

Chancen und Risiken neuer Technologien aus der Sicht des Datenschutzes

Der Weg in die Informationsgesellschaft wird durch den technischen Fortschritt bei den Informations- und Kommunikationstechniken gebahnt. Die Abhängigkeit der wichtigsten gesellschaftlichen Prozesse von der Sicherheit und Zuverlässigkeit solcher Systeme wächst derzeit noch stärker als das Bemühen, diese Sicherheit und Zuverlässigkeit zu gewährleisten und als wesentliches Gestaltungsziel moderner Technologien durchzusetzen. Für die informationstechnische Sicherheit werden jedoch gegenwärtig die methodischen Grundlagen gesetzt, die es möglich machen sollen, die vernetzte Gesellschaft, den elektronischen Handel und die Geldflüsse im "Cyberspace" beherrschbar zu machen. Auch demokratische Errungenschaften wie die Rücksichtnahme auf die Persönlichkeitsrechte der Bürger, das Recht auf Privatheit und informationelle Selbstbestimmung als Voraussetzung für die freie Entfaltung der Persönlichkeit müssen nicht auf dem Altar der Technik geopfert werden. "Datenschutz durch Technik" bietet die Chance, "altmodische" Werte wie Persönlichkeitsrechte in die Informationsgesellschaft hinüberzuretten.

Der Weg in die Informationsgesellschaft

Wenn man den heutigen gesellschaftlichen und wirtschaftlichen Wandel kurz beschreiben will, dann wird gern davon gesprochen, daß wir uns auf dem Weg von einer Produktions- in eine Dienstleistungsgesellschaft befinden und daß wir uns von einer Industriegesellschaft hin zu einer Informationsgesellschaft entwickeln [1]. Solche Plakatierungen sind natürlich oberflächlich. Wir werden weder auf Produktion noch auf Industrie verzichten können. Prägend sind jedoch die Trends: Der Anteil am Erwerbseinkommen durch Dienstleistungen gegenüber dem durch Produktion von Waren wächst ebenso wie die Bedeutung

von Informationen und ihrer Gewinnung und Verbreitung für den beruflichen und privaten Sektor.

Innerhalb weniger Jahrzehnte seit ihrer Erfindung hat die moderne Informations- und Kommunikationstechnik Wirtschaft, Verwaltung und Freizeit in einer Weise durchdrungen, daß man sich das Fehlen solcher Technologie nur noch als rückwärtsgewandten Nostalgetrip oder als Horrorszenario vorstellen kann. Arbeits- und Produktionsprozesse werden durch Computer gesteuert und beherrschbar gemacht, genauer: Sie können so komplex werden, weil es Computer gibt, mit denen man sie noch beherrschen kann. Die Umsetzung von modernen Gesetzen setzt den Einsatz

von Computern voraus, gäbe es sie nicht, müßten die Gesetze anders aussehen. Hätte man nicht die Computer für ihre Umsetzung, könnte man zum Beispiel die in eine Lohn- und Gehaltsrechnung einfließenden Vorschriften kaum so komplex fassen, wie es heute der Fall ist.

Wir sind also abhängig von der sicheren und zuverlässigen Funktion der Informations- und Kommunikationssysteme, die sich heute wie folgt darstellen:

Mit dem Internet besteht eine weltweite Vernetzung von vielen Millionen unterschiedlicher informationstechnischer Systeme - von den heimischen PCs bis zu den komplexen Großsystemen von Industrie, Verwaltung, Forschung und Militär. Weltweite E-Mail-Kommunikation und Informationsgewinnung über das World Wide Web (WWW) wird heute wie selbstverständlich jedem Schüler vertraut gemacht. Ihre Nutzung wird normal im beruflichen Alltag, gehört zur Gestaltung der Freizeit.

Gleiches gilt für die Mobilkommunikation: Handys sind innerhalb weniger Jahre zur Alltagstechnologie geworden. Wo immer man sich aufhält: Ihr Piepen erinnert uns daran.

Eine weitere Alltagstechnologie finden wir mittlerweile mehrfach in unseren Briefaschen: Chipkarten erobern den Zahlungsverkehr, das Gesundheitswesen, schließen uns Türen auf.

