger über personenbezogene Daten verfügen. „Niemals zuvor haben nichtöffentliche Stellen so viele personenbezogene Daten so systematisch gesammelt, verarbeitet und verwertet", stellt der Leiter der Forschungsstelle für Datenschutz an der Universität Frankfurt am Main, Prof. Dr. Spiros Simitis, fest.[264])

---

[257]) Vgl. Cohen, F. B.: Protection and Security on the Information Highway, New York u. a. 1995, S. 16 f.

[258]) Vgl. Bäumler, H.: Wie geht es weiter mit dem Datenschutz?, in DuD 1997, S. 446–452 (447).

[259]) Vgl. Simitis, S.: Der Datenschutz: Stolper- oder Baustein der Informationsgesellschaft, in: Bundesministerium des Innern: Informationsgesellschaft und Innere Sicherheit, Bonn 1996, S. 49–56 (51 f.).

[260]) Viele der für WWW-Seiten vergebenen Kennzeichen (Domainnamen) wie „.com", „.org." etc. lassen keinen Schluß darauf zu, in welchem Land ein Server steht. Überdies können auch falsche Domainnamen verwendet werden, etwa die einen in Deutschland stationierten Anbieter kennzeichnende Endung „.de" von einem Anbieter aus einem anderen Staat.

[261]) Zur technischen Funktionsweise von Email vgl. Schallbruch, M.: Electronic Mail im Internet. Wie steht es mit dem Datenschutz, in Datenschutz-Nachrichten 5/95, abrufbar unter http://www.rewi.hu-berlin.de~/mascha/mailds.html.

[262]) Vgl. European Parliament, Scientific and Technological Options Assessment (STOA): The Information Society. An Appraisal of Technical Instruments for Political Control and to Improve Participation in the Information Society (Part A), Working Document for the Project Steering Group, Luxembourg, January 1996 (PE: 165714), II.1.7.2.1 (S. 7).

[263]) Vgl. Dix, A.: Gesetzliche Verschlüsselungsstandards – Möglichkeiten und Grenzen der Gesetzgebung, in Computer und Recht 1997, S. 38–43 (41); Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 zum Datenschutz bei der Privatsierung der Deutschen Bundespost und der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste, abgedruckt in: Berliner Datenschutzbeauftragter: Datenschutz bei Telekommunikation und Medien, 1. Auflage, Berlin 1995, S. 16.

[264]) Simitis, S.: Der Datenschutz: Stolper- oder Baustein der Informationsgesellschaft, in: Bundesministerium des Innern: Informationsgesellschaft und Innere Sicherheit, Bonn 1996, S. 49–56 (52).

4. Risiken für das informationelle Selbstbestimmungsrecht in Netzen

Aus den beschriebenen Merkmalen der Datenverarbeitung in Telekommunikationsnetzen ergeben sich Risiken für das informationelle Selbstbestimmungsrecht. Es bestehen – nach Art des in Anspruch genommenen Dienstes unterschiedliche – Möglichkeiten, das Kommunikationsverhalten des Einzelnen ohne sein Wissen und ohne seine Einwilligung zu überwachen und daraus gewonnene Daten zu verarbeiten und zu nutzen:

4.1 Überwachung

Als eines der wichtigsten Probleme für das informationelle Selbstbestimmungsrecht in Telekommunikationsnetzen wird die Möglichkeit der Überwachung angesehen:[265]) Personenbezogene Daten können in Telekommunikationsnetzen ohne Einwilligung des Nutzers preisgegeben und Kommunikationsvorgänge – zeitgleich oder zeitversetzt – überwacht werden. Im Klartext versandte elektronische Briefe zum Beispiel können grundsätzlich an jedem Rechner, den sie passieren, kopiert, gespeichert und gelesen werden.[266]) Gleiches gilt für Angaben, die beim Teleeinkauf im Internet gemacht werden. Mit unter dem Namen „Packet Sniffer" (Paketschnüffler) bekannten Programmen kann der Datenverkehr auch automatisiert überwacht werden. Diese Abhörprogramme, die von öffentlichen Mailboxen und Internetservern heruntergeladen werden können, sind in der Lage, etwa im Klartext übertragene Nutzerkennungen mit den zugehörigen Paßworten aus dem Datenverkehr herauszufiltern und so die Möglichkeit zu weiterem Ausspähen zu bieten. Auch Kreditkartennummern sollen auf diese Weise in Erfahrung gebracht worden sein. Ein vergleichbares Überwachungspotential bieten scheinbar harmlose Programme, die als trojanische Pferde bezeichnet werden. Diese können zum Beispiel nach der Installation auf der Festplatte des Nutzers den Computer unbemerkt nach verwertbaren Informationen ausforschen und sie über das Internet an eine ihnen eingegebene Adresse versenden. Ähnlich arbeiten die sogenannten „Cookies", d. h. Computerprogranme, die – zum Teil unbemerkt – bei der Anwahl vieler Server auf der Festplatte des Nutzers installiert werden, um bei einer weiteren Anwahl dessen Identifikation zu ermöglichen, sofern der Nutzer seine personenbezogenen Daten offenbart hat.

Überwachungsgefahren bestehen auch bei Telefon- und Faxdiensten. Werden die Daten unverschlüsselt übertragen, ist bei der mobilen Telekommunikation zudem die Vertraulichkeit der Inhaltsdaten gefährdet – bei satellitengestützen Systemen besteht die Möglichkeit, die übertragenen Daten im gesamten Abstrahlbereich des Satelliten abzuhören und aufzuzeichnen.[267])

4.2 Profilbildung

Verknüpft können die gespeicherten Daten zu umfassenden Persönlichkeitsprofilen verarbeitet werden. Je häufiger etwa ein Nutzer das Angebot eines Versandhandels oder einer Zeitschrift im Internet anschaut oder bei neuartigen Fernsehangeboten bestimmte Filme bucht, um so genauer weiß der Betreiber des Servers um seine Interessen und Konsumgewohnheiten. Das Interesse an solchen Profilen ist insbesondere in der Werbewirtschaft immens,[268]) die ihren Kunden zunehmend die Buchung bestimmter Konsumentenprofile ermöglichen will.[269]) Der Nutzer würde dann mit auf seine Interessen zugeschnittener Werbung versorgt, wenn er sich ins Internet begibt. In der Datenbank einer amerikanischen Agentur, die Werbeplätze auf Internetseiten vermittelt, waren bereits 1997 16 Millionen Profile gespeichert;[270]) andere Anbieter offerierten Datenbanken mit Informationen über Adressen, Geburtsdaten und Telefonnummern von bis zu 300 Millionen Menschen.[271]) Ähnlich groß dürften die Bestände von Anbietern sein, die etwa das kostenlose Herunterladen von Software oder die kostenlose Einrichtung eines elektronischen Briefkastens an die Angabe persönlicher Daten knüpfen.

Ebenso wie Konsumprofile können auch andere Interessenprofile erstellt werden. Denkbar ist etwa die Aufzeichnung der Auswahl bestimmter Internetserver oder Fernsehsendungen mit politischem Inhalt, die – möglicherweise noch kombiniert mit in politischen Diskussionsgruppen im Internet getroffenen Aussagen – ein aussagekräftiges Bild über die politische Einstellung eines Nutzers vermitteln könnte. Wird der Telekommunikationsverkehr – wovon aus-

---

265) Vgl. OECD: Report of the Ad Hoc Meeting of Experts on Information Infrastructures. Issues Related to Security of Information Systems and Protection of Personal Data and Privacy, S. 30.

266) Vgl. Schallbruch, M.: Electronic Mail im Internet. Wie steht es mit dem Datenschutz, in Datenschutz-Nachrichten 5/95, abrufbar unter http://www.rewi.hu-berlin.de~/mascha/mailds.html.

267) Vgl. Vgl. Bäumler, H.: Wie geht es weiter mit dem Datenschutz?, in: DuD 1997, S. 446–452 (447).

268) Vgl. Information Policy Committee der National Information Infrastructure Task Force: Options for Promoting Privacy on the National Information Infrastructure, http://www.iitf.ipc/privacy.html, unter Privacy in the Marketplace, 3.

269) Vgl. new media report, Juni 1997: Auf der Suche nach dem Profil, S. 1–3.

270) Vgl. ebd. S. 3.

271) Vgl. Hoffman, Lance J.; Metivier Carrairo, K. A.: Computer Technology to Balance Accountability and Anonymity in Self-Regulatory Privacy Regimes, in: U. S. Department of Commerce, National Telecommunications and Information Administration: Privacy and Self Regulation in the Information Age, Washington D.C. Juni 1997, S. 169–173 (172).

zugehen ist[272]) – zunehmend mittels mobiler Endgeräte abgewickelt, ist zudem die Erstellung von Bewegungsprofilen möglich.[273]) Diese Gefahr bergen auch intelligente Verkehrsleit- und Navigationssysteme, die als ein Mittel für die Steuerung des LKW- und PKW-Verkehrs angesehen werden.[274])

4.3 Intransparenz der Datenerhebung und -verarbeitung

Bei der Datenerhebung und -verarbeitung in Netzen hat der Nutzer häufig keinerlei Möglichkeit, zu erfahren und zu kontrollieren, welche personenbezogenen Daten über ihn wo, wann und mit welchem Zweck gespeichert und verarbeitet werden. Der dezentrale Anfall der Daten, die technische Komplexität, die Tatsache, daß Daten unbemerkt erhoben werden können, sowie die Schnelligkeit und Globalität der Datenspeicherung führen immer mehr zu einer Intransparenz von Datenerhebung und Verarbeitung. Das gilt nicht nur im Internet, sondern auch in vielen anderen Lebensbereichen. Während früher etwa die Daten eines Patienten auf seinem Krankenschein auch für den Patienten selbst ohne weiteres lesbar waren, bedarf es dazu bei den von den gesetzlichen Krankenversicherungen eingeführten Chipkarten einer umfangreichen technischen Ausstattung und entsprechender Kenntnisse im Umgang mit dieser.

5. Möglichkeiten des Datenschutzes in Netzen

Wie kann den Gefahren für das informationelle Selbstbestimmungsrecht in Netzen begegnet werden? Grundsätzlich stehen die Möglichkeiten des technischen Datenschutzes, des normativen Datenschutzes und der Selbstregulation zur Verfügung:

5.1 Selbstschutz

Der technische Fortschritt läßt sich auch für den Schutz der Privatsphäre einsetzen.[275]) Die gleiche Technik, die die Vertraulichkeit von personenbezogenen Daten einerseits gefährdet, kann andererseits dazu beitragen, Datenanfall zu vermeiden, eine anonyme oder pseudonyme Nutzung von Telekommunikationsdiensten zu ermöglichen und Inhaltsdaten vor dem Zugriff Dritter zu schützen.[276]) Das ist indessen nicht zuletzt von der eigenen Initiative des Nutzers abhängig. Ihm steht schon heute eine Vielzahl von technischen Hilfsmitteln und Dienstleistungen zur Verfügung, die es ermöglichen, die Privatsphäre zu bewahren. Beispielhaft seien genannt:

- Kryptografische Verfahren, denen eine zentrale Rolle für den Datenschutz in Netzen zugemessen wird,[277]) ermöglichen ein sicheres Verschlüsseln von Dokumenten. Schon heute existieren sehr einfach zu bedienende Computerprogramme und Geräte, die eine schnelle und effektive Verschlüsselung von Daten zulassen und ohne weiteres in die Umgebung bereits bestehender Softwareprodukte integriert werden können.[278]) Ihr Einsatz kann nicht nur einen wirksamen Schutz gegen das Ausspähen von Kommunikationsdaten in Telefonnetzen und anderen Telekommunikationsnetzen darstellen, sondern auch gespeicherte Daten effektiv gegen Zugriffe Dritter schützen. Da außerordentlich starke Verschlüsselungsverfahren zur Verfügung stehen und die Möglichkeit besteht, den für die Kodierung benötigten Schlüssel durch den Nutzer selbst generieren zu lassen, kann eine Entschlüsselung durch Dritte als weitgehend ausgeschlossen betrachtet werden.
- Anonymisierungsserver ermöglichen eine anonyme Nutzung des Internet – eine Datenspur kann nicht zum Nutzer, sondern lediglich zu diesem Server zurück verfolgt werden.[279]) Gleiches gilt für sogenannte Remailer, die den pseudonymen und häufig auch verschlüsselten Versand von elektronischen Briefen ermöglichen.[280]) Personenbezogene Daten fallen in diesem Fall allerdings

[272]) Vgl. Europäische Kommission: Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen über die weitere Entwicklung der Drahtlos- und Mobilkommunikation in Europa. Herausforderungen für die Europäische Union vom 29. Mai 1997 (KOM (97) 217 endg.), derzufolge die Marktdurchdringungsraten des zellularen Mobilfunks in einigen Mitgliedsstaaten der EU bereits heute 30 Prozent erreicht haben. Bis zum Jahre 2005 werde mit einem Anstieg der Durchdringungsrate auf 40–50 Prozent der EU-Bevölkerung gerechnet.

[273]) Vgl. Bizer, J.; Fox, D.: Spurenlos mobil?, in: DuD 1997, S. 6; Berliner Datenschutzbeauftragter: Mobilfunk und Datenschutz, Berlin 1994.

[274]) Zu solchen Systemen: Funkschau 13/97, S. 26–31; zu ihrer Bewertung aus der Sicht des Datenschutzes vgl. OECD: Report of the Ad Hoc Meeting of Experts on Information Infrastructures. Issues Related to Security of Information Systems and Protection of Personal Data and Privacy, S. 32 m. w. N.

[275]) Vgl. Bäumler, H.: Wie geht es weiter mit dem Datenschutz?, in: DuD 1997, S. 446–452 (448).

[276]) Vgl. Hoffman, L.J.; Metivier Carrairo, K. A.: Computer Technology to Balance Accountability and Anonymity in Self-Regulatory Privacy Regimes, in: U.S. Department of Commerce, National Telecommunications and Information Administration: Privacy and Self Regulation in the Information Age, Washington D.C. Juni 1997, S. 169–173.

[277]) Zur Bedeutung der Kryptografie für die Informationsgesellschaft vgl. National Research Council, Computer Science and Telecommunications Board: Cryptography's Role in Securing the Information Society, Washington, D.C. 1996.

[278]) Vgl. Gerling, R. W.: Verschlüsselungsverfahren. Eine Kurzübersicht, in: DuD 1997, S. 197–201: Funkschau 4/97: Sichere Telekommunikation, S. 42–44.

[279]) Vgl. etwa das Angebot unter http://www.anonymizer.com

[280]) Vgl. Information and Privacy Commissioner/Ontario: Identity Theft: Who's Using Your Name, Juni 1997, abrufbar unter ipc.on.ca.

bei den Anoynymisierungsservern und bei den Remailern an – jedenfalls dann, sofern pseudonymer Versand vorliegt und eine Antwortmöglichkeit besteht. Vollständig anonyme Nutzung bieten die sogenannten „Mixmaster".

- Als „Identity Protectors"[281]) („Identitätsschützer") bezeichnete Programme vermögen es, für jede einzelne Nutzung eines Dienstes eine einmalige und einzigartige Pseudoidentität zu schaffen. Die Datenschutzbeauftragten der Niederlande und der kanadischen Provinz Ontario haben in einer gemeinsamen Erklärung empfohlen, internationale Standards für solche Programme zu entwikkeln.[282])
- Schließlich besteht für den Nutzer auch die Möglichkeit, die Transparenz der Datenerhebung und -verarbeitung zu erhöhen und sie weitgehend an seine Einwilligung zu binden. Ein Beispiel ist die „Platform for Privacy Preferences", ein von der Organisation World-Wide-Web-Consortium entwikkeltes Computerprogramm, das dem Nutzer im Prinzip die Möglichkeit gibt, bei der Nutzung von Internetangeboten jeweils selbst darüber zu entscheiden, welche seiner persönlichen Daten er preisgeben will.[283]) Die Software informiert den Nutzer jeweils darüber, ob und welche Daten bei einem Besuch auf der gerade angesteuerten Internetseite über ihn erhoben werden und überläßt ihm die Entscheidung, ob er das Angebot weiter wahrnehmen will. Das Programm läßt auch Einstellungen zum Schutz von kindlichen Nutzern zu, die auf manchen Webseiten gezielt angesprochen und ausgefragt werden. Ähnlich funktioniert der 1997 von Internetunternehmen vorgestellte „Open Profiling Standard", der es Nutzern ermöglichen soll, einen elektronischen Ausweis mit persönlichen Daten in ihrem Computer zu speichern und bei jedem Anbieter im Internet darüber zu entscheiden, welche dieser Daten er freigeben will.[284])

5.2 Systemdatenschutz

Ergänzt werden können die Möglichkeiten des technischen Selbstschutzes durch Maßnahmen des Systemdatenschutzes. Unter diesem Begriff werden Vorkehrungen verstanden, die die Erhebung und Verwendung personenbezogener Daten bereits durch eine entsprechende Gestaltung der Systemstrukturen vermeiden,[285]) also Maßnahmen die die Datenschutzfunktionen der in Telekommunikationsnetzen verwendeten Geräte, Programme und Übertragungswege sowie der in ihnen angebotenen Dienste unterstützen. Systemdatenschutz kann bei der Entwicklung von Endgeräten, Übertragungswegen und Computerprogrammen ebenso greifen wie bei der Planung bestimmter Angebote in Telekommunikationsnetzen.[286]) Beispielhaft genannt werden sollen folgende Möglichkeiten:

- Die Möglichkeit, vorbezahlte Chipkarten einzusetzen, kann helfen, den Anfall vieler Daten von vornherein zu verhindern. Können mit solchen Karten etwa die Dienste eines Internetproviders oder Mobilfunkunternehmens vergütet werden, bedarf es keines Vertragsverhältnisses, das die Speicherung von Bestands- und Verbindungsdaten erfordert,[287]) und ließen sich auch zuordenbare Bewegungsprofile bei der mobilen Telekommunikation vermeiden.
- Werden datensparsame elektronische Zahlungssysteme verwendet, kann eine Zahlung mit digitalem Geld ebenso anonym erfolgen wie eine Barzahlung.[288]) Dies ist etwa bei den derzeit von den Banken angebotenen Geldkarten nicht der Fall.[289])
- Wird ein technischer Zugriffsschutz in Form von Paßworten und der Vergabe genau definierter Zugriffsrechte realisiert, läßt sich ein sicherer Schutz gegen unbefugte Zugriffe auf Datenbestände schon auf technischer Ebene verhindern.[290])
- Wird, was die hohen Speicherkapazitäten und Verarbeitungsgeschwindigkeiten moderner Informationstechnik möglich machen, jeder Zugriff auf Datenbestände protokolliert, können unzulässige Zugriffe auf Datenbestände nachvollzogen und sanktioniert und durch den damit verbundenen Abschreckungseffekt präventiv verhindert werden. Dabei müßte indessen sichergestellt sein, daß die Protokolldatenbestände nicht auch für andere Zwecke verwendet werden.
- Werden zuverlässig auf ihre Datensicherheits- und Datenschutzfunktionen geprüfte Computerprogramme, Rechner, Modems, Telefonapparate und andere Geräte verwendet, ist der Nutzer auch

---

[281]) Vgl. Borking, J.: Der Identity-Protector, in DuD 1996, S. 654–658.

[282]) Vgl. Information and Privacy Commissioner/Ontario, Canada; Registratiekamer The Netherlands: Privacy-Enhancing Technologies: The Path to Anonymity, Vol. 1, August 1995, unter 3.1. (Das Dokument ist abrufbar unter http://www.ipc.on.ca/web_site.eng./matters/sum_pap/papers/anon-e.html).

[283]) Vgl. die unter http://www.w3.org/Privacy/Activity.html abrufbaren Informationen.

[284]) Vgl. die unter http://www.firefly.com/AboutFFN.html abrufbaren Informationen. Dazu und zum Modell des W3-Konsortiums Siegele, L.: Persönliche Daten sollen nicht länger öffentliche Güter sein, in: Frankfurter Rundschau vom 19. August 1997.

[285]) Vgl. Roßnagel, A.: Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger, in ZRP 1997, S. 26–30 (29); Engel-Flechsig, S.: „Teledienstedatenschutz", in DuD 1997, S. 8–16 (13f).

[286]) Vgl. Vgl. Ulrich, O.: Leitbildwechsel: dem (sicherheits)-technologisch aktivierten Datenschutz gehört die Zukunft, in: DuD 1996, S. 664–671 (668f); Engel-Flechsig, ebd., S. 13.

[287]) Vgl. Köhntopp, M.: Datenschutz in der Informationsgesellschaft, in: Buhlmann, E.; van Haaren, K.; Hensche, D.; Kiper, M.; Kubicek, H.; Rilling, R.; Schmiede, R. (Hrsg.): Informationsgesellschaft – Medien – Demokratie, Marburg 1996, S. 212–218 (215).

[288]) Zur Anonymität unterschiedlicher elektronischer Zalungssysteme vgl. Knorr, M.; Schläger, U.: Datenschutz bei elektronischem Geld. Ist das Bezahlen im Internet anonym?, in DuD 1997, S. 396–402; zu elektronischem Geld allgemein Funkschau 25/96, S. 60–63.

[289]) Vgl. Fox, D.; Bizer, J.: Wohin mit dem Geld?, in DuD 1997, S. 378.

[290]) Vgl. dazu und zu weiteren Möglichkeiten technischer Schutzmaßnahmen Bäumler, H., Wie geht es weiter mit dem Datenschutz?, in: DuD 1997, S. 446–452 (449).

gegen Hardware-bedingte Schwachstellen geschützt.

5.3 Normativer Datenschutz

Der Erlaß von gesetzlichen Bestimmungen, die zu einem bestimmten Umgang mit personenbezogenen Daten verpflichten, indem sie ihn etwa verbieten oder nur in bestimmten Grenzen zulassen, war in der Vergangenheit das wichtigste Instrument des Datenschutzes.[291]) In offenen Telekommunikationsnetzen stößt es zunehmend auf seine Grenzen. Denn zum einen ist Rechtsdurchsetzung auf die Macht des Staates oder von Staatenvereinigungen angewiesen. Diese kann jedoch nur innerhalb von Staatsgrenzen ausgeübt werden, die in den globalen Datennetzen binnen Sekunden überwunden werden können. Mögliche Folge vergleichsweise strenger datenschutzrechtlicher Bestimmungen wäre daher die Flucht von Unternehmen, die personenbezogene Daten erheben und verarbeiten, in Staaten mit weniger restriktiven Regelungen. Zum anderen bestehen auch innerhalb eines Staatsgebietes vielfältige Möglichkeiten, sich einer effektiven datenschutzrechtlichen Überwachung zu entziehen und staatliche Eingriffe zu konterkarieren;[292]) Abgesehen davon, daß es kaum möglich erscheint, die Millionen von Servern, die zumindest als potentiell datenverarbeitende Stellen angesehen werden können, wirksam auf die Einhaltung datenschutzrechtlicher Vorschriften zu überwachen, kann die Verarbeitung und Weiterleitung personenbezogener Daten auch verdeckt erfolgen. Steganografische und kryptografische Verfahren könnten Kontrolle ins Leere laufen lassen.

Zugleich ist jedoch festzuhalten, daß die Globalität von Datennetzen weder den Staat noch übergeordnete Organisationen davon entbindet, einen wirksamen Schutz der Privatsphäre des Bürgers zu gewährleisten. Auch muß ein effektives Datenschutzrecht nicht zwangsläufig einen Standortnachteil für Wirtschaftsunternehmen darstellen, sondern kann dadurch, daß es die Akzeptanz der neuen Informations- und Kommunikationstechniken fördert, ebenso einen Wettbewerbsvorteil darstellen.[293]) Zudem schafft es möglicherweise – wie es in der Vergangenheit im Bereich der Umwelttechnik das Umweltrecht getan hat – wichtige Impulse für die Entwicklung exportfähiger Produkte der Datensicherheit und stellt gleichzeitig eine geeignete Basis für Verhandlungen auf internationaler Ebene dar.

5.4 Selbstregulierung

Sinnvoll können weiter Bemühungen der Informations- und Kommunikationswirtschaft um Selbstregulierung sein.[294]) In den USA haben bereits eine Reihe von Wirtschaftsverbänden Verhaltensrichtlinien aufgestellt, die ihre Mitglieder zu einem bestimmten Umgang mit personenbezogenen Daten verpflichten.[295]) Kritisiert wird an diesem Regelungsmodell einer freien Selbstregulation auf eigene Initiative, daß es weitgehend auf eine freiwillige Befolgung der Richtlinien angewiesen ist, dem Einzelnen keine Möglichkeit gibt, seine Rechte notfalls auch gerichtlich durchzusetzen und Verhaltenskodizes häufig erst nach Aufdeckung eklatanter Datenschutzmängel erlassen würden.[296]) Diese Nachteile kann möglicherweise eine sogenannte „gesetzlich konditionierte Selbstregulation" vermeiden, wie sie in den Niederlanden praktiziert wird. Darunter wird ein System verstanden, das eine datenschützende Grundnorm gesetzlich festlegt, deren Konkretisierung über eine Selbstbindung jedoch den Berufs- und Wirtschaftsverbänden überläßt.[297])

---

[291]) Vgl. OECD: Report of the Ad Hoc Meeting of Experts on Information Infrastructures. Issues related to Security of Information Systems and Protection of Personal Dat and Privacy, Paris 1996 (OECD/GD(96)74), abufbar unter http://www.oecd.org.

