III. VORSCHLÄGE UND FORDERUNGEN

Ebenso wie die Bundesregierung die Planungen für das neue Bundesamt für Sicherheit in der Informationstechnik aus einem Rahmenkonzept zur Gewährleistung der Sicherheit bei der Anwendung der Informationstechnik entwickelt, sind auch konstruktive Vorschläge für eine sinnvolle Bestimmung der Aufgaben, Befugnisse und Organisationsform dieses Bundesamtes aus dem Gesamtspektrum der Sicherheitsprobleme in der 'Informationsgesellschaft' abzuleiten. Allerdings gehen sie vom Problem der Verletzlichkeit aus und nicht nur von technischer Sicherheit.

In diesem Teil werden daher Probleme, Aufgaben und Regelungsstrukturen allgemein und ohne Bezug zu den Planungen für das Bundesamt für Sicherheit in der Informationstechnik erörtert, um nicht vorschnell auf eine spezifische organisatorische Lösung aller Probleme zuzusteuern. Weil nur ein Teil dieser Aufgaben durch eine Behörde wie ein Bundesamt für Sicherheit in der Informationstechnik bewältigt werden kann, werden die Aufgaben an dieser Stelle ohne Bezug auf die zu wählenden Regelungsstrukturen umrissen. Im Gegenteil gehen wir davon aus, daß das neue Bundeamt nur unter bestimmten Bedingungen sinnvoll sein kann. Es ist zwar notwendig, daß es für die ihm zuzuteilenden Aufgaben über alle erforderlichen Befugnisse verfügt. In jedem Fall ist jedoch zu vermeiden, daß in ihm zu viel bürokratische Macht zentralisiert wird, es dezentralen Problemlösungen den Platz raubt und zu einem bürokratischen Wasserkopf wird.

Um Mißverständnisse zu vermeiden, sei noch einmal daraufhingewiesen, daß hier nur Verletzlichkeitsprobleme und nicht - bei Gelegenheit - 'alle' Probleme der 'Informationsgesellschaft' mitbehandelt werden können. Ausgehend von den Verletzlichkeitsproblemen werden die durch sie verursachten Regelungs- und Steuerungsaufgaben bestimmt (1.) und die Bedingungen erörtert, die gegeben sein müssen, um sie zu erfüllen. Daran anschließend wird diskutiert, welche in bereits bestehende Prüf- und Steuerungsverfahren mitberücksichtigt werden können(1.1), welche neue IuK-Technikspezifische Prüfverfahren erfordern (1.2) und welche durch Normung (1.3) oder Haftungsregelungen (1.4) behandelt werden sollten. Schließlich werden die Anforderungen an eine Organisation zur Gewährleistung sicherer Verschlüsselungsverfahren erörtert (1.5). Danach erst werden im Teil IV. die konkreten Vorschläge zur Aufgabenbestimmung, Befugniszuweisung und Organisationsstruktur des Bundesamt für Sicherheit in der Informationstechnik vorgestellt.

1. VERLETZLICHKEIT - NEUE AUFGABEN IN DER 'INFORMATIONSGESELLSCHAFT'

Im folgenden werden die Aufgaben beschrieben, die unserer Auffassung nach vordringlich bewältigt werden müssen, wenn die informationstechnische Entwicklung sich nicht zum Nachteil der Sicherheit und Grundrechte der Bürger auswirken soll. Das Rahmenkonzept der Bundesregierung beschränkt - wie in der Kritik bereits ausgeführt - seine Problemsicht und seine Handlungsvorschläge auf einen ausschließlich technischen Sicherheitsbegriff und berücksichtigt in erster Linie Interessen des internationalen Wettbewerbs sowie der 'inneren' und 'äußeren' Sicherheit. Unsere Vorschläge sind demgegenüber darauf gerichtet, die Verletzlichkeit der Gesellschaft und die Interessen der Menschen als Staatsbürger und Verbraucher systematisch in Sicherheitsüberlegungen einzubeziehen. Werden die Probleme aus diesem Blickwinkel definiert, so ergeben sich die fünf folgenden, vorrangig zu lösenden Sicherheitsaufgaben.

1.1 Verringerung der Verletzlichkeit der Gesellschaft

Das Rahmenkonzept der Bundesregierung zielt darauf ab, die informationstechnische Entwicklung durch ergänzende Maßnahmen des technischen Datenschutzes und der Erhöhung der Betriebssicherheit zu begleiten. Solche Maßnahmen sind notwendig, aber keineswegs ausreichend. Wenngleich dieser Ansatz zur Beherrschung nachteiliger Technikfolgen durchaus auch präventive Aspekte aufweist, so beschränken sich diese doch auf die Erhöhung technischer Sicherheit. Die Handlungsvorschläge zielen gerade nicht darauf, die technische Entwicklung unter Verletzlichkeitsgesichtspunkten zu beeinflussen. Dieser Ansatz führt zumindest zu zwei negativen Folgen: Er macht zum einen die Gesellschaft in hohem Maße davon abhängig, daß es - in einem noch völlig offenen Entwicklungsprozeß - den Sicherungssystemen gelingt, das Restrisiko der Informatisierung für jeden Entwicklungsschritt ausreichend gering zu halten. Zum anderen setzt er die Gesellschaft einem Zwang zur Sicherung aus, dessen externe Kosten an Freiheits- und Demokratieeinbußen die Bürger zu tragen haben.

Demgegenüber halten wir es für unbedingt erforderlich, die Prävention früher und umfassender wirksam werden zu lassen, um die Abhängigkeit der Gesellschaft von IuK-Systemen und die dadurch hervorgerufenen Schadenspotentiale zu verringern. Wirkliche Sicherheit ist nur dort zu finden, wo absolute Sicherheit erst gar nicht gefragt ist. Sicherheit ist nur zu erzielen, wenn das unvermeidbare Quantum an 'Unsicherheit' keine katastrophalen Schäden bewirkt. Die bessere Sicherungsstrategie ist daher, Verhältnisse zu schaffen, in denen ein Irrtum oder Mißbrauch keine verheerenden Folgen hat. Es kommt also darauf an, durch passive Sicherungsmaßnahmen das Schadenspotential zu reduzieren oder die Möglichkeiten katastrophaler Schadensentwicklungen zu unterbinden. Gelingt dies, werden viele aktive Sicherungsmaßnahmen überflüssig. Ist es möglich, wieder aus Versuch und Irrtum zu lernen, haben auch Freiheit und Demokratie bessere Chancen. Viele Maßnahmen der Prävention, der Arbeitsüberwachung und der Personenüberprüfung verlieren dann ihre Rechtfertigung.[93]

Methodisch erfordert dies, das Kriterium der technischen Datensicherheit durch das sozio-technische Kriterium der "Verletzlichkeit" zu ersetzen und von diesem Maßstab her auf die Informatisierung der Gesellschaft Einfluß zu nehmen. Zur Untersuchung der Verletzlichkeit der Gesellschaft sind folgende Komponenten des Kriteriums zu berücksichtigen[94]:

- Abhängigkeit und Schadenspotentiale

  Das Ausmaß möglicher Schäden hängt ab von der konkreten Anwendung des Techniksystems, d.h. der ihm übertragenen gesellschaftlichen Funktionen. Bei Schäden sind auch Folgeschäden zu berücksichtigen, die sich durch den hohen Grad gesellschaftlicher Verflechtung und Arbeitsteilung in mittelbaren betroffenen gesellschaftlichen Subsystemen ergeben.

- Schadensursachen

  Bei den möglichen Schadensursachen sind sowohl durch Menschen beabsichtigte Schäden (Angriffe) als auch von Menschen nicht beabsichtigte Schäden (Beherrschbarkeit der IuK-Technik) zu berücksichtigen.

- Motive

  Die Wahrscheinlichkeit von Angriffen hängt wesentlich von den kriminellen, politischen oder persönlichen Motiven potentieller Angreifer ab, Schäden herbeizuführen.

- Fehler- und Angriffsmöglichkeiten

  Welche Schäden verursacht werden können, hängt von den Versagensmöglichkeiten der IuK-Technik und den Mißbrauchsmöglichkeiten ab, die sie motivierten Angreifern bietet.

- Wirksamkeit von Sicherungsvorkehrungen zur Verhinderung von Angriffsfolgen

  Ob diese Fehler und Angriffe beherrscht werden können, entscheidet sich zum einen nach den technischen Möglichkeiten, diese auszuschließen oder zu behindern. Zum anderen werden aber ergänzend - insbesondere gegenüber den Insidern des zu sichernden Systems - personenbezogene Sicherungsmaßnahmen erforderlich sein.

- Wirksamkeit schadensreduzierender Maßnahmen.

  Zu überprüfen ist, welche Maßnahmen ergriffen werden können, um eingetretene Schäden in ihren Auswirkungen auf die Gesellschaft zu begrenzen.

---

[93] Vgl. hierzu näher Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 231 ff.

[94] Zum Kriterium der Verletzlichkeit vgl. näher Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 14 ff.; Vgl. auch die Kritik in II.2.

- Verläßlichkeit von Sicherungsmaßnahmen

  Die Realisierbarkeit durchzuführender Sicherungsmaßnahmen hängt von den dafür aufzuwendenden hohen, in jedem Falle aber unproduktiven Kosten ab. Ihre Verläßlichkeit ist abhängig von organisatorischen, sozialen und menschlichen Voraussetzungen, die häufig in der Praxis nicht erfüllt werden. Beide Faktoren begrenzen die Realisierbarkeit und Wirksamkeit von Sicherungsmaßnahmen und müssen in einer Verletzlichkeitsanalyse berücksichtigt werden.

- Soziale Kosten der Sicherungsmaßnahmen

  Da ausreichende Sicherheit ohne Sicherungsmaßnahmen, die gegen Menschen gerichtet sind, nicht gewährleistet werden kann, sind für die Beurteilung eines technischen Systems auch die sozialen Kosten zu berücksichtigen, die dessen Sicherungszwang verursacht.

Das Rahmenkonzept der Bundesregierung berücksichtigt nur einen Teil dieser notwendigen Untersuchungen und beschränkt daher den Handlungsbedarf auf einen zu eingeschränkten Problemkreis.[95]. Demgegenüber müßte das Handlungsziel einer an der Sicherheit der Bürger und der Gesellschaft orientierten Strategie sein, die Entwicklung und den Einsatz informationstechnischer Systeme so zu beeinflussen, daß die Verletzlichkeit reduziert und nicht nur die Datensicherheit erhöht wird. Neben Datensicherungsmaßnahmen geht es dabei vor allem darum

- für die künftige Techniknutzung einen breiten gesellschaftlichen Konsens zu suchen, weil nur so Anriffsmotive reduziert werden können,

- die gesellschaftliche Abhängigkeit von Techniksystemen und die dadurch entstehenden Schadenspotentiale zu reduzieren, indem etwa Substitutionsmöglichkeiten durch sozio-technische Alternativen erhalten oder geschaffen oder auch der Verzicht auf IuK-Technik-Nutzung in Betracht gezogen wird,

- die Technik so zu gestalten, daß Angriffsmöglichkeiten und Beherrschbarkeitsprobleme reduziert werden, sowie

- ausreichende Notfallmaßnahmen vorzusehen.

1.2 Gewährleistung der Daseinsvorsorge

Der Mensch kann in der hochindustrialisierten Gesellschaft nur noch überleben, wenn der Staat oder andere gesellschaftliche Organisationen die Basistechniken, die Infrastruktur und die Dienste bereit stellen, um die Grundbedürfnisse nach Unterkunft, Wärme, Wasser, Luft, Licht, Kraft, Nahrung, Kleidung, Fortbewegung, Zahlungsmittel usw. zu befriedigen. Diese Leistungen der Daseinsvorsorge sind für die Verletzlichkeit der Gesellschaft aus zwei Gründen von zentraler Bedeutung. Zum einen sind die Bürger und auch der gesellschaftliche Zusammenhalt auf sie existentiell angewiesen. Zum anderen werden gerade diese sozialen Funktionen zunehmend auf Technik übertragen. Bereits heute, jedenfalls aber in Zukunft werden sie ausnahmslos mit Hilfe von IuK-Technik gesteuert und sind von ihrem Funktionieren vollständig abhängig.

Bereits heute sind die Gefährdungen für die Versorgungssicherheit der Bevölkerung groß. Daher muß es ein zentrales Anliegen jeder Sicherheitsstrategie sein, die Verletzlichkeit der Gesellschaft durch Ausfall von Leistungen der Daseinsvorsorge nicht zu erhöhen, sondern durch gezielte Gegensteuerung auf ein vertretbares Maß zu verringern. Dies ist sowohl für den bereichsspezifischen Einsatz von IuK-Technik als auch für IuK-gesteuerte Infrastrukturen und Basistechniken geboten:

---

[95] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 9.

Bereichsspezifischer Einsatz von IuK-Systemen

Verletzlichkeitsuntersuchungen sind bei allen Planungsverfahren für den Einsatz von IuK-Systemen und deren Ausbau, Veränderung oder Abbau in allen für die Daseinsvorsorge wichtigen gesellschaftlichen Bereichen vorzusehen. Hohe Schadenspotentiale können durch die Abhängigkeit von IuK-Systemen unter anderen in folgenden wichtigen gesellschaftlichen Bereichen entstehen:

- Verkehrssysteme

  Aufgrund der zunehmenden Mobilitätsanforderungen an Menschen im beruflichen wie im privaten Leben nehmen die Anforderungen an die Zuverlässigkeit, Schnelligkeit und Pünktlichkeit von Verkehrssystemen ständig zu. Dies gilt gleichermaßen für den PKW-Verkehr, den öffentlichen Personennahverkehr, die Bundesbahn und den Flugverkehr. Viele Produktions-, Vertriebs- und Handelsunternehmen sind von der pünktlichen Lieferung von Gütern und Energie (just in time) vollständig abhängig. Um den wachsenden Anforderungen gerecht zu werden, werden in diesen Bereichen zunehmend IuK-Systeme eingesetzt. Deren Ausfall oder Manipulation kann sehr große volkswirtschaftliche Schäden zur Folge haben und die Versorgung der Bevölkerung beeinträchtigen.

- Prozeßsteuerung

  Industriegesellschaften nutzen Techniksysteme mit sehr großen Schadenspotentialen. Die absichtliche oder fehlerhafte Freisetzung großer Energiemengen oder giftiger Substanzen kann katastrophale Schäden bewirken.[96] Mit dem Einsatz von IuK-Systemen bei der Prozeßsteuerung können Risiken vermindert werden, aber auch neue Risiken entstehen.[97]

- Geldwirtschaft

  Nahezu sämtliche Austauschprozesse von Waren und Dienstleistungen sind auf den funktionierenden Austausch von Informationen über Geld angewiesen. Manipulationen oder Ausfälle von elektronischen Zahlungssystemen können zu großen volkswirtschaftlichen Schäden führen, einzelne Menschen oder Unternehmen ruinieren und zu Versorgungsengpässen führen.[98]

- Verwaltungen

  Die hocharbeitsteilige Gesellschaft ist auf eine stetige, wirksame und kalkulierbare Verwaltung existentiell angewiesen. Eine Störung oder der Ausfall von Verwaltungsdienstleistungen durch Manipulation oder Versagen der eingesetzten IuK-Technik können daher leicht große Gesellschaftsgruppen oder die gesamte Gesellschaft schädigen.[99]

Neben der bereichsbezogenen Sichtweise ist ergänzend eine übergreifende Betrachtung der Verletzlichkeit der gesamten Gesellschaft erforderlich. Denn die gegenseitige Abhängigkeit der gesellschaftlichen Bereiche kann bei eintretenden Schäden im sozialen System Kettenwirkungen entfalten, die vom einzelnen Anwendungsbereich nicht richtig erkannt und bewertet werden können.

IuK-Infrastruktursysteme

Eine anders gelagerte Problemstellung ergibt sich dort, wo die IuK-Technik als ein gesellschaftliches Infrastruktursystem eingesetzt wird wie bei Telekommunikationsdiensten und Teletransaktionssystemen.[100] Hier wird die steigende Abhängigkeit von keinem verantwortlichen Akteur, weder den Anwendern noch den Netzbetreibern, beabsichtigt, sondern ist das Ergebnis eines kontinuierlichen Prozesses der zunehmenden Nutzung

---

[96] Vgl. hierzu auch Roßnagel, Großtechnik und Bürgerfreiheit, 1986, S. 340 ff.

[97] Vgl. hierzu z.B. Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 81f.

[98] Vgl. hierzu z.B. Harmsen/Weiß, Aspekte der Datensicherheit und der Verletzlichkeit der Informationssysteme im Bankensektor, 1989; Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 92 ff.

[99] Vgl. hierzu z.B. Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 98 ff.

[100] Vgl. zum folgenden näher Pordesch, Katastrophenpotential der Telekommunikation, Zivilverteidigung II/1989, S. 41 ff.

der Telekommunikation und der Anpassung gesellschaftlicher Strukturen an die neuen Möglichkeiten. Dem Problem steigender Verletzlichkeit kann hier nicht nur bereichsbezogen begegnet werden. Das große Schadenspotential bei Ausfällen oder Manipulationen entsteht hier nämlich aus der komplexen Wechselwirkung vieler Einzelschäden, die für sich betrachtet tolerabel erscheinen können.

Die Problemlage erfordert, die Entwicklung der Abhängigkeit der Gesellschaft von IuK-Infratrukturen ständig zu beobachten. Um auf ungewollte Entwicklungen überhaupt reagieren zu können, sind für den weiteren Ausbau der Telekommunikations-Infrastruktursysteme hinsichtlich der Ausfallsicherheit unterschiedliche Optionen zu entwickeln und vergleichend zu bewerten.[101] Denn nur durch Substitutionsmöglichkeiten können die Schadenspotentiale unterhalb katastrophaler Schadensentwicklungen gehalten werden. Außerdem müssen öffentliche und private Netz- und Dienstbetreiber durch Auflagen zur Einhaltung eines ausreichenden Sicherheitsniveaus durch Notnetzplanungen und Diversifikation der Netztechnik gezwungen werden.

Basistechniken

IuK-Systeme sind komplexe Produkte, die aus verschiedenen Basissystemen aufgebaut werden, wie etwa aus Betriebssystemen, Datenbanksystemen, Benutzeroberflächensysteme, Drucker- und Bildschirmsteuerungen. IT-Sicherheitskriterien und Zertifizierungen, wie sie von der Bundesregierung im Rahmenkonzept vorgeschlagen werden, sind hier nützliche Instrumente, um die Sicherheit angebotener Produkte zu erhöhen. Wo Sicherheitsstandards nicht vorgeschrieben werden können, kann mit Zertifikaten wenigstens die Markttransparenz erhöht werden. Solange jedoch die Sicherheit von Programmen nicht bewiesen werden kann (und das wird kaum je für alle Programme möglich sein)[102], ist es erforderlich, Vielfachschäden - beispielsweise durch Softwaremanipulation - zu begrenzen. Deshalb muß beobachtet werden, welche IuK-Systeme in welchen Bereichen Einsatz finden und ob eine genügend große Diversifikation gegeben ist. Ein Ziel der Beeinflussung der Technikentwicklung muß es sein, für eine genügend große Diversifikation der Systeme zu sorgen und eine möglichst große Sicherheit, insbesondere häufig eingesetzter Systeme zu gewährleisten.