Die weiteren Trends werden von der Integration der Technologien geprägt: Das Internet entwickelt sich zur globalen Megamaschine. Seine Kapazitäten werden erweitert, die Sprachkommunikation wird integriert, über Satellitendienste wird die Welt zum Dorf gemacht. Der Handel mit allem, was sich in Bits und Bytes darstellen läßt, Daten, Informationen, Medien, Programme findet auf dem Netz der Netze statt. Mit virtuellem Geld wird bezahlt.

Stolpersteine auf dem Weg in die Informationsgesellschaft

Über die wirtschaftlichen, kulturellen, möglicherweise auch politischen Umwälzungen, die die Vervollkommnung der Informationsgesellschaft mit sich gebracht hat bzw. noch bringen wird oder kann, soll hier nicht gesprochen werden [2].

Die hier interessierenden Stolpersteine auf dem Weg in die Informationsgesellschaft sind die Risiken für

- \$** die Sicherheit in der Informationstechnik und
- \$** den Datenschutz in Gestalt der informationellen Selbstbestimmung.

Die Bedrohung der informationstechnischen Sicherheit spiegelt sich in den Schlagzeilen der Presse wider:

- \$** Durch das unbefugte Eindringen in Informationssysteme über Kommunikationsnetze (Hacking), ausnahmslos ermöglicht durch gravierende organisatorische und technische Sicherheitsmängel, werden vertrauliche Informationen (personenbezogene Daten, Firmengeheimnisse) Dritten bekannt. Die Wirtschaftsspionage mit Computern (Computerspionage) ist der Shooting-Star der Kriminalstatistik. Zuletzt hat sich die Zahl der bei der Polizei bekanntgewordenen Vorfälle dieser Art jährlich vervielfacht. Dabei spielt eine wesentliche Rolle, daß die Anbindung an das in vieler Hinsicht unsichere Internet auch für Unternehmen mittlerweile zum guten Ton gehört, ohne daß sie mit den notwendigen Sicherheitsmaßnahmen flankiert wird.
- \$** Neben der Offenbarung von Daten durch Hacking spielt die Datenmanipulation eine wesentliche Rolle bei der Computerkriminalität. Sie ist insbesondere

ein Insiderdelikt, denn unzureichende Sicherheitsmaßnahmen, die gegen die eigenen Mitarbeiter schützen sollen, verleiten zu solchen Manipulationen, sei es zur Bereicherung, sei es zur Schädigung. Motive lassen sich meistens finden.

§ Schadenbringende Programme oder Programmteile wie z. B. Computerviren werden aus den unterschiedlichsten Motiven erzeugt und verbreitet. Ihre Verbreitung wird - so ähnlich wie bei den biologischen Viren - durch leichtfertiges Verhalten der Computerbetreiber unterstützt. Die "Infektion" mit Computerviren, die teilweise nur lästige Computermeldungen verursachen, teilweise aber sogar Hardware beschädigen kann, erfolgt über das ungeprüfte und unkritische Einlesen von Programmen, die über Disketten oder Netzkommunikation, z.B. über E-Mail, das System erreichen. Inzwischen kann die Infektion auch mit Hilfe von Dokumenten erfolgen, denen virenverseuchte Makroprogramme (z.B. WORD-Makros) angehängt sind (sog. Makroviren).

§ Die Abhängigkeit aller wichtigen gesellschaftlichen Prozesse von einer funktionierenden Informations- und Kommunikationsinfrastruktur macht die Gesellschaft anfällig für Sabotageakte gegen diese Infrastruktur. Wirtschaftsunternehmen können irreparabel geschädigt werden, wenn die Informationstechnik für längere Zeit ausfällt, vor allem wenn sie von den schnellen Geldströmen abhängig sind, die ohne Informations- und Kommunikationssysteme nicht mehr fließen können. Bei vielen Technologien wie z. B. bei Atomkraftwerken, Verkehrssystemen - auch Flugzeugen -, von deren Funktion die Gesellschaft und von deren Sicherheit viele Menschenleben

abhängen, würde der Ausfall der sie steuernden und kontrollierenden IT-Systeme katastrophale Folgen nach sich ziehen.