[292]) Vgl. Roßnagel, A.: Rechtliche Gestaltung der Informationstechnik – Aufgaben und Chancen auf dem Weg in eine zivile Informationsgesellschaft, in: Alcatel SEL Stiftung für Kommunikationsforschung im Stifterverband für die Deutsche Wissenschaft, Stiftungsreihe 22, Fachtagung Darmstadt 1996, S. 8–16.

[293]) Vgl. Hoeren, T.: Datenschutz als Wettbewerbsvorteil. Das ungarische Datenschutzgesetz unter der ökonomischen Lupe, in DuD 1996, S. 542–549; Bizer, J., Fox, D.: Verpaßte Chancen?, in DuD 1997, S. 442; zur ökonomischen Bedeutung des Urheberrechts siehe auch oben S. 2.

[294]) Zur Selbstregulierung im Bereich des Datenschutzes vgl. U.S. Department of Commerce, National Telecommunications and Information Administration: Privacy and Self Regulation in the Information Age, Washington D.C. Juni 1997

[295]) Vgl. Information Policy Committee der National Information Task Force: Options for Promoting Privacy on the National Information Infrastructure, http://www.iitf.ipc/privacy.html, unter Privacy in the Marketplace, 3.

[296]) Vgl. Information Policy Committee, ebd.

[297]) Vgl. Overkleeft-Verburg, M.: Datenschutz zwischen Regulierung und Selbstregulation. Erahrungen aus den Niederlanden, in: Alcatel SEL Stiftung für Kommunikationsforschung im Stifterverband für die Deutsche Wissenschaft: Rechtliche Gestaltung der Informationstechnik, Stiftungsreihe 22, Fachtagung Darmstadt 1996, S. 41–46 (41); Kuitenbrower, Frank: Self-Regulation: Some Dutch Experiences, in: U.S. Department of Commerce, National Telecommunications and Information Administration: Privacy and Self Regulation in the Information Age, Washington D.C. Juni 1997, S. 109–117.

6. Bereits erfolgte und bevorstehende Anpassungen im deutschen Datenschutzrecht

Das erst Anfang der siebziger Jahre entstandene deutsche Datenschutzrecht hat sich inzwischen zu einer äußerst komplexen Materie entwickelt. Abgesehen davon, daß auch das Datenschutzrecht der bundesstaatlichen Ordnung folgt, es also aus Bundesgesetzen und Landesgesetzen besteht, ist es geprägt von der Aufteilung in ein subsidiär geltendes allgemeines Datenschutzrecht und bereichsspezifisches Datenschutzrecht. Inhaltlich wird das deutsche Datenschutzrecht in weiten Teilen von der Unterscheidung zwischen der Datenverarbeitung öffentlicher und der Datenverarbeitung privater Stellen bestimmt: Die Grundrechtsbindung staatlicher Stellen sowie die Überlegung, daß die Verarbeitung personenbezogener Daten vor allem eine Domäne des Staates sei, führt dazu, daß an die Datenverarbeitung öffentlicher Stellen in der Regel wesentlich höhere Anforderungen gestellt werden als an die privater.

Das allgemeine Datenschutzrecht normiert neben Zulässigkeitstatbeständen, Regeln für die Datenverarbeitung und Rechten des von der Datenverarbeitung Betroffenen auch technisch-organisatorische Maßnahmen, die von datenverarbeitenden Stellen zu ergreifen sind.[298]) Soweit es um Privatunternehmen geht, sieht das Bundesdatenschutzgesetz Meldepflichten von Unternehmen vor, die Daten geschäftsmäßig zum Zweck der Übermittlung speichern oder als Dienstleistungsunternehmen verarbeiten oder nutzen.[299])

6.1 Bereits erfolgte Reformen

6.1.1 Das Gesetz über den Datenschutz bei Telediensten und der Mediendienstestaatsvertrag

Neben dem subsidiär anwendbaren allgemeinen Datenschutzrecht sind in Deutschland für den Datenschutz in Netzen einerseits die Regelungen im Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz) und im Mediendienstestaatsvertrag der Länder, andererseits die Regelungen im Telekommunikationsgesetz von großer Bedeutung. Das Teledienstedatenschutzgesetz und der Mediendienstestaatsvertrag sind am 1. August 1997 in Kraft getreten.[300]) Ziel der Regelungswerke ist es, Rahmenbedingungen zu schaffen, die es sowohl ermöglichen, den Gefahren der neuen Informations- und Kommunikationstechniken für das informationelle Selbstbestimmungsrecht zu begegnen, als auch helfen, deren Chancen wahrzunehmen und zugleich einen Ausgleich zwischen den berechtigten Interessen von Nutzern, Wirtschaft und Allgemeinheit schaffen.[301])

- **Allgemeine Grundsätze für die Erhebung und Verarbeitung personenbezogener Daten**

Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag stellen – neben detaillierten Bestimmungen über die Erhebung und Verarbeitung von Bestands-, Nutzungs- und Abrechnungsdaten[302]) – eine Reihe von allgemeinen Grundsätzen für Datenerhebung und – verarbeitung auf. Hervorzuheben ist, daß sie im Gegensatz zum allgemeinen Datenschutzrecht eine Gleichstellung von öffentlicher und privater Datenverarbeitung vorsehen: Im Gegensatz zum Bundesdatenschutzgesetz, das an die Datenerhebung und -verarbeitung nichtöffentlicher Stellen weniger hohe Anforderungen stellt als an die öffentlicher Stellen, unterwerfen Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag jeden Anbieter von Tele- bzw. Mediendiensten den gleichen datenschutzrechtlichen Anforderungen.[303]) Sie tragen damit dem Umstand Rechnung, daß in den neuen Informations- und Kommunikationsdiensten vor allem nichtöffentliche Stellen personenbezogene Daten erheben und verarbeiten.

Beide Gesetze gehen davon aus, daß das grundsätzliche Verbot der Erhebung und Verarbeitung personenbezogener Daten auch in Kommunikationsnetzen gilt. Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist daher nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Nutzer eingewilligt hat.[304])

Abweichend vom Bundesdatenschutzgesetz weiten Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag den Datenschutz gegenüber nichtöffentlichen Stellen auch auf Daten aus, die nicht in Dateien verarbeitet oder genutzt werden.[305]) Insofern wird der Datenschutz nicht mehr an das Vorliegen einer Sammlung personenbezogener Daten geknüpft, die nach gleichartigen Merkmalen aufgebaut ist oder aber durch automatisierte Verfahren nach bestimm-

[298]) Vgl. § 9 Bundesdatenschutzgesetz und Anlage zum Bundesdatenschutzgesetz.
[299]) Vgl. § 32 Bundesdatenschutzgesetz.
[300]) Vgl. zum Teledienstedatenschutzgesetz Engel-Flechsig, S.: „Teledienstedatenschutz". Die Konzeption des Datenschutzes im Entwurf des Informations- und Kommunikationsgesetzes des Bundes, in: DuD 1997, S. 8–16.
[301]) Vgl. Begründung zu Artikel 2 Informations- und Kommunikationsdienstegesetz (Bundestagsdrucksache 13/7934 vom 11. Juni 1997); Begründung zum Mediendienstestaatsvertrag.
[302]) Vgl. §§ 5, 6 Teledienstedatenschutzgesetz; §§ 14, 15 Mediendienstestaatsvertrag.
[303]) Vgl. § 2 Teledienstedatenschutzgesetz; § 3 Mediendienstestaatsvertrag.
[304]) Vgl. § 3 Abs. 1 Teledienstedatenschutzgesetz, § 12 Abs. 1 Mediendienstestaatsvertrag.
[305]) Vgl. für das Teledienstedatenschutzgesetz Engel-Flechsig, S.: „Teledienstedatenschutz". Die Konzeption des Datenschutzes im Entwurf des Informations- und Kommunikationsgesetzes des Bundes, in: DuD 1997, S. 8–16 (12).

ten Merkmalen ausgewertet werden kann.[306]) Dadurch wird den Gefahren begegnet, die sich aus den Möglichkeiten der raschen Verknüpfung personenbezogener Daten aus dezentralen Speichern ergeben.

Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag verbieten die Verwendung erhobener personenbezogener Daten für andere Zwecke als den Erhebungszweck. Zulässig sind Datenverarbeitungsschritte für andere Zwecke nur, soweit dies durch eine Rechtsvorschrift erlaubt wird oder der Nutzer eingewilligt hat.

• Einwilligung und Unterrichtung des Nutzers

Zugleich akzeptieren Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag die Einwilligung des Nutzers als mit einer gesetzlichen Ermächtigung gleichwertigen Anknüpfungspunkt für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten.[307]) Erstmals ist auch die Möglichkeit vorgesehen, elektronisch in die Datenerhebung und –verarbeitung einzuwilligen.[308]) Die elektronisch oder anderweitig gegebene Einwilligung kann jederzeit widerrufen werden; der Nutzer ist auf sein Widerrufsrecht hinzuweisen.[309])

Beide Regelungswerke stellen umfassende Pflichten datenerhebender und datenverarbeitender Medien- und Teledienste zur Unterrichtung der Nutzer auf.[310]) Abgesehen davon, daß die Unterrichtung Voraussetzung einer wirksamen Einwilligung ist, muß der Nutzer in allen Fällen über die Erhebung, Verarbeitung und Nutzung seiner Daten unterrichtet werden. Dies betrifft Art, Umfang, Ort und Zweck von Erhebung und Verarbeitung. Einwilligungspflichtig ist damit auch das Setzen der sogenannten „cookies". Ein Verzicht auf die Unterrichtung ist möglich.

Neben die Pflicht des Diensteanbieters zur vorherigen Unterrichtung des Nutzers tritt das Recht des Nutzers, die beim Diensteanbieter zu seiner Person oder zu seinem Pseudonym gespeicherten Daten jederzeit unentgeltlich einzusehen, wobei dies auf Verlangen des Nutzers auch elektronisch zu ermöglichen ist.[311])

Um zu verhindern, daß der Nutzer faktisch gezwungen wird, seine Einwilligung zu erteilen, stellen Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag ein Koppelungsverbot auf: Der Diensteanbieter darf den Zugang von seinen Diensten nicht von der Einwilligung des Nutzers abhängig machen, wenn der Nutzer keine andere zumutbare Möglichkeit hat, den Dienst in Anspruch zu nehmen.[312])

• Systemdatenschutz

Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag enthalten weiter eine Reihe von Bestimmungen, die sich unter dem Begriff des Systemdatenschutzes zusammenfassen lassen. Die Anbieter von Tele- und Mediendienste sind verpflichtet, Auswahl und Gestaltung ihrer technischen Einrichtungen an dem Ziel auszurichten, möglichst keine oder wenige Daten zu erheben, zu verarbeiten und zu nutzen[313]) und eine anonyme und pseudonyme Inanspruchnahme ermöglichen, soweit dies technisch möglich und zumutbar ist.[314]) Darüber hinaus muß technisch und organisatorisch sichergestellt sein, daß die Daten über den Ablauf der Nutzung eines Dienstes unmittelbar nach deren Beendigung gelöscht werden, sofern Abrechnungszwecke nicht eine längere Speicherung erfordern, daß Dienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können und daß die personenbezogenen Daten über die Nutzung unterschiedlicher Teledienste grundsätzlich getrennt verarbeitet und nicht zusammengeführt werden.[315]) Nutzungsprofile sind nur bei pseudonymer Nutzung zulässig; sie dürfen nicht mit den Daten über den Inhaber des Pseudonyms zusammengeführt werden.[316]) Damit wird einerseits dem wirtschaftlichen Interesse Rechnung getragen, Nutzer unter ihrem Pseudonym zielgenau mit Werbeangeboten und ähnlichem zu versorgen, andererseits aber auch das legitime Bedürfnis des Nutzers berücksichtigt, daß ihm die Profile nicht persönlich zugeordnet werden können.

Der Mediendienstestaatsvertrag sieht ein sogenanntes „Datenschutz-Audit" vor[317]). Danach können Anbieter von Mediendiensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Die näheren Anforderungen an das Datenschutzaudit sollen durch ein besonderes Gesetz geregelt werden. In das Teledienstedatenschutzgesetz ist eine entsprechende – in ersten Entwürfen noch vorgesehene – Bestimmung – letztlich nicht aufgenommen worden.[318])

306) Vgl. § 3 Abs. 2 Bundesdatenschutzgesetz.
307) Vgl. § 3 Abs. 1, 2 Teledienstedatenschutzgesetz, § 12 Abs. 2, 3 Mediendienstestaatsvertrag.
308) Vgl. dazu und zu den Anforderungen an die elektronische Einwilligung und ihre Dokumentation § 3 Abs. 7 Teledienstedatenschutzgesetz, § 12 Abs. 8 Mediendienstestaatsvertrag.
309) Vgl. § 3 Abs. 6 Teledienstedatenschutzgesetz, § 12 Abs. 7 Mediendienstestaatsvertrag.
310) Vgl. § 3 Abs. 5 Teledienstedatenschutzgesetz, § 12 Abs. 6 Mediendienstestaatsvertrag.
311) Vgl. § 7 Teledienstedatenschutzgesetz, § 16 Abs. 1 Mediendienstestaatsvertrag.
312) Vgl. § 3 Abs. 3 Teledienstedatenschutzgesetz, § 12 Abs. 4 Mediendienstestaatsvertrag.
313) Vgl. § 3 Abs. 4 Teledienstedatenschutzgesetz; § 12 Abs. 4 Mediendienstestaatsvertrag.
314) Vgl. § 4 Abs. 1 Teledienstedatenschutzgesetz, § 13 Abs. 1 Mediendienstestaatsvertrag.
315) Vgl. § 4 Abs. 2 Teledienstedatenschutzgesetz, § 13 Abs. 2 Mediendienstestaatsvertrag.
316) Vgl. § 4 Abs. 4 Teledienstedatenschutzgesetz; § 13 Abs. 4 Mediendienstestaatsvertrag.
317) Vgl. § 17 Mediendienstestaatsvertrag.
318) Vgl. Engel-Flechsig, S.: „Teledienstedatenschutz". Die Konzeption des Datenschutzes im Entwurf des Informations- und Kommunikationsgesetzes des Bundes, in: DuD 1997, S. 8–16 (15).

- **Erweiterte Kontrollmöglichkeiten der Datenschutzbeauftragten**

Den Gefahren der Datenverarbeitung in Netzen begegnet das Teledienstedatenschutzgesetz schließlich damit, daß es den Aufsichtsbehörden erweiterte Kontrollbefugnisse gibt.[319]) Die Datenschutzbeauftragten dürfen die Anbieter von Telediensten und Mediendiensten auch dann überprüfen, wenn keine Anhaltspunkte für eine Verletzung von Datenschutzvorschriften bestehen. Das im allgemeinen Datenschutzrecht noch aufgestellte Erfordernis solcher Anhaltspunkte nach § 38 Bundesdatenschutzgesetz wird im Zusammenhang mit der Umsetzung der EU-Datenschutzrichtlinie entfallen.

- **Kontrollbefugnisse der Sicherheitsbehörden**

Im Interesse der öffentlichen Sicherheit ordnet das Teledienstedatenschutzgesetz an, daß die Befugnisse der Strafverfolgungsbehörden von dem Verbot der Übermittlung von Nutzungs- und Abrechnungsdaten unberührt bleiben.[320])

6.1.2 Das Telekommunikationsgesetz

Für den Datenschutz in Netzen sind neben den genannten Gesetzen Bestimmungen im Telekommunikationsrecht von erheblicher Relevanz*). Zentrale Bedeutung haben insofern §§ 85 – 93 Telekommunikationsgesetz. Diese enthalten im wesentlichen folgende Bestimmungen:

- **Allgemeine Grundsätze**

Das Telekommunikationsgesetz bestimmt, daß der Inhalt und die näheren Umstände der Telekommunikation – dazu zählt insbesondere, wer an der Telekommunikation beteiligt war oder ist – dem Fernmeldegeheimnis unterliegen.[321]) Dieser Bestimmung bedarf es, da das Fernmeldegeheimnis des Art. 10 Grundgesetz aufgrund des Charakters der Grundrechte als gegen den Staat gerichtete Abwehrrechte gegenüber privaten Anbietern von Telekommunikationsdienstleistungen zumindest nicht unmittelbar geltend gemacht werden kann. Eine Weitergabe von Inhalts- und Verbindungsdaten ist damit unzulässig, soweit nicht eine gesetzliche Vorschrift ausnahmsweise dazu berechtigt. Gleiches gilt für das Abhören von Telekommunikation; unbeabsichtigt empfangene Nachrichten dürfen anderen nicht mitgeteilt werden.[322]) Damit ist das sogenannte „Scannen" der Frequenzen schnurloser Telefone untersagt.

Im übrigen soll die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bei Telekommunikationsunternehmen nach dem Telekommunikationsgesetz durch eine Rechtsverordnung geregelt werden.[323]) Die Rechtsverordnung wird nach § 89 Telekommunikationsgesetz dem Grundsatz der Verhältnismäßigkeit, insbesondere der Beschränkung der Erhebung, Verarbeitung und Nutzung von Daten auf das Erforderliche, sowie dem Grundsatz der Zweckbindung genügen müssen. Dabei sind Höchstfristen für die Speicherung festzulegen und die berechtigten Interessen der Telekommunikationsunternehmen und ihrer Kunden zu berücksichtigen. Vorgesehen sind zudem ein grundsätzliches Verbot der Aufzeichnung von Inhaltsdaten[324]) sowie Einwilligungs bzw. Widerspruchsrechte der Nutzer.[325])

- **Systemdatenschutz**

Das Telekommunikationsgesetz verpflichtet dazu, technische und sonstige Maßnahmen unter anderem zum Schutz des Fernmeldegeheimnisses und der programmgesteuerten Telekommunikations- und Datenverarbeitungssysteme gegenüber unerlaubten Zugriffen zu ergreifen.[326]) Um eine nach dem Stand der Technik und internationalen Maßstäben angemessene Standardsicherheit zu erreichen, soll der Regulierungsrat zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik nach Anhörung von Verbraucher- und Wirtschaftsverbänden einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen erstellen, zu dem auch der Bundesbeauftragte für den Datenschutz Stellung nehmen kann.[327]) Überdies haben lizenzpflichtige Betreiber von Telekommunikationsanlagen einen Sicherheitsbeauftragten zu benennen sowie ein Sicherheitskonzept aufzustellen und umzusetzen.[328])

Das Bundesministerium für Post und Telekommunikation wird im Telekommunikationsgesetz ermächtigt, diese Pflichten in einer Rechtsverordnung zu konkretisieren.[329]) Nach dem derzeitigen Stand der Diskussion wird von der Ermächtigung jedoch kein Gebrauch gemacht, solange der von der Regulierungsbehörde gemeinsam mit der Fachöffentlichkeit erstellte Katalog von Sicherheitsanforderungen berücksichtigt und der Schutz des Fernmeldegeheimnisses auf diese Weise gewährleistet wird.[330])

- **Kontrollbefugnisse des Bundesbeauftragten für den Datenschutz**

Dem Bundesbeauftragten für den Datenschutz stehen nach dem Telekommunikationsgesetz gegenüber dem allgemeinen Datenschutzrecht erweiterte Kontrollbefugnisse zu. § 91 Abs. 4 Telekommunikationsgesetz erklärt die Vorschriften des Bundesdatenschutzgesetzes für anwendbar, die für die Kontrolle öffentlicher Stellen gelten.

---

319) Vgl. § 8 Abs. 1 Teledienstedatenschutzgesetz.
320) Vgl. § 6 Abs. 3 S. 2 Teledienstedatenschutzgesetz.
*) Vgl. dazu die Beiträge in: Büllesbach, A. (Hrsg.): Datenschutz in der Telekommunikation, Deregulierung und Datensicherheit in Europa, Köln 1997.
321) Vgl. § 85 TKG.
322) Vgl. § 86 TKG.
323) Vgl. § 89 TKG.
324) Vgl. § 89 Abs. 4 TKG.
325) Vgl. § 89 Abs. 7 TKG.
326) Vgl. § 87 Abs. 1 TKG.
327) Vgl. § 87 Abs. 1 S. 3, 4 TKG.
328) Vgl. § 87 Abs. 2 TKG.
329) Vgl. § 87 Abs. 3 TKG.
330) Vgl. Helf, K.-H.: Sicherheit in der Telekommunikation als Regulierungsaufgabe, in: Computer und Recht 1997, S. 331–335 (332).

- **Rechte der Sicherheitsbehörden**

Die technische Umsetzung der Wahrnehmung von gesetzlich vorgesehenen Überwachungsbefugnissen der Sicherheitsbehörden werden durch §§ 88, 90 TKG geregelt. Danach ist der Betreiber einer Telekommunikationsanlage verpflichtet, den gesetzlich zur Überwachung berechtigten Stellen einen Netzzugang für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen unverzüglich und vorrangig bereitzustellen.[331]) Er muß entsprechende technische Einrichtungen vor Aufnahme des Betriebs der Telekommunikationsanlage gestalten und vorhalten.[332]) Er ist weiter verpflichtet, Kundendateien zu führen und so verfügbar zu halten, daß die Regulierungsbehörde einzelne Daten oder Datensätze in einem automatisierten Verfahren abrufen kann, um sie an die darum ersuchende Sicherheitsbehörde weiterzuleiten.[333])

6.1.3 Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen

Noch auf der Grundlage des zum 31. 12. 1997 außer Kraft getretenen Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTReG) ist die sogenannte Telekommunikationsdienstleistungsunternehmen-Datenschutzverordnung (TDSV) vom 12. Juli 1996 erlassen worden.[334]) Sie regelt die Zulässigkeit der Datenerhebung und –verarbeitung durch Fernmeldeanlagenbetreiber und Anbieter von Telekommunikationsdienstleistungen. Ein Vertragsverhältnis betreffende Bestandsdaten dürfen danach im Rahmen des Erforderlichen erhoben, verarbeitet und genutzt werden.[335]) Im gleichen Umfang ist die Erhebung und Verarbeitung von Verbindungsdaten zulässig.[336]) An Dritte dürfen personenbezogene Daten nur unter bestimmten Voraussetzungen übermittelt werden.[337])

Die TDSV stimmt in ihren Begriffsdefinitionen nicht mit dem TKG überein[338]); sie wird durch die nach § 89 TKG zu erlassende Rechtsverordnung ersetzt werden.

6.1.4 Weitere für den Datenschutz in Netzen relevante Normen

Neben Bundesdatenschutzgesetz, Teledienstedatenschutzgesetz, Mediendienstestaatsvertrag und Telekommunikationsgesetz existiert noch eine Reihe weiterer für den Datenschutz in Netzen relevanter Normen, auf die im Rahmen dieses Zwischenberichts nur kurz eingegangen werden kann. Zu nennen ist zunächst das Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik vom 17. Dezember 1990.[339]) Diesem Gesetz zufolge hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter anderem die Aufgabe, die Vertraulichkeit von Informationen in informationstechnischen Systemen oder Komponenten zu fördern.[340]) Dies soll durch eine umfassende Evaluierung der Sicherheit von Produkten der Informationstechnik und eine Beratung von Herstellern, Betreibern und Anwendern geschehen.[341]) Hersteller und Vertreiber von informationstechnischen Systemen können diese Dienstleistungen in Anspruch nehmen und beim BSI ein Zertifikat beantragen, welches bescheinigt, daß das geprüfte Produkt den BSI festgelegten oder allgemein anerkannten Sicherheitskriterien entspricht.[342]) Das Verfahren der Zertifizierung wird in der BSI-Zertifizierungsverordnung vom 7. Juli 1992[343]) geregelt, die auf vom Bundesminister des Innern festgelegte und im Bundesanzeiger veröffentlichte Kriterien verweist. Diese Kriterien sind inhaltsgleich mit den auf europäischer Ebene aufgestellten Information Technology Security Evaluation Criteria (ITSEC), die durch die sogenannten Common Criteria (CC) abgelöst werden, auf die man sich mit den Vereinigten Staaten von Amerika und mit Kanada geeinigt hat. Die nach dem BSI-Errichtungsgesetz vorgesehene Möglichkeit einer freiwilligen Sicherheitszertifizierung ist in der Vergangenheit aus unterschiedlichen Gründen nur von wenigen Herstellern wahrgenommen – als Gründe dafür werden zu lange Zertifizierungszeiten und zu hohe Zertifizierungskosten genannt.[344])

Von Bedeutung für den Datenschutz ist ferner die Telekommunikationszulassungsverordnung,[345]) die bestimmte technische Anforderungen insbesondere für Telekommunikationsendeinrichtungen – zu denen etwa auch für den Datenverkehr von Computern erforderliche Modems und ISDN-Karten zählen – aufstellt.