1.3 Verbesserung der Bürgersicherheit

Das Rahmenkonzept erwähnt zwar unter der Darstellung seines Gegenstandes die Sicherheitsaspekte, die im öffentlichen Interesse liegen, und zählt dabei auch den Datenschutz auf.[103] Es betont in der Problembeschreibung und den Handlungskonzepten aber einseitig die Sicherung der Datenverarbeitung bei staatlichen Stellen zur Gewährleistung der inneren Sicherheit. Der mögliche Mißbrauch von IuK-Systemen durch staatliche Stellen wird nicht zum Bedrohungspotential gerechnet, gegen das Vorkehrungen zu treffen ein Ziel des Rahmenkonzeptes ist.[104] Im Hinblick auf ihre verfassungsrechtliche Aufgabenstellung darf die Bundesregierung aber Sicherheit nicht auf 'innere' oder 'Staatssicherheit' beschränken. Vielmehr muß in einem Rechtsstaat Sicherheit sogar vorrangig Sicherheit der Bürgergrundrechte vor staatlichem Machtmißbrauch bedeuten.[105]

Die Notwendigkeit staatlicher Vorsorge gegen und die Aufklärung von kriminellem Handeln ist nicht zu bestreiten. Hierfür ist auch der Einsatz von IuK-Technik erforderlich. Ebensowenig zu bestreiten ist aber auch der Satz politischer Grammatik, den wir Hobbes verdanken: Wer in der Lage ist, alle Bürger zu schützen, ist auch in der Lage, alle zu verfolgen. Soweit Technik Polizeiarbeit effektiviert, kann die Polizei Bürger besser schützen, aber auch deren Grundrechte stärker gefährden. Die Gewährleistung von IT-Sicherheit muß daher vor allem darauf zielen, die Freiheitsgrundrechte der Bürger zu sichern.[106]

In der 'Informationsgesellschaft' erfolgen erheblich mehr Lebensäußerungen über Netze und werden über jeden bedeutend mehr Daten gespeichert als heute. Dadurch sind die Verhaltensweisen und Lebensgewohn-

---

[101] Zu Entwicklungsalternativen im Telekommunikationsbereich vgl. Berger u.a., Optionen der Telekommunikation, 1988, Band III; Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 219 ff.

[102] "You can't trust code that you did not totally create yourself", Ken Thompson, Reflecting on Trusting Trust, Communications of the ACM, August 1984, Vol. 27, No. 8, S. 763.

[103] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 2.2.

[104] Vgl. hierzu IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 4.

[105] Vgl. hierzu z.B. Roßnagel u.a., Digitalisierung der Grundrechte? 1990, S. 118 ff.

[106] Vgl. zum folgenden auch Roßnagel, Technik und die Gefahr für das Individuum, 1990.

heiten eines jeden in breiterem Umfang und in größerer Tiefe elektronischem Zugriff offen. Durch die Fortschritte bei der Sprach-, Sprecher- und Bilderkennung ist zu erwarten, daß die Möglichkeiten zur Auswertung von Nutzdaten der Telekommunikation erheblich verbessert werden. Zugleich werden durch die gegenwärtigen Planungen von Telekommunikationsdiensten, z.B. die Digitalisierung des Fernsprechnetzes und ISDN, Möglichkeiten des Zugriffs auf Nutz- und Verbindungsdaten eröffnet.

Während die Transparenz des Bürgers für die Behörden zunehmen wird, dürfte deren Transparenz für die Bürger sinken. Niemand wird mehr in der Lage sein zu wissen, wo überall Daten über ihn gespeichert sind. Noch viel weniger kann er wissen, wie diese interpretiert und wann und wo gegen ihn verwendet werden können. Wer aber "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, aus eigener Selbstbestimmung zu planen oder zu entscheiden. ... 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 können, wird möglicherweise auf eine Ausübung seiner Grundrechte (Art. 8, 9 GG) verzichten."[107]

Zum Schutz der Grundrechte auf informationelle und kommunikative Selbstbestimmung[108] müssen Techniken entwickelt werden, die Eingriffe in diese Grundrechte verhindern. Hier wird die bereits oben erwähnte Verschlüsselung, durch die jeder Bürger selbst seine Informationen und Kommunikationen gegen staatliche - und auch private - Ausforschungsinteressen schützen kann, im Mittelpunkt des Interesses stehen.[109] Denn die Kryptotechnik könnte eine Intransparenz des Bürgers gewährleisten, indem sie ihn künftig in die Lage versetzt, die gewünschten Informationen automatisch vor jeder Übermittlung oder nach jeder Bearbeitung vollständig zu verschlüsseln und vor der Einsichtnahme oder dem Empfang wieder zu entschlüsseln. Ohne den Schlüssel aber könnten Texte, Daten und Programme nicht gelesen und Sprache nicht verstanden werden.[110] Die entscheidenden Fragen werden dann jedoch sein, ob in den kommenden Jahren Verschlüsselungsstandards normiert werden und wem die Generierung und Verwaltung der Schlüssel übertragen wird.

Darüberhinaus müßten - ähnlich wie das Problem "Versorgungssicherheit" - Datenschutzinteressen der Bürger schon bei der Planung von IuK-Systemen berücksichtigt werden. So sind für die staatliche Verwaltung Systeme zu bevorzugen, die die Speicherung möglichst weniger Daten erfordern. Entgegen dem zu beobachtenden Bestreben, ein Höchstmaß an Kompatibilität eingesetzter IuK-Systeme zu erreichen, sollten gezielt Inkompatibilitäten zwischen Systemen verschiedener Behörden geschaffen werden, um einen "amtshilfefesten Schutz gegen Zweckentfremdung"[111] technisch zu gewährleisten. Innerhalb der DV-Systeme muß durch technische Maßnahmen der Zugangs- und Zugriffskontrolle sichergestellt werden, daß Datenbestände nur zweckbezogen verarbeitet werden können. In allen Bereichen sollte darüber hinaus die Einhaltung der Datenschutzbestimmungen durch externe Kontrollen (z.B. durch Datenschutzbeauftragte) überprüft werden können. Hierzu müssen Unterstützungssysteme für die Revision entwickelt werden.

1.4 Verbrauchersicherheit

Sicherheit in der Informationstechnik darf nicht nur angestrebt werden, um die Absatzchancen bundesrepublikanischer Anbieter auf dem Weltmarkt zu verbessern oder die Akzeptanz für IuK-Produkte auf dem inländischen Markt zu erhöhen. Sie ist auch und vor allem notwendig, um den Verbraucher, den Käufer und Anwender von IuK-Technik ebenso wie den Betroffenen von IuK-Anwendungen zu schützen.

---

[107] BVerfGE 65, 1 (43); vgl. hierzu auch Denninger, E., Verfassungsrechtliche Grenzen polizeilicher Datenverarbeitung - insbesondere durch das Bundeskriminalamt, Computer und Recht, 1988, S. 55 f.; Peitsch, Grundrechtswesentlichkeit polizeilicher Informationssammlung und -verarbeitung, CR 1989, S. 721 ff.

[108] Vgl. hierzu ausführlich Roßnagel, Das Recht auf (tele-) kommunikative Selbstbestimmung, Kritische Justiz, Heft 2/1990.

[109] Vgl. hierzu Pfitzmann/Pfitzmann/Waidner, Datenschutz garantierende offene Kommunikationsnetze, 1988, S. 118 ff.

[110] Vgl. hierzu z.B. Pfitzmann/Pfitzmann/Waidner, Technischer Datenschutz in diensteintegrierenden Digitalnetzen - warum und wie? DuD 1986, S. 178 ff.; dies., Datenschutz garantierende offene Kommunikationsnetze, Informatik-Spektrum 1988, S. 118 ff.; Die Hefte 1/86 und 1/88 des GMD-Spiegel; Roßnagel/Wedde/Hammer/Pordesch, Die Verletzlichkeit der Informationsgesellschaft, 1989, S. 172, 192 ff.; dies., Digitalisierung der Grundrechte?, 1990, S. 144 ff., 239 ff., 296 f.

[111] BVerfGE 65, 1 (46).

Schutz vor Verbrauchertransparenz und -manipulation

Handelsunternehmen, Banken und Versicherungsunternehmen verfolgen neue Rationalisierungs- und Marketingstrategien, für die eine spezifische Sammlung von Kundendaten zunehmend zum Schlüssel des Erfolges wird.[112] Kundentransparenz soll den Unternehmen ermöglichen, die Marktentwicklung besser zu antizipieren und ihre Kapazitäten zur Steuerung des Marktes zu erhöhen.

Die Transparenz des Kundenverhaltens wird durch den Einsatz der IuK-Technik erreicht. Insbesondere die "Informatisierung der Kundenschnittstelle" ist ein Schlüssel zum Aufbau von Kundeninformationssystemen. In technischer Hinsicht können die Daten auf unterschiedlichste Weise gewonnen werden. Neben der manuellen Eingabe von Kundeninformationen aus Bestellungen, Kreditanträgen oder Auskünften von Schuldnerwarndiensten werden der elektronischen Kundenselbstbedienung und der Kundenidentifizierung am Kassenterminal besondere Bedeutung zukommen. Das Kreuzen der Kundendaten mit den Daten der gekauften Produkte ermöglicht dem Handelsunternehmen, detaillierte Kunden- und Warenprofile zu erstellen. Sie können so Konsumspektrum, Kaufrhythmen, typische Kombinationskäufe, Bewegungsprofile und die Ausgabenverteilung jedes Kunden erkennen. Außerdem lassen sich dadurch die Reaktionen jedes Haushalts oder einzelner Kundengruppen auf unterschiedliche Produkte, Promotionsmethoden, Werbemedien oder Preisgestaltungen orts- und zeitkongruent auswerten. Auf der Basis dieser Daten versuchen Marketingstrategen, das Verbraucherverhalten zeitstabil und zielgenau zu beeinflussen. Entsprechend den vorhandenen Daten über Finanzkraft, Interessen, Neigungen, bisherigen Konsumgewohnheiten oder der bereits erworbenen Ausstattung werden dem Kunden gezielte Angebote unterbreitet.

Das Individuum wird in seinen verschiedenen sozialen Rollen als Arbeitnehmer, als Kunde, als Bürger oder als Privatperson für unterschiedlichste Stellen zunehmend transparenter. Es wird zwar keinen 'Großen Bruder', keine zentrale, alle persönlichen Daten zusammenführende Institution geben. Personenbezogene Daten werden vielmehr dezentral und zweckspezifisch gesammelt. Alle diese vielen Stellen werden aber meist auf alle zur Durchsetzung ihrer spezifischen Interessen erforderlichen Informationen zurückgreifen können. Banken beispielsweise werden über Vermögens-, Einnahme- und Ausgabeprofile verfügen, Versicherungen über Einkommens-, Risiko- und Versicherungsprofile, Handels- und Marketingfirmen über Konsumprofile und Personalabteilungen über Leistungs-, Eignungs- und Verhaltensprofile. Verbrauchsdaten, Nutzungsdaten oder Abrechnungsdaten können für unterschiedliche Zeiträume bei Temex-Anbietern, Versorgungsunternehmen, Datenbankanbietern und TELEKOM gesammelt werden. Alle diese Stellen können also die personenbezogenen Informationen jeweils auch nutzen, um den einzelnen zu beeinflussen oder um im Konfliktfall ihre Interessen durchzusetzen. Die interessenspezifische Transparenz des einzelnen für je unterschiedliche Stellen dürfte daher die Einfluß- und Machtverteilung in den jeweiligen Beziehungen zu Lasten des Individuums verschieben.

Die Sicherheit der Verbraucher gegenüber Kundentransparenz und -manipulation könnte erheblich verbessert werden, wenn Teletransaktionen anonym durchgeführt werden könnten. Nun erlaubt die für die Rechtssicherheit von Teletransaktionen erforderliche eindeutige Identifizierung des Handelnden[113] gerade zugleich das Paradoxon einer weitgehenden Anonymität. Da nämlich in einem rechtssicheren System nicht der Name, sondern der auf einer Chipkarte implementierte Schlüssel für die Vertrauenswürdigkeit einer Telehandlung entscheidend ist, kann der einzelne unter verschiedenen Namen handeln. Er kann sich für jedes Pseudonym von unterschiedlichen Authentifikationsstellen eine Chipkarte ausstellen lassen und seine Teleüberweisungen, Teleeinkäufe, Telebuchungen, Teleberatungen und Informationsnachfragen unter wechselnden Namen abwickeln. Dadurch könnte er weitgehend verhindern, daß Teletransaktionen seiner Person zugeordnet werden können. Kundenprofile wären dann nicht mehr möglich. Mit Hilfe von TeleTrusT könnten im Normalfall bargeldlose Finanztransaktionen ebenso anonym erfolgen wie der Einkauf mit Bargeld auf dem Wochenmarkt. Dies ist möglich, weil in Streitfällen die Authentifikationsstelle - auf Beschluß eines Richters oder einer Schiedsstelle - die Identität hinter dem jeweiligen Pseudonym aufdecken könnte. Anonymität und Rechtssicherheit würden gleichzeitig gewährleistet werden.

Diese Beispiele zeigen, daß technische Maßnahmen auch die Verbrauchersicherheit erhöhen können und ein Rahmenkonzept für Sicherheit in der Informationstechnik auch diesen Aspekt von Sicherheit berücksichtigen und durch Forschung, Entwicklung und Technikzulassung unterstützen müßte.

---

[112] Vgl. zum folgenden ausführlicher Roßnagel u.a., Digitalisierung der Grundrechte?, 1990, S. 219 ff., 240 ff.

[113] Vgl. hierzu näher oben II.4.

Konsumentenschutz

Ein weiterer Aspekt der Verbrauchersicherheit ist die im Rahmenkonzept der Bundesregierung berücksichtigte Sicherheit der Verfügbarkeit und Funktionalität von Hardware und Software. Das Vorhaben, in dieser Hinsicht Qualitätskriterien für IuK-Systeme zu entwickeln und an ihnen IuK-Produkte zu überprüfen und das Prüfergebnis in Zertifikaten festzuhalten, ist zu begrüßen. Denn dadurch könnte ein höheres Maß an Markttransparenz erzielt werden.

Nachhaltig verbessert würde der Verbraucherschutz allerdings erst, wenn in diesem Zusammenhang auch die Produkthaftung verbessert würde. Einen gewichtigen Vorteil würde dem Verbraucher eine Regelung bringen, die für bestimmte Produkte eine Zertifizierung vorschreibt und an die zertifizierten Eigenschaften Haftungsregelungen knüpft. Dadurch bliebe das wirtschaftliche Risiko unsicherer Technik bei dem, der sie entwickelt und in den Verkehr bringt, der also ihre Produktsicherheit beeinflussen kann, und würde nicht auch noch auf diejenigen abgewälzt, die als Käufer und Anwender bereits den unmittelbaren Schaden unsicherer Technik tragen müssen.

1.5 Verbesserung der Funktionsicherheit technischer Systeme

Bei aller bisher vorgetragenen Kritik am Rahmenkonzept der Bundesregierung muß anerkannt werden, daß die darin beschriebenen Aufgaben zur Gewährleistung "informationstechnischer Sicherheit" auch unter der hier vertretenen erweiterten Zielsetzung von großer Bedeutung sind. Die technische Sicherheit ist eine der notwendigen Voraussetzung zur Reduzierung gesellschaftlicher Verletzlichkeit, wenngleich auch nicht die einzige und auch nicht die wichtigste.

Unabhängig von den Untersuchungen der Abhängigkeit und des Schadenspotentials ist die Sicherheit von eingesetzten und einzusetzenden IuK-Techniken durch unabhängige Instanzen zu bewerten. IT-Entwickler und -anwender können dieser Anforderung aufgrund ihrer häufig auf kurzfristige Rentabilität ausgerichteten Interessen nicht gerecht werden. Außerdem gibt es mit durch Systemversagen oder Manipulation vielfach eingesetzter Software oder Hardware eine Schadenskatagorie, die nicht im einzelnen Anwendungszusammenhang bewertet werden kann (Multiplikations- und Kopplungsschäden).[114]

Entwickelte Hardware und Software muß also durch unabhängige Validierungsinstanzen auf Korrektheit und Zuverlässigkeit und Manipulationsfreiheit überprüft und zertifiziert werden. Bei Kryptoverfahren muß auch geprüft werden, ob es möglich ist, die verwendeten Algorithmen zu brechen. Sollen diese Validierungsinstanzen ihre Funktion in vertrauenswürdiger Form erfüllen, müssen Interessenkonflikte wie die folgenden vermieden werden:

- Validierungs- und Revisionsinstanzen dürfen kein Interesse an den Daten haben, deren ordnungsgemäße und sichere Verarbeitung sie kontrollieren sollen.

- Sie dürfen nicht der Geheimhaltung unterliegen und gezwungen sein, der Öffentlichkeit gegenüber erkannte Sicherungslücken und praktizierte Sicherungsverfahren zu verheimlichen.

---

[114] Vgl. zur Beschreibung IuK-spezifischer Schäden Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 73 ff.

2. Bedingungen der Aufgabenerfüllung

Um diese erweiterten Aufgaben erfüllen zu können, müssen Staat und Gesellschaft über drei Fähigkeiten verfügen:

- Erkenntnisfähigkeit

  Sie müssen in der Lage sein, künftige Risiken so früh zu erkennen, daß ihnen rechtzeitig durch Technikauswahl und Technikgestaltung begegnet werden kann. Dies stößt aber für die IuK-Technik auf besondere Schwierigkeiten,

  - weil in diesem Bereich die Technik besonders rasant weiterentwickelt wird,
  - weil wegen der Multifunktionalität der Technik die künftigen Anwendungszwecke und -bedingungen nur sehr schwer abzuschätzen sind,
  - weil die sozio-technischen Wechselwirkungen von Technikfolgen sehr komplex sind und
  - weil die Technikfolgen oft erst sehr spät eintreten und daher wenig präzise prognostizierbar sind.

- Lernfähigkeit

  Wegen dieser technikbedingten Erkenntnisschwierigkeiten ist es besonders wichtig, daß Staat und Gesellschaft aus Fehlern, die zu untragbaren Risiken geführt haben, lernen können. Um sich diese Fähigkeit für die Zukunft zu erhalten, müssen sie durch Technikgestaltung und politische Strukturmaßnahmen die hierfür notwendigen Bedingungen schaffen:

  - Die technische Entwicklung muß dadurch korrigierbar bleiben, daß technische Alternativen offengehalten oder hergestellt werden.
  - Um möglichst vorgreiflich, und nicht nur nachträglich, lernen zu können, muß das erforderliche Zukunftswissen in organisierten Verfahren erworben und an die Öffentlichkeit und die Entscheidungsträger vermittelt werden. Bei der Langfristigkeit und Komplexität der Technikfolgen kann nicht mehr auf spontane Erfahrungsbildung vertraut werden.
  - Auch kann die Komplexität der Aufgaben nicht mehr durch individuelle Lernprozesse bewältigt werden. Mit der Aufgabe der Verringerung der Verletzlichkeit der Gesellschaft sind vielmehr verantwortliche Institutionen zu betrauen.
  - Schließlich muß aureichend Zeit zum Lernen verbleiben. Lernprozesse dürfen nicht durch sie überholende vollendete Tatsachen obsolet gemacht werden.