§ Neue Kriminalitätsformen wie Betrüge-
reien im Internet, Datendiebstahl, Geld-
fälschung von Cybermoney, Verbreitung
gesetzwidriger Informationsangebote
zeigen, daß die Phantasie der mehr oder
weniger organisierten Kriminellen durch
die Computer und ihre Netze erst rich-
tig angeregt wird.

§ Dies geht einher mit den Beschränkungen bei der Bekämpfung der organisierten Kriminalität, die darin besteht, daß die Kriminellen die sich für sie ergebenden Vorteile der weltweiten Vernetzung effizient zu nutzen vermögen, ohne auf rechtsstaatliche Garantien Rücksicht nehmen zu müssen. Damit steigt - sehr deutlich auch in Deutschland - der Druck der Organe zur Verbrechensbekämpfung auf die Politik, auch bei der Kriminalitätsbekämpfung rechtsstaatliche Garantien und Errungenschaften zur Disposition zu stellen (man beachte in diesem Zusammenhang die Debatten um den "Großen Lauschangriff", die Regelungen um die Telekommunikationsüberwachung und um den Einsatz starker kryptographischer Verfahren!).

Die Risiken für den Datenschutz, präziser die informationelle Selbstbestimmung, sind subtiler:

§ Die Informations- und Kommunikationstechnologie hält neue Formen zur Gewinnung persönlicher Daten bereit: Sie sind z. B. Nebenprodukte bei der Nutzung von Diensten der IuK-Infrastruktur, weil jede Inanspruchnahme solcher Dienste Datenspuren legt, die Rückschlüsse auf das kommunikative Verhalten, ggf. sogar auf inhaltliche Präferenzen der Nutzer zulassen.

- § Solche Daten dienen der Gewinnung von individuellen Kommunikations- und Konsumentenprofilen, die der direkten Ansprache, z.B. bei der Werbung, dienen können. Diese Potentiale der Daten für die individuell gesteuerte Direktwerbung, die besondere Resonanz erhoffen lassen, machen die Daten zu begehrten und damit teuren Handelsobjekten. Der Handel mit differenzierten, personenbezogenen Angaben von Konsumenten wird sich wesentlich verstärken. Ebenso werden die Methoden aggressiver, in den Besitz solcher Daten zu gelangen.
- § Daten über das Kommunikations- und Dienstnutzungsverhalten erlauben auch die vermehrte und differenzierte Kontrolle individuellen Verhaltens und von Vorlieben. Der Kontrolle der Individuen dient auch der zunehmende Einsatz von Kontrolltechnologien wie z.B. die Videoüberwachung einschließlich ihrer digitalen Auswertungsmöglichkeiten.
- § Den oben genannten Beschränkungen der Bekämpfung der organisierten Kriminalität werden staatliche Eingriffsbefugnisse entgegengesetzt, die die informationelle Selbstbestimmung abbauen.

Informationstechnische Sicherheit

Informationstechnische Sicherheit wird gemeinhin über die Bedrohungen der Sicherheit definiert. Danach werden vier Grundbedrohungen betrachtet, drei davon betreffen die Informationstechnik allgemein, eine vierte erhält ihre Relevanz in vernetzten Systemen, insbesondere in Datenkommunikationssystemen wie das Internet.

Zunächst sind die Bedrohungen und Risiken auszuschalten, die die Verfügbarkeit der Informationssysteme, der Infrastruktur,

der Programme und Daten betreffen. Sicherheitskonzepte müssen daher Maßnahmen vorsehen, die diese Objekte vor unbeabsichtigtem Verschwinden, Zerstörung, Beschädigung, Unbrauchbarmachung schützen oder zumindest die Folgen solcher Ereignisse entschärfen.

Als zweites ist die Integrität der Systeme, Programme und Daten vor Bedrohungen zu schützen. Es müssen demnach Maßnahmen ergriffen werden, die die Objekte vor unbefugten Manipulationen schützen, die das Verhalten der Systeme und die Ergebnisse der Verarbeitung verfälschen könnten.