6.2 Bevorstehende Anpassungen aufgrund europäischer Rechtssetzung

Ziel der Politik der Organe der Europäischen Union auf dem Gebiet der Telekommunikation war und ist es, ein wettbewerbsorientiertes Umfeld im Gemeinschaftsgebiet herzustellen und zu diesem Zweck einen offenen Zugang zu den bestehenden Telekom-

331) Vgl. § 88 Abs. 4 TKG.
332) Vgl. § 88 Abs. 2 S. 3 Nr. 1 TKG.
333) Vgl. § 90 Abs. 2, 4 TKG.
334) Das Außerkrafttreten des PTReG berührt die Wirksamkeit der Verordnung nicht, vgl. BVerfGE 9, 12 (44); 78, 179 (198).
335) Vgl. § 4 TDSV.
336) Vgl. § 5 TDSV.
337) Vgl. §§ 4 Abs. 1, 6 TDSV.
338) Vgl. Wuermeling, U.; Felixberger, S.: Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, in CR 1997, S. 230–238 (235).
339) BGBl. I 1990, S. 2834–2836.
340) Nach § 2 Abs. 2 BSI-Errichtungsgesetz bedeutet Sicherheit in der Informationstechnik im Sinne des Gesetzes „die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder *Vertraulichkeit* von Informationen betreffen ..."
341) Vgl. § 3 BSI-Errichtungsgesetz.
342) Vgl. § 4 BSI-Errichtungsgesetz.
343) BGBl. I 1992, S. 1230f.
344) Vgl. Abel, H.: Gedanken zur Sicherheitszertifizierung, in: Bundesamt für Datensicherheit: Mit Sicherheit in die Informationsgesellschaft, Tagungsband 5. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim 1997, S. 317–318.
345) Verordnung über die Konformitätsbewertung, Kennzeichnung, Zulassung und das Inverkehrbringen von Telekommunikationsendeinrichtungen, BGBl. I 1995, S. 1671.

munikationsnetzen zu schaffen und zu sichern.[346]) Der Datenschutz wird in den in diesem Zusammenhang erlassenen Richtlinien lediglich am Rande und in eher allgemein gehaltenen Verweisen auf nicht näher bestimmte Regelungen zum Schutz der Privatsphäre erwähnt.[347]) Die aktuelle Situation des Datenschutzes in Netzen auf europäischer Ebene wird daher in erster Linie von der EG-Datenschutzrichtlinie[348]) und der sogenannten ISDN-Richtlinie[349]) geprägt.

6.2.1 Die Datenschutzrichtlinie

Die am 24. Oktober 1995 verabschiedete Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr hat die Aufgabe, möglichst einheitliche Maßstäbe für die Erhebung und Verarbeitung von Daten in der Europäischen Union festzulegen. Damit soll zugleich der Datenschutz innerhalb der Union gewährleistet und der Datenfluß innerhalb der Gemeinschaft erleichtert werden.[350]) Die Richtlinie ist von den Mitgliedsstaaten bis zum 24. Oktober 1998 umzusetzen.[351]) Die Bundesregierung hat jetzt einen ersten Entwurf für die daher notwendige Novellierung des Bundesdatenschutzgesetzes vorgelegt.

Ebenso wie Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag verzichtet auch die EG-Datenschutzrichtlinie – von einigen Detailbestimmungen abgesehen – auf eine Unterscheidung zwischen öffentlicher und nichtöffentlicher Datenverarbeitung.[352]) Sie ordnet die Zweckbindung der Datenverarbeitung an[353]), verpflichtet datenverarbeitende Stellen zur Aufklärung und Information der Betroffenen[354]) und gibt letzteren ein Recht auf die Kontrolle der Verarbeitung ihrer personenbezogenen Daten.[355])

Der EG-Datenschutzrichtlinie zufolge ist Selbstregulierung zu fördern: Die Mitgliedsstaaten haben vorzusehen, daß Berufsverbände und anderen Vereinigungen Verhaltensregeln ausarbeiten.[356]) Kontrolliert werden sollen die Verhaltensregeln durch die zuständigen Aufsichtsbehörden in den Mitgliedsstaaten oder die auf EU-Ebene zuständige Instanz, die sogenannte Datenschutzgruppe.

Im Gegensatz zum deutschen Datenschutzrecht sieht die EG-Richtlinie bestimmte Daten als besonders sensibel an; sie verpflichtet die Mitgliedsstaaten daher dazu, die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit sowie von Gesundheitsdaten und Daten über das Sexualleben zu untersagen.[357]) Zugleich läßt sie jedoch eng definierte Ausnahmen zu.[358])

Für den Datenverkehr in Telekommunikationsnetzen von erheblicher Bedeutung sind die in Art. 25ff der Richtlinie aufgestellten Regelungen des Datenexports in Drittländer. Diesen zufolge ist die Datenübermittlung in ein Drittland untersagt, wenn dieses kein angemessenes Datenschutzniveau aufweist.[359]) Wann dies der Fall ist, soll in einem besonderen Verfahren geklärt werden können, um sicherzustellen, daß die Mitgliedsstaaten von einer gemeinsamen Beurteilung ausgehen.[360]) Eine wichtige Einschränkung des grundsätzlichen Verbots des Exports von Daten in Drittländer mit unangemessenem Schutzniveau enthält Art. 26 Abs. 2 der Richtlinie. Danach können die Mitgliedsstaaten der EU einen Datenexport in solche Länder dann genehmigen, wenn der für die Datenverarbeitung Verantwortliche ausreichende Garantien für den Schutz der Privatsphäre, der Grundrechte und der Grundfreiheiten der betroffenen Personen bietet. Solche Garantien sollen sich insbesondere durch entsprechende Klauseln in einem Vertrag mit dem für die Datenverarbeitung in dem Drittstaat Verantwortlichen ergeben können. In Drittländer exportiert werden dürfen personenbezogene Daten darüber hinaus unter anderem dann, wenn die betroffene Person ihre Einwilligung gegeben hat oder die Datenübermittlung aufgrund eines Vertrages zwischen der betroffenen Person und der datenverarbeitenden Stelle erfolgt.[361])

Daneben stellt die EG-Datenschutzrichtlinie Anforderungen auch an den technischen Datenschutz. Die Mitgliedsstaaten haben Vorschriften zu erlassen, die dazu verpflichten, angemessene technische und organisatorische Maßnahmen zum Schutz gegen den unberechtigten Zugang zu personenbezogenen Daten sowie gegen deren unberechtigte Änderung und Weitergabe zu ergreifen.[362])

Kontrolliert werden sollen die aufgrund der Richtlinie erlassenen Bestimmungen in erster Linie durch von den Mitgliedsstaaten beauftragte öffentliche Stellen,

346) Vgl. zum Stand der EU-Politik und Rechtssetzung auf dem Gebiet der Telekommunikation: European Commission, Directorate Generale XIII: Status Report on Telecommunications Policy, Brüssel 7. Mai 1997, abrufbar unter http://www.ispo.cec.be/infosoc/legreg/tcstatus.html; Dix, A.: Der Entwurf der ISDN-Datenschutzrichtlinie. Ein erstes Beispiel für ein bereichsspezifisches europäisches Datenschutzrecht, in DuD 1997, S. 278–283 (278).

347) Vgl. Dix, A., ebd., S. 278.

348) Richtlinie des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (95/46/EG), Abl. EG Nr. L 281 vom 23. 11. 1995, S. 31.

349) Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation; dazu: Dix, A.: Der Entwurf der ISDN-Datenschutzrichtlinie. Ein erstes Beispiel für ein bereichsspezifisches europäisches Datenschutzrecht, in DuD 1997, S. 278–283.

350) Vgl. Erwägungsgründe 7, 8.

351) Vgl. Schild, H.-H.: Die EG-Datenschutzrichtlinie, in EuZW 1996, S. 549–554 (554); ders: Zur Novellierung des BDSG, in: DuD 1997, S. 720–723 (720).

352) Vgl. dazu Schild, H.-H.: Die EG-Datenschutzrichtlinie, in EuZW 1996, S. 549–554 (550).

353) Vgl. Art. 6 Abs. 1 lit. b–e, Abs. 2 EG-Datenschutzrichtlinie.

354) Vgl. Art. 10, 11 EG-Datenschutzrichtlinie.

355) Vgl. Art. 12 EG-Datenschutzrichtlinie.

356) Vgl. Art. 27 EG-Datenschutzrichtlinie.

357) Vgl. Art. 8 Abs. 1 EG-Datenschutzrichtlinie.

358) Vgl. Art. 8 Abs. 2–5 EG-Datenschutzrichtlinie.

359) Vgl. Art. 25 Abs. 1 EG-Datenschutzrichtlinie.

360) Vgl. Art. 25 Abs. 2–6 EG-Datenschutzrichtlinie.

361) Vgl. Art. 26 Abs. 1 lit a, b EG-Datenschutzrichtlinie.

362) Vgl. Art. 17 Abs. 1 EG-Datenschutzrichtlinie.

die ihre Aufgabe in völliger Unabhängigkeit wahrnehmen können sollen.[363]) Die Richtlinie sieht umfassende Untersuchungs- und Einwirkungsbefugnisse dieser Stellen vor.[364])

6.2.2 Die ISDN-Datenschutzrichtlinie

Die häufig als ISDN-Datenschutzrichtlinie bezeichnete Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997[365]) ist nicht auf den Schutz der Privatsphäre in digitalen Telekommunikationsnetzen beschränkt, sondern stellt vielmehr bereichsspezifisches europäisches Datenschutzrecht für das Gebiet der Telekommunikation insgesamt dar.[366]) Sie enthält unter anderem Detailregelungen über die Verarbeitung der Verbindungsdaten, die Rufnummernanzeige auf dem Display des Angerufenen und die Anrufweiterschaltung. Der Vertraulichkeit der Kommunikation wird ein hoher Stellenwert eingeräumt.[367]) Unter anderem zum Schutz der Vertraulichkeit sind angemessene technische Vorkehrungen zu schaffen.[368]) In ursprünglichen Kommissionsvorschlägen enthaltene Verpflichtungen von Telekommunikationsanbietern, die Teilnehmer bei besonderen Gefahren z. B. im Bereich des Mobilfunks eine Verschlüsselung von Endgerät zu Endgerät anzubieten, sind in der vorliegenden Fassung jedoch gestrichen.[369]) Geblieben ist die Verpflichtung von öffentlich zugänglichen Kommunikationsdiensten, die Teilnehmer über technische Möglichkeiten des Datenschutzes und deren Kosten zu informieren.

6.2.3 Weitere für den Datenschutz in Netzen relevante Aktivitäten der EU

Die Europäische Union hat außerdem eine Vielzahl von Aktivitäten auf dem Gebiet der Informationssicherheit entfaltet. Der Rat der Europäischen Gemeinschaften hat mit seiner Entscheidung auf dem Gebiet der Sicherheit von Informationssystemen vom 31. März 1992 ein Komitee hoher Beamter ins Leben gerufen und unter anderem damit beauftragt, Rahmenbedingungen für die Sicherheit von Informationssystemen zu bestimmen. Am 7. April 1995 hat der Rat eine Empfehlung über gemeinsame Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik[370]) abgegeben, die unter anderem mit Erwägungen des Datenschutzes begründet wurde.[371]) Im Rahmen dieser und anderer politischen Vorgaben sind zahlreiche Projekte mit dem Ziel unternommen worden, die Sicherheit von Informationssystemen zu vergrößern, etwa die Open-Information-Interchange-Initiative[372]) und das Infosec-Projekt.[373]) Von Bedeutung für den technischen Datenschutz sind darüber hinaus die Aktivitäten europäischer Normungsinstitutionen wie des European Telecommunications Standards Institute (ETSI),[374]) das sich in Zusammenarbeit mit anderen europäischen sowie nationalen und internationalen Gremien um die Standardisierung auch von Datenschutzfunktionen bemüht.[375])

6.3 Bewertung und Empfehlungen der Enquete-Kommission

Die neuen Informations- und Kommunikationstechniken zwingen zu einer Neuorientierung des Datenschutzrechts. Denn das Datenschutzrecht ist noch nicht hinreichend an die durch den massenhaften Einsatz von Computern und ihre Vernetzung bedingten Veränderungen angepaßt. Während vor wenigen Jahren nur wenige Großrechenzentren automatisierte Datenverarbeitung in großem Umfang erlaubten, kann heute jeder PC-Besitzer zu einer datenverarbeitende Stellen mit einem großen Bestand an personenbezogenen Daten werden. Dies und der durch die Telekommunikation ermöglichte weltweite Zusammenschluß von Computern haben zur Folge, daß die Einhaltung datenschutzrechtlicher Erlaubnistatbestände und Verhaltensregeln immer weniger kontrolliert und durchgesetzt werden kann. Was den Datenschutz in Deutschland angeht, führt diese Entwicklung zu folgenden Feststellungen:

- Wie schon der von der Bundesregierung eingesetzte Rat für Forschung, Technologie und Innovation festgestellt hat, ist es notwendig, das traditionell normativ ausgerichtete Datenschutzrecht um Bestimmungen zu ergänzen, die einen Grundstandard an organisatorischen und technischen Sicherheitsmaßnahmen gewährleisten.[376]) Erforderlich ist, das Datenschutzrecht mehr und mehr darauf auszurichten, den Selbstschutz der Nutzer und den Systemdatenschutz zu unterstützen, indem es etwa datensparende und datenvermeidende Technik privilegiert. Dies kann zugleich dazu beitragen, auf die Verrechtlichung vieler Datenverarbeitungsvorgänge zu verzichten und das Datenschutzrecht erheblich zu vereinfachen.
- Ein wichtiger Schritt in diese Richtung ist nach Auffassung der Kommission bereits mit dem Teledienstedatenschutzgesetz und den entsprechenden Bestimmungen im Mediendienstestaatsvertrag gemacht worden. Diese Regelungswerke enthalten mit der Aufgabe der Unterscheidung zwischen öffentlicher und privater Datenverarbeitung, den Geboten der Datenvermeidung und der

363) Vgl. Art. 28 Abs. 1 EG-Datenschutzrichtlinie.
364) Vgl. Art. 28 Abs. 3 EG-Datenschutzrichtlinie.
365) Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation.
366) Vgl. Dix, A.: Der Entwurf der ISDN-Datenschutzrichtlinie, in DuD 1997, S. 278–283 (279).
367) Vgl. Artikel 5 ISDN-Datenschutzrichtlinie; Dix, ebd., S. 280.
368) Vgl. Artikel 4 ISDN-Datenschutzrichtlinie.
369) Vgl. Dix, ebd., S. 280.
370) abrufbar unter http://www. cordis.lu/infosec/src/conrec-de.html.
371) Vgl. Erwägungsgrund 6 der Empfehlung.
372) abrufbar unter http://www2.echo.lu/oii. html.
373) Vgl. http://www.cordis.lu/infosec.html.
374) Vgl. http://www.etsi.fr.
375) Vgl. etwa General Consumer Principles des Information & Communication Standards Board, abrufbar unter http://www. etsi.fr/consumer.html.
376) Vgl. Der Rat für Forschung, Technologie und Innovation: Informationsgesellschaft. Chancen, Innovationen und Herausforderungen, Bonn, Dezember 1995; S. 31f.

Datensparsamkeit sowie der Ausweitung des Datenschutzes auf nicht in Dateien gesammelte Daten richtige Ansätze für den Schutz des informationellen Selbstbestimmungsrechts in Telekommunikationsnetzen.[377]) Die Enquete-Kommission verkennt jedoch nicht, daß Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag vergleichsweise restriktive Regelungen enthalten. Das birgt einerseits die Gefahr von Wettbewerbsnachteilen für in Deutschland tätige Unternehmen und führt daher möglicherweise zur Auslagerung von Datenverarbeitung in Staaten mit einem weniger hohen Datenschutzniveau. Damit wäre weder dem Datenschutz noch dem Interesse an wirtschaftlichem Wachstum in der Branche der Informations- und Kommunikationstechnik gedient. Andererseits stellt sich die Frage, ob und inwieweit in Deutschland betriebene Server den Anforderungen des Teledienstedatenschutzgesetzes und des Mediendienstestaatsvertrages genügen und wie gegebenenfalls Verbesserungen erzielt werden können. Die Enquete-Kommission fordert den Gesetzgeber daher auf, die Entwicklung aufmerksam zu beobachten und gegebenenfalls korrigierend einzugreifen.

- Unabhängig davon bedarf es auf nationaler Ebene einer Angleichung der datenschutzrechtlichen Vorschriften im Recht der Medien- und Teledienste einerseits und dem Telekommunikationsrecht andererseits. Die derzeitige Rechtslage birgt erhebliche Unsicherheiten, die nicht zuletzt auch auf der noch unklaren Abgrenzung zwischen den Teledienste und Mediendienste betreffenden Vorschriften und dem Telekommunikationsgesetz beruhen.[378]) Wird in dieser Hinsicht keine Klarheit herbeigeführt, besteht die Gefahr, daß Anbieter wie Nutzer von Tele- und Mediendiensten durch die Existenz zweier unterschiedlicher Regelungswerke überfordert werden.

- Was die EU-Datenschutzrichtlinie angeht, so begrüßt die Enquete-Kommission, daß der Harmonisierungsprozeß innerhalb der Europäischen Union nunmehr auch das Datenschutzrecht erfaßt. Zu bedauern ist, daß die Datenschutzrichtlinie eine Reihe von Generalklauseln enthält, die den Mitgliedsstaaten relativ großen Raum für divergierende Regelungen lassen.[379]) Dies birgt in einem den freien Datenfluß ermöglichenden Gemeinschaftsgebiet die Gefahr von Wettbewerbsverzerrungen und das Risiko, daß die rechtlichen Garantien des einen Mitgliedsstaats aufgrund eines geringeren Schutzniveaus in einem anderen Mitgliedsstaat anderen unterlaufen werden.[380]) Gleiches gilt für die ISDN-Datenschutzrichtlinie, die zwar vergleichsweise detaillierte Regelungen etwa über die Rufnummernanzeige und deren Unterdrükkung enthält, es andererseits aber den Mitgliedsstaaten überläßt, zu bestimmen, ob und inwieweit die Richtlinie auch auf nichtöffentliche Telekommunikationsdienste (sogenannte Corporate Networks) anzuwenden ist.[381]) Zweifelhaft ist ferner, ob und inwieweit die Regelungen für den Export von Daten in Drittstaaten sich in der Praxis bewähren werden. Eine wirksame Kontrolle der Beachtung datenschutzrechtlicher Bestimmungen, die etwa in Verträgen mit Unternehmen in Drittstaaten enthalten sein können, wird in vielen Fällen ebensowenig möglich sein[382]) wie die Überwachung von Datenexporten überhaupt.[383]) Die weitere Entwicklung sollte daher auch in dieser Hinsicht aufmerksam beobachtet werden.

- Die Enquete-Kommission empfiehlt, die Umsetzung der EU-Datenschutzrichtlinie zu einer erheblichen Verschlankung und Vereinfachung des allgemeinen Datenschutzrechts, jedoch auch der Regelungen des bereichsspezifischen Datenschutzrechts zu nutzen.[384]) Die Akzeptanz des Datenschutzrechts wird bei Nutzern wie bei den datenverarbeitenden Stellen davon abhängen, inwieweit es gelingt, einfache und klare Regelungen zu finden, die sich ohne größeren Aufwand umsetzen lassen. Die Enquete-Kommission empfiehlt dem Gesetzgeber, den folgenden Punkten besondere Beachtung zu schenken:

  1. **Vereinfachung des Datenschutzrechts:** Im Datenschutzrecht verstellen außerordentlich komplizierte Regelungen den Blick auf das eigentliche Grundanliegen des Datenschutzes, den Menschen und sein informationelles Selbstbestimmungsrecht zu schützen.[385]) Werden diese Regelungen in Zukunft auch auf private Datenverarbeitung, also auch auf kleine und mittelständische Unternehmen Anwendung finden, müssen sie schon aus diesem Grund erheblich vereinfacht und klarer formuliert werden, um den Regulierungsaufwand in Grenzen zu halten. Ein Beispiel: In der derzeit geltenden Fassung des Bundesdatenschutzgesetzes wird zwischen der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten unterschieden. Diese Differenzierung bereitet in der

[377]) Vgl. Garstka, H.: Rede zur Einbringung des Tätigkeitsberichts 1996 im Abgeordnetenhaus, 11. September 1997, abrufbar unter http://www.datenschutz-berlin. de/ueber/aktuelle/red96.html.

[378]) Vgl. Moritz, W.; Winkler, M.: Datenschutz und Online-Dienste, in: NJW-CoR 1997, S. 43–48; Moritz, W.: Telekommunikations- und Medienrecht im Wandel, FIFF-Kommunikation 2/97, S. 27 ff.

[379]) Vgl. Lütkemeier, S.: EG-Datenschutzrichtlinie – Umsetzung in nationales Recht, DuD 1995, S. 597–603 (602); Simitis, S.: Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz, NJW 1997, S. 281–288 (286).

[380]) Vgl. Schild, H.-H.: Zur Novellierung des BDSG. Ein Problemanriß offener Fragen, in: DuD 1997, S. 720–723 (721).

[381]) Vgl. Dix, A.: Der Entwurf der ISDN-Datenschutzrichtlinie, DuD 1997, S. 278–283 (279).

[382]) Vgl. Lütkemeier, S.: EG-Datenschutzrichtlinie – Umsetzung in nationales Recht, DuD 1995, S. 597–603 (601)

[383]) Vgl. Dix, A.: Fallstudie: Nordamerika und die Europäische Richtlinie, Vortrag auf der 18. Internationalen Datenschutzkonferenz „Persönlichkeitsschutz über Grenzen hinweg", Ottawa, Kanada, 18.–20. September 1996, abrufbar unter http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex4.html.

[384]) Vgl. Schild, H.-H.: Dreigestirn des BDSG: Erheben, Verarbeiten und Nutzen. Zur Problematik unterschiedlicher Begriffe im Datenschutzrecht, in DuD 1997, S. 444–445.

[385]) Bäumler, H.: Wie geht es weiter mit dem Datenschutz?, in: DuD 1997, S. 446–452 (446).

Praxis erhebliche Schwierigkeiten.[386]) Es bietet sich daher an, sie durch den von der EG-Datenschutzrichtlinie verwendeten Begriff der Verarbeitung personenbezogener Daten zu ersetzen, wie dies etwa bereits im hessischen Landesdatenschutzgesetz geschehen ist.[387])

2. **Verschlankung des Datenschutzrechts:** Selbst Fachleute klagen über eine kaum noch zu überblickende Normenflut auf dem Gebiet des Datenschutzrechts. Das allgemeine und das bereichsspezifische Datenschutzrecht bedarf daher einer Durchforstung und Überprüfung. So soll etwa die Hälfte der Regelungen im Bundesdatenschutzgesetz bis heute ohne praktische Relevanz geblieben sein oder an Bedeutung verloren haben.[388]) Solche Bestimmungen sollten gestrichen und Überregulierung auf ein vernünftiges Maß zurückgeführt werden.[389])

3. **Förderung der Selbstregulierung.** Wenngleich Selbstregulierung kein Königsweg ist, kann sie gesetzlichen Detailregelungen im Hinblick auf ihre Akzeptanz, Flexibilität und Wirtschaftlichkeit überlegen sein.[390]) Die Enquete-Kommission empfiehlt daher, die mit der EU-Datenschutzrichtlinie aufgestellte Verpflichtung, Selbstregulierung zu ermöglichen, als Chance zu begreifen, dieses Instrument auch in Deutschland einzusetzen und sich bei der Umsetzung der Richtlinie an den Erfahrungen von mit Selbstregulierung bereits vertrauten Staaten zu orientieren.

4. **Datenschutzaudit:** Eine wirksame Selbstregulierung setzt allerdings voraus, daß der Nutzer die Möglichkeit hat, den Umgang von Unternehmen mit seinen personenbezogenen Daten auch zu überprüfen oder überprüfen zu lassen.[391]) In diesem Zusammenhang hält die Enquete-Kommission die im Mediendienstestaatsvertrag vorgesehene Möglichkeit eines Datenschutzaudits für einen guten Weg, einen Anreiz für die Hersteller auf dem Gebiet der Informations- und Kommunikationstechnik zu schaffen, ihre Produkte einer Kontrolle von Datenschutz- und Datensicherheitsfunktionen zu unterwerfen. Zugleich würde ein Datenschutzaudit dem Nutzer die Überprüfung des Umgangs eines Unternehmens mit personenbezogenen Daten ermöglichen. Die Enquete-Kommission fordert den Gesetzgeber daher dazu auf, die Praxis in den Bundesländern zu beobachten und gegebenenfalls ein Datenschutzaudit auch im Bundesrecht vorzusehen. Das entspricht der Empfehlung des Sachverständigenrates „Schlanker Staat"; dieser empfiehlt, die im Umweltbereich bereits erprobte Auditierung auch in anderen Bereichen – u. a. den Datenschutz – einzusetzen.[392])

386) Vgl. Schild, H. H.: Dreigestirn des BDSG: Erheben, Verarbeiten und Nutzen. Zur Problematik unterschiedlicher Begriffe im Datenschutzrecht, in: DuD 1997, S. 444–445.
387) Vgl. Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder; Schild ebd., S. 444.
388) Vgl. Weichert, T.: Anforderungen an das Datenschutzrecht für das Jahr 2000, in: DuD 1997, S. 712–719.
389) Vgl. Weichert, ebd.
390) Vgl. Kuitenbrower, F.: Self-Regulation: Some Dutch Experiences, in: U. S. Department of Commerce, National Telecommunications and Information Administration: Privacy and Self Regulation in the Information Age, Washington D. C. Juni 1997, S. 109–117 (115); Swire, P. P.: Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information, in: U. S. Department of Commerce, National Telecommunications and Information Administration: Privacy and Self Regulation in the Information Age, Washington D. C., Juni 1997, S. 3–19.
391) Vgl. Swire, ebd., S. 15.
392) Sachverständigenrat „Schlanker Staat": Abschlußbericht, Bonn 1997, S. 92.