- Steuerungsfähigkeit

Staat und Gesellschaft müssen schließlich in der Lage sein, die Lernergebnisse in Handlungsstrategien umzusetzen, die durch Beeinflussung der Technikentwicklung die Verletzlichkeit der Gesellschaft reduzieren. Um diese Fähigkeit zu erfolgreicher Techniksteuerung zu erlangen, müssen sie folgende Bedingungen gewährleisten:

- Sie benötigen Steuerungskriterien, die das Ziel einer Verringerung gesellschaftlicher Verletzlichkeit konkretisieren.

- Sie benötigen Steuerungsinstrumente, die ihnen ermöglichen, die Kriterien in konkrete Anforderungen an die Ausgestaltung eines Techniksystems umzusetzen.

- Erforderlich ist weiterhin ein Steuerungszugriff, der es Staat und Gesellschaft ermöglicht, diese Instrumente anzusetzten, und der verhindert, daß sich technische Entwicklung staatlicher oder gesellschaftlicher Einflußnahme entziehen.

- Notwendig ist außerdem eine ausreichende Steuerungsmacht, um die Technikgestaltung auch gegen widerstreitende Interessen durchsetzen zu können.

- Weiterhin sind die Bedingungen für die erforderliche Kontrollfähigkeit zu schaffen, damit kontrolliert werden kann, ob die gesetzten Ziele auch erreicht wurden.

- Schließlich ist ausreichende Steuerungszeit erforderlich, um von der technischen Entwicklung nicht vor vollendete Tatsachen gestellt zu werden.

3. Handlungsbedarf und Handlungsmöglichkeiten

Allein durch Entscheidungen für neue Institutionen und neue Verfahren können weder die genannten Aufgaben erfüllt noch die Bedingungen zu ihrer Erfüllung hergestellt werden. Die Verletzlichkeit der Gesellschaft zu verringern, bleibt eine ständige Aufgabe lebendiger Politik und demokratischen Engagements. Aber - Institutionen und Verfahren können, je nach dem wie sehr sie den Problemen adäquat oder inadäquat sind, das Erreichen der gesteckten Ziele sehr befördern oder behindern. Daher sind Entscheidungen über die Form, wie die gesellschaftliche Behandlung des Problems der Verletzlichkeit organisiert wird, von einer nicht zu unterschätzenden politischen Bedeutung.

Auf der Suche nach problemadäquaten Regelungen, Verfahren und Institutionen darf das Heil nicht vorschnell in der Errichtung eines neuen Bundesamtes für Sicherheit in der Informationstechnik gesucht werden, dem die Lösung aller Aufgaben übertragen wird. Denn dann entsteht ein bürokratischer Zentralismus, der zu schnell in einem bürokratischen Immobilismus endet und Sicherheit - wie im Bereich der Atomenergie - nur als Problem bürokratischer Verantwortlichkeit versteht: Als sicher gilt ein Technik-System dann, wenn der zuständige Beamte die bürokratischen Sicherheitsregeln überprüft hat und deshalb nicht mehr zur Verantwortung gezogen werden kann.

Auch könnte dem Systemcharakter der IuK-Technik je nach Anwendungsbedingungen ein Verfahren besser gerecht werden, das die Prüfung und Gestaltung der Technik nach Verletzlichkeitsgesichtspunkten nicht zentral und bürokratisch regeln will, sondern dezentraler und fortwährender Willensbildung überträgt. Die konkrete Gestaltung und Anwendung der IuK-Systeme sollte - soweit dies möglich ist - in sozialer Selbstverwaltung zwischen dem Anwender und den Betroffenen erfolgen. Aufgabe des Gesetzgebers wäre es, hierfür adäquate Verfahren und Sicherungen für eine ausgeglichene Beteiligung aller Betroffenen zu gewährleisten.

Bevor also Aufgaben, Befugnisse und Organisationsform des Bundesamt für Sicherheit in der Informationstechnik erörtert werden, ist zu fragen,

- Wo sind Verletzlichkeitsprüfungen in bestehende Strukturen (Technikprüfungen, Anwendungsregelungen, Verfahren des Interessenausgleichs) integrierbar, um nicht unnötigerweise neue Bürokratien zu schaffen?

- Wo kann die notwendige Steuerungsmacht zur Technikgestaltung dezentral verteilt werden, um bürokratische Machtballung zu verhindern, und wo muß sie, um überhaupt wirksam zu sein, zentral gebündelt werden?

- Wo kann die Öffentlichkeit am effektivsten in den Prozeß der Technikgestaltung einbezogen werden?

Zu fragen ist daher zuerst, welche Regelungen, Verfahren und Institutionen bestehen bereits, die sich mit Fragen der Verletzlichkeit befassen oder befassen könnten. Hierzu werden kurz die Möglichkeiten diskutiert, die das Haftungsrecht (3.3) und die technische Normung (3.4) haben und haben könnten, um die Verletzlichkeit der Gesellschaft zu verringern. Zuvor werden jedoch Verfahren beschrieben, die die Zulassung von Techniksystemen regeln, und es wird geprüft, inwieweit diese auf Verletzlichkeitsfragen ausgeweitet werden können (3.1) oder inwieweit eigene IuK-spezifische Zulassungsverfahren erforderlich sind (3.2).

3.1 Bestehende Zulassungsverfahren

Das Technikrecht kennt eine Vielzahl von unterschiedlichen Regelungsmodellen, in denen mit Hilfe von Zulassungen, Erlaubnissen oder Genehmigungen Gefahren abgewehrt, Risiken vermindert und ein Ausgleich zwischen verschiedenen Rechtspositionen hergestellt werden soll.

Die im folgenden erörterten Regelungs- und Verfahrensmodelle sind Beispiele dafür, wie Staat und Gesellschaft die Zulassung von Techniksystemen organisieren können. Eine systematische Prüfung, inwieweit Verletzlichkeits- und Sicherheitsfragen der IuK-Technik in bestehenden Verfahren geprüft werden oder werden könnten, erfordert eine eigene Untersuchung. Hier sind jedoch wichtige Regelungs- und Verfahrenstypen anzusprechen, um den Regelungsrahmen abstecken und die erforderlichen Aufgaben und Befugnisse des neuen Bundesamtes für Sicherheit in der Informationstechnik bestimmen zu können. Mit der Darstellung dieser Planungs- und Verfahrenstypen soll kritisch überprüft werden,

- inwieweit in ihnen Aspekte der Verletzlichkeit der Gesellschaft durch die Nutzung von IuK-Technik thematisiert werden kann.

- inwieweit die Prüfung von Verletzlichkeitsaspekten de lege late oder de lege ferenda in sie integriert werden könnte.

- inwieweit sie Vorbild für die Zulassung von IuK-Technik sein könnten.

3.1.1 IuK-Technik als Geräteteil - das Beispiel der Kraft- und Luftfahrzeugzulassung

Typisches Beispiel für die Zulassung einer gefährlichen Technik ist die Zulassung von Kraftfahrzeugen nach § 1 Abs. 1 Satz 1 Straßenverkehrsgesetz (StVG). Dort heißt es:

> "Kraftfahrzeuge, die auf öffentlichen Wegen oder Plätzen in Betrieb gesetzt werden sollen, müssen von der zuständigen Behörde zum Verkehr zugelassen sein."

Die Zulassung ergeht nach §§ 18 ff StVZO in Form einer Betriebszulassung. Sie wird im Regelfall dem Hersteller für die Serienproduktion als Allgemeine Betriebserlaubnis erteilt, wenn er die Gewähr für eine zuverlässige Ausübung der verliehenen Befugnis bietet (§ 20 Abs. 1 StVZO). Die Betriebserlaubnis kann auch für einzelne Teile des Kraftfahrzeugs erteilt werden (§ 22 StVZO). Zuständige Behörde für die Erteilung der Allgemeinen Betriebserlaubnis ist das Kraftfahrzeugbundesamt, das auch einen amtlich anerkannten Sachverständigen oder eine andere Stelle mit der Begutachtung beauftragen kann (§ 20 Abs. 2 StVZO). Bei Einzelfahrzeugen ist die zuständige Stelle die Zulassungstelle (§ 21 StVZO). Die Betriebserlaubnis ist zu er-

teilen, wenn das Fahrzeug den Vorschriften der StVZO sowie verschiedenen im einzelnen aufgeführten EG-Richtlinien entspricht (§ 19 Abs. 1 StVZO).[115]

Ein anderes Beispiel ist die Verkehrszulassung für Luftfahrzeuge nach § 2 Abs. 1 Luftverkehrsgesetz (LuftVG). Danach bedarf ein Luftfahrzeug der Verkehrszulassung sowie in der Regel der Eintragung in ein gesondertes Verzeichnis deutscher Luftfahrzeuge ("Luftfahrzeugrolle").

> "Zum Verkehr zugelassen wird ein Luftfahrzeug nur, wenn
> 1.das Muster des Luftfahrzeuges zugelassen ist (Musterzulassung),
> 2.der Nachweis der Verkehrssicherheit nach der Prüfordnung für Luftfahrtgerät geführt ist,
> 3.der Halter des Luftfahrzeuges nach den Vorschriften dieses Gesetzes versichert ist oder durch Hinterlegung von Geld oder Wertpapieren Sicherheit geleistet hat und
> 4.die technische Ausrüstung des Luftfahrzeuges so gestaltet ist, daß das durch seinen Betrieb entstehende Geräusch das nach dem jeweiligen Stand der Technik unvermeidbare Maß nicht übersteigt" (§ 2 Abs. 1, Satz 2 LuftVG).

Die Voraussetzungen, an die die Zulassung geknüpft ist, lassen sich zu folgenden Merkmalen zusammenfassen:

- Musterzulassung, d.h. Typenprüfung;
- Verkehrssicherheit, d.h. Funktionsprüfung zum Schutz Dritter;
- Haftung, d.h. Absicherung Dritter im Schadensfall;
- Lärmschutz, d.h. Schutz Dritter gegen spezifische Beeinträchtigungen[116].

Das vorgestellte Grundmodell der Kraft- oder Luftverkehrszulassung ist auf Massenprodukte eingerichtet. Es arbeitet daher mit allgemeinen Betriebszulassungen, die der Staat durch eigene Bundesoberbehörden erteilt. Ebenso wie die Produkte selbst typisiert sind, lassen sich auch die Gefahren der zugelassenen Technik spezifisch beschreiben, so daß die Zulassungsvoraussetzungen entsprechende Voraussetzungen formulieren. So spielt beispielsweise bei der Musterzulassung der Luftfahrzeuge der Verkehrslärm eine besondere Rolle.

Das Modell der Produktzulassung über die Erteilung einer allgemeinen Betriebserlaubnis kann auf den Bereich der Informationstechnik übertragen werden. Nach Produkttypen würde eine zentrale Stelle, wie das neue Bundesamt für Sicherheit in der Informationstechnik, Produkte der Hard- und Software prüfen und ihnen eine allgemeine Betriebszulassung erteilen. Die Zulassungsvoraussetzungen müßten vorher allgemein festgelegt werden.

Soweit IuK-Technik Bestandteil solcher Massenprodukte ist, kann auch sie im Rahmen der Zulassungsprüfungen auf ihre Basissicherheit überprüft werden. Dies wäre einer IuK-spezifischen Prüfung insoweit vorzuziehen, als dieses Verfahren erheblich anwendungsnäher ist. In ihm können die spezifischen Anwendungsrisiken besser beurteilt werden. In einem anwendungsunabhängigen Verfahren kann zwar die Gerätesicherheit, wie etwa der Schutz vor Abstrahlung, gewährleistet werden. Ob Software ausreichend sicher ist kann dagegen in der Regel nur geprüft werden, wenn bekannt ist, wofür sie eingesetzt werden soll.

In solchen allgemeinen Produktprüfungen können aber kaum die konkreten individuellen und gesellschaftlichen Risiken der jeweiligen Technikanwendung im Einzelfall berücksichtigt werden. Die Kumulation der vielen individuellen Anwendungen und der dadurch entstehende Grad von Abhängigkeit bleibt außerhalb des Blickfelds.

3.1.2. IuK-Technik als Anlagenteil - das Beispiel umweltrechtlicher Genehmigungsverfahren

Ein ganz anderes Beispiel technischer Sicherheitsprüfung findet sich im Bereich des Umweltschutzes. Nehmen wir zum Beispiel an, eine neue chemische Produktionsanlage solle errichtet und mit Hilfe eines Prozeßrechners gesteuert werden. Sie bedarf zur Errichtung und für den Betrieb einer Genehmigung nach dem Bundesimmisionsschutzgesetz (BImSchG). In diesem Genehmigungsverfahren hat der Antragsteller eine Si-

---

[115] Vgl. im übrigen Jagusch u.a., Straßenverkehrsrecht, 30. Auflage, München 1989.

[116] Vgl. im übrigen Hofmann, Luftverkehrsgesetz, München 1971.

cherheitsanalyse vorzulegen[117], die unter anderen auch eine Beschreibung der Gefahrenquellen beinhalten muß, die durch ein Versagen von Meß-, Steuer- und Regeleinrichtungen entstehen können.[118] Die Genehmigungsbehörde hat zu prüfen, ob der Antragsteller die Anlage mit ausreichend zuverlässigen Meßeinrichtungen und Steuer oder Regeleinrichtungen ausgestattet hat, die soweit dies sicherheitstechnisch geboten ist, jeweils mehrfach vorhanden, verschiedenartig und voneinander unabhängig sein müssen.[119]

In diesem Genehmigungsverfahren ist die Öffentlichkeit beteiligt. Vor der Erteilung der Genehmigung müssen die Antragsunterlagen öffentlich ausgelegt werden. In dieser Zeit kann jeder Einwendungen gegen die geplante Anlage und damit auch gegen die vorgesehene Prozeßsteuerung erheben. Die Einwendungen sind in einem gesonderten Erörterungstermin zwischen Einwendern, Antragsteller und Genehmigungsbehörde zu erörtern. Vorgebracht werden können alle Einwendungen, die mit der zu genehmigenden Anlage zusammenhängen. Es gibt keine sachliche Beschränkungen.[120] Innerhalb eines solchen Verfahrens kann daher auch die Fehlerabhängigkeit der angewendeten IuK-Techniken und deren Auswirkungen auf die Rechte der Betroffenen wie Gesundheit, Eigentum und Umwelt diskutiert werden. Es können aber auch gesamtgesellschaftliche Auswirkungen eingewendet werden.

Diese Erörterungsmöglichkeit sagt noch wenig über den Erfolg einer Einwendung aus, die sich kritisch mit der eingesetzten IuK-Techniken auseinandersetzt. Sie setzt zum Beispiel voraus, daß die Einwenderseite auch über Sachverständige verfügt, die sich mit der Anfälligkeit eines geplanten Prozeßsteuerungs-Systems auseindersetzen können. Hinzu kommt, daß die Genehmigungsbehörde, wenn überhaupt, nur solchen Einwendungen Beachtung schenkt, die eine Verletzung subjektiver Rechte geltend machen. Damit ist jedenfalls rechtlich - unabhängig von den politischen Wirkung - eine "bloß" auf die Verletzlichkeit der Gesellschaft abzielende Einwendung gegen die Anwendung einer bestimmten Prozeßsteuerung wenig erfolgversprechend. Sie müßte mit den konkreten gesundheitlichen oder eigentumsrechtlichen Auswirkungen des Versagens einer solchen Technik begründet werden.

Das hier gewählte Beispiel einer BImSchG-Genehmigung steht für eine Fülle von umweltrechtlichen Genehmigungs- oder Planfeststellungsverfahren, bei denen Voraussetzung für die Zulassung ein öffentliches Genehmigungsverfahren ist. Dadurch ermöglichen diese Verfahren im Gegensatz zu den oben dargestellten produktbezogenen Zulassungsverfahren wenigstens in den Ansätzen eine breitere Erörterung der spezifischen Risiken einer Technik. Hinzu kommt, daß die Teilnahme an der Erörterung grundsätzlich jedem offen steht, soweit er gegen die Anlage Einwendungen erhoben hat. Ebenso lassen sich auf diese Weise auch Erfahrungen über Folgewirkungen bisher erteilter Genehmigungen einbringen. Gleichwohl zeigt die Entwicklung der Erörterungsverfahren im Umweltrecht, daß die Einwenderseite nur dann Chancen auf die Berücksichtigung ihrer Interessen hat, wenn sie sich selbst professioneller Hilfe (z.B. Öko-Institut) bedient und mit wissenschaftlichen Gegengutachten eigene Befürchtungen substantiiert und Einwendungen begründet. Damit wohnt derartigen Verfahren inzident die Gefahr einer Entfremdung inne.

In umweltschutzrechtlichen Genehmigungs- und Planfeststellungsverfahren sollte grundsätzlich der Einsatz von IuK-Techniken geprüft und auf sein anwendungsbezogenes Gefährdungspotential hin untersucht werden. Im Rahmen des geltenden Rechtes können Einwender und Einwenderinnen schon jetzt den Einsatz von IuK-Techniken problematisieren. Allerdings sind diese Verfahren in der Regel ungeeignet, den Kumulationseffekt individueller Anwendungen und damit die gesellschaftliche Abhängigkeit vom Funktionieren der Technik zu steuern. Denn die Genehmigungsvorschriften gewähren dem Antragsteller einen Rechtsanspruch auf Genehmigung, wenn er die Genehmigungsvoraussetzungen - z. B. ausreichende Sicherheit der individuellen Anlage - erfüllt.

---

[117] Vgl. § 4 Abs. 2a der 9. BImSchV und § 7 der 12. BimSchV.

[118] Vgl. Punkt 3.2.4.1 der 2. StörfallVwV.

[119] § 4 Nr. 4 der 12. BImSchV.

[120] Vgl. Führ, Sanierung von Industrieanlagen, Düsseldorf, 1989, S. 76.

Umweltrechtliche Genehmigungsverfahren könnten - bei allem Unterschied in der zu beurteilenden Technik - als Orientierung für ein öffentliches Zulassungsverfahren für IuK-Technik dienen. Mit Hilfe derartiger Zulassungsverfahren könnte der Einsatz von IuK-Techniken anwendungsbezogen geprüft werden. Im Vordergrund stünde dann aber nicht die Gerätesicherheit, sondern der Einsatz von IuK-Techniken wie beispielsweise die Vernetzung einer Produktionsstätte in einem CIM-System oder die Einführung eines Krankenhausinformationssystems.

3.1.3 IuK-Technik in Anwendungssystemen - das Beispiel der Unternehmerzulassung und der betrieblichen Mitbestimmung

Nicht die staatliche Prüfung und Zulassung von Technik liegt dem Regelungsmodell der betrieblichen Mitbestimmung zugrunde, sondern das Modell einer (weitgehend) autonomen Regelung von Interessenkonflikten zwischen den Konfliktparteien selbst. Hier kann von Zulassung im eigentlichen Sinn nicht gesprochen werden, weil die von einer Technik betroffenen Arbeitnehmer über Mitbestimmung, wie gleich zu zeigen ist, eine Technik nicht "kippen" können. Die Mitbestimmung nach dem bundesdeutschen Recht beschränkt sich auf Unterrichtungs-, Mitsprache- und in bestimmten Fällen eben Mitbestimmungsrechten, die unterhalb einer Zulassungsgrenze liegen. Abgesehen davon handeln im Betrieb bzw. der öffentlichen Verwaltung die Parteien Kapital und Arbeit ohne staatliche Machtmittel.