Als drittes, aber auch aus datenschutzrechtlicher Sicht nicht zuletzt, geht es darum, durch geeignete technische und organisatorische Maßnahmen die Vertraulichkeit der Daten gegen unbefugte Offenbarung bzw. Kenntnisnahme zu schützen.

In Kommunikationssystemen kommt es zusätzlich darauf an, die Authentizität des jeweiligen Kommunikationspartners (Person oder technisches System) und der empfangenen Nachrichten zu gewährleisten: Ist der Kommunikationspartner der, als der er sich ausgibt, und ist die empfangene Nachricht jene, die der autorisierte Kommunikationspartner gesendet hat?

Technische Grundlagen der informationstechnischen Sicherheit

Es gibt eine Reihe von Basistechniken für die Gewährleistung informationstechnischer Sicherheit, die Bestandteile aller konkreten Maßnahmen gegen die Bedrohungen der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität von Systemen, Programmen, Daten und ggf. Kommunikationspartnern sind.

Befugnisregelungen

Weniger eine Technik als vielmehr eine zwingende Organisationsaufgabe ist es zuallererst, eindeutige Regelungen zu schaffen, bekannt zu machen und durchzusetzen, die die Befugnisse bei der Datenverarbeitung, d.h. beim Umgang mit und bei der Nutzung von Systemen, Programmen und Daten, festlegen. Die Trennschärfe zwischen Befugnis und Nichtbefugnis ist auch in Detailspekten zwingende Voraussetzung für einen sicheren Einsatz der Informationstechnik, denn die wichtigsten Basistechniken dienen gerade dazu, dem Befugten seine Befugnisse einzuräumen und den Unbefugten von seinem Tun abzuhalten.

Maschinelle Authentifikation

Damit erhalten erst Verfahren zur maschinellen Authentifikation einen Sinn. Mit solchen Verfahren soll ein informationstechnisches System befähigt werden, Unbefugte von Befugten und unbefugtes Handeln von befugtem Handeln zu unterscheiden, die Befugnisse einzuräumen und das Unbefugte zu verhindern. Die Methoden zur Mensch-Maschine-Authentifikation unterscheiden sich durch die Authentifikationsmittel: Wissen, Besitz und persönliche Merkmale der zu authentifizierenden Person.

Die verbreiteten Paßwort-Verfahren basieren auf dem möglichst exklusiven Wissen eines Paßworts zu einer meist nicht geheimen Kennung. Nur wer das dazugehörige Paßwort kennt, kann unter dieser Kennung mit den Rechten des so authentifizierten Benutzers arbeiten. Die Sicherheit einer solchen Authentifikation hängt von der Vertraulichkeit des Paßworts ab. Sie hängt ab von der Sorgfalt des Benutzers bei der Geheimhaltung, von der Gültigkeits-

dauer, von der Länge und der Auswahl der als Paßwort dienenden Zeichenkette sowie von der geschützten Speicherung des Paßworts im System.

Eine weitere Authentifikationstechnik arbeitet mit maschinenlesbaren personenbezogenen Ausweisen, die über einen Speicher verfügen, der die notwendigen Authentifikationsinformationen enthält. Diese Speicher bestehen meist aus Magnetstreifen und sind entsprechend leicht manipulierbar, zunehmend sind es aber auch Chipkarten oder sog. Token, die größere Sicherheit vor Manipulationen gewährleisten können. Dabei handelt es sich um Authentifikation durch Besitz.

Die dritte Klasse der Authentifikationsverfahren arbeitet mit den biometrischen Merkmalen von Personen. Ansätze dafür bieten Fingerabdrücke, Stimmanalysen, Iris-Analysen, Unterschriftenanalysen und die Wiedererkennung von Gesichtsphysiognomien usw. Die biometrischen Verfahren versprechen für die Zukunft verlässliche und manipulationsgeschützte Authentifikationen. Trotz erster Markteinführungen biometrischer Erkennungssysteme haben sie sich noch nicht sehr weit durchgesetzt, auch deshalb, weil die Präzision der Unterscheidung befugter und nicht befugter Personen noch nicht immer alle Wünsche erfüllen konnte.