7. Internationales Datenschutzrecht

7.1 Internationale Abkommen und Aktivitäten

Bislang stehen sich auf internationaler Ebene sehr unterschiedliche einzelstaatliche Datenschutzsysteme und –niveaus gegenüber; sie reichen von Staaten mit einem relativ starken und elaborierten Regelungsgefüge zum Schutz der Privatsphäre bis hin zu Rechtssystemen, die den Datenschutz nur marginal oder überhaupt nicht garantieren.[393]) International ist es bisher vor allem im Rahmen des Europarats, der Vereinten Nationen und der Organisation für wirtschaftliche Zusammenarbeit gelungen, Mindeststandards festzuschreiben:

- **Europarat:** Das Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 stellt unter anderem ein datenschutzrechtliches Zweckbindungsgebot auf und verlangt Sicherungsmaßnahmen gegen unbefugten Zugang zu Datenbeständen. Ergänzt wurde das Übereinkommen um mehrere Empfehlungen des Ministerkomitees u. a. über den Schutz von personenbezogenen Daten, die zu Zwecken des Direktmarketing genutzt werden[394]), den Schutz von Sozialdaten[395]) und den Schutz von personenbezogenen Daten, die im Zahlungsverkehr verwendet werden[396]) und den Datenschutz auf dem Gebiet der Telefondienstleistungen.[397])
- **Vereinte Nationen:** 1990 wurden von der Generalversammlung die Richtlinien betreffend personenbezogene Daten in automatisierten Dateien beschlossen. Diese Richtlinien legen für die Datenerhebung und -verarbeitung in automatisierten Dateien die Grundsätze der Richtigkeit und der Zweckbestimmung und -gebundenheit fest und geben dem Betroffenen ein Informationsrecht. Zugleich räumen sie den Staaten jedoch weite Ausnahmebefugnisse ein und überlassen es der Initiative der Einzelstaaten, überhaupt datenschutzrechtliche Vorschriften zu erlassen.
- **OECD:** 1980 hat die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) „Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten" verabschiedet.[398]) Sie enthalten an die Mitgliedsstaaten gerichtete Empfehlungen, denen zufolge unter anderem die Grundsätze von Zweckbindung, Transparenz und der Beteiligung des Betroffenen bei der Datenverarbeitung zu beachten sind. Insgesamt können die Leitlinien als Ausdruck eines internationalen Konsenses über Datenschutzprinzipien zu Beginn der Computerrevolution angesehen werden.[399]) 1985 wurden sie ergänzt um eine Erklärung über den grenzüberschreitenden Datenverkehr.[400])

  1992 verabschiedete die OECD Leitlinien für die Sicherheit von Informationssystemen[401]), die ebenfalls unter anderem dem Schutz der Vertraulichkeit und der Privatsphäre dienen sollen. 1996 veröffentlichte die OECD einen Expertenbericht über die Sicherheit von Informationssystemen und Datenschutz, in dem sie weiteren Handlungsbedarf konstatiert.[402])

7.2 Bewertung und Empfehlung der Enquete-Kommission

Internationale Regelungen zum Datenschutz, die möglichst alle datenverarbeitenden Stellen den gleichen rechtlichen Bedingungen unterwerfen, sind gegenüber nationalen und supranationalen Regelungen vorzugswürdig. Denn aufgrund der Globalität der Datennetze wird ein nationales Datenschutzrecht die Privatsphäre in Zukunft in vielen Fällen immer weniger schützen können. Die Enquete-Kommission empfiehlt daher, entsprechende Verhandlungen in internationalen Organisationen zu initiieren und voranzutreiben. Sie ist sich allerdings der Tatsache bewußt, daß der Prozeß der Internationalisierung des Datenschutzes aufgrund des unterschiedlichen Schutzniveaus und der unterschiedlichen Regelungsansätze in vielen Staaten eine geraume Zeit in Anspruch nehmen wird und es daher notwendig ist, Zwischenlösungen zu finden.

---

393) Vgl. die von „Privacy International" unter http://www.privacy.org/pi/ zum Abruf bereitgestellten Informationen.

394) Recommendation No. R (85) 20 of the Committee of Ministers to Member States on the Protection of Personal Data Used for the Purposes of Direct Marketing.

395) Recommendation No. R (86) 1 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Social Security Purposes.

396) Vgl. Recommendation No. R (87) 15 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Payment and Other Related Operations.

397) Recommendation No. R (95) 4 of the Committee of Ministers to Member States on the Protection of Personal Data in the Area of Telecommunication Services, with Particular Reference to Telephone Services.

398) Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, abrufbar unter http://www.oecd.org/dsti/iccp/legal/priv-en.html

399) Vgl. Information Policy Committee der National Information Task Force: Options for Promoting Privacy on the National Information Infrastructure, Draft for Public Comment, Executive Summary, April 1997, unter I.1.

400) Declaration on Transborder Data Flow, abrufbar unter http://www.oecd.org/dsti/iccp/legal/d-flow-e.html.

401) Guidelines for the Security of Information Systems, abrufbar unter http://www.oecd.org/dsti/iccp/legal/secur-en.html.

402) Report of the Ad Hoc Meeting of Experts on Information Infrastructures: Issues Related to Security of Information Systems and Protection of Personal Data and Privacy (OCDE/GD (96)74).

8. Außerrechtliche Lösungsansätze

Darüber hinaus sollten nach Auffassung der Enquete-Kommission weitere Maßnahmen in Erwägung gezogen werden, um den Datenschutz in der Informationsgesellschaft wirksam zu gewährleisten:

• Erhöhung des Risikobewußtseins der Nutzer

Es ist oben bereits ausgeführt worden, daß die Furcht vor den Gefahren der neuen Informations- und Kommunikationstechniken in weiten Teilen der Bevölkerung ausgeprägt ist.[403]) Jedenfalls bei denjenigen, die die neuen Techniken noch nicht nutzen, sind die Ängste jedoch eher allgemein und diffus, also nicht durch bestimmte und identifizierbare Risiken ausgelöst.[404]) Nur das Bewußtsein um bestimmte Risiken versetzt die Nutzer jedoch in die Lage, sich wirksam gegen sie zu schützen. Aufgrund dessen ist die Entwicklung eines Bewußtseins, das den Risiken offener Telekommunikationsnetze gerecht wird, von großer Bedeutung für den Datenschutz.[405]) Notwendig ist die Aufklärung der Nutzer über die spezifischen Gefahren für das informationelle Selbstbestimmungsrecht in Netzen. Dies kann durch staatliche Aufklärungskampagnen, aber auch dadurch geschehen, daß die Anbieter von Diensten in den neuen Medien zur Aufklärung verpflichtet werden.

• Förderung des Selbstschutzes der Nutzer

Zu der Aufklärung über die Gefahren offener Datennetze muß die Information über die Möglichkeiten des Selbstschutzes kommen. Der Nutzer muß wissen, wie er sich gegen Überwachung und Profilbildung zur Wehr setzen, wo er entsprechende Software bekommen und wie er sie verwenden kann. Auch dies kann durch eine Informationskampagne vermittelt werden, die zudem noch die marktwirtschaftliche Entwicklung auf dem Gebiet des Angebots von Sicherheitsprodukten für die Kommunikation in Datennetzen unterstützen könnte. Hilfreich wäre es auch, wenn die öffentliche Verwaltung die Möglichkeiten dieser Produkte in ihrem eigenen Bereich nutzen und aufzeigen würde. Denkbar ist auch, Möglichkeiten des Selbstschutzes bei den Anbietern von Diensten in Telekommunikationsnetzen zwingend vorzusehen.

• Beibehaltung der freien Verwendung kryptografischer Verfahren

Aufgrund der Notwendigkeit des Selbstschutzes von Bürgern und Unternehmen sollte nach dem derzeitigen Erkenntnisstand keine Einschränkung der Verwendung kryptografischer Verfahren in Betracht gezogen werden. Die mit einer solchen Einschränkung möglicherweise verbundenen Vorteile wären so gering, daß sie die mit ihr verbundenen Nachteile für den Datenschutz nicht aufwiegen könnten. Denn zum einen bestehen viele Möglichkeiten, ein Verbot der freien Verwendung kryptografischer Verfahren zu umgehen – etwa durch mehrfache Verschlüsselung oder steganografische Verfahren. Und zum anderen ließe sich ein solches Verbot kaum wirksam überwachen.

• Förderung der anonymen Nutzung der neuen Dienste

Um die Gebote der Datensparsamkeit und der Datenvermeidung zu erfüllen, sollte die anonyme und pseudonyme Nutzung der neuen Dienste gefördert werden. Dies ist nach dem Bericht des Bundesbeauftragten für den Datenschutz der wirksamste Weg, um Mißbräuchen mit personenbezogenen Daten vorzubeugen, die in den Datennetzen anfallen.[406]) Einschränkungen der Möglichkeiten zur anonymen Nutzung aufgrund von Erwägungen der Kriminalitätsbekämpfung sind allenfalls in den Fällen sinnvoll, in denen der Nutzer selbst zum Informationsanbieter wird, etwa bei Newsgruppen. In diesem Fall besteht jedoch die Möglichkeit, die Provider und etwaige Anbieter von Anonymisierungsdiensten zur Aufdekkung von Identitäten heranzuziehen.

• Erhöhung der Sicherheit von Produkten der Informations- und Kommunikationstechnik

Einhergehen muß die Aufklärung über Risiken und Möglichkeiten der Kommunikation in Netzen mit Maßnahmen, die das Vertrauen in die Sicherheit von Produkten der Informations- und Kommunikationstechnik steigern. Berichte über die Unzuverlässigkeit etwa von sogenannten „Browsern" – Computerprogrammen, die das Aufrufen von Seiten im Internet ermöglichen – und anderen Anwendungen verunsichern viele Nutzer und können davon abschrecken, von den neuen Medien Gebrauch zu machen. Vertrauensbildende Maßnahmen können helfen, das zu verhindern. Geprüft werden sollte insbesondere, wie eine freiwillige Prüfung und Zertifizierung der Datenschutzfunktionen von Produkten der Informations- und Kommunikationstechnik durch unabhängige Stellen auf einer breiten Basis durchgesetzt wer-

---

[403]) Vgl. oben S. 2.

[404]) Vgl. INRA (Europe – E. C. O.: Information Technology and the Protection of Personal Data – A Qualitative Study – For the European Commission, DG XV: Internal Market and Financial Services, Brüssel 30. Juli 1997.

[405]) Vgl. Merold, R. N.: The Necessary Elements of Self-Regulatory Privacy Regimes and the Role of Consumer Education in a Self-Regulatory Privacy Regime, in: U.S. Department of Commerce, National Telecommunications and Information Administration: Privacy and Self Regulation in the Information Age, Washington D.C. Juni 1997, S. 141–145.

[406]) Vgl. BT-Drs. 13/7500 unter 8.3.1.

den können.[407]) Das hätte neben dem unmittelbaren Effekt der technischen Sicherheitskontrolle auch die Wirkung, daß Datenschutzfunktionen zunehmend als ein Qualitätsmerkmal wahrgenommen würden.[408]) Dies gilt um so mehr, als auch große Unternehmen der Informations- und Kommunikationstechnik inzwischen die Bedeutung des Datenschutzes erkannt haben und beginnen, mit dieser Bedeutung entsprechenden Eigenschaften ihrer Produkte zu werben.[409])

- **Unterstützung von Standardisierungsbemühungen**

Auf internationaler Ebene erfolgversprechend erscheinen in diesem Zusammenhang die Bemühungen um technische Datenschutzstandards:[410]) Die Internationalen Standardisierungs Organisation (ISO) untersucht derzeit, ob und inwieweit ein Bedarf zur Entwicklung eines internationalen Datenschutzstandards besteht.[411]) Der Schlußbericht des damit befaßten Gremiums soll 1998 erscheinen. Um internationale Standards unter anderem im Hinblick auf Datenschutz- und Datensicherheitsfunktionen bemühen sich daneben noch etwa die Internationale Telekommunikations-Union (ITU) und die Internationale Elektrotechnische Kommission (IEC)[412]). Parallel dazu, jedoch auch in Zusammenarbeit mit den Normungsorganisationen sind die Europäische Union, die USA und Kanada dabei, gemeinsame Kriterien für die Bewertung der Sicherheit von Informationssystemen zu schaffen, die möglicherweise auch weltweit Standards setzen soll.[412])

Die Enquete-Kommission empfiehlt, die Bemühungen auf nationaler, europäischer und internationaler Ebene, technische Standards zu entwickeln, die einen angemessenen Schutz der Privatsphäre gewährleisten können, zu unterstützen und voranzutreiben. Hinzuweisen ist jedoch auf die Gefahr, daß technische Standards auf einem so innovativen Gebiet der neuen Informations- und Kommunikationstechniken schnell veralten können. Das zwingt möglicherweise zu kontinuierlichen und gerade auf internationaler Ebene langwierigen Verhandlungen über Anpassungen der Standards an die technische Entwicklung. Etwa in Kanada unternommene Versuche, Datenschutz durch eine Verbindung rechtlicher Vorgaben und technischer Standards zu schaffen, sollten aufmerksam beobachtet werden.

9. Abschließende Empfehlungen zum Berichtsteil Datenschutz

1. Die Enquete-Kommission ist der Auffassung, daß mit Teledienstedatenschutzgesetz und den datenschutzrechtlichen Bestimmungen im Mediendienstestaatsvertrag ein Schritt in Richtung eines Datenschutzrechts getan worden ist, das den Anforderungen der Informationsgesellschaft gerecht werden kann. Sie empfiehlt dem Gesetzgeber jedoch, aufmerksam zu beobachten, ob sich die Regelungen im internationalen Vergleich als sachgerecht, den Bürgerrechten dienlich, wettbewerbsfördernd oder als zu restriktiv erweisen. Gleichzeitig sollte überprüft werden, wie sich Abgrenzungsprobleme zwischen den beiden Regelungswerken und zum Telekommunikationsgesetz auswirken.

2. Die Gesetzgeber in Bund und Ländern haben in § 3 Abs. 4 Teledienstedatenschutzgesetz und § 12 Abs. 5 Mediendienstestaatsvertrag einen ersten und richtungsweisenden Ansatz formuliert, das Datenschutzrecht um technikrechtliche Elemente der datenminimierenden Gestaltung und Auswahl von Einrichtungen der Informations- und Kommunikationstechnik zu ergänzen. Diese Steuerungselemente sind um die Anforderungen zu ergänzen, die im Zusammenhang mit organisatorischen, technischen und rechtlichen Vorkehrungen zur Erhöhung der Datensicherheit (IT-Sicherheit) in der Informations- und Kommunikationstechnik entwikkelt worden sind.

3. Prinzipien des Datenschutzes sollten nach Möglichkeit integraler Bestandteil von Dienstleistungen und Produkten auf dem Gebiet der Informations- und Kommunikationstechnik werden. Entsprechende Forschungs- und Entwicklungsarbeiten sollten verstärkt gefördert und

---

407) Vgl. Büllesbach, A.: Datenschutz bei Informations- und Kommunikationsdiensten, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Bonn 1998, S. 42.

408) Vgl. Sieber, P.: Datenschutz als Qualitätsmerkmal, in DuD 1996, S. 661–663.

409) Vgl. die Informationen über die „Internet Privacy Initiative" der Firmen Firefly Network, Microsoft und Netscape unter http://www.microsoft.com/cio/articles/privacyinitiative.html sowie die unter http://www.truste.org abrufbaren Informationen.

410) Vgl. dazu: Bennett, C. J.: The Canadian Standards Association Model Code for the Protection of Personal Data: Reaching Consensus on Principles and Developing Enforcement Mechanisms, in: U.S. Department of Commerce, National Telecommunications and Information Administration: Privacy and Self Regulation in the Information Age, Washington D.C. Juni 1997, S. 157–165 (162).

411) Einzelheiten sind unter http://www.iso.ch abrufbar.

412) IEC und ITU veranstalteten im September 1997 unter Beteiligung der EU eine Global Standards Conference in Brüssel.

413) Vgl. OECD Report of the Ad Hoc Meeting of Experts on Information Infrastructures, S. 52f.

unterstützt werden. Dies gilt auch für die Bemühungen um eine internationale Standardisierung von technischen Datenschutzfunktionen. Die öffentliche Hand soll die Beteiligung der von ihr beauftragten Stellen an entsprechenden Verhandlungen im Rahmen ihrer Möglichkeiten unterstützen.

4. Die Enquete-Kommission hält die Umsetzung der EU-Datenschutzrichtlinie für eine Chance, die zu einer umfassenden Novellierung des Bundesdatenschutzgesetzes und anderer datenschutzrechtlicher Regelungswerke genutzt werden sollte. Angesichts der Unübersichtlichkeit und Kompliziertheit des Datenschutzrechts sollte im Interesse von datenverarbeitenden Stellen und Nutzern eine erhebliche Vereinfachung und Verschlankung des Datenschutzrechts im Vordergrund stehen. Dabei sollte vor dem Hintergrund der internationalen Entwicklung auch die Kompetenzverteilung zwischen Bund und Ländern einer kritischen Überprüfung unterzogen werden.

5. Das Datenschutzrecht insgesamt sollte – wie bereits im Teledienstedatenschutzgesetz geschehen – auf die Unterscheidung zwischen Datenverarbeitung durch öffentliche und private Stellen verzichten. Es sollte ferner, wie von der EU-Datenschutzrichtlinie vorgesehen, ein allgemeines Recht des Betroffenen zum Widerspruch gegen die Verarbeitung von personenbezogenen Daten geschaffen werden.

6. Erforderlich ist eine Überarbeitung der Technischen Maßnahmen nach der Anlage zu § 9 BDSG, die zehn Regeln zum technischen und organisatorischen Schutz personenbezogener Daten aufstellt. In einem ersten Schritt ist dieser Katalog dahingehend zu überprüfen, ob er den Anforderungen moderner vernetzter Systeme noch genügt. In einem zweiten Schritt ist seine Kompatibilität mit international anerkannten Sicherheitsmaßnahmen zu überprüfen. Gegebenenfalls ist der Maßnahmenkatalog nach der Anlage zu § 9 BDSG anzupassen, um seine praktische Anwendung durchzusetzen und internationale Akzeptanz zu erreichen. Schließlich sind Modelle exemplarischer Sicherheitsanforderungen zu entwickeln, um ihre praktische Durchsetzung zu erleichtern.

7. Die in der EU-Datenschutzrichtlinie enthaltene Verpflichtung, im nationalen Datenschutzrecht Möglichkeiten der Selbstregulierung vorzusehen, sollte als Chance begriffen werden, dieses Instrument für den Schutz des Rechts auf informationelle Selbstbestimmung fruchtbar zu machen. Entsprechende Regelungen sollten sich an den Erfahrungen von Staaten orientieren, die bereits Erfahrungen mit Selbstregulierung im Bereich des Datenschutzes gesammelt haben.

8. Die Vereinfachung und Verschlankung des Datenschutzrechts sollte nicht zur Einschränkung oder Abschwächung bewährter Verfahren des Datenschutzes führen. Eine Differenzierung zwischen Bereichen, in denen solche Verfahren exisitieren und Bereichen, in denen neue Verfahren eingesetzt werden sollen, ist daher notwendig. Die Kommission empfiehlt, dies bei der Novellierung des Bundesdatenschutzgesetzes zu berücksichtigen.

9. Bei der Schaffung neuer datenschutzrechtlicher Regelungen ist die Dynamik des Veränderungsprozesses der Informations- und Kommunikationstechnik zu berücksichtigen. Diese Dynamik schafft einen erheblichen Druck zur Anpassung der Datenschutzgesetze. Verdeutlicht wird dies dadurch, daß etwa Videodateien und andere im Netz anzutreffende Formen der Datenhaltung nicht den Datenschutzgesetzen unterfallen. Regelungen des Datenschutzes sollten daher permanent evaluiert werden. Mit den Entschließungsanträgen zum Informations- und Kommunikationsdienstegesetz wurde in bezug auf dieses Gesetz ein entsprechender Auftrag an die Bundesregierung erteilt. Ebenso sollte auch bei der anstehenden Novellierung des Bundesdatenschutzgesetzes vorgegangen werden.

10. Die Enquete-Kommission empfiehlt im Einklang mit den Empfehlungen des Sachverständigenrates „Schlanker Staat", die Möglichkeit einer Auditierung auch im Datenschutzrecht vorzusehen. Abgesehen von der mit einer Auditierung verbundenen Entlastung des Staates, würde sie die Ergebnisse der Selbstregulierung transparent machen können. Zugleich könnte sie die Wahrnehmung von Datenschutzfunktionen als ein Qualitätsmerkmal stärken und damit deutlich machen, daß Datenschutz nicht nur als Kostenfaktor für Unternehmen anzusehen ist, sondern längerfristig einen entscheidenden Wettbewerbs- und Standortvorteil darstellen kann.

11. Um zu verhindern, daß sich an der Sammlung und Verwendung von personenbezogenen Daten interessierte Unternehmen in Staaten ansiedeln, in denen kein oder nur ein schwacher Datenschutz besteht, sind möglichst globale Datenschutzregelungen erforderlich. Die Enquete-Kommission empfiehlt, entsprechende Verhandlungen zu initiieren bzw. zu unterstützen.

12. Die Enquete-Kommission empfiehlt, die Möglichkeiten des Selbstschutzes für den einzelnen Nutzer zu fördern. Dazu bedarf es insbesondere der Förderung des Bewußtseins um die Möglichkeiten des Selbstdatenschutzes und des Systemdatenschutzes. Dies kann zum einen durch Maßnahmen zur Aufklärung über die Chancen und Risiken der neuen Informations- und Kommunikationstechniken geschehen, zum anderen aber auch dadurch, daß die öffentliche Verwaltung selbst entsprechende Techniken einsetzt. Ziel sollte es sein, den Datenschutz zu einem Thema der gesellschaftlichen Debatte zu machen.

13. Die Möglichkeiten der Nutzer zum Selbstschutz durch kryptografische Verfahren sollten nach

dem derzeitigen Erkenntnisstand rechtlich nicht eingeschränkt werden. Eine Einschränkung der freien Verwendung solcher Verfahren kann bei einer Abwägung von Nutzen und Schaden nach diesem Erkenntnisstand nicht gerechtfertigt werden. Denn während sie rechtstreue Unternehmen und Bürger bei ihrem Bemühungen, vertraulich zu kommunizieren, erheblich behindern würde, dürfte der Nutzen aufgrund der Umgehungsmöglichkeiten für die staatliche Sicherheit gering sein. Verschlüsselungsprogramme, die eine Entschlüsselung verschlüsselter Inhalte durch Dritte ermöglichen, sollten als solche gekennzeichnet werden müssen.

14. Um die Gebote der Datensparsamkeit und der Datenvermeidung zu erfüllen, sollte die anonyme und pseudonyme Nutzung der neuen Dienste gefördert werden. Dies ist nach dem Bericht des Bundesbeauftragten für den Datenschutz der wirksamste Weg, um Mißbräuchen mit personenbezogenen Daten vorzubeugen, die in den Datennetzen anfallen.

15. Der Schutz des Fernmeldegeheimnisses als Grundvoraussetzung des Schutzes in Netzen ist auszubauen. Dabei ist insbesondere dem Umstand Rechnung zu tragen, daß Eingriffe in das Fernmeldegeheimnis nicht nur durch Anbieter von Telekommunikationsdienstleistungen und andere Dienstleistungsunternehmen möglich sind, sondern auch durch Dritte.

16. Geprüft werden sollte, wie eine freiwillige Prüfung der Datenschutzfunktionen von Produkten der Informations- und Kommunikationstechnik durch unabhängige Stellen auf breiter Basis durchgesetzt werden kann. Eine solche Zertifizierung, mit der die Unternehmen werben könnten, hätte nicht nur die unmittelbare Folge, daß aus Perspektive des Datenschutzes unbedenkliche Produkte auf den Markt kommen, sondern könnte ebenfalls das Bewußtsein um die Bedeutung des Datenschutzes in der Informationsgesellschaft erhöhen.