Eine umfassende Diskussion der Verletzlichkeit eines IuK-Systems ist in Betrieben und öffentlichen Verwaltungen grundätzlich schwieriger als etwa in umweltrechtlichen Genehmigungsverfahren. Regelmäßig bestehen zwar für die Gestaltung des Arbeitsplatzes Mitspracherechte des Betriebs- bzw. Personalrates. Die Mitspracherechte beschränken sich aber auf die Verhaltens- und Leistungskontrolle der Arbeitnehmer[121] sowie die Verarbeitung der Personaldaten[122].

An diesem Tatbestand hat auch die Neufassung des BetrVG nichts geändert[123]. Das Mitbestimmungsrecht nach § 91 BetrVG erstreckt sich nur auf Änderungen der Arbeitsplätze, des Arbeitsablaufes oder der Arbeitsumgebung, wenn sie "den gesicherten arbeitswissenschaftlichen Erkenntnissen über die menschengerechte Gestaltung der Arbeit offensichtlich widersprechen". Hinzugekommen ist nach § 90 Abs. 1 BetrVG lediglich eine Unterichtungspflicht des Arbeitsgeber gegenüber dem Betriebsrat über die Planung

1. von Neu-. Um- und Erweiterungsbauten von Fabrikations-, Verwaltungs- und sonstigen betrieblichen Räumen,
2. von technischen Anlagen,
3. von Arbeitsverfahren und Arbeitsabläufen oder
4. der Arbeitsplätze

unter rechtzeitiger Vorlage der erforderlichen Unterlagen. Die Beratungspflicht nach § 90 Abs. 2 BetrVG gegenüber dem Betriebsrat beschränkt sich auf die Auswirkungen der genannten Planungen auf die Arbeitnehmer. Ähnlich begrenzt sind die Mitwirkungsmöglichkeiten des Betriebsrats nach § 111 BetrVG. Diese sowieso nur beschränkten Einflußmöglichkeiten der Personalvertretungen können lediglich für die unmittelbaren Arbeitnehmerinteressen eingesetzt werden. Gesellschaftliche Auswirkung der im Betrieb angewendeten Techniksysteme bleiben jenseits ihrer Einflußsphären.

Die Interessen Dritter, beispielsweise der Kunden eines Unternehmens oder der Behördenbesucher, bleiben im Regelfall außer Acht. Unberücksichtigt bleiben etwa die Auswirkungen, die der Ausfall einer verwendeten IuK-Technik eines privaten Dienstleistungsunternehmens oder einer Behörde auf die Gesellschaft haben. Re-

---

121 § 87 Abs. 1 Nr. 6 BetrVG (v. 23.12.1988, BGBl. 1989 I, S. 1 ff); BAG NZA 1086, 526; BGA AuR 1988, 126; Dazu auch Fitting, u.a., Betriebsverfassungsgesetz, 15. Aufl., München 1987, § 87, Rn. 64 ff., insb. 75 ff.; Hess, u.a., BetrVG, Darmstadt, 1986, § 87, Rn. 276 ff. Hinzuweisen ist auch auf Steinmüller, CR 1989, S. 606 ff.

122 Vgl. beispielsweise für den öffentlichen Bereich die Personalvertretungsgesetze der Länder zum Beispiel § 74 Abs. 1 Nr. 17, § 81 HessPVG (vom 24.3.1988, GVBl. I, 103. Einen Überblick über die Rechtsprechung gibt Gola, NJW 1989, S. 2595 (2600); VGH Kassel, NJW 1989, S. 2641: Die Änderung einer Datenverarbeitungsanlage (Systemwechel) kann Mitbestimmungsrechte auslösen.

123 BetrVG vom 23. 12. 1988, BGBl. 1989 I, S. 1 ff. Dazu auch Schneider, Recht der Datenverarbeitung 1989, S. 113 ff.

levant ist dies vor allem bei wichtigen Dienstleistungen, wie etwa Notrufsystemen, Verkehrsleitsystemen, Banken, Verkehrsunternehmen wie der Bahn oder Flugunternehmen oder Sozialhilfe und Sozialversicherungen. Immerhin nennt das Rahmenkonzept der Bundesregierung für den Bereich der öffentlichen Verwaltung als besonders sensibele Anwendungsbereiche:

> "z.B. das Haushalts-, Kassen- und Rechnungswesen, Nachweisverfahren für Sondermüll und die Flugsicherung".[124]

Das Betriebsverfassungsgesetzes und die Personalvertretungsgesetze enthalten keine Zulassungsverfahren für IuK-Systeme. Es bestehen lediglich begrenzte Mitwirkungsmöglichkeiten, die keine Entscheidungskompetenz der Arbeitnehmervertretungen vorsehen. Außerdem ist die Mitwirkung auf die Rechtspositionen und die Interessen der im Betrieb Beschäftigten beschränkt. Dadurch besteht zwar die Möglichkeit, den Einsatz von IuK-Techniken anwendungsbezogen zu diskutieren, nicht aber "betriebsfremde" Interessen, wie einseitige Abhängigkeiten durch den Einsatz einer IuK-Technik zu berücksichtigen.

Zwar könnte die betriebliche Mitbestimmung auf alle Aspekte, auch Verletzlichkeitsgesichtspunkte, der im Betrieb genutzten IuK-Technik ausgeweitet werden. Solange in diesen Verfahren aber nur die Arbeitgeber und die Arbeitnehmervertreter beteiligt sind, bleiben die Interessen Dritter ohne Repräsentation. Um sie zu berücksichtigen, sind staatliche Verfahren mit Öffentlichkeitsbeteiligung erforderlich.

Zu fragen bleibt, ob Anwendungssysteme im Rahmen von Unternehmergenehmigungen geprüft und geregelt werden könnten. Aus der Liste der Dienstleistungen wird hier als Beispiel der Geldverkehr herausgegriffen. Eine große Bedeutung spielen IuK-Techniken für den Transfer von Geld. Dabei geht es nicht nur um die Geschäftsabwicklung zwischen einem privaten Kunden und einer Bank, sondern um das Banking zwischen Banken einschließlich des Börsen- und Wertpapiergeschäftes.

Das Betreiben von Bankgeschäften bedarf nach § 32 Abs. 1 Kreditwesengesetz (KWG) der Erlaubnis durch das Bundesaufsichtsamt für das Kreditwesen. Allerdings darf die Erlaubnis nur unter bestimmten im Gesetz näher aufgeführten Voraussetzungen versagt werden (§ 33 Abs. 1 KWG). Unter diesen Voraussetzungen ist die technische Sicherheit der verwendeten IuK-Techniken nicht aufgeführt.

Eine Erlaubnis kann zwar unter Auflagen erteilt werden. Diese muß sich allerdings an die Zweckbestimmung des KWG halten (§ 32 Abs. 2 KWG). Zu diesen Zwecken zählen nach der Aufgabenbestimmung des Bundesaufsichtsamtes die Sicherheit der Vermögenswerte, die ordnungsgemäße Durchführung der Bankgeschäfte oder die Abwehr erheblicher Nachteile für die Gesamtwirtschaft (§ 6 Abs. 2 KWG). Auflagen, die sich auf die Sicherheit von IuK-Techniken beziehen, könnten demnach, soweit sie diesen Zwecken dienen, möglich sein. Gleichwohl ist zu berücksichtigen, daß bestehende Banken über eine Erlaubnis verfügen, nachträgliche Auflagen durch das KWG aber nicht vorgesehen sind, so daß im Ergebnis das KWG keine rechtliche Handhabe bietet, bestimmte technische Standards im Wege der nachträglichen Auflage durchzusetzen.[125]

Das Beispiel des Kreditwesens steht für Erlaubnisverfahren in Bereichen, die zwar von der Anwendung der IuK-Techniken betroffen sind, deren Gefahren und Risiken aber keine Berücksichtigung finden. Dabei kann es offen bleiben, ob es wünschenswert wäre, daß die Erlaubnis für das Betreiben von Bankgeschäften zusätzlich an Voraussetzungen bestimmter technischer Standards der IuK-Techniken geknüpft wäre. Schließlich kann die Einhaltung bestimmter Standards in einem "empfindlichen" Gewerbe wie dem Geldgeschäft auch über andere Regulative erfolgen. Das Beispiel soll hier lediglich belegen, daß durch die IuK-Techniken sensible Dienstleistungen des privaten Bereiches betroffen sind, denen keine staatlichen Regelungen gegenüberstehen, die die Risiken eines Einsatzes von IuK-Techniken oder die Verletzlichkeit der Gesellschaft berücksichtigen.

---

[124] Kabinettsvorlage des BMI vom 25.10.1989, S. 1, Pkt. 1.1., auch DuD 1989, S. 291.

[125] Vgl. Szagunn/Neumann/Wohlschieß, Gesetz über das Kreditwesen, 3. Aufl, Stuttgart 1976, § 32, Rn. 16; Bähre/Schneider, Kreditwesengesetz. 3. Aufl., München 1986, § 32, Nr. 5.

3.1.4 IuK-Technik in Infrastruktursystemen - das Beispiel der Telekommunikation

Von erheblicher Bedeutung für die Einschätzung der Risiken von IuK-Techniken sind die Dienste der Deutschen Bundespost TELEKOM. Zu prüfen ist, in welchem Umfang die Zulassung bestimmter IuK-Techniken an Voraussetzungen geknüpft sind, die ihr anwendungsspezifisches Gefährdungspotential berücksichtigen.

Nach § 1 Abs. 2 Gesetz über Fernmeldeanlagen (FAG)[126] hat die Post noch das Netzmonopol, d.h. das Recht, Übertragungswege einschließlich der zugehörigen Abschlußeinrichtungen zu errichten und zu betreiben. Die Befugnis zur Errichtung und zum Betrieb einzelner Fernmeldeanlagen kann der Postminister verleihen (§ 2 Abs. 1 FAG).

Hingegen können Endgeräte von jedermann errichtet und betrieben werden, die Endgeräte müssen aber zugelassen werden (§ 1 Abs. 3 FAG). Das Zulassungsverfahren regelt im einzelnen der Postminister durch Rechtsverordnung. Auf die Zulassung besteht aber ein Rechtsanspruch, wenn die gesetzlichen Voraussetzungen erfüllt sind (§ 2 a Abs. 3 FAG). Dazu zählt, daß

> durch die Anschaltung oder den Betrieb der zuzulassenden Einrichtungen weder Übertragungswege der Deutschen Bundespost TELEKOM
>
> noch Endeinrichtungen und Personen geschädigt oder gefährdet werden ...(§ 2 a Abs. 1 Satz 1 FAG).

Die privaten Endeinrichtungen dürfen nur von Personen errichtet, geändert oder instandgehalten werden, die aufgrund ihrer Sach- und Fachkunde dazu zugelassen sind, soweit es zur Vermeidung von Störungen erforderlich ist (§ 2 a Abs. 2 FAG).

Ebenso ist jedermann berechtigt, Telekommunikationsdienstleistungen für andere zu erbringen mit Ausnahme des Telefondienstes (§ 1 Abs. 4 FAG). Die Betreiber müssen die Aufnahme des Betriebes sowie Änderungen und Aufgabe beim Postminister schriftlich innerhalb eines Monates anzeigen, der die Anzeigen im Amtsblatt veröffentlicht (§ 1 a Abs. 1 FAG).

Die hier aufgezählten Regelungen beschränken sich auf kaum nennenswerte Voraussetzungen für die Zulassung von IuK-Techniken. Private Telekommunikationsdienste müssen nur angezeigt werden. Endgeräte müssen zwar zugelassen werden, die Regelungen im Detail bleiben aber dem Verordnungsgeber vorbehalten und beziehen sich lediglich auf die Betriebssicherheit. Andere Aspekte der Verletzlichkeit bleiben unberücksichtigt. Auch fehlen gesetzliche Steuerungsinstrumente schon in der Netzgestaltung, die die Bundespost zur Berücksichtigung solcher Aspekte zwingt, sowie Zulassungsverfahren für einzelne Dienste, die eine Prüfung von Verletzlichkeitsgesichtspunkten ermöglichen.

Die Telekommunikationsdienstleistungen bilden eine wichtige Grundlage für den gesamten Einsatz der IuK-Technik. Ohne sie kann keine institutionsübergreifende Vernetzung stattfinden. Gleichwohl sieht das geltende Recht keine Verfahren vor, bei denen die Dienstleistungen der Post auf ihre Risiken, und sei es nur für die Rechte Dritter, überprüft werden.

Durch entsprechende Regelungen - etwa im FAG - könnte zwar die Post zur Berücksichtigung von Verletzlichkeitsaspekten in der eigenen Planung und der Zulassung von Telekommunikationsdiensten angehalten werden. Es ist jedoch sehr fraglich, ob ausgerechnet die Post ihre eigenen Leistungen oder die Leistungen der Konkurrenten überprüfen sollte. Denn die Post kann nicht mit ihrem Unternehmen TELEKOM in Konkurrenz zu anderen Diensteanbietern agieren und zugleich als objektiver und neutraler Schiedsrichter sowohl die Regeln des Wettbewerbs festlegen als auch deren Einhaltung bei sich selbst und bei der Konkurrenz überprüfen. Hierfür ist eine tatsächlich neutrale und von der Post völlig unabhängige staatliche Institution erforderlich.

---

[126] FAG vom 21.7. 1989, BGBl I. 1989, S. 1456

3.1.5 Zusammenfassung

Diese Auswahl geltender Zulassungs- und Genehmigungsverfahren zeigt, daß zwar verschiedene Zulassungsverfahren technischer Einrichtungen bestehen, die spezifischen Risiken der IuK-Technik aber, wenn überhaupt, nur begrenzt Berücksichtigung finden. Am offensten, aber je nach Rechtsbetroffenheit auch unverbindlichsten, sind in Bezug auf IuK-Techniken umweltrechtliche Genehmigungsverfahren.

Hingegen bietet das Verfahren der Kraftfahrzeug- oder Luftverkehrszulassung ein Beispiel typisierender Prüfungen der spezifischen Risiken. Es beschränkt sich allerdings auf die Verkehrssicherheit und bestimmte typische Gefahren für Dritte (wie den Lärm von Flugzeugen).

Die Leistungsfähigkeit der Arbeitnehmervertretungen beschränkt sich rechtlich auf die Betroffenheit der Mitarbeiter. Die Arbeitnehmervertretung gewährleistet zwar eine Verknüpfung von technischer Sicherheit mit den Datenschutzinteressen der Beschäftigten, aber schon gegenüber den durch die Produktion betroffenen Belangen Dritter wie bsp. den Kunden einer Firma/eines Produktes ist das Instrument der betrieblichen Mitbestimmung wirkungslos.

Der Unternehmergenehmigung sind Gestaltungsvorgaben fremd, auch wenn die Tätigkeit des Unternehmers nur mit Hilfe technischer Systeme durchgeführt werden kann und große Schadenspotentiale hervorruft. Für den Bereich der Bankwirtschaft etwa, deren Ausübung erlaubnispflichtig ist, kann im Rahmen des KWG durch die Bankaufsicht kein Einfluß auf die Ausgestaltung der IuK-Technik genommen werden.

Für IuK-Infrastrukturen finden keine öffentlichen Planungsverfahren statt. Neue Telekommunikationsdienste können sogar völlig unkoordiniert, lediglich auf Anzeige hin, vom Anbieter betrieben werden.

Diese bestehenden Prüf- und Genehmigungsverfahren sind intensiv darauf hin zu untersuchen, inwieweit sie zur Überprüfung der eingesetzten IuK-Technik ausgeweitet werden können. Es wäre insbesondere zu kontrollieren, welchen spezifischen Anteil die IuK-Technik zur Verletzlichkeit der Gesellschaft beiträgt und wie durch ihre Gestaltung diese Verletzlichkeit reduziert werden kann. Doch selbst wenn hier Fortschritte zu einer Integration von Verletzlichkeitsprüfungen erzielt werden könnten, sind staatliche Verfahren erforderlich, in denen IuK-Systeme, die ein gewisses Schadenspotential überschreiten können, auf ihre Verletzlichkeit hin überprüft werden.

3.2 IuK-spezifische Zulassungsverfahren

So radikal, wie der Vorschlag für manchen klingen mag, ist er gar nicht. Wie wir gesehen haben, dürfen andere Techniksysteme nur genutzt werden, wenn sie zuvor auf ihre Sicherheit hin überprüft und zugelassen wurden. Für das Technikrecht ist es sogar eher ungewöhnlich, daß gesellschaftlich riskante Systeme wie viele IuK-Systeme nicht längst einer präventiven staatlichen Kontrolle unterliegen. Auch IuK-Systeme einem Zulassungsverfahren zu unterwerfen, wäre also nur systemgerecht.

Strukturiert nach möglichen Anwendungsfällen ergibt sich, daß das Grundmodell der Produktzulassung über allgemeine Betriebszulassungen am ehesten für die Zulassung von einzelnen Geräten geeignet ist. Diesen Bereich der Prüfung von IuK-Techniken deckt das Rahmenkonzept zumindest durch die Herausgabe von Sicherheitsstandards und die Vergabe von Sicherheitszertifikaten ab, wenngleich die unmittelbare Anwendung und damit die Beurteilung von möglichen Folgen des Technikeinsatzes ausgeschlossen bleibt.

Umfassendere Überlegungen müssen bei der Datensicherheit und damit auch für Zulassungsverfahren angestellt werden, wenn es um die Verarbeitung personenbezogener Daten geht oder aber um Systeme, deren Ausfall sonstige Schäden hervorrufen kann. Im ersten Fall ist beispielsweise an ein Personalinformationssystem, im zweiten Fall an das oben erwähnte Beispiel einer chemischen Industrieanlage zu denken. Quer zu diesen beiden Fällen liegt die Einrichtung und der Betrieb einzelner Kommunikationsnetze, die sowohl Risiken für die verarbeiteten personenbezogenen oder -beziehbaren Daten bergen als auch, im Rahmen der Steuerung von Produktion und Dienstleistungen, indirekt zu materiellen und immateriellen Schäden führen können. In diesen Fällen ist im Einzelfall an öffentliche Genehmigungs- und Zulassungsverfahren zu denken.