Zunehmende Bedeutung erlangt auch die Authentifikation zwischen zwei automatisierten Systemen, die Maschine-Maschine-Authentifikation. Diese ist vor allem für die gesicherte Rechner-Rechner-Kommunikation in Netzen notwendig. Praktische Bedeutung erlangt sie zunehmend bei Chipkarten-Anwendungen, weil dort eine gegenseitige Authentifikation zwischen Chipkarte und Chipkarten-Leseinheit erforderlich ist, um das mißbräuchliche Auslesen

von Chipkarten zu verhindern. Das bekannteste und sicherste Verfahren ist das Challenge-Response-Verfahren, bei dem beide Maschinen sich den gegenseitigen Nachweis durch kryptographische Verfahren erbringen, daß sie zur gleichen Anwendung gehören.

Kryptographie

Kryptographische Verfahren werden für diverse Sicherheitsziele eingesetzt: Für die Vertraulichkeit der Daten bei der Übertragung oder Speicherung, für die Authentifizierung und den Nachweis der Authentizität. Dabei sind zwei grundsätzlich unterschiedliche Ansätze zu erwähnen, die in Kombination miteinander besondere praktische Bedeutung erlangen.

Symmetrische kryptographische Verfahren verschlüsseln einen Text mit dem gleichen Schlüssel, mit dem dann auch die Entschlüsselung erfolgt. Es gibt dazu heute eine Reihe von mathematisch sehr sicheren Verfahren. Das bekannteste darunter ist der DES-Algorithmus (Data Encryption Standard). DES und ähnliche Verfahren gelten insoweit als sicher, als sie praktisch nur mit "brutaler Gewalt", d.h. mit dem sog. Brute-Force-Angriff gebrochen werden können. Bei diesem Angriff handelt es sich um das computergestützte Ausprobieren aller denkbaren Schlüssel. Die Anzahl aller denkbaren Schlüssel hängt allein von der Schlüssellänge ab, die beim klassischen DES 56 Bit beträgt. Bei Daten, für die es sich für Dritte lohnt, einen größeren technischen Aufwand zu treiben, um sie zu entschlüsseln, gilt dies nicht mehr als hinreichend sicher, denn die $2^{56} = \text{ca. } 7 \cdot 10^{21}$ verschiedenen Schlüssel stellen für spezielle Kryptoanalyse-Systeme keine zu große Hürde mehr dar. Symmetrische Verschlüsselungsverfahren sollten daher heu-

te über 112 oder 128 Bit lange Schlüssel (Beispiel: Triple-DES als DES-Variante arbeitet mit 112 Bit) verfügen.

Das Problem symmetrischer Verfahren liegt allerdings in der Organisation der Schlüsselverteilung, denn die möglichen Kommunikationspartner müssen auf irgendeinem Wege den Schlüssel erfahren, womit eine Schwachstelle des Verfahrens offenbar wird: Die Vertraulichkeit des Schlüssels ist auf diesem Wege in Gefahr. Mit jedem Kommunikationspartner sind Schlüssel auszutauschen - ein praktisches Problem in offenen Netzen, in denen diese Umstände hinderlich sind.

Symmetrische Verfahren haben allerdings den Vorteil, daß die Verschlüsselung praktisch in Echtzeit erfolgen kann, eine Übertragungsverzögerung durch die Verschlüsselung praktisch vernachlässigt werden kann. Symmetrische Verfahren dienen ausschließlich der Vertraulichkeit bei der Datenübertragung und -speicherung.

Bei asymmetrischen Verfahren gibt es Schlüsselpaare. Was mit dem einen Schlüssel verschlüsselt wird, kann mit dem jeweils anderen Schlüssel entschlüsselt werden. Das Besondere ist, daß nur einer der beiden Schlüssel geheim gehalten werden muß, der andere kann öffentlich gemacht werden. Verschlüsselt man einen Text mit dem öffentlichen Schlüssel des Kommunikationspartners, so kann nur dieser den Text mit seinem geheimen Schlüssel entschlüsseln: Die Vertraulichkeit des Textes ist gewährleistet. Wenn jemand aber den Text mit seinem geheimen Schlüssel verschlüsselt, so ist zwar die Vertraulichkeit nicht mehr gewährleistet, weil jeder den Text mit dem öffentlichen Schlüssel entschlüsseln kann, jedoch hat der Empfänger die Gewähr, daß der Text nur von dem be-

kannten Absender stammen kann, denn nur dieser kennt den geheimen Schlüssel: Der Text ist elektronisch unterschrieben.