D. Dritter Berichtsteil: Strafrecht

(Verabschiedet am 23. März 1998)

1. Bedeutung des Strafrechts in Netzen

Schattenseite des mit großen Chancen verbundenen Aufkommens der neuen Informations- und Kommunikationstechniken ist, daß sie auch von Kriminellen genutzt werden: Computersysteme und ihre Vernetzung haben die Möglichkeit zur Begehung neuartiger Straftaten geschaffen; sie ermöglichen es zudem, bereits bekannte Straftaten auf neue Weise zu begehen.[414])

Den polizeilichen Kriminalstatistiken zufolge nimmt die Computerkriminalität in Deutschland rapide zu.[415]) Danach stieg allein von 1994 auf 1995 die Anzahl der unter diesem Begriff zusammengefaßten Straftaten um 32,9 Prozent.[416]) Das Bundesinnenministerium geht in einer 1996 veröffentlichten Schrift von einem Zuwachs von mehr als 50 Prozent aus;[417]) auch für die Folgejahre wird ein kontinuierlicher Anstieg der Deliktszahlen prognostiziert.[418])

Gestiegen ist zum einen die Anzahl der Delikte, bei denen informationstechnische Anlagen Gegenstand kriminellen Handelns sind – etwa der Computerbetrug oder die Manipulation von Datenbeständen; gestiegen ist jedoch auch die Menge der Straftaten, bei denen Computer als Mittel der Tatbegehung dienen.[419]) Als Folge der Vernetzung informationstechnischer Anlagen – etwa durch das Internet – und des zunehmenden Einsatzes von Computern als Mittel der klassischen Telefonie hat dabei auch die Kriminalität in Telekommunikationsnetzen zugenommen.[420])

Zugleich wird der Schutz vor Straftaten im Zusammenhang mit den neuen Informations- und Kommunikationstechniken immer wichtiger. Denn die Gesellschaft hat sich zunehmend in die Abhängigkeit von Computersystemen begeben.[421]) Nahezu jeder Lebensbereich ist von den neuen Informations- und Kommunikationstechniken durchdrungen: Der Bahn- und Luftverkehr und viele weitere Bereiche der Wirtschaft ebenso wie die medizinische Versorgung und militärische Einrichtungen.[422]) Angriffe auf Computersysteme können daher dramatische Auswirkungen haben – man denke an die Sabotage etwa der Steuerungssysteme von Kernkraftwerken oder militärischer Informationssysteme.[423]) Hinzu kommt, daß Information selbst immer mehr zu einem wichtigen Wirtschaftsgut wird und ein entsprechend hohes Gefährdungspotential aufweist: Die Schäden, die allein durch Softwarepiraterie entstehen, werden für 1996 weltweit auf ca. 18 Milliarden Mark geschätzt, wobei in Deutschland eine Schadenssumme von rund 800 Millionen Mark entstanden sei.[424]) Überdies ist die Nutzung neuer Informations- und Kommunikationstechniken für Straftäter ein Mittel, das die Strafverfolgungsbehörden vor häufig nur schwer lösbare Schwierigkeiten stellt: Während die Täter sich in den weltweiten Datennetzen mit einer zuvor unbekannten Mobilität bewegen können, sind die Behörden nach wie vor in hohem Maße auf die Grenzen ihres Nationalstaates beschränkt und ihre Bemühungen daher häufig erfolglos.[425])

Den durch diese Umstände bedingten Bedrohungen müssen wirksame Abwehrmechanismen gegenübergestellt werden, um die Sicherheit in der Informationsgesellschaft zu gewährleisten. Was dazu geschehen muß, ist Gegenstand der folgenden Darstellung. Sie gibt zunächst einen knappen Überblick über den verfassungsrechtlichen Rahmen des Strafrechts innerhalb des Staatswesens der Bundesrepublik Deutschland (4.2.) und beschreibt den Begriff (4.3.),

---

414) Vgl. United Nations Manual on the prevention and control of computer-related crime, abrufbar unter http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html, Ziffer 22.

415) Vgl. Dannecker, G.: Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, in: Betriebsberater 1996, S. 1285–1294 (1286); Computerzeitung vom 18. August 1997.

416) Vgl. Bundeskriminalamt (Hrsg.): Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Berichtsjahr 1995, Wiesbaden 1995, S. 251 f.

417) Vgl. Kanther, M.: Sicherheit für die Bürger auf dem Weg in die Informationsgesellschaft, in: Bundesministerium des Innern: Informationsgesellschaft und innere Sicherheit, Bonn, Juni 1996, S. 13–35 (17).

418) Die statistische Situation wird im allgemeinen als unsicher bezeichnet, dennoch wird von einer Steigerung ausgegangen, vgl. dazu näher unten 4.4. sowie Council of Europe: Computer-Related Crime. Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg 1990, S. 17.

419) Vgl. Bundeskriminalamt (Hrsg.): Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Berichtsjahr 1995, Wiesbaden 1995, S. 251 f.

420) Zum Begriff der Computerkriminalität bzw. der Telekommunikationskriminalität siehe unten unter 4.3.

421) Vgl. Riklin, F.: Information Highway und Strafrecht, in: Hilty, R. M. (Hrsg.): Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen, Bern, München 1996, S. 559–595 (563 f.).

422) Vgl. Cohen, F. B.: Protection and Security on the Information Superhighway; New York u. a. 1995, S. 1–4.

423) Vgl. Sieber, U.: Mißbrauch der Informationstechnik und Informationsstrafrecht, Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft, in Tauss, J.; Kollbeck, J.; Mönikes, J.: Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik, Baden-Baden 1996, S. 608–651 (624).

424) Ergebnis einer im Auftrag der Software Publishers Association (SPA) und der Business Software Alliance (BSA) erstellten Studie des International Planning and Research-Instituts, vgl. Pressemitteilung des Verbandes der Softwareindustrie Deutschlands (VSI), abrufbar unter http://www.vsi.de.

425) Vgl. Welt am Sonntag vom 25. August 1996: Weshalb Ermittler am Internet scheitern; Süddeutsche Zeitung vom 10. September 1996: Kommissar Computer. Informationstechnologie ist schneller als die Polizei erlaubt. Näher dazu 4.8.–4.10.

den Umfang (4.4.) sowie die Begehungsformen (4.5.) und die Tätergruppen (4.6.) der Kriminalität in Netzen. Auf der Basis einer Darstellung der bereits erfolgten Reformen des Strafrechts und des Strafprozeßrechts (4.7.) wird im Anschluß daran der gegenwärtige Reformbedarf im deutschen Straf- und Strafverfahrensrecht herausgearbeitet (4.8.). Sodann werden darüber hinausgehende Probleme und die Vorstellungen der Enquete-Kommission zu ihrer Lösung beschrieben (4.9. und 4.10.). Am Schluß der Darstellung steht eine Zusammenfassung der Empfehlungen der Kommission (4.11.).

2. Der verfassungsrechtliche Rahmen des Strafrechts

Eine umfassende Beschreibung des verfassungsrechtlichen Rahmens des Strafrechts in einem freiheitlich verfaßten Staatswesens erscheint im hier gegebenen Zusammenhang nicht notwendig. Die Strafrechtsordnung hat die Aufgabe, das Zusammenleben der Menschen dadurch zu schützen, daß es Verletzungen und Gefährdungen elementarer Rechtsgüter mit staatlichem Zwangsmaßnahmen sanktioniert.[426]) Durch die Androhung, aber auch durch die Verhängung der Strafe wirkt es der Begehung von Straftaten entgegen und dient damit der Sicherung des öffentlichen Friedens; zugleich schützt es die grundgesetzlich garantierte freie Entfaltung der Persönlichkeit und andere Grundrechte.[427])

Der grundrechtsschützenden Funktion des Strafrechts gegenüber steht die mit seiner Durchsetzung verbundene Notwendigkeit, die Grundrechte von Verdächtigen und Straftätern durch Strafverfolgung, Strafverhängung und Strafvollzug so stark einzuschränken wie in keinem anderen Bereich staatlichen Handelns. Der Grundsatz der Verhältnismäßigkeit gebietet es daher, das Strafrecht lediglich als ultima ratio, d. h. als letztes Mittel staatlichen Handelns zu verstehen, es also nur zurückhaltend und nur dann einzusetzen, wenn ein effektiver Schutz eines Rechtsguts auf andere Weise nicht erreicht werden kann.[428]) Die mit der Bestrafung verbundenen Grundrechtseinschränkungen verlangen zudem, daß die Umstände, die zu einer Bestrafung führen können, hinreichend präzise bestimmt sein müssen und an das Strafverfahren besonders strenge Anforderungen zu stellen sind.[429])

Die Geltung, Anwendung und Durchsetzung deutschen Strafrechts ist grundsätzlich auf das deutsche Staatsgebiet beschränkt.[430]) Denn das völkerrechtliche Territorialitätsprinzip, welches nach Art. 25 Grundgesetz den Gesetzen vorgeht, begrenzt die Wirkung jeder staatlichen Rechtsordnung in der Regel auf das jeweilige staatliche Hoheitsgebiet.[431])

3. Begriff der Kriminalität in Netzen

Ein einheitlicher Begriff für die Kriminalität in Telekommunikationsnetzen hat sich bislang nicht herausgebildet.[432]) Häufig verwendet werden dagegen die Begriffe „Computerkriminalität" und computerbezogene Kriminalität (computer-related crime). Eine weite Definition versteht darunter alle kriminellen Handlungen, bei denen ein Computer Mittel oder Objekt der Straftat ist; eine engere sieht alle Straftaten als erfaßt an, bei deren Begehung eine computergestützte Datenverarbeitung stattgefunden hat.[433]) Welcher Deutung man auch den Vorzug geben will – aufgrund des Zusammenwachsens von Computertechnik und Telekommunikationstechnik trifft der Begriff der Computerkriminalität häufig auch auf Delikte zu, die in Telekommunikationsnetzen begangen werden können. Denn immer mehr Computer sind an das Telekommunikationsnetz angeschlossen, und viele Telefongeräte sind zugleich Computersysteme. Daher ist zum Beispiel das illegale Kopieren urheberrechtlich geschützter Informationen im Internet gleichermaßen durch den Einsatz von Computertechnik wie durch den Einsatz von Telekommunikationstechnik geprägt; gleiches gilt für den unerlaubten Online-Zugriff auf fremde Datenbestände und die über Telekommunikationsnetze durchgeführte computergestützte Manipulation von Datenbeständen in betrügerischer Absicht.

Eine Differenzierung zwischen Telekommunikations- und Computerkriminalität ist angesichts dieser Entwicklung für eine Untersuchung, die sich mit der Kriminalität in Netzen befaßt, nicht hilfreich. Sinnvoller ist, die Begriffe Computerkriminalität und Kriminalität in Telekommunikationsnetzen in einem Sinne zugrunde zu legen, der die Schnittmenge von Telekommunikations- und Computerkriminalität beschreibt. Das soll im folgenden geschehen. Erfaßt werden also Straftaten, zu deren Begehung sich die Täter gleichzeitig die Computertechnik und die Telekommunikationstechnik zunutze machen. Ausgeklammert werden dagegen Erscheinungsformen der Computerkriminalität, die außerhalb der Telekommunikationsnetze einzuordnen sind – etwa das ille-

426) Vgl. BVerfGE 39, 1 (47); Schönke-Schröder (Eser), 25. Auflage, München 1997, Vorbem. § 1, Rn. 27.

427) Vgl. BVerfGE 45, 187 (253ff); Tröndle, H.: Strafgesetzbuch, 48. Auflage, § 46, Rn. 3ff.

428) Vgl. BVerfGE 39, 1 (47).

429) Vgl. Roxin, C.: Strafrecht Allgemeiner Teil, Bd. I, München 1992, S. 65ff m. w. N.

430) Vgl. Schönke-Schröder: Strafgesetzbuch, 25. Auflage, München 1997, Vorbem. §§ 3–7 (Eser), Rn. 3; Lackner: Strafgesetzbuch, 22. Auflage, München 1997, Vorbem. §§ 3–7, Rn. 3.

431) Vgl. von Münch, I. (Hrsg.): Grundgesetz-Kommentar, 3. Auflage, München 1995, Art. 25 (Rojahn), Rn. 22; Seidl-Hohenveldern: Völkerrecht, 9. Auflage, Köln u. a. 1997, Rn. 1504ff. Zu Ausnahmen von diesem Grundsatz vgl. §§ 3–7 Strafgesetzbuch. Näher dazu unten unter 4.9.

432) Vgl. zu den Schwierigkeiten einer hinreichend präzisen Begriffsbildung Council of Europe: Problems of criminal procedural law connected with information technology. Recommendation No. R (95) 13 and explanatory memorandum, Straßbourg 1996, S. 20f, Ziffern 28, 29; Council of Europe: Computer-Related Crime. Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg 1990, S. 12ff.

433) Vgl. Möhrenschlager, M.: Computer Crimes and Other Crimes against Information Technology in Germany, in: Sieber, U. (ed.): Information Technology Crimes. National Legislations and International Initiatives, Köln. u. a. 1994, S. 197–233 (197f).

gale Kopieren von Disketten oder der offline-Zugriff auf fremde Datenbestände. Gleiches gilt für Erscheinungsformen der Telekommunikationskriminalität, die ohne Zuhilfenahme von Computertechnik begangen werden können, zum Beispiel die per Telefongespräch begangene Beleidigung.

4. Umfang der Kriminalität in Netzen

Obwohl das Bundeskriminalamt aufgrund eines 1985 gefaßten Beschlusses einen jährlichen Bericht zur Kriminalität in Verbindung mit der Informations- und Kommunikationstechnologie erstellt, kann der Umfang der Kriminalität in Netzen anhand des vorliegenden statistischen Materials kaum zuverlässig festgestellt werden.[434]) Abgesehen von den begrifflichen Unklarheiten ergeben sich erhebliche Unsicherheiten daraus, daß in der polizeilichen Kriminalstatistik nicht zwischen den Formen der Computerkriminalität, die unter Nutzung von Telekommunikationsnetzen begangen werden, und den Delikten, bei denen dies nicht der Fall ist, unterschieden wird. Überdies wird die Dunkelziffer im Bereich der Computerkriminalität im allgemeinen als sehr hoch angesehen: Schätzungen zufolge werden nicht mehr als fünf Prozent der Delikte den Strafverfolgungsbehörden gemeldet.[435]) Als Gründe dafür werden Schwierigkeiten, Rechtsverletzungen festzustellen, die unzureichende sachliche und personelle Ausstattung der Behörden, die Furcht der Opfer vor weiteren Angriffen und dem Verlust des Vertrauens in ihre Dienstleistungen sowie ein unzureichendes Meldeverhalten der Polizeidienststellen genannt.

Trotz dieser Unsicherheiten dürfte die vielfach gemachte Feststellung, daß die Kriminalität in Telekommunikationsnetzen stark ansteigt, zutreffend sein. Der von der polizeilichen Kriminalstatistik – allerdings mit großen Unterschieden bei den einzelnen Delikten – verzeichnete Anstieg der Computerkriminalität kann zumindest als ein Indiz dafür gewertet werden. Zudem spricht die allgemeine Lebenserfahrung dafür, daß mit der zunehmenden Durchdringung aller Lebensbereiche durch die neuen Informations- und Kommunikationstechniken eine Zunahme der Kriminalitätsformen einhergeht, die sich dieser Techniken bedienen.[436])

5. Delikte

Die Deliktsarten, die unter dem Begriff der Computer- oder Telekommunikationskriminalität zusammengefaßt werden können, sind vielfältig. Üblich ist ihre Unterteilung in Wirtschaftsdelikte, Verbreitungsdelikte, Persönlichkeitsrechtsverletzungen und sonstige Delikte[437]):

5.1 Wirtschaftsdelikte

Computerbezogene Wirtschaftsdelikte gelten als Kernbereich der Computerkriminalität.[438]) Unter diesem Begriff werden vor allem Computermanipulationen, Computerbetrug, Computersabotage und damit verbundene Erpressung, das sogenannte Computerhacking, Computerspionage sowie unterschiedliche Formen der Produktpiraterie zusammengefaßt.

- Computermanipulationen und Computerbetrug gehören bereits zum Alltag der Informationsgesellschaft. Spektakuläre Veränderungen von Bilanzierungsprogrammen sowie über Datennetze vorgenommene Manipulationen der Buchhaltung von Banken[439]) werden ebenso verzeichnet wie Mißbräuche von Bankautomatenkarten und vergleichbaren Zahlungsmitteln. Die Zahl der Kartenmißbräuche geht inzwischen um ein Vielfaches über die Zahl klassischer Manipulationen hinaus; die Begehungsarten reichen von der schlichten Verwendung gestohlener Karten über die Veränderung von Karten mit Hilfe von Computern bis hin zur selbständigen Anfertigung von Kartenkopien.[440]) Die Bandbreite der von den Tätern eingesetzten Methoden, sich die zur Verwendung der Karten notwendige Geheimnummer zu verschaffen, ist ähnlich groß: Zum Ziel führten zum Beispiel Trickanrufe, das Präparieren der Tastatur, die Verwendung von Tastaturattrappen und das Abhören von Datenfernleitungen.[441])

  Als Massendelikt werden Mißbräuche des Telefonnetzes bezeichnet.[442]) Die Fälschung und Manipulation von Telefonkarten, mit denen an öffentlichen Fernsprechern telefoniert werden kann und das auf unterschiedliche Weisen ermöglichte Telefonieren auf Rechnung anderer Netzteilnehmer

[434]) Vgl. zur Bewertung der Kriminalstatistiken auf dem Gebiet der Computerkriminalität Council of Europe: Computer-Related Crime. Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg 1990, S. 14ff.

[435]) Vgl. United Nations Manual on the prevention and control of computer-related crime, abrufbar unter http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html, Ziffer 27.

[436]) Vgl. Riklin, F.: Information Highway und Strafrecht, in: Hilty, R. M. (Hrsg.): Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen, Bern, München 1996, S. 559–595 (563f.).

[437]) Vgl. zu dieser Einteilung und zum folgenden Sieber, U.: Mißbrauch der Informationstechnik und Informationsstrafrecht, Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft, in Tauss, J.; Kollbeck, J.; Mönikes, J.: Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik, Baden-Baden 1996, S. 608–651 (609ff).

[438]) Vgl. Sieber, ebd., S. 611.

[439]) 1994 gelang es einer russischen Tätergruppe, von St. Petersburg aus über das Telekommunikationsnetz eine amerikanische Bank zur Überweisung von über 10 Millionen Dollar zu veranlassen, vgl. Sieber, ebd., m. w. N.

[440]) Zu unterschiedlichen Begehungsarten vgl. Altenhain, K.: Der strafbare Mißbrauch kartengestützter eklektronischer Zahlungssysteme, in: JZ 1997, S. 752–760.

[441]) Vgl. Yamaguchi, A.: Computer Crimes and Other Crimes against Information Technology in Japan, in: Sieber, U. (Hrsg.): Information Technology Crime. National Legislations and International Initiatives, Köln u. a. 1994, S. 305–321 (307).

[442]) Vgl. Sieber, U.: Mißbrauch der Informationstechnik und Informationsstrafrecht, Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft, in Tauss, J.; Kollbeck, J.; Mönikes, J.: Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik, Baden-Baden 1996, S. 608–651 (613ff).

sind ebenso verbreitet wie der Mißbrauch der in den 90er Jahren eröffneten Möglichkeiten, das Telefonnetz zu Abrechnungszwecken einzusetzen. Schätzungen zufolge sind über 80 Prozent der Umsätze der unter bestimmten gebührenpflichtigen Vorwahlen zu erreichenden Angebote von Telefonsexanbietern das Ergebnis von Manipulationen zu Lasten von Telekommunikationsunternehmen und ihrer Kunden.[443]) In München wurde 1997 ein Student verurteilt, der mehrere Telefongesellschaften auf diese Weise um insgesamt 1,86 Millionen Mark geschädigt hatte.[444]) In den USA wurde ein Computerprogramm vertrieben, das angeblich allein zum Betrachten bestimmter Internetseiten dienen sollte. In Wahrheit manipulierte das Programm das Modem und Funktionen der Rechner, auf denen es installiert wurde. Aufgrund der Manipulationen wählte der Computer eine Reihe von ausländischen Telefonnummern an.[445]) 38000 Verbraucher wurden durch das Computerprogramm geschädigt; im November 1997 kündigte die US-amerikanische Federal Trade Commission (FTC) an, sie würden eine Entschädigung in Höhe von insgesamt 2,74 Millionen Dollar erhalten.[446])

- Großen wirtschaftlichen Schaden richten das unbefugte Kopieren und Nutzen fremder Computerprogramme an. Zur Verteilung von Piraterieprodukten werden dabei zunehmend auch Telekommunikationsnetze eingesetzt. Der Martktanteil illegal kopierter Software wird in Westeuropa auf 43 Prozent der Bundesrepublik Deutschland und in Osteuropa auf 80 Prozent geschätzt.[447]) Mit der Digitalisierung von Informationen aller Art nimmt daneben auch das illegale Kopieren sonstiger Dateien zu. Mit den damit verbundenen Herausforderungen hat sich die Enquete-Kommission in ihrem Zwischenbericht „Neue Medien und Urheberrecht" auseinandergesetzt.[448]) Auf diesen wird daher verwiesen.

- Ebenfalls einen erheblichen Anteil an der Computerkriminalität in Netzen hat Computersabotage in Form von Schädigungen von Computern durch Viren- und Wurmprogramme.[449]) Das sind Computerprogramme, die sich entweder in den anderen Programmen eines Computers ausbreiten, um von dort aus Schäden anzurichten, oder aber fremde Computersysteme selbständig angreifen. Der „Internet-Wurm" eines amerikanischen Studenten legte 1988 binnen weniger Tage mehrere Tausend an das Internet angeschlossener Computer lahm.[450]) Viren und ähnliche Programme werden vor allem über raubkopierte Software verbreitet; die durch sie angerichteten Schäden gelten als immens.[451]) Die Abhängigkeit der modernen Gesellschaft von einer funktionsfähigen Informations- und Kommunikationstechnik macht Computersabotage zu einem gefährlichen Mittel der Erpressung: Ein amerikanischer Wissenschaftler versandte 1989 über 20000 Disketten, die vorgeblich medizinische Informationen über den AIDS-Virus enthielten, jedoch einen Computervirus auf der Festplatte des Nutzers installierten. Der Computervirus verschlüsselte nach einer bestimmten Anzahl von Neustarts des Computers dessen Festplatte und forderte den Nutzer per Bildschirmanzeige auf, eine Geldsumme auf ein panamesisches Bankkonto zu überweisen, um den Entschlüsselungscode zu erhalten.[452]) Ein entsprechendes Vorgehen ist auch in Telekommunikationsnetzen mit dem Versand von emails oder einem „verseuchten" Angebot auf einer Internetseite möglich: Im Dezember 1997 drang eine Gruppe von Hackern in die Internet-Suchmaschine Yahoo! ein und drohte mit der massenhaften Verbreitung eines Computervirus, um den aufgrund spektakulärer Angriffe auf Computersysteme inhaftierten Kevin Mitnick freizupressen.[453])

- Anlaß zu polizeilichen Ermittlungen geben immer wieder auch Fälle des sogenannten Computerhakking, des unbefugten Eindringens in fremde Computer. Geschieht dies allein aus der Motivation heraus, die eigenen Fähigkeiten an der Überwindung von technischen Hindernissen zu beweisen, entsteht zumeist lediglich eine Gefährdung des betroffenen Computersystems. Neben Fällen von Rufschädigung – 1996 gelang es Hackern in den Internetserver der CIA einzudringen und die Bezeichnung „Central Intelligence Agency" in „Central Stupidity Agency" umzuwandeln[454]) – werden jedoch auch Fälle verzeichnet, in denen erhebli-

443) Vgl. Sieber, ebd., S. 615.
444) Vgl. Süddeutsche Zeitung vom 6. Februar 1997: Maulwurf im globalen Netz – „Erotische Talklines" manipuliert – drei Jahre Haft.
445) Vgl. die „News" des Legal Advisory Board der Europäischen Kommission vom November 1997, abrufbar unter http://www2.echo.lu/legal/en/news/9711/frontpage.html.
446) Vgl. ebd. mit weiterführenden Nachweisen.
447) Vgl. Pressemitteilung des Verbandes der Softwareindustrie Deutschlands, abrufbar unter http://www.vsi.de; zur Schadenshöhe vgl. auch oben unter 4.1.
448) BT-Drs. 13/8110. Der Zwischenbericht ist mit begleitenden Materialien auch in Buchform veröffentlicht worden: Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft (Hrsg.): Neue Medien und Urheberrecht, Bonn 1997.
449) Vgl. Brunnstein, K.: Computerviren und andere bösartige Software – Tschernobyl der Informationstechnik, in Computer und Recht 1993, S. 456–462.
450) Vgl. Sieber, U.: Mißbrauch der Informationstechnik und Informationsstrafrecht, Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft, in Tauss, J.; Kollbeck, J.; Mönikes, J.: Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik, Baden-Baden 1996, S. 608–651 (616).
451) Die US-amerikanische National Computer Security Association schätzte den Schaden 1995 auf eine Milliarde US-Dollar und erwartete für 1996 mindestens eine Schadensverdoppelung, vgl. Frankfurter Rundschau vom 14. August 1996: Der Hare-Virus schlug am Donnerstag erstmals zu.
452) Vgl. Kaspersen, W. T.: Computer Crimes and Other Crimes against Information Technology in the Netherland, in: Sieber, U. (ed.): Information Technology Crime. National Legislations and International Initiatives, Köln u.a. 1994, S. 343–376 (351f); Sieber a.a.O., S. 612.
453) Vgl. die Meldung in Der Spiegel-Netzwelt vom 13. Dezember 1997 abrufbar unter http://www.spiegel.de/netzwelt/aktuell/yahoo.html.
454) Dieser „Hack" ist im World Wide Web vielfach dokumentiert, vgl. etwa unter http://www.otrics.com/cia.html.

che weitere Schäden verursacht wurden: 1986 drangen deutsche Jugendliche in zahlreiche amerikanische Computersysteme ein und verkauften dort gesammelte Informationen für insgesamt mehr als 90000 Mark an den KGB, den Geheimdienst der UdSSR.[455]) Eingedrungen wird nicht nur in klassische Computersysteme, sondern zunehmend auch in Einrichtungen der Sprachtelefonie wie Telefonleitungen, Anrufbeantworter und sogenannte Voice-Mail-Systeme (Sprachboxcomputer). Als „Phreaker"[456]) bezeichneten Tätern gelang es etwa, sich in die Vermittlungsstellen von Telefongesellschaften einzuwählen und so die über diese Stellen geführten Telefongespräche mitzuhören.[457]) Abgehört – und verkauft – wurden dabei auch die Nummern der Telefonberechtigungskarten. Deutsche Jugendliche drangen 1992 in den Sprachcomputer einer Bankfiliale in Hamburg ein, auf dem sich Geheimnummern von Kreditkarten und Anträge auf Erhöhung von Kreditlinien befanden.[458])

- In engem Zusammenhang mit dem Eindringen in Computersysteme und Telekommunikationseinrichtungen steht Computerspionage im Sinne eines Eindringens in fremde Rechner zu Zwecken des Ausforschens. Da in Computersystemen größte Datenmengen gespeichert sind und binnen Sekunden kopiert sowie über Telekommunikationsnetze versandt werden können, stellt die Computerspionage eine unter Umständen sehr effektive Form der Wirtschaftsspionage dar. Betrieben wird sie nicht nur von jugendlichen Hackern und Wirtschaftsunternehmen, sondern zunehmend auch von Nachrichtendiensten.[459])
- Wirtschaftliche Schäden kann auch das unbefugte Nutzen von EDV-Anlagen anrichten, der sogenannte „Zeitdiebstahl". Soweit dies als strafwürdiges Delikt diskutiert wird, ist man sich einig darüber, solche Nutzungen auszuschließen, bei denen kein oder nur geringer Schaden entsteht.[460]) Indessen sind auch Fälle denkbar, in denen die – auch über Telekommunikationsverbindungen mögliche – Nutzung fremder Rechner erhebliche Vermögensschäden anrichten kann. Dies ist etwa der Fall, wenn ein Unternehmen, dessen Computer von Unbefugten genutzt wird, diesen Computer nur angemietet hat und sich der Mietzins nach der Nutzungsdauer des Computers berechnet.[461])

5.2 Verbreitungsdelikte

Größte Aufmerksamkeit in der Öffentlichkeit finden nach wie vor Delikte, die durch die Äußerung oder Weitergabe von mißbilligten Inhalten – etwa pornographischer oder gewaltverherrlichender Darstellungen – begangen werden.[462]) Die Begehung solcher Delikte wird durch die Vernetzung von Computern erheblich vereinfacht.[463]) Zugleich sind die Möglichkeiten zur Kontrolle des Datenflusses und zur Durchsetzung von Verboten beim derzeitigen Stand von Recht und angewendeter Technik äußerst begrenzt.[464])

5.3 Persönlichkeitsrechtsverletzungen

Aufgrund der Verlagerung vieler Datenverarbeitungs- und Kommunikationsvorgänge auf Computernetze wächst die Gefahr strafrechtlich relevanter Verletzungen des persönlichen Lebens- und Geheimnisbereiches. Wenngleich solche Delikte im Sinne des Strafrechts den offiziellen Statistiken zufolge nur geringe Bedeutung haben[465]), ist ihr Gefährdungspotential nicht zu unterschätzen. Die Ausforschung etwa digital aufbereiteter Gesundheitsdaten könnte verheerende Folgen für den Betroffenen und das Sicherheitsgefühl der Allgemeinheit haben. Aus Südafrika ist ein Fall bekannt, in dem es Unbekannten gelang, an medizinische Daten von Personen zu gelangen, die sich einem AIDS-Test unterzogen hatten, und sie an die Arbeitgeber der Betroffenen zu übermitteln.[466])

5.4 Sonstige Delikte

Ebenso wie bei den Verbreitungsdelikten lassen sich Computertechnik und Vernetzung als Mittel für die Begehung anderer Delikte einsetzen, die bereits vor den durch die Informationstechnik bedingten Veränderungen bekannt waren. Selbst Angriffe auf Leib und Leben wurden bereits verzeichnet. 1994 veränderte ein britischer Hacker auf dem Rechner eines

---

455) Vgl. zu diesem Fall Bär, W.: Der Zugriff auf Computerdaten im Strafverfahren, S. 37f.