Diese Zulassungsverfahren sollten so anwendungsnah wie möglich angelegt sein. Denn die Gefahr anwendungsunabhängiger Technikprüfungen liegt in der abstrakten und anwendungsvorgreifenden Zulassung, die bei der Prüfung des Anwendungsfalles zu einem Rückgriff auf schon Zugelassenes führt und damit weitere Einwendungen automatisch ausschließt (Präklusion). Als Beispiel sei hier aus dem Atomrecht auf die schließlich gescheiterten Pläne zur Genehmigung des HTR-Moduls verwiesen.[127] Als zweites Beispiel aus dem Bereich des Abfallrechtes sind die Versuche verschiedener Landesregierungen zu nennen, durch verbindliche Abfallentsorgungspläne für das nachfolgende öffentliche Planfeststellungsverfahren, Standortentscheidungen vorwegzunehmen, und auf diese Weise die umfassende Erörterung der Technikanwendung und ihrer Folgen wenigstens in Teilbereichen vorzuziehen.[128]

Für die Zulassungsverfahren ist zu berücksichtigen, daß eine inhaltliche Beteiligung der gefährdeten Bürger an den Entscheidungen über Techniksysteme nicht nur politisch gefordert, sondern auch rechtlich geboten ist. Technikstenerung verteilt nämlich Risiken und gestaltet Grundrechtsbeziehungen. Die Schutzpflicht des Staates kann es gebieten, den betroffenen Bürgern Gelegenheit zu geben, in einem vorverlagerten Rechtsschutzverfahren befürchtete Beeinträchtigungen ihrer Grundrechte geltend zu machen. "Für einen effektiven Grundrechtsschutz der potentiell Gefährdeten ist angesichts des Ausmaßes denkbarer Gefahren entscheidend, daß bereits das behördliche Verfahren geeignet ist, im konkreten Fall zu 'richtigen' sicherheitsrelevanten Entscheidungen zu führen. Wahrscheinlich läßt sich nur über das Verfahrensrecht verhindern, daß der Bereich zwischen Recht und Technik zum juristischen Niemandsland wird."[129]

Allerdings bereitet die Vorstellung einer erfolgreichen, das heißt informierten und ernstzunehmenden Öffentlichkeit in vielen Fällen Schwierigkeiten. Selbst bei einem mit hochsensiblen Patientendaten arbeitenden Krankenhausinformationssystem werden Patienten, deren Daten verarbeitet werden und deren Rechte gefährdet sind, kaum Gelegenheit haben, Einwendungen zu erheben. Zumal, anders als bei den Nachbarn einer Chemieanlage, die Fluktuation der Betroffenen in einem Krankenhaus größer ist. Realistisch sind daher nur Zulassungsverfahren, die im Rahmen eines öffentlichen Hearings ablaufen, bei der sich sowohl die Betroffenen als auch Betroffenenvertreter äußern können. Nichts anderes gilt für andere Dienstleistungsbereiche wie den Geldverkehr oder ein Verkehrsleitsystem.

Auch wenn aus den erwähnten und anderen Gründen die Zulassungsverfahren nur in beschränktem Ausmaß die Verletzlichkeit der Gesellschaft zu verringern vermöchten, wäre es schon ein großer Fortschritt, wenn in solchen Zulassungsverfahren Geräte und Programme auf Aspekte ihrer Verletzlichkeit hin überprüft werden könnten. So wäre es für die Sicherheit des Rechts auf informationelle Selbstbestimmung beispielsweise schon ein großer Gewinn, wenn alle angebotenen Terminals mit Verschlüsselungsprozessoren bestückt oder TeleTrusT-fähig, alle Temex-Geräte mit Betriebsanzeigen versehen, alle Computersysteme mit (hardwaregeschützten) datenschutzgerechten Zugriffssicherungen oder automatischen Protokollroutinen ausgestattet oder in ihrer Konstruktion transparent und kontrollfreundlich wären.

Die Integration von Verletzlichkeitprüfungen in bestehende Genehmigungsverfahren und ihre Etablierung in IuK-spezifischen Zulassungsverfahren sollten nicht als einziges Instrument zur Steuerung der Verletzlichkeit in Betracht gezogen werden. Die behördliche Zulassung kann zum Beispiel auch mit der ausdrücklichen Verpflichtung zur Schadensvorsorge - sei es durch Hinterlegung entsprechender Sicherheiten oder der Verpflichtung zum Abschluß einer Haftpflichtversicherung - gekoppelt werden. Neben einem staatlichen Zulassungsverfahren kann auch gesetzlich eine Gefährdungshaftung eingeführt werden.

---

[127] Vgl. Hahn, Der Hochtemperaturreaktor-Modul, Öko-Mitteilungen 2/1989, S. 6 (11 f.).

[128] § 6 AbfG, § 8 HessAbfAG.

[129] BVerfGE 53, 31 (76) - Minderheitsvotum; vgl. auch das Mehrheitsvotum (61 f.).

3.3 Haftung

Im Haftungsrecht sind die vertragliche Haftung von der deliktischen Haftung und diese wiederum von der Gefährdungshaftung zu unterscheiden. Während die vertragliche Haftung für Fehler eines IuK-Systems nur zwischen den Vertragspartnern besteht[130], erstreckt sich die deliktische Haftung auch auf Schäden, die bei Dritten verursacht werden.[131] In beiden Fällen hat der Verursacher eines Schadens dem Verletzten seinen Schaden allerdings nur dann zu ersetzen, wenn er den Schaden vorsätzlich oder fahrlässig verursacht hat. Dies setzt daher voraus, daß der Geschädigte sowohl beweisen kann, daß ihm ein Schaden durch eine konkrete Verletzungshandlung des Schädigers (Kausalität) zugefügt worden ist, als auch, daß der Schaden von dem Verursacher verschuldet wurde (Verschulden). Lediglich im Rahmen der sogenannte Produzentenhaftung muß ein Produzent bei Herstellerfehlern[132] beweisen, daß ihn ein Verschulden nicht trifft[133]. Der ganze Bereich, der nicht durch den Hersteller, sondern durch Dritte verursachten Schäden fällt aus der für den Geschädigten günstigeren Umkehr der Beweislast heraus.

Diese Lücke wird allerdings durch das neue Produkhaftungsgesetz (ProdhaftG) nicht geschlossen, das den Bereich der Herstellerhaftung entsprechend einer Richtlinie der EG gesetzlich regeln soll.[134] In ihm ist die Haftung für Schäden, die durch ein fehlerhaftes Produkt entstehen, geregelt (§ 1 Abs. 1 ProdhaftG). Ein Produkt hat nach § 3 Abs. 1 ProdhaftG einen Fehler,

> "wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere
> a) seiner Darbietung,
> b) des Gebrauches, mit dem billigerweise gerechnet werden kann,
> c) des Zeitpunktes, in dem es in den Verkehr gebracht wurde,
> berechtigerweise erwartet werden kann".

Auch wenn angenommen wird, daß das ProdhaftG nicht nur Hardwarefehler, sondern - was bestritten wird - auch Softwarefehler erfaßt[135], so ergeben sich doch noch immer relevante Einschränkungen für die Haftung aus Schäden, die durch IuK-Technik verursacht werden können. Nach § 1 Abs. 4 ProdhaftG trägt der Geschädigte für den Fehler, den Schaden und den ursächlichen Zusammenhang zwischen Fehler und Schaden die Beweislast. Damit muß der Geschädigte zwar nicht mehr das Verschulden des Herstellers nachweisen, aber seine Prozeßsituation ist nach wie vor nicht zufriedenstellend. Gerade für den Nachweis von Softwarefehlern werden die Geschädigten weiterhin immense Gutachterkosten investieren müssen, um zum Erfolg zu kommen. Hier bleibt es letztlich der Rechtsprechung überlassen, die Beweisanforderungen zu senken und auf die Fehlfunktionen der Programme zu beschränken.[136]

Außerdem ist die Haftung des Herstellers ausgeschlossen,

- wenn der Fehler darauf zurückzuführen ist, daß das Produkt zwingenden staatlichen Rechtsvorschriften entspricht (§ 1 Abs. 2 Nr. 4 ProdhaftG).

- wenn der Fehler nach dem Stand von Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das betreffende Produkt in den Verkehr brachte, nicht erkannt werden konnte (§ 1 Abs. 2 Nr.5 ProdhaftG). Das Beweisrisiko trägt der Geschädigte.

- wenn der Fehler erst entstanden ist, nachdem das Produkt in den Verkehr gebracht wurde (§ 1 Abs. 2 Nr. 2 ProdhaftG). Die Beweislast trägt der Hersteller. Eine Entlastungsmöglichkeit wird gerade im Softwarebereich nicht selten gegeben sein.[137]

---

130 Z.B. für Mängel einer Kaufsache nach §§ 459 ff. BGB.

131 Z.B. nach §§ 823 ff. BGB

132 Unterschieden werden Instruktionsfehler, Konstruktionsfehler und Fabrikationsfehler.

133 BGHZ 51, 91.

134 Bundestags-Drucksache 11/2447. EG-Produkhaftungsrichtlinie vom 25. Juli 1985 (Abl. EG vom 7. August 1985, Nr. L 210/29).

135 Koutses, in: Dafta, 1989, Register 16; dies., RDV 1989, S. 1 (5 ff.).

136 Koutses, in: Dafta, 1989, Register 16, S. 6.

137 Koutses, in: Dafta, 1989, Register 16, S. 6.

Insbesondere durch die Übertragung des Entwicklungsrisikos neuer IuK-Produkte auf die Anwender (§ 1 Abs. 2 Nr.5 ProdhaftG) wird von dem neuen ProdhaftG nur ein sehr begrenzter Beitrag zur Reduzierung der Verletzlichkeit ausgehen.

Müßte dagegen außer dem Hersteller jeder, der ein IuK-System einsetzt, nicht nur bei nachweisbarem Verschulden, sondern wie ein Autohalter auch ohne eigenes Verschulden für jeden Schaden haften, den sein gefährliches Technik-System verursacht, dann würden viele riskante Systeme wohl nicht entwickelt und vorhandene Anwendungen besser gesichert. Würden außerdem immaterielle Schäden durch ein hohes Schmerzensgeld ausgeglichen und der Nachweis, daß der Schaden kausal durch das IuK-System verursacht wurde, wie bei der Produkthaftung durch eine Umkehr der Beweislast erleichtert, müßten zumindest nicht die Geschädigten die Risikofreude des Technikanwenders 'ausbaden'.

Jener würde zwar versuchen, seine Haftpflicht zu versichern. Doch dadurch wäre das Problem nur verschoben, denn die Versicherungen werden entweder riskante Anwendungen gar nicht oder nur unter hohen Sicherungsauflagen versichern. Sie würden also weitgehend die Aufgaben wahrnehmen, die sonst einem Zulassungsverfahren zugedacht sind. Dennoch kann eine Verschärfung des Haftungsrechts nicht die staatliche Kontrolle der Technikanwendung ersetzen. Schließlich werden die privaten gewinnorientierten Versicherungen nicht die gleichen Gestaltungsziele einer schadensmindernden Sicherheitspolitik vertreten wie beispielsweise Behörden, die dem Interesse einer sozialverträglichen Technikgestaltung verpflichtet sind.

Aber auch bei einer Verschärfung der Haftungsbedingungen darf nicht übersehen werden, daß ein Schadensausgleich nur begrenzt zu einer Vermeidung von Schäden führt. Zwar besteht eine nicht unbegründete Hoffnung, daß eine Verpflichtung zum Schadensersatz Hersteller oder Verwender von IuK-Techniken zu besonderen Vorkehrungen der Sicherheit der verwendeten IuK-Technik bewegen könnte. Diese präventive Funktion von Schadensausgleichregeln ist allerdings umstritten. Zu berücksichtigen ist einerseits, daß Haftung betriebswirtschaftlich Kosten sind und verhaltenssteuernd wirken können. Gleichwohl bemißt sich die präventive Wirkung von Haftungsregelungen oft nach dem Risiko, "ungeschoren" davon zu kommen. Hinzu kommen gerade im Bereich der IuK-Techniken Schadensursachen in Betracht, die typischerweise nicht einem bestimmten Schädiger zugeordnet werden können und damit das Entdeckungsrisiko klein halten. Das Haftungsrecht kann daher zunächst nur eine flankierende verhaltenssteuernde Funktion haben. Diese Funktion kann aber durch eine geeignete Ausgestaltung des Instrumentes der Gefährdungshaftung unterstützt werden.

Die Gefährdungshaftung ist eine verschuldensunabhängige Haftung für Schäden, die regelmäßig beim Betrieb bestimmter erlaubter Anlagen oder Verhaltensweisen anfallen. Die Gefährdungshaftung folgt dem Gedanken, daß derjenige der Gefahrenquellen beherrscht, und in dessen Interesse ein gefährlicher Betrieb gestattet wird, auch die Wagnisse auf sich nehmen muß, die mit dem Betrieb verbunden sind. Beispiele einer solchen Haftung sind im Technikrecht nicht selten: § 22 Wasserhaushaltsgesetz (WHG), § 7 Straßenverkehrsgesetz (StVG), § 84 Arzeneimittelgesetz (AMG), § 25 Atomgesetz (AtG) u.a.. Teilweise wird die Gefährdungshaftung mit einer obligatorischen Haftpflicht gekoppelt, weil auf diese Weise dem Verletzten wenigstens ein solventer Schädiger gesichert werden kann (vgl. § 43 LuftVG, §§ 13 f AtG). Auch einzelne Datenschutzgesetze der Länder enthalten solche Haftungsregelungen für Schäden, die im Zusammenhang mit der Verarbeitung personenbezogener Daten entstanden sind.[138] Für das Bundesdatenschutzgesetz sind sie in der Diskussion.[139]

Die Gefährdungshaftung vermag aber auch nicht alle Haftungsprobleme zu lösen. Auch sie setzt die Feststellung der Kausalität zwischen der schädigenden Handlung und dem Schaden voraus. Damit läuft diese Haftung für den Geschädigten leer, wenn der Verursacher der Schäden nicht festgestellt werden kann. Die Gefährdungshaftung umfaßt regelmäßig auch kein Schmerzensgeld. Dies ist vor allem bei der Verletzung von Persönlichkeitsrechten von Bedeutung.

---

[138] § 13 BayDSG; § 15 BerlDSG; § 17 HmbgDSG; § 20 HessDSG; § 4 Abs. 2 NdsDSG; § 20 GFD NW; § 16 RlPfDSG. Vgl. hierzu auch Müller/Wächter, Zur Aufnahme einer verschulden-unabhängigen Schadenersatzregelung in das BDSG, DuD 1989, S. 239; Beier, Novellierung des Bundesdatenschutzgesetzes, DuD 1988, S. 506 (509).

[139] BDSG-Entwurf, Bundestags-Drucksache 11/4306, S. 7 f; SPD-Entwurf (1989) Bundestags-Drucksache 11/3730, S. 7.

Ein befriedigendes Sicherungssystem nur allein mit Hilfe von Haftungsregelungen wird nicht erreicht werden können, weil die schadenverhütende Funktion von Haftungsregelungen allgemein nicht ausreichend gesichert ist und im besonderen Schäden im Bereich der IuK-Techniken nur mit Schwierigkeiten einem Verursacher zugeordnet werden können. Zulassungsverfahren und Haftungsregelungen sind daher nebeneinander zur Sicherheit der IuK-Techniken einzuführen.[140]

Sowohl Zulassungsverfahren als auch Haftungsregelungen setzen jedoch Beschaffenheitsangaben voraus, denen die IuK-Technik entsprechen muß, wenn sie als genehmigungsfähig oder fehlerfrei gelten will. Daher erfordert eine Beeinflussung der Technikentwicklung unter Gesichtspunkten der Verletzlichkeit eine Regelung der technischen Normung.

3.4 Normung

In den Normen der meist privaten Vereine wie DIN, VDI oder VDE werden der Stand der jeweiligen Technik festgehalten und konkrete Anforderungen an die Beschaffenheit technischer Produkte gestellt. Auf europäischer Ebene sind für die Normung u.a. der CEN (Comité Européen de Normalisation) und der CENELEC (Comité Européen de Normalisation Electrotechnique) von großer Bedeutung - ebenfalls nichtstaatliche Einrichtungen.[141] Die technische Normung beeinflußt sehr stark die konkrete Ausgestaltung von Technik-Systemen.

In noch viel stärkerem Maße gilt dies für die Normung der IuK-Technik. Denn sie unterscheidet sich von der Normung anderer Techniksysteme in zwei wichtigen Aspekten: Sie erfolgt zum einen bereits heute überwiegend auf europäischer und internationaler Ebene. So wurde etwa mit der Gründung des Europäischen Instituts für Telekommunikationsnormen im März 1988 eine wichtige Voraussetzung geschaffen, rasch europaweit geltende Telekommunikationsspezifikationen zu schaffen. Zum anderen gilt für die IuK-Technik, daß nicht nur - wie in den meisten anderen Bereichen technischer Normung - der bereits erreichte Stand der Technik nachvollzogen wird, sondern im Gewand technischer Spezifikationen entwicklungssteuernd, zumindest entwicklungsbegleitend, zentrale Eckwerte für neue Techniksysteme gesetzt werden.

Auch das Rahmenkonzept sieht die besondere Relevanz der Normungsarbeit. Daher empfiehlt es, "die Einbettung der einschlägigen ZSI-Aktivitäten in das europäische Prüf- und Zertifizierungssystem anzustreben".[142] Erste Ansätze wurden mit den von der ZSI 1989 herausgegebenen "IT-Sicherheitskriterien" ergriffen. Diese haben eine doppelte Funktion. Anwendern sollen sie die Spezifizierung von Sicherheitsanforderungen ermöglichen und Herstellern Richtlinien für die Systementwicklung an die Hand geben. Längerfristig erhofft man sich jedoch, daß die offiziellen Prüfkriterien in zunehmendem Maße von Herstellern für die Realisierung sicherer EDV-Systeme angewendet werden und Anwender, um sich nicht mangelnde Sorgfaltspflicht vorwerfen zu lassen, zunehmend unter Druck geraten nur noch zertifizierte Systeme einsetzen.[143]

Auf die Normungsarbeit sollte zumindest in zweierlei Hinsicht Einfluß genommen werden: Soweit in dieser technische Sicherheit normiert wird, bestimmt sich dieser Begriff nicht nach gesellschaftlichen Erfordernissen, sondern ausschließlich an der Verkehrsfähigkeit der hergestellten Waren. So nennt zum Beispiel der Beschluß des Europäischen Rats "über die Normung auf dem Gebiet der Informationstechnik und Telekommunikation" vom Dezember 1986 als Ziele für die künftigen Normungsaktivitäten zwar die Verbesserung der internationalen Wettbewerbsfähigkeit, die Schaffung eines europäischen Binnenmarktes, die Erleichterung eines gemeinschaftsweiten Informationsaustauschs, die Sicherstellung von Anwenderbedürfnissen und gleiche Konkurrenzbedingungen bei der Vergabe öffentlicher Aufträge. Kein Ziel der Normung ist jedoch, die Verletzlichkeit der Gesellschaft zu verringern. Wegen der Bedeutung der Normung darf diese jedoch nicht nur an Effizienz und Wettbewerbsfähigkeit ausgerichtet werden, sondern muß auch Sicherheitsziele berücksichtigen.

---

[140] Auch für die Tätigkeit des neuen Bundesamts für Sicherheit in der Informationstechnik muß daran gedacht werden, daß mögliche Schäden haftungsrechtlich ausreichend abgesichert werden.

[141] Einen Überblick über die bestehenden Organisationen und deren Arbeit gibt Haberzettl, Normung und Zertifizierung, CR 1989, S. 943 ff.

[142] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 8.

[143] Vgl. hierzu z.B. Weck, Datensicherung - Konzepte und Bewertung, DuD 8/89, S. 391. Für Hersteller und Anwender von IT-Systemen sind spezielle Handbücher zur Anwendung der Kriterien in Erarbeitung, das "IT-Evaluationshandbuch" und das "IT-Sicherheitshandbuch".