Das Prinzip asymmetrischer Verfahren beruht auf mathematischen Funktionen, die zwar schnell berechnet werden können, deren Umkehrfunktion jedoch außerordentlichen Rechenaufwand erfordert. Der bekannteste asymmetrische Algorithmus, der RSA-Algorithmus (nach den Erfindern **R**ivest, **S**hamir, **A**dleman benannt) beruht darauf, daß man zwar zwei sehr große Primzahlen leicht miteinander multiplizieren kann, die unbekanntes Faktoren aber nur mit extremem - und bei ausreichend großen Primzahlen in heute denkbarer Rechenzeit nicht leistbarem - Aufwand aus dem Produkt errechnen kann.

Asymmetrische Verfahren gelten heute als sicher, wenn die Schlüssellänge mindestens 1024 Bit beträgt. Ihr Vorteil ist die breite Nutzbarkeit, ihr Nachteil der erhebliche Rechenaufwand.

Die jeweiligen Vorteile der beschriebenen Methoden werden in den hybriden Verfahren genutzt. Für die Benutzer handelt es sich um asymmetrische Verfahren. Allerdings werden nicht die zu übertragenden Nachrichten damit verschlüsselt, sondern ein für den jeweiligen Übertragungsvorgang automatisch und zufallsgesteuert erzeugter Sitzungs-Schlüssel (Session Key) für ein symmetrisches Verschlüsselungsverfahren. Damit wird der Text verschlüsselt. Der asymmetrisch verschlüsselte Session Key und der symmetrisch verschlüsselte Text werden übertragen. Wie beim reinen asymmetrischen Verfahren kann damit ebenfalls entweder die Vertraulichkeit oder die Authentizität des übertragenen Textes sichergestellt werden.

Bekanntestes Hybrid-Verfahren ist das PGP-Verfahren (Pretty Good Privacy), das

jedem bekannt ist, der sich schon mal um die sichere Übertragung von E-Mails im Internet gekümmert hat.

Steganographie

Steganographische Verfahren werden ebenfalls zum Schutz der Vertraulichkeit übertragener oder gespeicherter Daten verwendet. Sie werden ferner für die Anbringung "elektronischer Wasserzeichen" zur Authentizitätsabsicherung von Datenobjekten, die große Datenmengen repräsentieren, verwendet, z.B. bei der Übertragung und Speicherung von digitalisierten Bildern, Videoaufnahmen, Sprachaufnahmen oder Telefonaten.

Bei steganographischen Verfahren werden digitale Nachrichten in große Datenbestände "eingehüllt", die in dem Maße Redundanzen aufweisen, daß die Veränderung einer bestimmten Anzahl von Bits unbemerkt bleiben kann. Deutlich wird das zum Beispiel bei digitalisierten Videosequenzen, die viele Megabytes an Daten repräsentieren und deren optische Veränderungen unbemerkt bleiben, wenn Bytes im Umfang einer kurzen digitalen Nachricht so gezielt verändert werden, daß sie durch entsprechende Methoden wieder herausgefiltert werden können. Auch bei der digitalen Übertragung von Sprache bleibt ein "Rauschen" unauffällig, welches durch die gezielte Veränderung einzelner Bits entsteht.

Die Existenz steganographischer Verfahren - sie stehen auch schon als Freeware im Internet zur Verfügung - ist ein wichtiges Argument der Befürworter starker Kryptographie in der sog. Kryptokontroverse zwischen den Interessenten an unbeobachtbarer Kommunikation und den Sicherheitsbehörden, die sich Hintertürchen zur Entschlüsselung verschlüsselter Kommunika-

tion für die Verfolgung organisierten Verbrechens freihalten wollen [3]. Während man die Anwendung kryptographischer Verfahren am Datenstrom und so im Falle eines Verbotes rechtswidriges Handeln erkennen kann, ist einer digitalen Sprach- oder Videosequenz nicht anzumerken, ob sie Hülle einer steganographierten Nachricht ist [4].