456) Der Begriff ist von der Bezeichnung „Phone-Freak" abgeleitet.

457) Vgl. Sieber, U.: Mißbrauch der Informationstechnik und Informationsstrafrecht, Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft, in Tauss, J.; Kollbeck, J.; Mönikes, J.: Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik, Baden-Baden 1996, S. 608–651 (618).

458) Vgl. Der Spiegel Nr. 34/1992, S. 206f.

459) Vgl. Süddeutsche Zeitung vom 7. Januar 1997: Internet-Spionage gegen US-Firmen; Der Spiegel 36/1996; S. 194ff: Lauscher im Datenreich.

460) Vgl. Council of Europe: Computer-Related Crime. Recommendation No. R 89 (9) on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg 1990, S. 66; Möhrenschlager, M.: Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland, in: Wistra 1991, S. 321–331 (326).

461) Vgl. Möhrenschlager ebd.

462) Vgl. z.B. Süddeutsche Zeitung vom 30. Januar 1997: Kriminalität im Internet ist besorgniserregend.

463) Vgl. Altenhain, K.: Die strafrechtliche Verantwortung für die Verbreitung mißbilligter Inhalte in Computernetzen, in CR 1997, S. 485–496 (485f).

464) Vgl. Sieber, U.: Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, in: Computer und Recht 1997, S. 581–598 sowie 653–669.

465) Vgl. Möhrenschlager, M.: Computer Crimes and Other Crimes against Information Technology in Germany, in: Sieber, U. (ed.): Information Technology Crimes. National Legislations and International Initiatives, Köln. u.a. 1994, S. 197–233 (200); Bundeskriminalamt (Hrsg.): Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Berichtsjahr 1995, Wiesbaden 1995, S. 251f.

466) Vgl. van der Merwe, D. P.: Computer Crimes and Other Crimes against Information Technoloy in South Africa, in: Sieber, U. (ed.): Information Technology Crime. National Legislations and International Initiatives, Köln. u.a. 1994, S. 421–425.

britischen Krankenhauses die ärztlichen Rezepte für die Patienten und machte so aus dem einem neunjährigen Jungen verordneten Medikament eine hochgiftige Rezeptur; Der Patient überlebte nur, weil eine aufmerksame Schwester die Manipulation bemerkte.[467]) Ähnlich schlimme Folgen wie die Manipulation von medizinischen Daten können Angriffe auf Flugleitsysteme oder militärische Computeranlagen haben. Angehörigen der amerikanischen Air-Force gelang es 1995, sieben Schiffe der amerikanischen Marine durch Veränderungen in Computernetzen in die Irre zu führen.[468])

Darüber hinaus ist die Begehung weiterer Delikte in Datennetzen vorstellbar. Mit dem zunehmenden Einsatz von Telekommunikationsnetzen zur Abwicklung finanzieller Transaktionen und der Schaffung „virtueller" Zahlungsmittel rückt zum Beispiel die Möglichkeit ihres Mißbrauch zu Zwecken der Geldwäsche in das Blickfeld.[469])

6. Täter

Der Bandbreite der in Telekommunikationsnetzen und mit Computertechnik begangenen Delikte entspricht die Vielfalt der möglichen Täter. Es kommen ebenso Studenten wie Terroristen und Täter aus dem Bereich der organisierten Kriminalität in Betracht; danach ist jede Person mit dem notwendigen Minimum an Fähigkeiten im Umgang mit den modernen Informations- und Kommunikationstechniken ein potentieller Täter, soweit sie sich durch technische Herausforderungen, die Möglichkeit eines finanziellen Gewinns, die Chance, bekannt zu werden, Rache zu nehmen oder weltanschauliche Überzeugungen zu verbreiten, motivieren läßt.[470]) Einer australischen Untersuchung zufolge kommen vor allem männliche Schüler, Studenten und in unterschiedlichen Berufen arbeitende Angestellte in Betracht, wobei das Alter der letzteren in der Regel zwischen 30 und 45 Jahren liege.[471]) Dabei macht offensichtlich vor allem die Gelegenheit Bürger zu Tätern: Personen, die über Insiderwissen verfügen, etwa Paßwörter kennen oder über besondere Zugriffsrechte verfügen, gelten als die größte Tätergruppe, wobei bereits 1992 Steigerungen auch der Anzahl von Taten prognostiziert wurde, die von nicht mit solchem Wissen ausgestatteten Tätern begangen werden.[472])

7. Bereits erfolgte Reformen

7.1 Materielles Strafrecht

Die Entwicklung der Computerkriminalität hat in Deutschland bereits zu zahlreichen Anpassungen des Strafrechts geführt. Im wesentlichen handelt es sich dabei um folgende Änderungen:

- In den Datenschutzgesetzen wurden die traditionellen Geheimschutzdelikte (z. B. Verletzung des Arztgeheimnisses) um datenschutzrechtliche Strafvorschriften erweitert.[473])
- Mit dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität[474]) wurden Maßnahmen gegen Wirtschaftsdelikte ergriffen, die im Zusammenhang mit den neuen Informations- und Kommunikationstechniken begangen werden können: Um Computermanipulationen erfassen zu können, wurden durch die Schaffung der Tatbestände des Computerbetrugs (§ 263a Strafgesetzbuch) und der Fälschung beweiserheblicher Daten (§ 269 StGB) bestehende Strafbarkeitslücken geschlossen und der Sachbeschädigungstatbestand (§ 303 Strafgesetzbuch) um die Tatbestände der Datenveränderung (§ 303a Strafgesetzbuch) und der Computersabotage (§ 303b Strafgesetzbuch) ergänzt. Zur Bekämpfung des Eindringens in fremde Computersysteme wurde mit § 202a Strafgesetzbuch eine Bestimmung geschaffen, die das Ausspähen von Daten unter Strafe stellt. Zum Schutz gegen Wirtschaftsspionage wurde darüber hinaus der Straftatbestand des Verrats von Geschäfts- und Betriebsgeheimnissen (§ 17 des Gesetzes gegen den unlauteren Wettbewerb) verschärft. Dem Schutz gegen unbefugtes Abhören von Telekommunikation dient § 94 in Verbindung mit. § 84 Telekommunikationsgesetz.[475])
- Verschiedene Gesetzesänderungen weiteten den strafrechtlichen Schutz des geistigen Eigentums aus. Von Bedeutung sind insofern insbesondere die zweite Urheberrechtsnovelle von 1985, das Produktpirateriegesetz von 1990[476]), das Urheberrechtsänderungsgesetz von 1993[477]) und die mit Art. 7 des Informations- und Kommunikationsdienstegesetzes eingeführten Änderungen zugunsten der Betreiber von Datenbanken. Weitere Anpassungen werden bei der Umsetzung der im Rahmen der World Intellectual Property Organisa-

---

467) Vgl. Der Spiegel vom 28. 2. 1994, S. 243.

468) Vgl. Sieber, U.: Mißbrauch der Informationstechnik und Informationsstrafrecht, Entwicklungstendenzen in der internationalen Informations- und Risikogesellschaft, in Tauss, J.; Kollbeck, J.; Mönikes, J.: Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik, Baden-Baden 1996, S. 608–651 (624).

469) Vgl. Flechsig, N. P.: Strafrechtlich relevantes Verhalten im Internet, in: Schwarz, Matthias (Hrsg.): Recht im Internet, Stand Juli 1997, 8.2.1., S. 6.

470) Vgl. United Nations Manual on the Prevention and Control of Computer-Related Crime, in: International Review of Criminal Policy 1994; abrufbar unter http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html, Ziffern 32ff.

471) Vgl. Hayward, I. J.; Sullivan, P. J.: A Profile of a Computer Criminal, abrufbar unter http://westgate.vut.edu.au/~ianh/interpol96.html.

472) Vgl. United Nations Manual on the Prevention and Control of Computer-Related Crime, in: International Review of Criminal Policy 1994; abrufbar unter http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html, Ziffer 35 sowie Council of Europe: Computer-Related Crime. Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg 1990, S. 19.

473) Vgl. § 43 Bundesdatenschutzgesetz.

474) BGBl. I 1986, S. 721.

475) BGBl. I 1996, S. 1120–1150.

476) BGBl. I 1990, S. 422.

477) BGBl. I 1993, S. 910.

tion im Dezember 1996 geschlossenen Verträge folgen.[478])

- 1974 wurde der Schriftenbegriff angepaßt, auf den die Verbreitungsdelikte verweisen: Die allgemeine Vorschrift des § 11 Abs. 3 Strafgesetzbuch wurde um einen Passus ergänzt, nach dem „Ton- und Bildträger, Abbildungen und andere Darstellungen" den Schriften gleichstehen.[479]) Weitere durch die technische Entwicklung notwendig gewordene Änderungen wurden 1997 mit dem Informations- und Kommunikationsdienstegesetz[480]) eingefügt; nach Art. 4 dieses Gesetzes sind den Schriften neben den oben genannten Darstellungsformen auch Datenspeicher gleichgestellt. Zudem kann der Tatbestand des § 86 Strafgesetzbuch (Verbreiten von Propagandamitteln verfassungswidriger Organisationen) aufgrund der durch das Informations- und Kommunikationsdienstegesetz herbeigeführten Änderungen auch durch das Zugänglichmachen einschlägigen Materials in Datenspeichern verwirklicht werden und ist die Verbreitung bestimmten pornographischen Materials auch dann strafbar, wenn es kein tatsächliches, jedoch ein wirklichkeitsnahes Geschehen wiedergibt (vgl. § 184 Abs. 4, 5 StGB).

- Ebenfalls durch das Informations- und Kommunikationsdienstegesetz sowie durch den in dieser Hinsicht gleichlautenden Mediendienstestaatsvertrag geregelt wurde die zuvor kontrovers diskutierte Frage der Verantwortlichkeit von Service-Providern für die auf ihren Computersystemen und Datennetzen transportierten Inhalte. Nach den Haftungsbestimmungen dieser Regelungswerke ist die Verantwortlichkeit wie folgt geregelt:

  1. Für eigene Inhalte, die sie zur Nutzung bereithalten, sind die Diensteanbieter nach den allgemein geltenden Bestimmungen verantwortlich.

  2. Für fremde Inhalte, die sie zur Nutzung bereithalten, sind die Diensteanbieter nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern.

  3. Für fremde Inhalte, zu denen die Diensteanbieter lediglich den Zugang zur Nutzung vermitteln, sind sie nicht verantwortlich. Als Zugangsvermittlung in diesem Sinne gilt auch die automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund von Nutzerabfrage etwa auf sogenannten Proxy-Servern.

- Durch das am 1. Januar 1998 in Kraft getretene Begleitgesetz zum Telekommunikationsgesetz wurde der Schutz des Fernmeldegeheimnisses (zuvor § 354 Strafgesetzbuch) in einem neuen § 206 Strafgesetzbuch erweitert und verschärft. Geschützt werden durch § 206 Strafgesetzbuch nicht mehr nur die Inhalte von Telekommunikation, sondern auch „ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war." Eingeschränkt ist der Schutz allerdings nach wie vor dadurch, daß nur der Bruch des Fernmeldegeheimnisses durch Personen unter Strafe gestellt wird, die entweder Inhaber, Mitarbeiter oder Beauftragte eines Telekommunikationsunternehmens sind oder aber Aufgaben der Aufsicht über ein Telekommunikationsunternehmen wahrnehmen.

7.2 Strafverfahrensrecht

Verfahrensrechtliche Rechtsgrundlage für die Überwachung der Telekommunikation sind §§ 100a, 100b Strafprozeßordnung. Die mit dem G-10-Gesetz eingefügten Bestimmungen sind bereits seit 1968 in Kraft.[481]) Sie sind seither zahlreichen Änderungen unterworfen worden, die vor allem der Bekämpfung bestimmter Kriminalitätsformen dienen, welche aufgrund des arbeitsteiligen Zusammenwirkens mehrerer Täter oder ganzer Tätergruppen die Telekommunikation in besonderem Maße einsetzen.[482])

Nach §§ 100a, 100b Strafprozeßordnung ist die Überwachung und Aufzeichnung des Fernmeldeverkehrs bei Verdacht auf die Begehung abschließend aufgezählter Straftaten aufgrund richterlicher Anordnung – bei Gefahr im Verzug auch aufgrund staatsanwaltschaftlicher Anordnung – zulässig. Ob diese Bestimmungen auch moderne Formen der Telekommunikation wie email und andere Formen der computergestützten Kommunikation über das öffentliche Fernsprechnetz erfassen, war umstritten.[483]) Durch das Telekommunikationsbegleitgesetz wurde der Begriff des Fernmeldeverkehrs durch den der Telekommunikation ersetzt und insofern Klarheit geschaffen; der Begriff der Telekommunikation umfaßt nach der Legaldefinition des § 3 Nr. 16 Telekommunikationsgesetz den „technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen". Erfaßt wird aufgrund der durch das Telekommunikationsbegleitgesetz herbeigeführten Änderungen nunmehr auch Telekommunikation innerhalb geschlossener Benutzergruppen, also der Telekommunikationsverkehr in nichtöffentlichen Netzen, etwa betriebsinternen Anlagen.[484]) Diese schieden zuvor als Überwachungsobjekte aus.[485])

---

[478]) Vgl. zur Umsetzung dieser Verträge die Informationen über den Vorschlag für eine EG-Richtlinie, abrufbar unter http://www.europa.eu.int/comm/dg15/en/intprop/intprop/1100.html

[479]) BGBl. I 1974, S. 474.

[480]) BGBl. I 1997, S. 1870–1880.

[481]) BGBl I 1968, S. 949–952.

[482]) Vgl. die Nachweise in: Schönfelder: Deutsche Gesetze, zu § 100a StPO.

[483]) Vgl. Karlsruher Kommentar zur Strafprozeßordnung, 3. Aufl., München 1993, § 100a (Nack), RdNr. 2; Bär, W.: Polizeilicher Zugriff auf kriminelle Mailboxen, in: Computer und Recht 1995, S. 489–500; kritisch Eisenberg U.; Nischan, A.: Strafprozessualer Zugriff auf digitale multimediale Videodienste, in: JZ 1997, S. 74–83 (79); Herzog; B., wistra 1994, S. 86f.

[484]) Vgl. BT-Drs. 13/8016 vom 23. 06. 1997, Begründung zu Art. 2 Abs. 9 Nr. 4 Buchstabe c.

[485]) Vgl. Kleinknecht/Meyer/Meyer-Goßner: Strafprozeßordnung, 43. Auflage, München 1997, § 100a, RdNr. 2.

Die technische Umsetzung der nach den Bestimmungen der Strafprozeßordnung – und nach dem Gesetz zu Artikel 10 Grundgesetz sowie dem Außenwirtschaftsgesetz – zulässigen Überwachungsmaßnahmen ist in § 88 Telekommunikationsgesetz geregelt. Danach sind die technischen Einrichtungen, welche die Überwachung ermöglichen, von den Betreibern der Telekommunikationsanlage auf eigene Kosten zu gestalten und vorzuhalten, wobei die technische Gestaltung der Genehmigung der Regulierungsbehörde bedarf und in einer Rechtsverordnung näher bestimmt werden soll.

Für die Bekämpfung der Kriminalität in Netzen sind weiter §§ 102, 103 Strafprozeßordnung von Bedeutung, welche die Durchsuchung bei Verdächtigen und Dritten und damit die Inbetriebnahme der ihnen gehörenden EDV-Anlagen erlauben.[486]) Problematisch ist, ob diese Rechtsgrundlagen auch dazu berechtigen, mit einem in der Wohnung oder dem Unternehmen des Verdächtigen oder eines Dritten befindlichen Computers an Dateien zu gelangen, die auf anderen Rechnern gespeichert sind;[487]) zu verneinen ist dies aufgrund des Territorialitätsprinzips in der Regel jedenfalls dann, wenn dieser Rechner im Ausland stationiert ist.[488])

Neben die Möglichkeit der Überwachung des Fernmeldeverkehrs und der Durchsuchung tritt die Befugnis der Strafverfolgungsbehörden zur Beschlagnahme nach §§ 94 ff Strafprozeßordnung. Beschlagnahmt werden dürfen nur körperliche Gegenstände – dazu zählen auch Computersysteme und Datenspeicher.[489]) Unter engen Voraussetzungen dürfen beschlagnahmte Dateien mit Dateien der Strafverfolgungsbehörden abgeglichen werden (sogenannte Rasterfahndung, vgl. §§ 98a ff Strafprozeßordnung).[490])

8. Aktueller Reformbedarf im deutschen Recht

8.1 Materielles Strafrecht

Die bereits erfolgten Anpassungen und Ergänzungen der Tatbestände im Besonderen Teil des Strafgesetzbuchs haben erkannte Strafbarkeitslücken in Bereich der Computerkriminalität weitgehend geschlossen.[491]) Im Urheberrechtsschutz noch bestehende Defizite werden im Zuge der Umsetzung der Verträge[492]) der Welturheberrechtsorganisation (World Intellectual Property Organization) behoben werden. Im Bereich des materiellen Strafrechts besteht daher nach dem gegenwärtigen Erkenntnisstand kein dringender Reformbedarf. Geprüft werden sollte allerdings, ob und inwieweit das Freisetzen von Computerviren und Wurmprogrammen unter Strafe gestellt werden soll.[493]) Dabei sollten jedoch die Schwierigkeiten der Durchsetzung eines solchen Straftatbestandes berücksichtigt werden.[494]) Untersucht werden sollte zudem, ob gegen das Freisetzen von Computerviren und ähnlichen Programmen nicht bereits durch § 303a Strafgesetzbuch (Datenveränderung) und § 303b Strafgesetzbuch (Computersabotage) hinreichender Schutz gewährt wird.

Die allgemeinen Regelungen für die Verantwortlichkeit für Straftaten in Telekommunikationsnetzen bedürfen nach dem derzeitigen Erkenntnisstand keiner Modifizierung. Die Enquete-Kommission ist der Auffassung, daß die in § 5 Teledienstegesetz und im Mediendienstestaatsvertrag getroffenen Regelungen grundsätzlich sachgerecht sind. Sie weist aber darauf hin, daß die Abgrenzung zwischen den beiden Regelungswerken in der wissenschaftlichen Literatur als problematisch angesehen wird.[495]) Die Enquete-Kommission empfiehlt daher, die praktische Umsetzung dieser Regelungen durch Staatsanwaltschaften und Gerichte aufmerksam zu verfolgen, um gegebenenfalls korrigierend eingreifen zu können. Das gilt insbesondere für die Frage, ob und inwieweit auch die im Mediendienstestaatsvertrag enthaltenen Privilegierungen die gewünschten Auswirkungen für die strafrechtliche Haftung von Betreibern von Mediendiensten haben. Dies ist aus kompetenzrechtlichen Gründen nicht unumstritten.[496]) Das kann erhebliche Konsequenzen haben. Denn greift die Privilegierung für Anbieter von Mediendiensten mangels einer entsprechenden Gesetzgebungskompetenz der Länder im Hinblick auf die strafrechtliche Haftung nicht, würde dies bei der Rechtsanwendung zu der schwierigen Abgrenzung zwischen Tele- und Mediendiensten zwingen, die durch die im wesentlichen gleichlautenden Formulierungen von Teledienstegsetz und den entsprechenden Bestimmungen im Mediendienstestaatsvertrag vermieden werden sollte. Das hat möglicherweise Rechtsunsicherheit zur Folge, welche die weitere Entwicklung der neuen Dienste in der Bundesrepublik behindern kann.

Wichtig erscheint der Kommission unabhängig davon, daß die privilegierenden Regelungen in Teledienstegesetz und Mediendienstestaatsvertrag auch auf das Setzen sogenannter Hyperlinks Anwendung

---

[486]) Vgl. Kleinknecht/Meyer/Meyer-Goßner, ebd., § 102, RdNr. 10a.

[487]) Vgl. Möhrenschlager, M.: Computer Crimes and Other Crimes against Information Technology in Germany, in: Sieber, U. (ed.): Information Technology Crimes. National Legislations and International Initiatives, Köln. u.a. 1994, S. 197–233 (228).

[488]) Vgl. Bär, W.: Durchsuchungen im EDV-Bereich (II), in: Computer und Recht 1995, S. 227–234 (232 ff).

[489]) Vgl. Möhrenschlager a.a.O.

[490]) Vgl. Kleinknecht/Meyer/Meyer-Goßner, a.a.O., § 94, RdNr. 4; § 98a RdNr. 9f.

[491]) Vgl. Vassilaki, I. I.: Multimediale Kriminalität, Computer und Recht 1997, S. 297–302 (300); Sieber, U.: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2), JZ 1996. S. 494–507 (506).

[492]) abrufbar unter http://www.wipo.int.

[493]) Vgl. Dannecker, G.: Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, in: Betriebsberater 1996, S. 1285–1294 (1291).

[494]) Vgl. Brunnstein, K.: Computerviren und andere bösartige Software – Tschernobyl der Informationstechnik, in Computer und Recht 1993, S. 456–462 (462)..

[495]) Vgl. Kröger, D.; Moos, F.: Mediendienst oder Teledienst? Zur Aufteilung der Gesetzgebungsmaterie Informations- und Kommunikationsdienste zwischen Bund und Ländern, in: AfP 1997, S. 675–680.

[496]) Vgl. Koch, F. A.: Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen, in: Computer und Recht 1997. S. 193–203 (198).

finden, mit denen im Internet auf Dokumente auf anderen WWW-Seiten verwiesen wird.[497]) Denn die Möglichkeit der Verweisung mit Hyperlinks ist einer der wichtigsten Vorteile der Vernetzung von Computern und sollte möglichst wenig eingeschränkt und mit rechtlichen Risiken belastet werden.