Außerdem ist das Verfahren der Normung nach den Mindestkriterien demokratischer Entscheidung zu gestalten. Derartig weitreichende Entscheidungen dürfen nicht im geschlossenen Kreis der marktbeherrschenden Herstellerindustrien und der organisierten Großanwender getroffen werden. Die Zusammensetzung der Normungsgremien ist zumindest um Vertreter betroffener Arbeitnehmer und Benutzer zu erweitern und das Normungsverfahren selbst öffentlich durchzuführen.

3.5 Voraussetzungen der Grundrechtssicherung durch Verschlüsselungsverfahren

In einem Rahmenkonzept zur Verringerung der Verletzlichkeit ist auch Vorsorge zu treffen, um durch Forschungsförderung, durch rechtliche Regelungen und organisatorische Maßnahmen die technischen Grundlagen für mehr Bürgersicherheit zu verbessern. Um zum Beispiel die oben angedeuteten Möglichkeiten nützen zu können, Informationsverarbeitung und Kommunikation durch Verschlüsselungsverfahren vor fremder Einsichtnahme zu schützen, sind eine Reihe organisatorischer Voraussetzungen erforderlich, die im Rahmen eines an der Bürgersicherheit orientierten Handlungskonzepts rechtzeitig berücksichtigt werden müßten. Aus ihrer Untersuchung können sich Hinweise auf mögliche Aufgaben eines neuen Bundesamts für Sicherheit in der Informationstechnik ergeben.

Zu diesen Voraussetzungen gehören:

- die Sicherung der Verschlüsselungsalgorithmen

  Da das Kryptoverfahren wesentlich die Sicherheit der Anwendungen bestimmt, dürfen nur "sichere" Verfahren zur Anwendung kommen.

- die sichere Implementierung

  Die Implementierung des Kryptoverfahrens oder der benötigten Verwaltungsprogramme zur Berechnung und Ausgabe der Schlüssel, zu Aktualisierung von Verzeichnissen oder der Bereitstellung von Zertifikaten darf weder fehlerhaft noch manipulierbar sein.

- eine unabhängige Prüfung der Soft- und Hardware

  Eine Validierung und gegebenenfalls sogar Verifikation der eingesetzten Hard- und Software kann der Hersteller nicht selbst vornehmen, da er vorrangig seine Kosten minimieren will und deshalb in einem Interessenkonflikt zu aufwendigen Prüfmaßnahmen steht.

- Sicherung des Schlüsselmanagements

  Die sensibelste Stelle von Verschlüsselungkonzepten ist das Schlüsselmanagement. Nur wenn sichergestellt werden kann, daß Unbefugte keinen Zugang zu den verwendeten Schlüsseln erhalten, können die Kommunikationspartner die Nachrichten vor unerwünschter Einsichtnahme schützen.

Um diese Voraussetzungen zu erfüllen, ist insbesondere in einem Public-Key-System die Verteilung und Organisation der einzelnen Teilaufgaben von besonderer Bedeutung. Für ein solches System lassen sich sechs Rollen ausmachen:

- Die Entwickler von Chipkarten und Systemen
- Die Validierungsinstanz für Algorithmen, Chips und Systeme
- Die Karteninitialisierungs-Instanz(-en)
- Die Ausgabeinstanz(-en) für Karten
- Die Zertifizierungs-/Authentifizierungsinstanzen
- Die Revisionsinstanz

Nicht alle diese Rollen müssen auch getrennt institutionalisiert sein, bei einigen Aufgaben sind jedoch Interessenkonflikte zu erwarten. Die Einrichtung einer Bundesbehörde für Sicherheit in der Informationstechnik wirft die Frage auf, welche Aufgaben von staatlichen Institutionen in einem Konzept wahrgenommen werden sollen und wo das Gebot der informationellen Gewaltenteilung eher andere Organisationsformen nahelegt.

Soll eine "Infrastruktur" zur Sicherstellung der Vertrauenswürdigkeit elektronischer Kommunikation gesellschaftlich breite Akzeptanz finden, dann muß die für die technische Abwicklung und im Anwendungskontext notwendige Organisation so gestaltet sein, daß Risiken für den Einzelnen und die Gesellschaft minimiert werden. Wenn einzelne Stellen Doppelfunktionen wahrnehmen und dadurch in Interessenkonflikte geraten, dann wird der organisatorische Zusammenhang nicht das nötige Vertrauen bei betroffenen Bürgern, in Gesellschaft, Regierung, Parlament und Wirtschaft finden. Dadurch ergeben sich für die jeweiligen Rollen folgende Anforderungen:

- Entwickler

  Vorsorge ist erforderlich gegen das Risiko, daß Entwickler Fehler machen oder die Chipkarten bzw. Systeme manipulieren, um sich Vorteile zu verschaffen. Entwickler unterliegen einem starken ökonomischen Druck. Auch in anderen Zusammenhängen wird deshalb davon ausgegeangen, daß sensible Produkte unabhängig zu prüfen sind (Militär, Gütesiegel, TÜV).

- Validierungsinstanz

  Die Systeme müssen unabhängig vom Entwickler und Anwender validiert werden. Deshalb muß durch organisatorische Maßnahmen die Unabhängigkeit der Validierungsinstanz so weit wie möglich gesichert sein. Der Einsatz eines Systems darf nur dann erfolgen, wenn die Validierungsinstanz neben der Sicherheit der Technik die Sicherheit der Gesellschaft überprüft hat.

  Wesentlich für eine wirksame Kontrolle ist es deshalb, daß für die Prüfung ein umfassender Kriterienkatalog Anwendung findet. Es ist nicht ausreichend, nur die relative Sicherheit der einzelenen Teilsysteme zu überprüfen. Insbesondere müssen mögliche kummulative Schäden durch die Betrachtung der Anwendungskonzepte herausgearbeitet und in den zu entwickelnden Gestaltungsalternativen und -anforderungen als Bewertungsgrundlage neben der Datensicherheit berücksichtigt werden. Nur wenn die Verletzlichkeit des gesamten sozio-technischen Zusammenhangs untersucht wird, können kritische Schadenspotentiale für die Gesellschaft vermindert werden.

- Karteninitialisierungsinstanz

  Der private Schlüssel ist vor jeglicher Kenntnisnahme zu schützen. Die sichere Übermittlung und Speicherung des öffentlichen Schlüssels (public key) ist zu gewährleisten. Zur Initalisierung der Chipkarten müssen die Schlüsselpaare berechnet werden. Der private Schlüssel (private-key) wird nur in der Chipkarte gespeichert und sonst niemandem zur Kenntnis gegeben. Von größter Bedeutung für die Sicherheit und die Vertrauenswürdigkeit ist deshalb das gesamte Schlüsselmanagement.

  Die Karteninitialisierungsinstanz berechnet die Schlüsselpaare und setzt sie in die Karte. Wenn sie den geheimen Schlüssel nun nicht löscht, sondern ihn in einem Verzeichnis speichert, verfügt sie über umfassende Manipulationsmöglichkeiten. Sie kann dann geheime Nachrichten aller Karteninhaber entschlüsseln und deren elektronische Signatur fälschen. Weil diese Funktion so sensibel ist, sollte dafür eine möglichst unabhängige und vertrauenswürdige Institution eingesetzt werden. Es ist detailliert zu prüfen, ob eine gewisse Dezentralisierung erfolgen kann. Sie bietet Vorteile für die Verminderung des Schadenspotentials, erhöht aber den Revisionsaufwand und u.U. die Grundrechtseinschränkungen durch die erforderlichen Sicherungsmaßnahmen.

- Kartenausgabe

  Die Chipkartenausgabe muß die Zuordnung von initialisierten Karten zu Personen, Rollen oder Institutionen festlegen. Dies kann von vielen Ausgabestellen in eigener Regie durchgeführt werden. Dazu müssen die Verantwortlichkeiten und Haftungsfragen geklärt sein. Solange die Chipkarten gegen das Auslesen der geheimen Schlüssel gesichert sind, ist die Kartenausgabe nur für die Anonymität der Karteninhaber sensibel. Sofern Anwendungen darauf beruhen, daß die Identität des Kartenbesitzers von der Ausgabestelle vertraulich behandelt wird, müssen Interessenkonflikte der Ausgabestellen vermieden werden. Die Inhaberverzeichnisse müssen auch gegen Manipulation gesichert sein, um den Kartenmißbrauch zu verhindern (Urheberschaft).

- Zertifikate und Identifizierung

  Die Identifikation erfolgt im Streitfall durch die zuständige Ausgabestelle. Sie muß die Identifizierbarkeit des Karteninhabers garantieren.

- Revisionsinstanz

  Die Revision der Datenspeicherung in Public-Key-Systemen und der Funktionalität der Systeme selbst muß einer unabhängigen Instanz übertragen werden.

In einem Handlungskonzept zur Verbesserung der Bürgersicherheit wäre darzustellen, welche Funktionen von welchen staatlichen oder gesellschaftlichen Instanzen übernommen werden sollen und wie gewährleistet werden kann, daß die jeweilige Instanz die genannten Voraussetzungen erfüllt. Welche Aufgaben in einem Public-Key-System das neue Bundesamt für Sicherheit in der Informationstechnik übernehmen könnte und sollte und welche Funktionen ihm nicht übertragen werden dürften, wird im Rahmen seiner Aufgabenbeschreibung im folgenden Abschnitt erörtert.

IV. DAS BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Die Aufgaben, Befugnisse und die Organisation des neuen Bundesamt für Sicherheit in der Informationstechnik sind im Rahmen des im vorherigen Abschnitts umrissenen Handlungskonzepts zur Verringerung der Verletzlichkeit der Gesellschaft zu bestimmen. Allerdings können im Rahmen dieser Untersuchung nur einige wichtige Aspekte angedeutet werden.

1. AUFGABEN UND BEFUGNISSE

Um seine Aufgabe, Überwachung und Verminderung der Verletzlichkeit der Gesellschaft durch die Informations- und Kommunikationstechnik erfüllen zu können, benötigt das Bundesamt für Sicherheit in der Informationstechnik folgende Befugnisse:

1.1 Befugnisse zur Erhaltung der Lernfähigkeit der Gesellschaft

Angesichts der rasanten Entwicklung der IuK-Technik und der sehr schwierigen Revidierbarkeit von Infrastrukturentwicklungen vernetzter Informationsverarbeitung ist es wichtig, die Lernfähigkeit der Gesellschaft hinsichtlich der Verletzlichkeit der Gesellschaft sicherzustellen.[144] Hierfür sind vor allem Befugnisse notwendig, das notwendige Wissen zu erwerben und öffentliche Lernprozesse zu initiieren.

1.1.1 Studien zu Alternativentwicklungen

Eine Beeinflussung der Technikentwicklung unter Gesichtspunkten der Verletzlichkeit ist nur möglich, wenn zwischen der Nutzung und der Nichtnutzung einer bestimmten Technik oder zwischen funktional-äquivalenten Alternativen gewählt werden kann. Zu einer geplanten Entscheidung müßten daher immer auch mögliche Alternativen dargestellt werden. Dies könnte von dem jeweiligen Entwickler oder Anwender verlangt werden. Es ist jedoch zu befürchten, daß die Darstellung von Alternativen durch diese nur zur Rechtfertigung der gewählten Planung benutzt wird, nicht als Vorbedingung einer Infragestellung dieser Planung. Daher wäre zu empfehlen, dem Bundesamt für Sicherheit in der Informationstechnik die Befugnis zu erteilen, Alternativen zu geplanten IuK-Systemen zu untersuchen oder Aufträge dazu zu vergeben.

Soweit das Bundesamt für Sicherheit in der Informationstechnik auf wissenschaftliche Zuarbeit angewiesen ist, sollte es vermeiden, von einer Seite der wissenschaftlichen Kontroverse abhängig zu sein und dadurch möglicherweise relevante Gesichtspunkte zu vernachlässigen. Durch Parallelforschung, Reviewstudien und institutionelle Absicherung kritischer Diskursprozesse sollten jeweils die ungesicherten Behauptungen und impliziten Vorurteile des Gegenstandpunktes herausgearbeitet werden. Durch die institutionalisierte gegenseitige Kritik könnte auch die Attitüde der Irrtumslosigkeit in der Wissenschaft aufgehoben werden. Die Gutachtenaufträge sollten nicht eindeutige Aussagen über Risikobereiche verlangen, wo allenfalls Näherungswissen möglich ist. Als Anstoß kritischer Diskussionen müßten sie vielmehr fordern, daß jedes Gutachten jeweils ein Spektrum von Alternativen, die Unsicherheitsbereiche, die Nachteile und Gefahren einer jeden Alternative angibt. Die Gutachten sollten die Debatte also eröffnen, nicht abschließen. Jedenfalls hätte das Bundesamt für Sicherheit in der Informationstechnik zu gewährleisten, daß konkurrierender Sachverstand zur Verfügung steht und der Zugriff auf alle wissenschaftlichen Kenntnisse und Anschauungen sichergestellt ist.

Ingesamt hätte das Bundesamt für Sicherheit in der Informationstechnik unstrukturierte Handlungszusammenhänge und die durch die Technologie ausgelösten Veränderungsprozesse systematisch zu strukturieren und durch Bündelung von Informationen und Optionen beobachtbar und evaluationsfähig zu machen. Entscheidungsmöglichkeiten erhält sich die Gesellschaft nur dann, wenn sie bestehende sozio-technische Verzweigungssituationen identifiziert und offenhält oder mögliche erkennt und herzustellen versucht. Diesen Entscheidungsspielraum kann sie jedoch nur erhalten oder sogar ausweiten, wenn sie sich nicht auf ein Technik-System fixiert und sich von diesem abhängig macht, sondern technologiepolitisch neutral möglichst viele technische Alternativen fördert.

---

[144] Vgl. hierzu oben III. 2.

1.1.2 Implikationsanalysen und Gestaltungsvorschläge

Für diese Alternativen sind die Verletzlichkeitsaspekte und die von ihnen ausgehenden sozialen, rechtlichen und wirtschaftlichen Folgen abzuschätzen. Da die wissenschaftliche Kapazität zur Durchführung der erforderlichen zukunftsorientierten Implikationsanalysen weitgehend fehlt, ist sie durch entsprechende Nachfrage und den dauerhaften Aufbau von Forschungsmöglichkeiten zu schaffen. Folgenabschätzungen dieser Art sind die Voraussetzung jeder normativen Steuerung des technischen Wandels nach sozialen Kriterien. Sie sollten auch dazu beitragen, daß sich die betroffenen gesellschaftlichen Gruppen möglichst frühzeitig mit den technischen Veränderungen auseinandersetzen.

In einem dritten Schritt sind die Implikationen der technischen Alternativen nach allen relevanten Beurteilungskriterien zu bewerten. Die in einer demokratischen Gesellschaft notwendig offenen Bewertungsprozesse erfordern eine hinreichend diskursive Erörterung der verschiedenen Alternativen im Bundesamt für Sicherheit in der Informationstechnik, in den zuständigen Gremien, in den gesetzgebenden Körperschaften und in der Öffentlichkeit. Nur wenn alle kontroversen Argumente aufgenommen und bearbeitet werden, sind die Bewertungen intersubjektiv vermittelbar, konsensfähig und demokratisch legitimierbar.[145]

1.1.3 Modellversuche

Wo Bedarf dafür besteht, sollte das Bundesamt für Sicherheit in der Informationstechnik Modellvorhaben anstoßen und soziale Experimente unterstützen, die Alternativen zur Trendentwicklung in die 'Informationsgesellschaft' darstellen. In solchen Modellversuchen sollte immer auch versucht werden, Gegengewichte gegen die negativen Folgen einer Informatisierungsstrategie zu stärken. Ziel muß es sein, individuelle und soziale Freiräume zu schaffen und vielfältige Alternativen anzubieten.

1.1.4 Wissensvermittlung

Eine der wichtigsten Aufgaben des Bundesamt für Sicherheit in der Informationstechnik hat darin zu bestehen, in der Öffentlichkeit Problembewußtsein zu schaffen, die Beurteilungskompetenz zu stärken und Gestaltungswissen zu vermitteln. Daher sollte das Bundesamt für Sicherheit in der Informationstechnik verpflichtet werden, alle Ergebnisse der von ihm initiierten Studien breit zu veröffentlichen, Informationsveranstaltungen für Entwickler, Nutzer und Betroffene durchzuführen, für Anfragen zu Verletzlichkeitsproblemen zur Verfügung zu stehen und die Bürgergruppen, die die öffentliche Diskussion über Verletzlichkeitsfragen aufgreifen, zu unterstützen.

1.2. Befugnisse zur Gewährleistung von Öffentlichkeit

Die Beurteilung der Risiken und die Bewertung von Schutzmaßnahmen ist weitgehend von subjektiven Wertungen abhängig. Gerade deshalb ist es erforderlich, den Gefahren möglicher einseitiger Bewertungen durch institutionalisierte kritische Diskurse zu begegnen. Diese sollten eine kontroverse Reflexion über die Verletzlichkeit wichtiger Technikanwendungen in Gang bringen. Sie sollten jedoch nicht auf einen vorschnellen Konsens zielen, sondern vielmehr einer kritischen Aufarbeitung der Verletzlichkeitsrisiken dienen.

---

[145] Vgl. hierzu 1.2.

1.2.1 Anzeigepflicht

Um überhaupt in die Lage versetzt zu werden, die Entwicklung der Verletzlichkeit der Gesellschaft beurteilen zu können, benötigt das Bundesamt für Sicherheit in der Informationstechnik ausreichende Informationen über die entwickelten und eingesetzten Systeme. Daher sollte vorgesehen werden, daß jeder Anbieter und jeder Anwender von IuK-Systemen von einem noch zu bestimmenden Zuschnitt dem Bundesamt für Sicherheit in der Informationstechnik gegenüber anzeigt, daß er ein bestimmtes IuK-System auf dem Markt anbietet oder daß er ein solches System in einer bestimmten Anwendungsumgebung einsetzt. Die Anzeige sollte eine Beschreibung

- der Konfiguration
- der Funktionen
- der Schadensmöglichkeiten und Schadensfolgen
- der Sicherungskonzepte
- der Notfallplanung und
- der verfügbaren funktionalen Äquivalente

beinhalten.

1.2.2 Jährlicher Verletzlichkeitsbericht

Das Bundesamt für Sicherheit in der Informationstechnik sollte verpflichtet werden, in einem zusammenfassenden Bericht jährlich die Entwicklung der Verletzlichkeit der Gesellschaft zu bewerten. Es sollte die Abhängigkeit der Gesellschaft von IuK-Systemen überwachen und allen involvierten gesellschaftlichen und staatlichen Instanzen Vorschläge unterbreiten, wie sie durch Technikgestaltung die Verletzlichkeit der Gesellschaft reduzieren können. Dies ist eine wichtige Voraussetzung, um besondere Verletzlichkeitsrisiken erkennen und in einem öffentlichen Diskurs Gegenmaßnahmen entwickeln zu können.