Das gezielte Einbringen von unbemerkbaren "Rauscheffekten" in digitalisierte Bilder, Video- oder Sprachsequenzen dient den Urhebern auch dazu, ihre Urheberschaft daran zu vermerken und auch an späteren Kopien nachweisen zu können (Watermarking).

Datenschutz durch Technik

Informationstechnische Sicherheit ist auch Voraussetzung für den Datenschutz, also für die Gewährleistung informationeller Selbstbestimmung, denn wenn die Sicherheit der Systeme und Programme, mit denen personenbezogene Daten verarbeitet werden, und der personenbezogenen Daten selbst nicht gewährleistet ist, dann ist die informationelle Selbstbestimmung berührt. Wenn Daten nicht oder falsch verarbeitet werden, wenn sie in unbefugte Hände geraten und so zu mißbräuchlichen Zwecken verwendet werden können, dann sind sie dem Willen des Betroffenen entzogen, ohne daß vorwiegende Interessen der Allgemeinheit dieses verlangen.

Der Einsatz von Informationstechnik bei der Verarbeitung personenbezogener Daten wird jedoch meist als risikoverstärkend für den Datenschutz angesehen. Der Datenschutz soll die Gefahren für die Grundrechte der Bürger oder Kunden kompensieren, die vom extensiv ausgeweiteten Einsatz der Informationstechnik und damit auch von den vergrößerten Potentialen für den Eingriff in Grund-

rechte oder mißbräuchliche Verwendungen ausgehen. Datenschutz trotz Technik ist das Ziel, das auch der Entwicklung der Datenschutzgesetzgebung zugrunde lag.

Die obige Darstellung der Methoden der informationstechnischen Sicherheit zeigt, daß inzwischen Potentiale verfügbar sind, die viele Sicherheitsziele durch Einsatz von Informationstechnik besser erreichbar machen als mit der klassischen nicht-automatisierten Datenverarbeitung. Die Kontrollaktivitäten der Datenschutzbeauftragten zeigen, daß dort, wo auch die technische Datensicherung bei der Gestaltung von informationstechnischen Systemen eine Rolle gespielt hat, das Sicherheitsniveau für die schutzbedürftigen Daten wesentlich höher ist, als wenn sie weiterhin in Karteien und Akten verarbeitet worden wären. Wenn man dann noch die beschriebenen modernen Verfahren der IT-Sicherheit zugrunde legt, dann kann schon insoweit von Datenschutz durch Technik gesprochen werden. Die Defizite liegen nicht in der Existenz solcher Verfahren, sondern in dem verbreiteten Leichtsinn von vielen Entscheidungsträgern, Planern, Anwendern und Nutzern, die Investitionen in Sicherheit für herausgeworfenes Geld halten oder die Anwendung von Sicherheitstechniken als lästig ansehen - zumindest, solange sie nicht selbst von Katastrophen oder Skandalen betroffen sind.

Datenschutz durch Technik bedeutet aber auch, mit technischen Möglichkeiten alternative Systeme zu entwickeln, die die angestrebten Automatisierungsziele mit größtmöglicher Vermeidung datenschutzbezogener Risiken erreichen können. Solche "datenschutzfreundliche Technologien" (privacy enhanced technologies - PET) lassen sich wie folgt charakterisieren [5]:

§ Sie kommen ganz oder weitgehend ohne personenbezogene Daten aus. Sie sind dahingehend optimiert, daß die Verwendung personenbezogener Daten so viel wie unbedingt nötig und so sparsam wie irgend möglich stattfindet.

§ Personenbezogene Daten werden anonymisiert, wenn es auf die Identität der einzelnen Person nicht ankommt.

§ Personenbezogene Daten werden dort pseudonymisiert, wo es auf die Identität der einzelnen Person nicht ankommt. Die Systemsphären, in denen es auf die Identität ankommt und das Pseudonym daher aufgehoben werden muß, sind durch organisatorische Gestaltungsmaßnahmen und durch technische Mittel zu minimieren. Solche technischen Mittel werden als "Identity Protector" [6] bezeichnet. Es sind Schnittstellen zwischen den Pseudonymitäts- und Identitätssphären der Informationssysteme, die die Sphären voneinander abgrenzen und die Identitätsmerkmale der Betroffenen von der Pseudonymitätssphäre abschotten.