8.2 Strafverfahrensrecht

Der Überprüfung bedarf nach Auffassung der Enquete-Kommission jedoch das Strafverfahrensrecht. Dieses muß den Erfordernissen des Informationszeitalters und der in diesem gegebenen Möglichkeiten der Deliktsbegehung gerecht werden. Wichtig ist, daß es die Unkörperlichkeit von Informationen und das Recht auf informationelle Selbstbestimmung angemessen berücksichtigt.[498]) Beispielhaft seien folgende Punkte genannt:

- § 94 Strafprozeßordnung (Gegenstand der Beschlagnahme) erlaubt seinem Wortlaut nach eine Sicherstellung und Beschlagnahme körperlicher Gegenstände. In Betracht kommen bewegliche Sachen jeglicher Art, auch Magnetbänder oder sonstige Datenträger. Das zwingt die Strafverfolgungsbehörden unter Umständen zu der Beschlagnahme von Datenträgern, die auch andere als die beweisrelevanten Informationen enthalten können. Nach einer im Schrifttum geäußerten Auffassung besteht dadurch in vielen Fällen die Gefahr, daß die Gewinnung beweisrelevanter Informationen mit einem erheblichen Eingriff in das informationelle Selbstbestimmungsrecht unbeteiligter Dritter verbunden ist [499])

  Richtig ist, daß durch Sicherstellung und Beschlagnahme in grundrechtlich geschützte Positionen der Betroffenen eingegriffen wird. § 94 Strafprozeßordnung enthält die dafür erforderliche gesetzliche Ermächtigung. Der Eingriff findet jedoch seine Grenze in dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Dieser gebietet es, das beschlagnahmte Material unverzüglich durchzusehen und Materialien, denen keine Beweisbedeutung zukommt, zurückzugeben. Darüber hinaus wird der Betroffene vor einer Sicherstellung oder förmlichen Beschlagnahme regelmäßig von den Strafverfolgungsbehörden dazu angehalten werden, die Beschlagnahme durch eine freiwillige Herausgabe des beweisrelevanten Materials abzuwenden, also einzelne Dateien kopieren zu lassen. Die im Schrifttum gesehene Gefahr von erheblichen Eingriffen in das informationelle Selbstbestimmungsrecht unbeteiligter Dritter dürfte daher in der Praxis gering sein. Die Enquete-Kommission empfiehlt dennoch, aufmerksam zu beobachten, ob und inwieweit die §§ 94 ff Strafprozeßordnung einer Anpassung an die Erfordernisse der Datenverarbeitung mit Hilfe der neuen Informations- und Kommunikationstechniken bedürfen.

- Prüfungsbedarf besteht auch bei den Überwachungsbefugnissen der Strafverfolgungsbehörden nach § 100a Strafprozeßordnung (Überwachung des Fernmeldeverkehrs). Denn mit der prognostizierten Zunahme der Telekommunikation dürfte sich der Anwendungsbereich dieser Vorschrift erheblich vergrößern. Wenn etwa mehr Briefe elektronisch verfaßt und verschickt werden, wird die herkömmliche Postbeschlagnahme nach §§ 94, 99 Strafprozeßordnung an Bedeutung verlieren und die Überwachungsbefugnis nach § 100a Strafprozeßordnung an Bedeutung gewinnen. Das bedeutet zum einen, daß die Überwachung an erheblich strengere Voraussetzungen gebunden ist, da die Überwachungsbefugnis des § 100a Strafprozeßordnung nur beim Verdacht auf die Begehung von bestimmten schwereren Straftaten besteht, während für die herkömmliche Postbeschlagnahme solche Voraussetzungen nicht vorliegen müssen. Andererseits ist nicht zu verkennen, daß digitalisierte Information – etwa mit Hilfe von Suchprogrammen – erheblich besser überwacht und ausgewertet werden kann als traditionelle Kommunikationsformen.[500]) Ob und inwieweit sich aus diesen Umständen Änderungsbedarf ergibt, kann derzeit noch nicht abgesehen werden. Die Kommission empfiehlt, die Entwicklung aufmerksam zu beobachten und gegebenenfalls korrigierend einzugreifen.

- Auch in anderer Hinsicht bedarf § 100a Strafprozeßordnung möglicherweise der Modifizierung. Nach der gegenwärtigen Rechtslage ist die Überwachung des Fernmeldeverkehrs zwar etwa bei Verdacht auf gewerbsmäßige Hehlerei oder schwere Brandstiftung möglich, nicht aber bei Verdacht auf die Verwirklichung von Straftatbeständen, die dem Schutz der Datensicherheit dienen. Der Europarat empfiehlt angesichts des großen Gefährdungspotentials von bestimmten Begehungsformen der Computerkriminalität, auch bei besonders schweren Fällen der Computerkriminalität eine Befugnis der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs vorzusehen.[501]) Auf andere Weise ließen sich in Computersystemen und mit Hilfe von Computertechnik begangene Straftaten in vielen Fällen kaum wirksam bekämpfen.[502]) Wird eine entsprechende Ausweitung des Straftatenkatalogs des § 100a StPO für notwendig erachtet, sollte allerdings geprüft werden, ob er an anderer Stelle reduziert werden kann.

- Soweit die §§ 102 ff StPO die Durchsuchung der Wohnung von Verdächtigen und Dritten zulassen, kann zwar als gesichert gelten, daß diese Ermäch-

[497]) Vgl. dazu Eichler, A.; Helmers, S.; Schneider, T.: Link(s) – Recht(s). Technische Grundlagen und Haftungsfragen bei Hyperlinks, in: Betriebsberater 1997, Heft 48, Supplement Kommunikation & Recht, S. 23–26 (24f).

[498]) Vgl. Dannecker, G.: Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, in: Betriebsberater 1996, S. 1285–1294 (1292).

[499]) Vgl. Bär, W.: Der Zugriff auf Computerdaten im Strafverfahren, Köln u. a. 1992, S. 276.

[500]) Vgl. Bär, W., ebd., S. 276, 336.

[501]) Vgl. Council of Europe: Problems of criminal procedural law connected with information technology. Recommendation No. R (95) 13 and explanatory memorandum, Straßbourg 1996, S. 48, Ziffern 124, 125.

[502]) Vgl. ebd.

tigung auch die Inbetriebnahme und Durchsuchung von in der Wohnung befindlichen EDV-Anlagen einschließt.[503]) Fraglich ist jedoch, ob sie auch die mittels dieser EDV-Anlage betriebene Suche nach Informationen auf anderen Rechnern erfaßt, etwa auf dem in anderen Räumlichkeiten befindlichen Zentralrechner.[504]) Soweit dies verneint wird, führt das bei Computernetzwerken, an die Rechner an verschiedenen Standorten angeschlossen sind, möglicherweise zu der Konsequenz, daß ein Durchsuchungsbefehl auch für andere Räumlichkeiten erlangt werden muß, in dem ein an ein Computernetz angeschlossener Rechner vermutet wird.[505]) Dementsprechend müssen unter Umständen aufwendige Recherchen über Rechnerstandorte angestellt und entsprechende Durchsuchungsanordnungen beantragt und erlassen werden, um die dem Verdächtigen zur Verfügung stehenden Speichermöglichkeiten insgesamt durchsuchen zu können. Das ist jedenfalls dann unbefriedigend, wenn erst bei einer Durchsuchung festgestellt wird, daß ein Anschluß an ein Computernetz besteht. Denn in diesem Fall müßte möglicherweise erhebliche Zeit aufgewendet werden, um herauszufinden, wo sich die anderen Rechner befinden, und entsprechende Durchsuchungsanordnungen zu erlassen.[506]) Zwar ist das Problem dadurch entschärft, daß bei Gefahr in Verzug auch Staatsanwaltschaft und Polizei Durchsuchung und Beschlagnahme anordnen dürfen. Dennoch ist fraglich, ob und inwieweit die herkömmlichen Mitteln des Strafverfahrensrechts ausreichen oder möglicherweise eine unabhängig von bestimmten Räumlichkeiten geschaffene Möglichkeit zur Durchsuchung jedenfalls von geschlossenen, lokalen Computernetzen (Local Area Nets, LANs) innerhalb des Zuständigkeitsbereichs der deutschen Strafverfolgungsbehörden.[507]) geschaffen werden sollte. Dies wird freilich erst nach einer intensiven Auseinandersetzung mit den in der Praxis gemachten Erfahrungen geklärt werden können. Die Enquete-Kommission empfiehlt daher, zu überprüfen, ob die Durchsuchungsbefugnisse der Strafverfolgungsbehörden im Hinblick auf Computernetze ausreichend sind oder erweitert werden müssen.

- Fraglich ist auch, ob die aktiven Mitwirkungspflichten insbesondere von Zeugen einer Anpassung bedürfen. Nach der derzeit geltenden Rechtslage hat ein Zeuge lediglich die Pflicht, vor Gericht zu erscheinen, wahrheitsgemäße Angaben zu machen und seine Aussage gegebenenfalls zu beeiden. Ihn trifft dagegen keine Verpflichtung, sich auf die Vernehmung vorzubereiten oder gar Erkundigungen einzuholen.[508]) Auf eine solche Mitwirkung sind die Strafverfolgungsbehörden nach Stimmen in der wissenschaftlichen Literatur im Bereich der Computerkriminalität jedoch häufig angewiesen, wenn sie der Hilfestellung bei der Inbetriebnahme von EDV-Anlagen – etwa Informationen über Paßwortinhaber oder technische Anleitungen – bedürfen oder Informationen über gespeicherte Daten benötigen.[509]) Aus Sicht der Enquete-Kommission ist jedoch zweifelhaft, ob dies dazu zwingt, die Zeugenpflichten entsprechend zu erweitern. Denn zum einen stellt sich die Frage nach den Mitteln der Durchsetzung der so erweiterten Pflichten. Und zum anderen haben die Strafverfolgungsbehörden auch andere Möglichkeiten als die Zeugenaussage, um die benötigten Informationen zu erhalten.
- Notwendig sind weiter verfahrensrechtliche und organisatorische Schutzvorkehrungen für den Umgang mit personenbezogenen Daten, die im Zusammenhang mit einem Ermittlungsverfahren erlangt worden sind. Diese Defizite sollen mit den derzeit in der parlamentarischen Beratung befindlichen Entwürfen eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (BT-Drs. 13/194; 13/9718) behoben werden. Um die Unsicherheiten für die Betroffenen wie für die Strafverfolgungsbehörden schnell auszuräumen, empfiehlt die Enquete-Kommission ein möglichst rasches Handeln des Gesetzgebers.

9. Weitergehende Probleme und Lösungsvorschläge

Über die beschriebenen Probleme im Strafverfahrensrecht, die durch den deutschen Gesetzgeber gelöst werden können, hinaus bestehen weitere Probleme, die völkerrechtlicher und außerrechtlicher Lösungen bedürfen. Zum einen ist fraglich, inwieweit deutsches Strafrecht auf Delikte in Datennetzen anwendbar ist. Zum anderen stellen sich Probleme bei dem Nachweis und der Verfolgung von Straftaten in Netzen.

9.1 Anwendungsprobleme

Die Globalität des Informationsflusses in den weltumspannenden Datennetzen erzeugt Probleme bei der Anwendung eines grundsätzlich auf ein bestimmtes Territorium bezogenen Rechtssystems.[510]) Zwar gilt das deutsche Strafrecht nach §§ 3–7 Strafgesetzbuch auch für im Ausland begangene Straftaten, soweit inländische oder international geschützte Rechtsgüter – zu denen auch das Interesse an der Verhinderung der Verbreitung sogenannter harter Pornografie zählt – betroffen sind oder ein Deutscher Täter oder Opfer einer Straftat ist. Darüber hinaus ist

503) Vgl. Kleinknecht/Meyer/Meyer-Goßner: Strafprozeßordnung, 43. Auflage, München 1997, § 102, RdNr. 10a.
504) Vgl. Möhrenschlager, M.: Computer Crimes and Other Crimes against Information Technology in Germany, in: Sieber, U. (ed.): Information Technology Crimes. National Legislations and International Initiatives, Köln. u.a. 1994, S. 197–233 (228); Bär, Der Zugriff auf Computerdaten im Strafverfahren, S. 217ff.
505) Vgl. Bär, W.: Durchsuchungen im EDV-Bereich (II), in: Computer und Recht 1995, S. 227–234.
506) Vgl. Council of Europe: Problems of criminal procedural law connected with information technology. Recommedation No. R (95) 13 and explanatory memorandum, Straßbourg 1996, S. 33, Ziffer 71.
507) Vgl. ebd. S. 7, Ziffer I.3.
508) Vgl. Bär, W.: Der Zugriff auf Computerdaten im Strafverfahren, S. 375ff m.w.N.
509) Vgl. ebd., S. 375 ff, 504ff.
510) Vgl. zum Territorialitätsprinzip oben 4.2.

deutsches Strafrecht nach § 3 Strafgesetzbuch anwendbar, wenn die Tat im Inland begangen ist, also der Tatort im Inland liegt. Und dies ist nach § 9 Abs. 1 Strafgesetzbuch bereits dann der Fall, wenn der zu einem Straftatbestand gehörende Verletzungserfolg in Deutschland eintritt oder nach der Vorstellung des Täters eintreten sollte.

Die Anwendung dieses in § 9 Strafgesetzbuch aufgestellten Ubiquitätsprinzips auf innerhalb der weltumspannenden Telekommunikationsnetze begangene Straftaten führt zu Schwierigkeiten insbesondere bei den sogenannten Verbreitungsdelikten wie etwa dem Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 Strafgesetzbuch).[511]) Einerseits kann es für die Anwendbarkeit deutschen Strafrechts allein nicht ausreichen, daß ein Internetangebot – ebenso wie in anderen Ländern – auch in Deutschland abgerufen werden kann.[512]) Denn damit würde sich die Bundesrepublik Deutschland anmaßen, ihre Rechtsvorstellungen der übrigen Welt aufzuzwingen. Als die Staatsanwaltschaft München 1995 gegen den Internetprovider CompuServe vorging und dieser daraufhin 200 Newsgroups sperren ließ, kam es weltweit zu Protesten.[513]) Andererseits fällt es schwer, zu akzeptieren, daß es straflos bleiben soll, wenn vom Ausland aus gezielt Inhalte eingespeist werden, deren Verbreitung nach deutschem Strafrecht strafbar ist.

Die Enquete-Kommission ist der Auffassung, daß den Problemen bei der Anwendung deutschen Strafrechts eher durch eine Einschränkung als durch eine Ausweitung seines Anwendungsbereichs begegnet werden sollte. Andernfalls besteht die Gefahr von Konflikten mit anderen Staaten und ihren Bürgern[514]) – die Tatsache, daß etwa die Leugnung des Holocaust in Deutschland eine Straftat darstellt, in den Vereinigten Staaten von Amerika dagegen als vom Grundrecht auf Meinungsfreiheit gedeckt angesehen wird,[515]) vermag dies schlaglichtartig zu beleuchten. Hinzu kommt die Gefahr, daß strafrechtliche Ge- und Verbote immer weniger durchgesetzt werden können und dadurch die Abschreckungsfunktion des Strafrechts und der Strafverfolgung beeinträchtigt wird.

Einer gesetzgeberischen Initiative, die diesen Überlegungen Rechnung trägt, bedarf es nach Meinung der Enquete-Kommission jedoch zumindest zunächst noch nicht. Entgegen einem im Schrifttum vielfach geweckten Eindruck[516]) kann das Problem der Anwendbarkeit deutschen Strafrechts gerade auf Verbreitungsdelikte nämlich bereits auf der Basis des bestehenden Rechts durch eine restriktive Auslegung gelöst werden. Denn diese Delikte gehören fast durchweg der Kategorie der sogenannten abstrakten Gefährdungsdelikte an, die nach ganz herrschender Meinung keinen zum Tatbestand gehörenden Verletzungserfolg im Sinne von § 9 Strafgesetzbuch aufweisen.[517]) Da mithin in Deutschland auch kein Tatort begründet wird, wenn etwa eine kanadische Internetseite eine Volksverhetzung im Sinne von § 130 Strafgesetzbuch enthält, kann deutsches Strafrecht auf diese Delikte in der Regel nur unter den Voraussetzungen des § 7 Strafgesetzbuch angewendet werden. Dazu muß die Tat allerdings auch nach dem Recht des Staates strafbar sein, in dem sie begangen wurde. Ist dies der Fall, dürfte die Möglichkeit von Konflikten mit dem ausländischen Staat weitgehend ausgeschlossen sein. Die Enquete-Kommission empfiehlt gleichwohl, die Praxis der Staatsanwaltschaften und der Gerichte aufmerksam zu verfolgen, um gegebenenfalls mit dem Ziel korrigierend eingreifen zu können, Konflikte mit den Rechtsordnungen ausländischer Staaten zu vermeiden.

Notwendig sind zugleich Bemühungen um internationale Standards auf dem Gebiet des materiellen Strafrechts. Nur mit einer internationalen Harmonisierung des Strafrechts kann schrittweise das Strafbarkeitsgefälle abgebaut werden, das es heute ermöglicht, in den globalen Datennetzen Straftaten von Staaten aus zu begehen, die keine entsprechenden strafrechtlichen Bestimmungen kennen. Will man verhindern, daß es „Internetoasen" für Straftäter gibt, setzt dies freilich eine weltweite Einigung auf einen gewissen Grundbestand rechtlicher Vorschriften voraus. Schritte in diese Richtung sind auf internationaler Ebene insbesondere im Rahmen der OECD unternommen worden.[518]) Die Europäische Kommission hat einen Aktionsplan zur sicheren Nutzung des Internet vorgelegt, in dem unter anderem auch rechtliche Maßnahmen vorgesehen sind.[519]) Darüber hinaus wird auf europäischer Ebene derzeit im Auftrag des Europarates u. a. an einem Modell-

[511]) Vgl. Hilgendorf, E.: Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter des Internet, NJW 1997, S. 1873–1878.

[512]) Vgl. Engel, C.: Inhaltskontrolle im Internet, AfP 1996, 220–227 (225).

[513]) Vgl. Hilgendorf, E.: Überlegungen zur strafrechtlichen Interpretation des Ubiqutitätsprinzips im Zeitalter des Internet, NJW 1997, S. 1873–1878 (1874).

[514]) Vgl. BBC-News vom 11. Dezember 1997: G8 wages war on cyber-crime, abrufbar unter http://news.bbc.co.uk, zum deutschen Recht mit den Worten: „But aside from the fact that the law does not stop Germans accessing banned materials from sites broadcast outside national borders, many Americans believe their approach smacks of censorship".

[515]) Vgl. Ringel, K.: Rechtsextremistische Propaganda aus dem Ausland im Internet, in: Computer und Recht 1997, S. 302–307 (307) m. w. N.; zur amerikanischen Rechtsprechung zu pornographischen Inhalten Wiegandt, M. H.: Die Zulässigkeit von Pornographie als Maßstab der Freiheit oder die nackte Halbwahrheit, in: NJW 1997, S. 1352–1354; Roellecke, G.: Der Rechtsstaat für einen Störer! – Erziehung vs. Internet?, in: NJW 1996, S. 1801–1802.

[516]) Vgl. etwa Beisel, D.; Heinrich, B.: Die Zulässigkeit der Indizierung von Internet-Angeboten und ihre strafrechtliche Bedeutung, in: Computer und Recht 1996, S. 360–363 (363) sowie die Nachweise bei Hilgendorf, E.: Überlegungen zur strafrechtlichen Interpretation des Ubiquititätsprinzips im Zeitalter des Internet, NJW 1997, S. 1873–1878 (1875).

[517]) Vgl. Ringel, K.: Rechtsextremistische Propaganda aus dem Ausland im Internet, in: Computer und Recht 1997, S. 302–307 (303) m. w. N.

[518]) Vgl. dazu die Mitteilung der EG-Kommission an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen: Aktionsplan zur Förderung der sicheren Nutzung des Internet, S. 19.

[519]) Vgl. – auch zu weiteren Aktivitäten der EU – die Mitteilung der EG-Kommission an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen: Aktionsplan zur Förderung der sicheren Nutzung des Internet, S. 2f, 12.

strafgesetzbuch gearbeitet,[520]) und das Legal Advisory Board der Europäischen Kommission will bald eine umfassende Studie zum Thema Computerkriminalität vorlegen.[521]) Erste Ansätze zu einer internationalen Harmonisierung des materiellen Rechts finden sich auch in dem im Dezember 1997 von den Justiz- und Innenenministern der G-8-Staaten aufgestellten Aktionsplan[522]) und dem Bericht der sogenannten Carnegie-Gruppe.[523])

Die Enquete-Kommission empfiehlt, diese Bemühungen nachhaltig zu unterstützen.

9.2 Nachweisprobleme

Nachweis- und Zurechnungsprobleme entstehen durch die in Telekommunikationsnetzen gegebenen Möglichkeiten anonymer, pseudonymer und verschlüsselter Kommunikation. Täter von Verbreitungsdelikten können auf ihre Person hinweisende Spuren etwa dadurch verwischen, daß sie beim Versand elektronischer Dokumente per email Anonymisierungsserver[524]) verwenden oder schlicht ihre Absenderadresse fälschen.[525]) Sie können zudem Verschlüsselungstechniken oder steganografische Verfahren einsetzen, um zum Beispiel pornografische oder rassistische Inhalte so zu übertragen, daß sie weder bei einer Überwachung des Fernmeldeverkehrs noch bei einer Durchsuchung als solche identifiziert werden könnten. Ebenso besteht die Möglichkeit auch andere Informationen verschlüsselt zu übermitteln, etwa Piraterieprodukte; selbst Sprachtelefonie kann mit Hilfe einfach zu bedienender und leicht erhältlicher Computerprogramme abhörsicher verschlüsselt werden. Auch das Eindringen in fremde Computersysteme läßt sich einem Täter häufig nur schwer nachweisen. Hinzu kommen rechtliche Schwierigkeiten: Konnte früher bei Hausdurchsuchungen der Nachweis einer Straftat oder der Beteiligung an einer Straftat durch das Auffinden von Adressenlisten oder anderen Dokumenten geführt werden, ist es heute möglich, Daten, die für die Polizei von Interesse sein könnten, auf einen Rechner im Ausland auszulagern und damit den auf das jeweilige Staatsgebiet beschränkten Zugriff der Strafverfolgungsbehörden zu verhindern.

Zur Verbesserung der Nachweisbarkeit und Zurechnung von Straftaten wird in der öffentlichen Diskussion vorgeschlagen, die Möglichkeiten der anonymen Kommunikation in Telekommunikationsnetzen einzuschränken.[526]) Notwendig seien Authentifizierungsmechanismen, die eine sichere Zuordnung von über Telekommunikationsnetze verbreiteten Informationen und in Telekommunikationsnetzen vorgenommenen Handlungen zulassen. Die damit notwendige Verpflichtung der Nutzer zur Verwendung bestimmter Verfahren könne durchgesetzt werden, indem man die Service- und Zugangsprovider gesetzlich dazu veranlaßte, ihre Kunden zur Verwendung dieser Verfahren anzuhalten und bei Verwendung anderer Verfahren von dem Verkehr in Telekommunikationsnetzen auszuschließen.[527]) Zugleich wird jedoch darauf hingewiesen, daß die Möglichkeit zu anonymer Kommunikation nicht völlig ausgeschlossen werden sollte, da auch ein berechtigtes Interesse eines Nutzers bestehen kann, seine Identität nicht preiszugeben – etwa aufgrund von Angst vor Repressalien oder mangelndem Vertrauen in den Umgang mit personenbezogenen Daten.[528]) Als Mittelweg wird ein Verbot echter Anonymität bei gleichzeitiger Ermöglichung der Verwendung von Pseudonymen vorgeschlagen, die unter bestimmten gesetzlichen Voraussetzungen von den Strafverfolgungsbehörden aufgedeckt werden dürfen.[529])

Hinzu kommen Vorschläge, die nicht lediglich die Möglichkeit anonymer Kommunikation, sondern auch die Möglichkeit zu verschlüsselter und damit absolut vertraulicher Kommunikation einschränken wollen. Diese Vorschläge gehen dahin, nur die Verwendung von solchen Verschlüsselungsverfahren zu erlauben, bei denen die Strafverfolgungsbehörden – etwa mit Hilfe eines hinterlegten Schlüssels – unter gesetzlich bestimmten Voraussetzungen die Möglichkeit zur Entschlüsselung haben.[530]) In den USA sind Bemühungen um eine entsprechende „Kryptoregulierung" bislang am öffentlichen Widerstand gescheitert.[531])

Die Enquete-Kommission meint, daß die mit den Fragen der anonymen und verschlüsselten Kommunikation zusammenhängenden Probleme aufgrund einer differenzierten Betrachtungsweise gelöst werden sollten:

- Nach Auffassung der Enquete-Kommission sollte nach dem gegenwärtigen Erkenntnisstand eine

---

[520]) Vgl. Sieber, U.: Memorandum für ein Europäisches Modellstrafgesetzbuch, in: JZ 1997, S. 369–381; Dannecker, G.: Strafrecht in der Europäischen Gemeinschaft. Eine Herausforderung für Strafrechtsdogmatik, Kriminologie und Verfassungsrecht, in: JZ 1996, S. 869–880.

[521]) Vgl. European Commission, Legal Advisory Board: Minutes of the meeting of 25 November 1996, abrufbar unter http://www2.echo.lu/legal/en/crime/minutes.html.

[522]) Vgl. Meeting of Justice and Interior Ministers of The Eight, December 9–10, 1997: Communiqué sowie Statement of Principles und Action Plan. Vgl. insbesondere Ziffer 3 des Aktionsplans.

[523]) Abrufbar unter http://www.iid.de

[524]) Vgl. Computer-Zeitung vom 26. September 1996: Dank Anonym-Remailern verlaufen die Datenspuren der Internet-Surfer im Sand; vgl. auch das Angebot unter http://www.anonymizer.com.

[525]) Vgl. Sieber, U.: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1), JZ 1996, S. 429–442 (431).

[526]) Vgl. Sieber, U.: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2), S. 506; Vassilaki, I. E.: Multimediale Kriminalität, a.a.O., S. 301.