2.2.3 Organisation kritischer Diskurse

Lernprozesse der Gesellschaft im Umgang mit riskanter Technik setzen Bürger voraus, die in der Lage sind, sich selbst ein Urteil zu bilden und sich zu engagieren. Bürgerinitiativen waren die ersten, die auf Risiken der Atomenergie und der Umweltverschmutzung aufmerksam gemacht haben. Ohne den starken Druck der Öffentlichkeit hätte das Allgemeininteresse an Umweltschutz und sicherer Energieversorgung keine Chancen, sich gegen die mächtigen Partikularinteressen durchzusetzen. Ebenso wie in der Ökologiedebatte ist die Sensibilität und politische Kraft engagierter Bürger notwendig, um Verfassungsrisiken durch IuK-Technik zu erkennen und ins öffentliche Bewußtsein zu heben. Nur durch eine kritische Öffentlichkeit sind Risikominderungen gegen Widerstände durchzusetzen. Die Informations-, Organisations- und Artikulationsmöglichkeiten von Bürgergruppen zu verbessern, muß daher ein überlebenswichtiges Anliegen einer demokratischen Gesellschaft sein.

Zumindest müßte auf allen Ebenen der Technikgestaltung eine ausführliche Information der Bürger über die anstehenden Entscheidungen erfolgen. Dabei müssen sie nicht über jedes Detail unterrichtet werden. Aber sie sollten wissen, was auf dem Spiel steht; sie sollten um die Zwänge, die möglichen Alternativen und deren Kosten, das einzugehende Risiko und die Unsicherheiten seiner Abschätzung wissen. Nur so können die Menschen überhaupt entscheiden, große Risiken für Freiheit und Demokratie um ihrer Vorteile willen in Kauf zu nehmen. Die Information der Öffentlichkeit müßte dazu jeweils in einen öffentlichen Diskurs einmünden, der finanziell, zeitlich und organisatorisch abgesichert ist. Die Interessen nichtorganisationsfähiger Gruppen sollten dabei durch Repräsentanten wahrgenommen werden. Unter noch näher zu diskutierenden Voraussetzungen wäre auch zu ermöglichen, daß nicht-hochorganisierte gesellschaftliche Vereinigungen ebenfalls in die Lage versetzt werden, einen Alternativvorschlag auszuarbeiten und darzustellen. Ziel solcher Organisations- und Verfahrensregelungen wäre, eine möglichst weitgehende Verzahnung der institutionellen Techniksteuerung mit den Gestaltungsvorstellungen von unten zu gewährleisten.[146]

---

[146] Vgl. hierzu auch oben 1.1.4

1.3. Befugnisse zur Unterstützung Dritter

Um bürokratische Formen der Techniksteuerung soweit wie möglich zu vermeiden, muß eine Hauptaufgabe des Bundesamtes für Sicherheit in der Informationstechnik darin bestehen, die Entscheidungsträger zu unterstützen, das Kriterium der Verletzlichkeit in ihren Entscheidungen adäquat zu berücksichtigen. Dies sollte, soweit es effektiv möglich ist, ohne Zwang auf freiwilliger Basis erfolgen.

1.3.1 Kriterien der Verletzlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik sollte Kriterien der Verletzlichkeit der Gesellschaft entwickeln, für einzelne Techniksysteme konkretisieren und zur Diskussion stellen, damit für die Öffentlichkeit und jeden Entwickler und Anwender die Möglichkeit besteht, zu überprüfen, nach welchen Kriterien das Bundesamt für Sicherheit in der Informationstechnik IuK-Systeme bewertet.

1.3.2 Empfehlungen zur Reduzierung der Verletzlichkeit

Empfehlungen zur Reduzierung der Verletzlichkeit sollten allgemeine Maßnahmenbündel beschreiben, wie in bestimmten Anwendungsbereichen das Schadenspotential vermindert und die Wahrscheinlichkeit von Fehlern oder Mißbrauchsaktionen gesenkt werden kann. Für die Planung und Beschaffung von IuK-Systemen des Bundes könnten diese Empfehlungen (nach Übernahme durch die zuständigen Ressorts in Form von Verwaltungsvorschriften) verbindlich werden. Die Länder könnten sich an diesen Vorarbeiten orientieren und sie für ihren Kompetenzbereich übernehmen. Dadurch würde nicht nur die Informationsverarbeitung und Telekommunikation der Bundes- und Landesbehörden weniger verletzlich, sondern auch über die Nachfragemacht der öffentlichen Hand ein nicht zu unterschätzender Druck auf die Anbieter von IuK-Systemen ausgeübt, das Kriterium der Verletzlichkeit bereits in der Entwicklung ihrer Systeme zu berücksichtigen.

1.3.3 Beratungen

Auf Nachfrage eines Anbieters oder Anwenders hat das Bundesamt für Sicherheit in der Informationstechnik im Rahmen seiner Möglichkeiten diese zu beraten. Dabei darf sich die Beratung nicht auf den Hinweis auf die neueste Sicherungstechnik beschränken, sondern hätte immer auch auf die Reduzierung von Schadenspotentialen und die Verringerung der Abhängigkeit von Technik-Systemen zu zielen.

1.3.4 Standardisierung

Wie bereits im Rahmenkonzept vorgesehen, ist eine wichtige Aufgabe des Bundesamtes für Sicherheit in der Informationstechnik, Sicherheitskriterien zu entwerfen und Sicherheitsstandards zu entwickeln. Allerdings sollte das Bundesamt nur die Standardisierung organisieren. Die Normung selbst sollte von pluralistisch zusammengesetzten Gremien in öffentlichen Sitzungen erfolgen.[147]

1.3.5 Zertifikate

Im Rahmenkonzept ist vorgesehen, daß Hersteller von IuK-Produkten für diese auf freiwilliger Basis ein Zertifikat des Bundesamtes für Sicherheit in der Informationstechnik erhalten können, in dem bescheinigt wird, daß das Produkt die Anforderungen einer gewissen Sicherheitsklasse erfüllt. Diese Maßnahme erhöht jedenfalls die Markttransparenz für die Anwender und verbessert die Martchancen für die Hersteller.

Standardisierung und Zertifikate könnten darüberhinaus eine steigende Bedeutung erlangen, wenn diese Aufgaben des Bundesamts für Sicherheit in der Informationstechnik mit einer Verschärfung des Haftungsrechts

---

[147] Vgl. hierzu näher oben III.3.4.

verbunden würden.[148] Dann könnten die Standards den Pflichtenmaßstab bilden, den ein Anbieter von IuK-Systemen erfüllen muß, um keine Gefährdungshaftung auszulösen. Und umgekehrt könnte ein Zertifikat des Bundesamtes für Sicherheit in der Informationstechnik der Nachweis sein, der von der Gefährdungshaftung befreit.

Allerdings ist hier nochmals[149] daraufhinzuweisen, daß positive Auswirkungen auf die Verletzlichkeit der Gesellschaft nur zu erreichen sind, wenn die Haftungsregelungen verbessert werden. Dazu zählen insbesondere die Einführung einer summenmäßig unbeschränkten Gefährdungshaftung, eine Beweislastumkehr beim Nachweis von Kausalität und Verschulden zugunsten des Geschädigten und die Einführung einer Pflichtversicherung für Hersteller und Anwender von IuK-Techniken zur Abdeckung des Insolvenzrisikos.

1.3.6 Beteiligungsrechte

Das Bundesamt für Sicherheit in der Informationstechnik sollte das Recht - für bestimmte, näher zu bezeichnende Bereiche auch die Pflicht - haben, sich an allen relevanten Planungs- und Entscheidungsverfahren zu beteiligen (z.B. von TELEKOM oder von Beschaffungsprogrammen des Bundes), um in diesen das Kriterium der Verletzlichkeit als Entscheidungskriterium zur Geltung zu bringen. Denn nur wenn präventiv auf die mögliche Abhängigkeit von Techniksystemen und die damit entstehenden Schadenspotentiale hingewiesen wird, besteht überhaupt eine Chance, die Verletzlichkeit in dem jeweiligen Gesellschaftsbereich zu verringern.

1.4 Befugnisse zur Kontrolle und Steuerung der Technikentwicklung

Künftig werden die Verbreitung und Vernetzung von IuK-Systemen exponentiell zunehmen und in gleichem Maße ihre Durchschaubarkeit abnehmen. Hinzu kommt, daß die 'Anwendungsschwelle' durch benutzerfreundliche Systeme und die frühzeitige Vermittlung von Computerkenntnissen absinken wird. Die Vorstellungen von wirksamer reaktiver Kontrolle werden dadurch weitgehend zur Illusion. Verletzlichkeitsaspekte müssen daher schwerpunktmäßig bereits in der Planungs- und Entscheidungsphase von IuK-Systemen berücksichtigt werden. Nur wenn Technikkontrolle präventiv erfolgt, läßt sich sicherstellen, daß die Anforderungen zur Schadensbegrenzung sowie Fehler- und Mißbrauchsverhinderung bereits die Wahl technischer Gestaltungsoptionen beeinflussen und technisch gewährleisten.

Daher sind für Systeme mit besonders großem Schadenspotential Zulassungsverfahren vorzusehen. Das gleiche wird für die Fälle gelten müssen, in denen aus der spezifischen Interessenkonstellation bei der Entwicklung oder Einführung der IuK-Systeme befürchtet werden muß, daß das Kriterium der Verletzlichkeit nur unzureichend berücksichtigt werden dürfte.[150]

1.4.1 Eingriffsbefugnisse

In den Fällen, in denen sich aus der Anzeige[151] ergibt, daß die Auswirkungen auf die Verletzlichkeit der Gesellschaft in einem unvertretbaren Ausmaß vernachlässigt werden, sollte das Bundesamt für Sicherheit in der Informationstechnik die Befugnis haben, Auflagen für die technische oder organisatorische Gestaltung des IuK-Systems erlassen zu können.

---

[148] Vgl. hierzu näher oben III.3.3.

[149] Vgl. bereits oben III.3.3.

[150] Vgl. hierzu näher oben III.2.

[151] Vgl. oben IV.1.2.1.

1.4.2 Zulassungs und Genehmigungsverfahren

Um die Verletzlichkeit der Gesellschaft zu verringern, sollte das Bundesamt für Sicherheit in der Informationstechnik die Befugnis einer Validierungsstelle erhalten, die - wie dies für fast alle anderen Techniksysteme auch verlangt wird - in einem Zulassungsverfahren dafür sorgt, daß für IuK-Systeme der jeweils festzulegende Mindeststandard an Sicherung und Schadensvorsorge gewährleistet ist. In diesem Zulassungsverfahren könnte neben der Verletzlichkeit auch das Kriterium der Verfassungsverträglichkeit berücksichtigt werden und beispielsweise die datenschutzadäquate Gestaltung des jeweiligen Systems überprüft werden.[152]

Zulassungsverfahren und öffentliche Genehmigungsverfahren sind voneinander nach Risiken und Anwenderkreis zu unterscheiden. So kann die Zulassung von Hard- und Softwareteilen im Wege der abstrakten Musterzulassungen oder in Form von allgemeinen Betriebsgenehmigungen erteilt werden. Diese Aufgabe kann und sollte dem Bundesamt für Sicherheit in der Informationstechnik übertragen werden.

Öffentliche Genehmigungsverfahren sind vor allem vorzusehen, wenn es um die lokale Anwendung einer IuK-Technik eines bestimmten Zuschnitts geht. Hier sind umfassende Risikoabschätzungen notwendig, die nur erreicht werden können, wenn die Verfahren öffentlich stattfinden, d.h. Transparenz gewahrt ist. So sollte beispielsweise der Einführung von Krankenhausinformationssystemen ein öffentliches Erörterungsverfahren vorgeschaltet sein, bei dem alle betroffenen Stellen (Netzanbieter, Betreiber, Datenschutzbeauftragte, betriebliche Datenschutzbeauftragte, Personalräte, Interessensvertreter) beteiligt werden müssen. Jeder muß Einwendungen erheben können. Derartige Verfahren sollten allerdings nicht zentral von dem Bundesamt für Sicherheit in der Informationstechnik, sondern eventuell mit dessen fachlicher Unterstützung dezentral durchgeführt werden. Vergleichbare Verfahren finden sich im Umweltschutzrecht, wobei die zuständige Genehmigungsbehörde die jeweilige Landesoberbehörde ist.

Bei der Einführung von Genehmigungsverfahren für bestimmte IuK-Techniken sind im Einzelfall Kompatibilitäten mit anderen Erlaubnisverfahren zu prüfen und gegebenenfalls herzustellen. So wäre es beispielsweise sinnvoll, für den Bereich der Geldwirtschaft die Prüfung von IuK-Techniken in Zusammenhang mit der Erlaubnis nach dem KWG zu sehen.

Weil die Anwendung einer IuK-Technik Auswirkung sowohl auf den Datenschutz hat als auch auf den Bereich der "nur" technischen Sicherheit, sind die Datenschutzbeauftragten des Bundes und der Länder an diesen Verfahren zu beteiligen. Es muß gewährleistet werden, daß sowohl die technische Sicherheit als auch spezifische anwendungsbezogene Risiken für die Grundrechte Dritter (Datenschutz) in die Verfahren institutionell getrennt Eingang finden. Konkret bedeutet das, daß die jeweiligen Datenschutzbeauftragten des Bundes und der Länder als sachverständige Fachbehörden mit einer eigenen Stellungnahme an den Genehmigungsverfahren zu beteiligen sind. Ebenso müssen die betrieblichen Datenschutzbeauftragten beteiligt werden, soweit die Verletzlichkeitsuntersuchung den betrieblichen Bereich betrifft. Soweit beispielsweise Verbraucherschutz- oder Naturschutzbelange betroffen sind, sind auch die entsprechenden Verbände zu beteiligen.

Zulassungs- und Genehmigungsverfahren erfordern detaillierte gesetzliche Regelungen, die den Kreis der zulassungspflichtigen IuK-Techniken und genehmigungspflichtigen IuK-Systeme bestimmen, die materiellen Voraussetzungen für eine Genehmigung festsetzen sowie die wesentlichen Verfahrensregelungen insbesondere über eine Öffentlichkeitsbeteiligung vorschreiben. Als Prüfkriterien sind (nicht abschließend) insbesondere vorzusehen,

- Bestandsaufnahme der Verletzlichkeit,
- Verletzlichkeitsprognose unter Berücksichtigung der eingesetzen IuK-Technik,
- Erforderlichkeit der IuK-Technik und damit verbunden eine Prüfung von Alternativen einschließlich der "Nullvariante",
- Bewertung der eingesetzten Sicherheitstechnik und des Sicherungskonzepts,
- Bewertung der verbleibenden Risiken.

Verfassungsrechtlich sind gesetzliche Regelungen über Zulassungs- und Genehmigungsverfahren möglich, soweit sie die Bundesverwaltung und die private Wirtschaft betreffen (Art. 86 ff. und 73 Nr. 11 GG). Keine Gesetzgebungskompetenz besitzt der Bund allerdings für den Bereich der Länderverwaltungen. Für diesen

---

[152] Vgl. hierzu z.B. näher Roßnagel u.a., Digitalisierung der Grundrechte?, 1990, S. 286 ff.

Bereich einbeziehende bundeseinheitliche Regelungen müßte durch Verfassungsänderung eine Gesetzgebungskompetenz geschaffen werden wie sie beispielsweise Art. 73 Nr. 22 GG für den Bereich Abfallwirtschaft und Luftreinhaltung vorsieht und aufgrund dessen das Bundesrecht Planfeststellungsverfahren für Abfallentsorgungsanlagen oder Genehmigungsverfahren für luftverschmutzende Anlagen vorsieht.

1.4.3 Planungsverfahren

Ein wie gerade beschriebenes Genehmigungsverfahren ist der Zulassung von Kraftfahrzeugen oder der Genehmigung emittierender Anlagen nachgebildet und daher strukturell an dem Maschinenmodell der Technik orientiert. Mit diesem können die sozialen Auswirkungen einer Technik, die wie die IuK-Technik Systemcharakter hat, jedoch nur unzureichend erfaßt werden. Auch wenn sich die Genehmigungsbeamten große Mühe geben, künftige Technikfolgen abzuschätzen, ist es fraglich, ob die punktuelle Zulassungsentscheidung den künftigen Wechselwirkungen der Vernetzung und Multifunktionalität der Systeme gerecht werden kann. Für Infrastruktursysteme wäre daher ein Planungsverfahren ähnlich der Fachplanung für Straßen u.ä. mit Öffentlichkeitsbeteiligung vorzusehen. An diesem wäre das Bundesamt für Sicherheit in der Informationstechnik zu beteiligen.

Zu beachten ist zudem, daß die Einführung bestimmter Technologien, die Auswirkungen auf die Grundrechtsausübung der Bürger haben, wie beispielsweise ISDN, einer gesetzlichen Grundlage bedürfen.[153]

1.5 Befugnisse in Public-Key-Systemen

Je nach Struktur und Anbindung des Bundesamt für Sicherheit in der Informationstechnik wird es Teile der oben genannten[154] Aufgaben in Public-Key-Systemen wahrnehmen können oder dazu in einem Interessenkonflikt stehen.

Die Entwicklung von Chipkarten und Systemen wird wohl nicht zu seinen Aufgaben gehören. Wohl aber könnte eine "Verletzlichkeits-Abteilung" Anforderungen für die Teilsysteme im Zuge eines Planungsverfahrens festlegen.

Die Validierung von Algorithmen Chips und Systemen könnte die ZSI im Rahmen ihres derzeitig geplanten Aufgabenspektrums wohl übernehmen. Für ein gesellschaftsweit eingesetztes Public-Key-System wäre allerdings weitergehend zu fordern:

- Die Prüfung muß öffentlich erfolgen. Dazu müssen sowohl die zu prüfenden Systeme als auch die Prüfergebnisse der Fachöffentlichkeit wie der Allgemeinheit zugänglich sein.

- Eine reine Funktionsprüfung ist unzureichend, weil dadurch das Schadenspotential von Anwendungungen und Kummulationseffekten nicht erfaßt wird. Das Kriterium "Verletzlichkeit" muß als Oberkriterium das Prüfverfahren bestimmen.

Diese Anforderungen stellen in Frage, ob die jetzt geplante Struktur und das zugewiesene Aufgabenfeld ausreichend sind, um eine umfassende gesellschaftliche Prüfung einer Infrastruktur durchzuführen. Die Entwicklungen in USA und möglicherweise weiter bestehende Aufgaben im Geheimschutzbereich deuten auf einen Interessenkonflikt hin.

Die Karteninitialisierungs-Instanz(-en) dürfen auf keinen Fall aus anderen Aufgaben heraus ein Interesse an der Speicherung der geheimen Schlüssel haben. Die historische Entwicklung zum Bundesamt für Sicherheit in der Informationstechnik spricht deutlich gegen eine Anbindung an die neue Bundesbehörde. Wegen der For-

---

[153] Vgl. Kubicek, ISDN im Lichte von Demokratieprinzip und informationeller Selbstbestimmung, DuD 1987, S. 21 ff. sowie Roßnagel u.a. Digitalisierung der Grundrechte?, 1990, S. 97 mwN.

[154] Vgl. hierzu oben III.3.5.

derung nach einem amtshilfefesten Schutz wäre sogar eine nichtöffentliche Einrichtung zu erwägen.