Bereits heute sind Ideen der datenschutzfreundlichen Technologien in die deutsche Gesetzgebung eingeflossen. So wurden im Teledienstschutzgesetz (TDDSG) aus dem Jahre 1997 [7] unter den Grundsätzen für die Verarbeitung personenbezogener Daten festgelegt, daß die Gestaltung und Auswahl technischer Einrichtungen für Teledienste sich an dem Ziel auszurichten hat, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen [8]. Ferner gehört zu den datenschutzrechtlichen Pflichten des Diensteanbieters, dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym

zu ermöglichen, soweit dies technisch möglich und zumutbar ist [9].

Es bleibt zu hoffen, daß auch die im Zuge der Anpassung an die europäische Datenschutzrichtlinie [10] anstehenden Novelierungen der Datenschutzgesetze des Bundes und der Länder diese Gedanken aufnehmen [11].

[1] Bundesministerium für Wirtschaft: Info 2000: Deutschlands Weg in die Informationsgesellschaft, Februar 1996, Drucksache 13/4000 des Deutschen Bundestages v. 7.3.1996, Beginn des Abschnitts I.1. Technisch-wirtschaftlicher Wandel: "Die modernen Informations- und Kommunikationstechniken lösen nach allgemeiner Einschätzung einen technisch-wirtschaftlichen Wandel aus, der in Ausmaß und Folgewirkungen mit dem Übergang von der Agrar- in die Industriegesellschaft zu vergleichen ist."

[2] Zur Vertiefung wird die Lektüre des eben zitierten Berichts des Bundesministeriums für Wirtschaft empfohlen.

[3] Eine gute neutrale Zusammenfassung findet sich im Vierten Zwischenbericht der Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft" zum Thema "Sicherheit und Schutz im Netz", Bundestags-Drucksache 13/11002 vom 22. Juni 1998.

[4] Siehe z.B. Michaela Huhn und Andreas Pfitzmann: "Technische Randbedingungen jeder Kryptoregulierung", Datenschutz und Datensicherheit, Vieweg, 20/1 (1996), 23 ff.

[5] Siehe Registratiekamer of The Netherlands, Information and Privacy Com-

missioner of Ontario, Canada: "Privacy-enhancing Technologies - The path to anonymity", Vol. I und II, Rijswijk, 1995.

- [6] John Borking: "Der Identity Protector", Datenschutz und Datensicherheit, Vieweg, 20/11 (1996), 654 ff.
- [7] Artikel 2 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) vom 22. Juli 1997 (BGBl. I, Jahrgang 1997, Nr. 52, ausgegeben zu Bonn am 28. Juli 1997).
- [8] § 3 Abs. 4 TDDSG
- [9] § 4 Abs. 1 TDDSG
- [10] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Amtsblatt der Europäischen Gemeinschaften Nr. L 281 vom 23. November 1995 S. 31).
- [11] Solche Gedanken sind in den ersten Novellierungen vorhanden: Hessisches Datenschutzgesetz i.d.F. v. November 1998, § 10 Abs. 2 Satz 1: Werden personenbezogene Daten automatisiert verarbeitet, ist das Verfahren auszuwählen oder zu entwickeln, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Zwecks erforderlich ist. Entwurf des Brandenburgischen Datenschutzgesetzes mit Stand vom 23. September 1998: § 11 b Grundsätze der System- und Verfahrensgestaltung: (1) Die datenverarbeitenden Stellen können die

Inanspruchnahme von Leistungen auch anonym oder unter Pseudonym ermöglichen, soweit dies technisch durchführbar ist. Die Person, die das Angebot in Anspruch nehmen will, ist über diese Möglichkeit zu informieren. (2) Bei der Gestaltung und Auswahl informationstechnischer Produkte und Verfahren hat die datenverarbeitende Stelle sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu verarbeiten.