[527]) Vgl. Vassilaki, ebd.

[528]) Vgl. Kommission der Europäischen Gemeinschaften: Illegale und schädigende Inhalte im Internet. Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß sowie den Ausschuss der Regionen, Brüssel, 16. Oktober 96, Kom (96) 487 end., S. 17.

[529]) Vgl. ebd.

[530]) Vgl. Hannoversche Allgemeine Zeitung vom 18. Dezember 1996: Peter Frisch, Präsident des Bundesamtes für Verfassungsschutz: „Wir müssen verschlüsselte Botschaften lesen können."

[531]) Vgl. die unter http://www.eff.org abrufbaren Dokumente zu diesem Thema.

Lösung nicht in einer allgemeinen Einschränkung der Möglichkeiten zur Verschlüsselung von Kommunikationsinhalten gesucht werden. Eine solche Regulierung, die etwa zur Verwendung von Verschlüsselungsverfahren zwingen würde, bei denen die Strafverfolgungsbehörden Zugriff auf den geheimen Schlüssel haben, würde jedenfalls bei der Kommunikation im Internet den mit ihr verfolgten Zweck nicht erreichen. Angesichts der Tatsache, daß Software zur Verschlüsselung von Nachrichten im Internet frei erhältlich ist, kann nicht erwartet werden, daß gerade Kriminelle sie nicht verwenden.[532]) Zudem würde ein Verbot der Verwendung bestimmter Verschlüsselungsprogramme nicht hinreichend effektiv überwacht und durchgesetzt werden können. Denn es besteht die Möglichkeit, mit einem nicht zugelassenen Verschlüsselungsprogramm verschlüsselte Nachrichten noch einmal mit einem zugelassenen Verschlüsselungsprogramm zu verschlüsseln und die Verwendung des nicht zugelassenen Verschlüsselungsprogramms dadurch zu verdecken.[533]) Hinzu kommt, daß Vertreter der Wirtschaft ernsthafte Bedenken gegen eine Kryptoregulierung geäußert haben; sie befürchten, daß durch die technische Umsetzung einer solchen Regelung Sicherheitslücken entstehen, die Industriespionage erleichtern könnte.[534]) Und schließlich sind deutsche Unternehmen dabei, sich auf dem Gebiet der Datensicherheit eine Spitzenposition zu erobern.[535]) Dieses Bemühen würde durch eine restriktive Regelung des Einsatzes Verschlüsselungstechniken behindert.

- Was die Möglichkeiten anonymer Kommunikation angeht, besteht ein Konflikt mit den Intentionen des Datenschutzrechts. Aus Sicht des Datenschutzes ist es sinnvoll, möglichst wenige personenbezogene Daten überhaupt entstehen zu lassen. Aus Sicht der Strafverfolgung führt der Grundsatz der individuellen Verantwortlichkeit eines jeden für sein Verhalten dagegen zu dem Schluß, daß Verhalten auch in Datennetzen zugerechnet können werden muß, der einzelne also identifiziert werden können muß. Ob und inwieweit dieser Konflikt zufriedenstellend aufgelöst werden kann, wird nicht zuletzt von der technischen Entwicklung abhängen. Soweit Maßnahmen zur Einschränkung der Möglichkeiten anonymer Kommunikation erwogen werden, sollte jedoch der Einsatz von Pseudonymen ermöglicht werden, deren Aufdeckung durch Unbefugte ausgeschlossen sein und den durch das Fernmeldegeheimnis aufgestellten Anforderungen entsprechen muß. In jedem Fall sollten Maßnahmen in enger internationaler Zusammenarbeit ergriffen werden, um der Globalität der Datennetze gerecht zu werden.[536]) Die auf dem Treffen der Justiz- und Innenminister der G-8-Staaten am 8.-12. Dezember 1997 abgegebene Grundsatzerklärung und der dort aufgestellte Aktionsplan stellen aus Sicht der Enquete-Kommission insofern einen wichtigen Schritt in die richtige Richtung dar[537])

- Kein geeignetes Mittel zur Verbesserung der Nachweismöglichkeiten ist nach Auffassung der Enquete-Kommission eine in der wissenschaftlichen Literatur diskutierte Vorverlagerung der Strafbarkeit von Taten, die in Telekommunikationsnetzen begangen werden können: Danach soll für eine Strafbarkeit die Möglichkeit der bloßen Gefährdung eines Rechtsguts ausreichend sein, da der Nachweis einer konkreten Rechtsgutverletzung häufig nicht zu führen ist. Erforderlich seien präzise Handlungspflichten, wobei Strafbestimmungen allerdings nur flankierend hinzutreten sollen.[538]) Im Ergebnis liefe dies auf die Einführung weiterer Tatbestände der sogenannten abstrakten Gefährdungsdelikte hinaus, die keine konkrete Rechtsgutverletzung voraussetzen, sondern die allgemeine Gefährlichkeit eines bestimmten Verhaltens als Anknüpfungspunkt für eine Strafbarkeit ausreichen lassen.[539])

  Die Enquete-Kommission empfiehlt insofern Zurückhaltung. Denn das Strafrecht als ultima ratio staatlichen Handelns sollte auch in der Informationsgesellschaft vor allem dem Schutz von Rechtsgütern vor Verletzungen dienen. Abstrakte Gefährdungsdelikten sollten schon aus diesem Grunde nur in Ausnahmefällen geschaffen werden.[540]) Dies gilt im Bereich der Computerkriminalität um so mehr, als auch die Einführung von abstrakten Gefährdungsdelikten die übrigen Anwendungs-[541]), Nachweis- und Verfolgungsprobleme nicht lösen kann und daher die Möglichkeiten der Verfolgung von Straftätern kaum erheblich verbessern würde.

---

[532]) Vgl. National Research Council, Computer Science and Telecommuncations Board: Cryptography's Role in Securing the Information Society, Washington, D.C., 1996, S. 303f.

[533]) Vgl. National Research Council, Computer Science and Telecommuncations Board: Cryptography's Role in Securing the Information Society, Washington, D.C., 1996, S. 303f.

[534]) Vgl. Süddeutsche Zeitung vom 24. November 1997: Soll der Staat einen „Zweitschlüssel" erhalten? Die deutsche Wirtschaft will ihre Daten weiterhin ohne Kontrolle und Einschränkung sichern.

[535]) Vgl. Frankfurter Rundschau vom 28. November 1997: „Immer einen Tick schneller als die Konkurrenten" – Software-Zwerg Brokat hat im Internet-Banking die Nase vorn/Metronet setzt Online-Zahlungssystem der Böblinger ein.

[536]) Vgl. Sieber, U.: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2), S. 506.

[537]) Vgl. Meeting of Justice and Interior Ministers of The Eight, December 9–10, 1997: Communiqué sowie Statement of Principles und Action Plan. Vgl. insbesondere Ziffern V., VI. und IX. der Grundsatzerklärung sowie Ziffern 7, 9 und 10 des Aktionsplans.

[538]) Vgl. Sieber, U.: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2), S. 506.

[539]) Vgl. Vassilaki, I.: Multimediale Kriminalität, in: Computer und Recht 1997, S. 297–302 (301).

[540]) Vgl. Hassemer, W.: Symbolisches Strafrecht und Rechtsgüterschutz, in: NStZ 1989, S. 553–559.

[541]) Vgl. zur Anwendbarkeit deutschen Strafrechts bei abstrakten Gefährdungsdelikten Hilkgendorf, E.: Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter des Internet, in: NJW 1997, S. 1873–1878.

9.3 Verfolgungs- und Durchsetzungsprobleme

Selbst dann, wenn eine Straftat einem bestimmten Täter nachgewiesen werden kann, ist es häufig schwierig, ihn strafrechtlich zur Verantwortung zu ziehen. Aufgrund der Globalität der Telekommunikationsnetze können sich Kriminelle dem Geltungsbereich eines nur räumlich begrenzt geltenden Rechts und der Verfolgung durch ebenso begrenzt wirkende Behörden entziehen. Verbreitungsdelikte, Computersabotage, Persönlichkeitsrechtsverletzungen und Urheberrechtsstraftaten, die in der Bundesrepublik Deutschland Rechtsgüter verletzen oder gefährden, lassen sich über das weltweite Datennetz ohne größeren Aufwand von anderen Staaten aus begehen, in denen ein bestimmtes Verhalten möglicherweise nicht strafbar oder die Gefahr einer Strafverfolgung aus anderen Gründen geringer ist.

Um dies zu verhindern, müssen die Bemühungen um eine internationale Harmonisierung des Strafrechts um eine Verbesserung der internationalen Zusammenarbeit bei der Verbrechensbekämpfung ergänzt werden. Zwar existiert bereits eine Vielzahl entsprechender Übereinkommen, Empfehlungen und Initiativen: Allein im Rahmen des Europarates sind zwanzig Übereinkommen getroffen worden,[542]) zudem gibt es mehrere Empfehlungen des Ministerkomittees dieser Organisation zur Bekämpfung der Computerkriminalität.[543]) Die Europäische Kommission hat sich in einem Grünbuch und in einer Mitteilung mit dem Phänomen der Verbreitungsdelikte in Telekommunikationsnetzen befaßt[544]) und einen Aktionsplan zur sicheren Nutzung des Internet veröffentlicht.[545]), Hinzu kommen Empfehlungen und Richtlinien der OECD[546]) sowie eine Deklaration des Kongresses der Vereinten Nationen über Verbrechensprävention und die Behandlung von Straftätern.[547])

Soweit die internationalen Abkommen bereits praktische Relevanz haben – insbesondere innerhalb Europas –, gelten ihre Bestimmungen jedoch als zu unübersichtlich und die Verfahren der internationalen Rechtshilfe als zu schwerfällig. Es wird befürchtet, die Vielzahl der unterschiedlichen Bestimmungen führe zum Kollaps der Kooperation in Strafsachen.[548]) In der praktischen Umsetzung sei das Netzwerk der internationalen Rechtshilfe zu langwierig, um eine effektive Strafverfolgung zu gewährleisten.[549])

Die Enquete-Kommission hält diesen Zustand gerade im Hinblick auf die Strafverfolgung in Telekommunikationsnetzen für nicht akzeptabel. Der hohen Mobilität von Straftätern und von strafbaren Inhalten in den Datennetzen muß eine entsprechend erhöhte Mobilität der Strafverfolgung gegenüber gestellt werden. Wie auf dem Treffen der Justiz- und Innenminister der G-8-Staaten im Dezember 1997 zu Recht festgestellt wurde, erfordert dies eine internationale Zusammenarbeit von beispiellosem Ausmaß.[550]) Vorschläge der Gestaltung einer solchen Zusammenarbeit enthält der Bericht der sogenannten Carnegie-Gruppe.[551]) Die Kommission fordert den Gesetzgeber daher dazu auf, sich nachdrücklich für eine Vereinfachung und Effektivierung der Verfahren der internationalen Rechtshilfe einzusetzen.

10. Außerrechtliche Lösungsansätze

10.1 Technische und organisatorische Prävention

Das Strafrecht selbst hat durchaus präventive Wirkung, indem es mit der Strafandrohung potentielle Straftäter von der Deliktsbegehung abschreckt. Im eigentlich Sinne anwendbar ist das Strafrecht in der Regel jedoch erst, wenn bereits ein Rechtsgut verletzt oder zumindest gefährdet wird. Einer Ausweitung des Strafrechts vorzuziehen sind daher technische und organisatorische Maßnahmen, welche die Begehung von Straftaten und damit die Verletzung von Rechtsgütern von vornherein verhindern oder wesentlich erschweren. Ähnlich wie die Einführung der Wegfahrsperre für PKW zu einem Rückgang der Kfz-Diebstähle geführt hat, lassen sich auch in Telekommunikationsnetzen bedrohte Rechtsgüter schützen. Beispielhaft seien folgende Maßnahmen genannt:

- Zur Bekämpfung des Eindringens in fremde Computersysteme sowie des Ausspionierens und der Beschädigung fremder Datenbestände kommen Maßnahmen zur Erhöhung der Datensicherheit in Betracht, etwa der – technisch allerdings noch problematische[552]) – Einsatz biometrischer Verfahren zur Zugangskontrolle oder eine sorgfältige Auswahl, Beaufsichtigung und Kontrolle von „Insidern" mit besonderen Zugriffsmöglichkeiten.

---

542) Vgl. Schübel, E.: Wie gut funktioniert die Strafverfolgung innerhalb Europas?, NJW 1997, S. 105–110 (106).

543) Recommendation No. R (81) 20 on the Harmonisation of Laws relating to the Requirement of Written Proof and to the Admissibility of Reproductions of Documents and Recordings on Computers, die Recommendation No. R (89) 9 on computer-related Crime; Recommendation No. R (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology Recommendation.

544) Vgl. Kommission der Europäischen Gemeinschaften: Illegale und schädigende Inhalte im Internet. Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß sowie den Ausschuss der Regionen, Brüssel, 16. Oktober 96, Kom (96) 487 endg.

545) Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen: Aktionsplan zur Förderung der sicheren Nutzung des Internet, Brüssel 1997.

546) Vgl. die zusammenfassende Darstellung der OECD-Aktivitäten in: National Police Agency: Intermediate Report on Security of the Information Systems, abrufbar unter http://www.npa.go.jp/soumu/ereport.html.

547) vgl. die unter http://www.ifs.univier.ac.at/~pr2gq1/reviews.html abrufbaren Informationen.

548) Vgl. Schomburg, W.: Strafrecht und Rechtshilfe im Geltungsbereich von Schengen II, NJW 1995, S. 1931–1936 (1936).

549) Vgl. Schübel, E.: Wie gut funktioniert die Strafverfolgung innerhalb Europas?, NJW 1997, S. 105–110.

550) Vgl. Meeting of Justice and Interior Ministers of The Eight, December 9–10, 1997: Communiqué sowie Statement of Principles und Action Plan. Vgl. insbesondere S. 1 des Communiqués sowie Ziffern II., VI. der Grundsatzerklärung.

551) Abrufbar unter http://www.iid.de.

552) Vgl. oben Erster Berichtsteil, Gliederungspunkte 3.5. und 3.6.

- Urheberrechtsverletzungen kann durch Kopierschutzvorkehrungen vorgebeugt werden. Projekte zur Entwicklung „digitaler Wasserzeichen"[553]), die die Herkunft eines Werks verraten, und anderer Techniken sowie von Standards werden zum Beispiel von der Europäischen Union unterstützt.[554])

- Die Manipulation von Daten würde durch die Verwendung von Techniken, welche die Fälschung erkennen lassen, zwar nicht verhindert werden können, jedoch an Reiz verlieren. In diesem Zusammenhang kann der Einsatz digitaler Signaturen hilfreich sein. Denn mit Hilfe digitaler Signaturen kann nicht nur zuverlässig festgestellt werden, von wem eine Nachricht stammt, es kann auch überprüft werden, ob sie manipuliert worden ist.[555])

- Filtersysteme, die den Zugang zu bestimmten Inhalten blockieren, können Straftaten im Bereich des Jugendmedienschutzes zwar nicht verhindern, wohl aber die Zugänglichkeit von jugendgefährdenden Inhalten einschränken.[556]) Das setzt allerdings voraus, daß entsprechende Inhalte auch sicher identifiziert werden können. Wirksamkeit, Zugänglichkeit und Kosten solcher Einrichtungen werden derzeit von der Europäischen Kommission geprüft.[557])

Die Enquete-Kommission fordert den Gesetzgeber dazu auf, die Entwicklung und den Einsatz solcher technischer und organisatorischer Maßnahmen zu fördern. Sie erachtet zudem die Prüfung der Frage für sinnvoll, wie es ermöglicht werden kann, von bestimmten Techniken ausgehende strafrechtlich relevante Gefahren zu erkennen, bevor eine Technik zur Begehung von Straftaten mißbraucht wird. Durch die Etablierung eines Frühwarnsystems, das bereits bei der Produktentwicklung die Erkennung von Mißbrauchsmöglichkeiten gewährleistet, könnte verhindert werden, daß die technische und organisatorische Prävention der technischen Entwicklung hinterherhinkt.[558]) Wird die Gefahr der Begehung bestimmter Straftaten erkannt, könnten die Hersteller der entsprechenden Produkte dann im Wege von Selbstbeschränkungsabkommen innerhalb der Wirtschaft, notfalls aber auch mit legislativen Maßnahmen, dazu gedrängt werden, ihre Produkte so zu gestalten, daß ihr Mißbrauch zu kriminellen Zwecken unmöglich oder zumindest erschwert wird.[559]) Wären solche Überlegungen zum Beispiel frühzeitig in die Entwicklung von Farbkopierern eingeflossen, hätte möglicherweise der rasante Anstieg der Falschgeldproduktion mit Hilfe dieser Technik bereits in den Anfängen gebremst werden können.[560]) Die Einführung solcher Verfahrens zur Früherkennung von strafrechtlich relevanten Mißbrauchsmöglichkeiten bestimmter Techniken sollte allerdings nach Auffassung der Enquete-Kommission die Wettbewerbsfähigkeit deutscher Unternehmen nicht beeinträchtigen.

10.2 Aufklärung

Technische und organisatorische Prävention muß zumindest teilweise im Wege des Selbstschutzes der Nutzer erfolgen. Daher müssen diese in die Lage versetzt werden, sich entsprechend auszustatten und zu verhalten. Dazu ist Aufklärung über die spezifischen Risiken des Umgangs mit der Informations- und Kommunikationstechnik erforderlich. Die Enquete-Kommission fordert dazu auf, entsprechende Informations- und Aufklärungskampagnen zu veranstalten bzw. zu unterstützen. Sinnvoll wäre etwa ein ständig aktualisiertes Online-Informationsangebot.

10.3 Verbesserung der Ausstattung der Strafverfolgungsbehörden

Dringend erforderlich erscheint der Enquete-Kommission darüber hinaus eine Verbesserung der sachlichen und personellen Ausstattung der Strafverfolgungsbehörden im Hinblick auf die Computerkriminalität. Noch heute verfügen Staatsanwaltschaft und Polizei häufig nicht über die technischen Möglichkeiten, um konkrete Ermittlungsmaßnahmen durchführen zu können.[561]) Die Enquete-Kommission schließt sich daher der bereits seit geraumer Zeit erhobenen Forderung nach dem Auf- und Ausbau kriminaltechnischer Dienststellen mit qualifizierten polizeilichen EDV-Sachverständigen an.[562]) Denn Gesetze, die mangels geeigneter Ausstattung nicht durchgesetzt werden können, sind sinnlos und führen letztlich zu einer Reduzierung der Autorität des Strafrechts und damit auch seiner präventiven Wirkung. Aus Kostengründen und aus Gründen der Effektivität sollten diese – in den Grenzen der von der Verfassung vorgegebenen bundesstaatlichen Ordnung – möglichst zentral eingerichtet werden und

---

553) Vgl. Die Welt vom 6. August 1997: Wasserzeichen schützen vor Internet-Piraten. Urheberschutz für Bilder und Musik verbessert.

554) Vgl. den Überblick über die unterschiedlichen Programme unter http://www.kaapeli.fi~eblida/ecup/related/index.html.

555) Vgl. Anhang 1 zur Mitteilung der Europäischen Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen: Sicherheit und Vertrauen in elektronische Kommunikation. Ein europäischer Rahmen für digitale Signaturen und Verschlüsselung, Kom (97) 503, S. i.

556) Vgl. Stange, A.: Pornographie im Internet. Versuch einer strafrechtlichen Bewältigung, in: Computer und Recht 1996, S. 424–428 (428).

557) Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen: Aktionsplan zur Förderung der sicheren Nutzung des Internet, S. 4, 7.

558) Vgl. Kube, E.; Bach, W.; Erhardt, E.; Glaser, U.: Technologische Entwicklung und Kriminalitätsvorbeugung, ZRP 1990, S. 301–305.

559) Vgl. ebd, S. 304.

560) Vgl. ebd. S. 302.

561) Dannecker, G.: Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, in: Betriebsberater 1996, S. 1285–1294 (1293).

562) Vgl. zu dieser Forderung Dannecker, ebd.; konkret: Paul, W.: Eine andere Betrachtungsweise der Computerkriminalität 1991, in: Computer und Recht 1993, S. 233–235.

eng mit entsprechenden Stellen anderer Staaten zusammenarbeiten.[563]) Die Kommission meint darüber hinaus, daß neben Polizisten und Staatsanwälten auch Richtern die Möglichkeit gegeben werden muß, sich verstärkt im Hinblick auf die Anforderungen des Informationszeitalters aus- und fortzubilden. Vermittelt werden sollten zumindest die technischen Grundlagen der Kommunikation in Datennetzen. Andernfalls besteht die Gefahr, daß die an Strafverfahren beteiligten Juristen die relevanten Fakten und Zusammenhänge nicht hinreichend kompetent erfassen können.[564])

11. Abschließende Empfehlungen

1. Im Bereich des materiellen Strafrechts besteht im Hinblick auf die Bekämpfung der Computerkriminalität kein größerer Reformbedarf. Die Enquete-Kommission empfiehlt jedoch, zu prüfen, ob und inwieweit der strafrechtliche Schutz gegen das Freisetzen von Computerviren und ähnlichen Programmen ausreicht, und gegebenenfalls einen eigenen Straftatbestand zu schaffen. Die Kommission regt zudem an, insbesondere die praktische Umsetzung der Haftungsprivilegierungen in Teledienstegesetz und Mediendienstestaatsvertrag, nach denen die Anbieter von Tele- und Mediendiensten für fremde Inhalte nicht oder nur unter bestimmten Voraussetzungen verantwortlich sind, im Rahmen der Evaluierung des Informations- und Kommunikationsdienstegesetzes aufmerksam zu beobachten.

2. Beobachtungs- und Prüfungsbedarf sieht die Enquete-Kommission auch auf dem Gebiet des Strafverfahrensrechts. Das Strafverfahrensrecht insgesamt sollte auf seine Praktikabilität in bezug auf Computerkriminalität hin untersucht werden. Gegebenenfalls sollten weitere Anpassungen erfolgen.

3. Die aufgrund der Globalität der Telekommunikationsnetze entstehenden Probleme bei der Anwendung und Durchsetzung nationalen Strafrechts sollten nach Auffassung der Enquete-Kommission vor allem durch internationale Vereinbarungen gelöst werden. Solche Vereinbarungen sollten einerseits einen Mindeststandard materieller Strafrechtsbestimmungen anstreben. Dringend erforderlich ist zum anderen jedoch auch, die Strafverfolgung durch eine Vereinfachung der Verfahren der internationalen Rechtshilfe zu effektivieren.

4. Die Enquete-Kommission ist der Auffassung, daß die Belange der Strafverfolgung nach dem gegenwärtigen Erkenntnisstand nicht zu einer Einschränkung in der freien Verwendung kryptografischer Verfahren zwingen. Die mit einer solchen Einschränkung möglicherweise verbundenen Vorteile für die Strafverfolgung wären aufgrund der vielfach gegebenen Umgehungsmöglichkeiten so gering, daß sie die mit einer Kryptoregulierung verbundenen Nachteile für Bürger und Unternehmen nicht aufwiegen könnten.

5. Soweit erwogen wird, die Möglichkeiten anonymer Kommunikation in den Datennetzen einzuschränken, sollten entsprechende Maßnahmen den datenschutzrechtlichen Grundsätzen der Datenvermeidung und der Datensparsamkeit nicht widersprechen. Maßnahmen sollten überdies nur in enger internationaler Zusammenarbeit erfolgen.

6. Gefördert werden müssen nach Auffassung der Enquete-Kommission Maßnahmen zur technischen und organisatorischen Prävention von Straftaten. Geprüft werden sollte, inwieweit es möglich ist, durch die Etablierung eines Frühwarnsystems die Möglichkeiten zum Mißbrauch bestimmter Techniken bereits bei der Produktentwicklung zu erkennen und zu verhindern.

7. Da technische und organisatorische Prävention zumindest teilweise nur durch den Nutzer selbst geleistet werden kann, bedarf es der Aufklärung über spezifische Risiken des Umgangs mit den neuen Formen der Informations- und Kommunikationstechnik und über die Möglichkeiten, diesen Gefahren zu begegnen.

8. Die Strafverfolgungsbehörden müssen nicht nur rechtlich, sondern auch technisch und personell in die Lage versetzt werden, Straftaten in Telekommunikationsnetzen zu verfolgen. Angesichts der großen Dynamik der Entwicklung auf dem Gebiet der Informations- und Kommunikationstechnik hält es die Enquete-Kommission für sinnvoll, in den Grenzen der von der Verfassung vorgegebenen bundesstaatlichen Ordnung zentrale Einheiten zu errichten, die durch ständige Schulung und Weiterbildung stets auf dem aktuellen Stand der Technik gehalten werden kann. Bei der Aus- und Fortbildung von Staatsanwälten und Richtern sollten verstärkt die technischen Grundlagen der Kommunikation in Datennetzen vermittelt werden.

---

563) Vgl. zu entsprechenden Vorstellungen der G-8-Staaten Meeting of Justice and Interior Ministers of The Eight, December 9–10, 1997: Communiqué sowie Statement of Principles und Action Plan, insbesondere Ziffer 2 des Aktionsplans.

564) Vgl. Meier, B.-D.; Böhm, B.: Strafprozessuale Probleme der Computerkriminalität, in: wistra 1992, S. 166–172 (172).

Druck: Bonner Universitäts-Buchdruckerei, 53113 Bonn
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon: 02 28/3 82 08 40, Telefax: 02 28/3 82 08 44
ISSN 0722-8333