Die Ausgabeinstanz(-en) für Karten sollten aus den vorstehenden Argumenten auf keinen Fall exklusiv an das Bundesamt für Sicherheit in der Informationstechnik gebunden sein.

Da die Zertifizierungsinstanzen im wesentlichen die Bonität des Karteninhabers im Rahmen der Anwendung bestätigen, ist eine Ansiedlung beim Bundesamt für Sicherheit in der Informationstechnik nicht sinnvoll. Zuverlässigkeitsfragen sind durch gesetzliche Vorgaben, der Prüfung der Einhaltung durch die Revisionsinstanz und das Haftungsrecht zu regeln.

Die Revisionsinstanz darf wegen Interessenkonflikten nicht an den Geheimschutzbereich angebunden sein. Allerdings sind dort umfassende Fachkenntnisse über die technische Prüfung erforderlich. Sie sollte in keiner anderen Weise in sicherheitskritische Rollen eines Public-Key-Systems eingebunden sein, da nur die Funktionstrennung eine unabhängige Prüfung sichert und Manipulationsmöglichkeiten erschwert.

2. Organisation

"Bundesoberbehörden sind zentrale Verwaltungsbehörden des Bundes, die den Ministerien (hier das BMI) nachgeordnet sind, aber keinen weiteren Unterbau besitzen". Ihre Zuständigkeit erstreckt sich über das ganze Bundesgebiet.[155] Sie sind Behörden, die entweder das jeweilige Ministerium von Routinearbeiten entlasten oder im speziellen, insbesondere technischen Sachverstand zu Verfügung stellen sollen.[156]

Das Bundesamt für Sicherheit in der Informationstechnik kann als eine solche technische Spezialbehörde verstanden werden und ist insofern mit dem Bundesumweltamt, dem Bundesgesundheitsamt, dem Bundeskriminalamt oder dem Bundesamt für Verfassungsschutz vergleichbar, die ebenfalls Bundesoberbehörden sind. Die Selbständigkeit der Bundesoberbehörden bedeutet nicht , daß sie weisungsfrei sind. Da das Bundesamt für Sicherheit in der Informationstechnik im Geschäftsbereich des Bundesministers des Innern errichtet werden soll, wird es von diesem weisungsabhängig sein[157], es sei denn die Weisungsfreiheit wird im Errichtungsgesetz ausdrücklich festgestellt.[158]

Nur theoretisch denkbare Alternativen für die Organisation der genannten Aufgaben wäre die Errichtung einer Anstalt oder Körperschaft des öffentlichen Rechts. Eine Anstalt faßt unter einer Verwaltungsaufgabe persönliche und sachliche Mittel zusammen. Körperschaften haben eine mitgliedschaftliche Struktur. Beide Verwaltungsformen sind für die Funktion des Bundesamt für Sicherheit in der Informationstechnik nicht geeignet.

Zu überlegen wäre, statt der Einrichtung einer Bundesoberbehörde die Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik auf die Länder zu verteilen und damit zu dezentralisieren. Gleichwohl müßte aber wegen des überwiegenden Interesses der Anwender und wohl auch der Betroffenen an transparenten und einheitlichen Sicherheitsstandards eine zentrale Stelle geschaffen werden, deren Kompetenzen und insbesondere Eingriffsbefugnisse beschränkt sind.

---

155 Bull, in: Alternativ-Kommentar zum Grundgesetz, Art. 87, Rn. 25.

156 Bull, in: Alternativ-Kommentar zum Grundgesetz, Art. 87, Rn. 27; Maunz, in: Maunz/Dürig, 1989, Art. 87, Rn. 83.

157 Das Bundesstatistikamt ist nach § 2 BStatG eine weisungsgebundene Bundesoberbehörde.

158 Beispiele bei Bull, in : Alternativ-Kommentar zum Grundgesetz, Art. 87, Rn. 28, Rn. 28: Bundeskartellamt (nach § 48 f.GWB nur allgemeine Weisungen); Bundesprüfstelle, § 10 GjS; Bundesschuldenamt (vgl. Bull, a.a.O.).

Beispielhaft können für die Erfüllung der Aufgaben eines künftigen Bundesamtes für Sicherheit in der Informationstechnik im Rahmen eines im gesellschaftlichen Alltag zur Sicherung der Freiheitsgrundrechte genutzten Public-Key-Systems weitere spezifische Strukturanforderungen gestellt werden:

Vermieden werden muß jedenfalls die Einrichtung nahe bei den Geheimschutzbereichen. Denn dann besteht die Gefahr, daß in einem Interessenkonflikt die Interessen der inneren Sicherheit explizit oder implizit höher gewichtet werden als die Grundrechte der Bürger. Ein unvoreingenommener Interessenausgleich kann wegen der Konzentration der Fachkompetenz nicht mehr erfolgen. Dies ist zu befürchten, wenn das Bundesamt für Sicherheit in der Informationstechnik weisungsabhängig im Geschäftsbereich des Bundesministers des Innern oder der Verteidigung oder des Bundeskanzleramts errichtet wird. Denn diese sind zugleich gegenüber dem Bundesamt für Verfassungsschutz, dem Militärischen Abschirmdienst und dem Bundesnachrichtendienst weisungsbefugt und könnten und dürften die Tätigkeiten dieser Geheimdienste und des Bundesamtes für Sicherheit in der Informationstechnik koordinieren. In diesen Fällen müßte damit gerechnet werden, daß das Bundesamt ähnliche Strategien wie die amerikanische NSA verfolgen wird.[159] Dies gilt insbesondere dann, wenn die Vertreter der neuen Bundesoberbehörde - wie bisher die ZfCH und die ZSI - mit den Sicherheitsdiensten anderer NATO-Staaten zusammenarbeiten und ihnen gegenüber vertrauenswürdig bleiben sollen.

Eine daraus unter Umständen resultierende geheime Validierung oder gar das Monopol auf die Schlüsselvergabe stünden in Konflikt mit dem Ziel der Öffenlichkeit des Prüfverfahrens oder der Autonomie des Schlüsselmanagements, die für die Schutzziele Anonymität und Vertraulichkeit übermittelter Nachrichten unabdingbar sind. Die Bürger könnten dann dem Verschlüsselungsverfahren und dem Schlüsselmanagement nicht mehr vertrauen. Gefährdet wäre damit nicht nur der Grundrechtsschutz der Bürger, sondern auch die Akzeptanz für alle Arten vertrauensbedürftigen Teletransaktionen. Das Schlüsselmanagement und die Kartenausgabe sind daher unabhängig von Behörden mit Geheimschutzinteressen zu organisieren. Das Bundesamt für Sicherheit in der Informationstechnik könnte sie also nur übernehmen, wenn es im Errichtungsgesetz von Weisungen des zugeordneten Ministeriums freigestellt wird.

Die Organisationsform der Behörde muß auch gewährleisten, daß Bedenken der Sicherheitsbehörden nicht gegen den Schutz der Freiheitsgrundrechte den Einsatz von Public-Key-Systemen generell verhindern. In diesem Sinne sind Chipkarten unzureichend, die lediglich eine Authentifizierung ermöglichen, Verschlüsselung aber nicht zulassen. Dann wäre zwar manchen Sicherheitsbedenken der Boden entzogen und entsprechende Dienste könnten in öffenlichen Netzen zur Verfügung gestellt werden. Sie verbesserten allerdings nur die Rechtssicherheit. Sie würden aber im Interesse der Behörden der inneren Sicherheit und der Geheimdienste kein anonymes Handeln und keine Vertraulichkeit von Nachrichten gewährleisten.[160]

Weitere Aufgaben - neben der unabhängigen und öffentlichen Systemvalidierung - sollte das Bundesamt nicht übernehmen. Insbesondere sollte in jedem Fall die Revision aller Systeme im Zusammenhang mit dem Public-Key-System durch eine vom Schlüsselmanagement unabhängige Behörde übernommen werden. Sie ist entsprechend mit Personal und Mitteln für ergänzende Fachgutachten auszustatten.

Für die Errichtungsentscheidung ist in jedem Fall zu bedenken, daß durch sie nicht nur die Grundrechte der informationellen Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und des Fernmeldegeheimnisses (Art. 10 GG) betroffen sein können, sondern das ganze informationelle Gleichgewicht einer demokratischen Gesellschaft. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil die Bedeutung des informationellen Selbstbestimmungsrechts als Strukturprinzip einer freien Demokratie ausdrücklich betont und es als

> "elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens"[161]

bezeichnet. Diesem Strukturprinzip würde eine Organisationsregelung nicht gerecht, die nicht zugleich auch wirksame Vorkehrungen gegen Möglichkeiten einer staatlichen Verhaltenskontrolle und damit mittelbaren

---

[159] Vgl. hierzu oben II.4.

[160] In diesem Sinne wäre nur der liberalste Vorschlag von Rihaczek, K.: "Ein Kompromißvorschlag zur Datenverschlüsselung", DuD Heft 6/1987, S. 299 ff. zu akzeptieren, der allerdings die geschilderten Konflikte nicht löst.

[161] BVerfGE 65, 1 (43).

Verhaltenssteuerung ausschließt. Schon deshalb muß die Weisungsabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik vom Bundesministerium des Inneren als dem "Ministerium der Bundespolizei" auf schwere Bedenken stoßen. Hinzu kommt das Gebot der "informationellen Gewaltenteilung"[162], worunter in diesem Zusammenhang eine Denzentralisierung von Wissen und damit Macht im Bereich der Entwicklung und Anwendung einzelner zentraler Sicherheitskomponenten - wie etwa Verschlüsselungsverfahren - verstanden werden muß.

Soll nicht nur eine Kompetenzerweiterung bestehender Dienststellen erreicht werden, muß im Mittelpunkt einer neuen Behörde der Schutz der Privatsphäre und der Freiheitsgrundrechte stehen. Eine Behörde, die lediglich das Bedürfnis nationaler Sicherheit in Verbindung mit den internationalen Schutzanstrengungen der Militärs und in zweiter Linie wirtschaftliche Sachzwänge vertritt, kann den konfligierenden Interessen des Bürgerschutzes nicht gerecht werden.

[162] BVerfGE 65, 1 (69).

LITERATUR

Abel, Horst / **Schmölz**, Werner: Datensicherung für Betriebe und Verwaltung, Sicherungsmaßnahmen in der modernen Informationstechnik - Erfahrungen aus der Praxis, München 1968.

Alternativ-Kommentar zum Grundgesetz, Hrsg. Rudolf Wassermann, Band. 2, Art. 38 - 146, 2. Aufl., Darmstadt 1989.

Beier, Bernd: Novellierung des Bundesdatenschutzgesetzes - Neuauflage alter Ideen oder tasächliche Reform? Datenschutz und Datensicherung 1988, S. 506 (509).

Bähre, Inge L. / **Schneider**, Werner: Kreditwesengesetz. 3. Aufl., München 1986.

Berger P. / **Kühn**, M. / **Kubicek**, H. / **Mettler-Meibom**, B. / **Voogd**, G.: Optionen der Telekommunikations-Infrastruktur, Düsseldorf 1988, Band III.

Bernhard, U. / **Ruhmann**, I. (ZSI): Die Bundesregierung will den Bock zum Gärtner machen, Computerwoche vom 22.12.89 S. 6 f.

Schreiben der **Botschaft der Bundesrepublik** an das Auswärtige Amt vom 7.1.1987.

Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (**BSI-Errichtungsgesetz, BSIG**), Entwurf vom 9.2.1990.

Cerny, D.: Vertrauenswürdige DV-Systeme nach dem Orange Book, Datenschutz und Datensicherung 1/1988, S. 11-13.

Cerny, D.: Vertrauenswürdige Netze, die "Trusted Network Interpretation", Datenschutz und Datensicherung 7/1988, S. 354-359.

Computer Security Act of 1987, USA, Public Law 100-235, 8.Jan. 1988, abgedruckt ebenfalls in Datenschutz und Datensicherung 11/1987 S. 544 ff.

Coy, Wolfgang: Geheime Schriften - geheime Dienste, in: Michel, K./ Spengler, T. (Hrsg.): Kursbuch 66, Kursbuchverlag, Berlin 1981, S. 83ff.

Denning, E.: Cryptography and Data security, Addison Wesley, Reading 1982.

Denninger, Erhard: Verfassungsrechtliche Grenzen polizeilicher Datenverarbeitung - insbesondere durch das Bundeskriminalamt, Computer und Recht, 1988, S. 51-60.

EG-Produkthaftungsrichtlinien vom 25.7.1985, Bundestags-Drucksache 11/2447 (Abl. EG vom 7.8.1985, Nr. L 210/29).

van Essen, Ulrich: IT-Sicherheitskriterien, Computer und Recht 1989, S. 947 ff.

Fitting, Karl, u.a.: Betriebsverfassungsgesetz, Kommentar, 15. Aufl., München 1987.

Fölsing, A.: Die hohe Schule der Kryptologie, S. 103 in: Michel, K./ Spengler, T. (Hrsg.): Kursbuch 66, Kursbuchverlag, Berlin 1981, S. 92ff.

Führ, Martin: Sanierung von Industrieanlagen, Düsseldorf, 1989.

Gola, Peter: Zur Entwicklung des Datenschutzrechtes im Jahre 1988, Neue Juristische Wochenzeitung 1989, S. 2595 ff.

Haberzettl, Gerhard: Normung und Zertifizierung, Bausteine für den Europäischen Binnenmarkt, Computer und Recht 1989, S. 943 ff.

Hahn, Lothar: Der Hochtemperaturreaktor-Modul, Öko-Mitteilungen 2/1989, S. 6 ff.

Hammer, Volker: TeleTrusT: Verletzlichkeit und Verfassungsverträglich-keit eines Konzepts für rechtssichere Transaktionen in der Informationsgesellschaft, Datenschutz und Datensicherung 1988, 391 ff.

Hammer, Volker: Die künftige Informationsinfrastruktur und das Grundrecht auf Information, in: Roßnagel, A. (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, 49 ff.

Hammer, Volker / **Pordesch**, Ulrich / **Roßnagel**, Alexander: Freiheit oder Sicherheit - Ein Widerspruch informationstechnischer Vernetzung, in: Valk, R. (Hrsg.), Vernetzte und komplexe Informatik-Systeme, 18. GI-Jahrestagung Hamburg 1988, Heidelberg 1988, 506 ff.

Hammer, Volker / **Pordesch**, Ulrich / **Roßnagel**, Alexander: Gestaltungsanforderungen für die ISDN-Nebenstellenanlage der Hochschulregion Darmstadt, provet Darmstadt 1989.

Hammer, Volker / **Pordesch**, Ulrich / **Roßnagel**, Alexander: Rechtsgemäße Gestaltung von ISDN-Nebenstelleanlagen, in: Paul, M. (Hrsg.), GI - 19. Jahrestagung, Computergestützter Arbeitsplatz, Berlin u.a. 1989, Band II, 507 ff.

Hammer, Volker / **Pordesch**, Ulrich / **Roßnagel**, Alexander: Gestaltungsanforderungen an ISDN-Systeme, erscheint in: Tagungsband der FIFF-Jahrestagung 1989, Frankfurt 1990.

Harmsen, Dirk-Michael / **Weiß**, Gerhard: Aspekte der Datensicherheit und der Verletzlichkeit der Informationssysteme im Bankensektor, SoTech-Werkstattbericht Nr. 68, Karlsruhe 1989

Haushaltsausschuß: Protokoll der Sitzung des Haushaltsausschusses vom 27.9.89, erstellt am 19.10.89.

Hess, Harald / **Schlochauer**, Ursula / **Glaubitz**, Werner: Betriebsverfassungsgesetz, Kommentar, Darmstadt, 1986.

Hofmann, Max: Luftverkehrsgesetz, Kommentar, München 1971.

IT-Sicherheitskriterien - Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT), hrsg. von der Zentralstelle für Sicherheit in der Informationstechnik, Bundesanzeiger, Köln 1989.

IT-Sicherheitsrahmenkonzept: Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik (IT), 3 verschiedene Fassungen:
- Rahmenkonzept vom 30.12.1988
- Rahmenkonzept ohne Datum, in: Datenschutz und Datensicherung 1989, S 291 ff.
- Rahmenkonzept vom 27.9.1989, Kabinettsvorlage des Bundesinnenministeriums vom 25.10.89.

Jagusch, Heinrich u.a.: Straßenverkehrsrecht, 30. Auflage, München 1989.

Kersten, Heinrich: Vertrauenswürdige DV-Systeme und ihre Validierung nach dem Deutschen Kriterienkatalog. 13. DAFTA-Tagung am 16./17.11.89, Tagungsband Register 15.

Koutses, Irene: Auswirkungen des Produkhaftungsgesetzes (ProdhaftG) auf Informations- und Steuerungstechnologien, Referat, 13. DAFTA, 16.-17. November 1989, Register 16.

Koutses, Irene / Lutterbach, Sabine: Auswirkung des Produkthaftungsgesetzes auf Informations- und Steuerungstechnologien, Recht der Datenverarbeitung 1989, S. 5-10.

Kubicek, Herbert: ISDN im Lichte von Demokratieprinzip und informationeller Selbstbestimmung, Datenschutz und Datensicherung 1987, S. 21 ff.

Leiberich, Otto (ZSI): Hintergrundpapier Wissenschafts-Pressekonferenz vom 6.2.1990 zum Thema: Computersicherheit: Risiken ausschalten und neue Standards entwickeln.

Maunz, Theodor / **Dürig**, Günter: Kommentar zum Grundgesetz, Band 3, Art. 38-91 GG, Loseblatt, München, Stand 1989.

Müller, Gerhard F. / **Wächter**, Michael: Zur Aufnahme einer verschulden-unabhängigen Schadenersatzregelung in das BDSG., DuD 1989, S. 239 ff.

Neusel, Hans (BMI): Hintergrundpapier Wissenschafts-Pressekonferenz vom 6.2.1990 zum Thema: Computersicherheit: Risiken ausschalten und neue Standards entwickeln.

NSA & CO - Aufklärungsdienste der USA in der Bundesrepublik, MEDIATUS, Sondernummer Juni 1989.

Orange Book: Department of Defense (USA), Trusted Computer System Evaluation Criteria, DoD 5200.28 STD, Dezember 1985.

Peitsch, Dietmar: Grundrechtswesentlichkeit polizeilicher Informations-sammlung und -verarbeitung, Computer und Recht 8/1989, S. 721 ff.

Pfitzmann, Birgit / **Pfitzmann**, Andreas / **Waidner**, Michael: Technischer Datenschutz in diensteintegrierenden Digitalnetzen - warum und wie? Datenschutz und Datensicherung 1986, S. 178 ff.

Pfitzmann, Andreas / **Pfitzmann**, Birgit / **Waidner**, Michael: Datenschutz garantierende offene Kommunikationsnetze, Informatik-Spektrum 1988, S. 118 ff.

Pordesch, Ulrich: Informatisierung und neue Polizeistrategien, in: Roßnagel, A. (Hrsg.): Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, 87 ff.

Pordesch, Ulrich: Zum Katastrophenpotential der Telekommunikation, Zivilverteidigung 1989, Heft 2, 41 ff.

Pordesch, Ulrich / **Wedde**, Peter: Die Verletzlichkeit der Gesellschaft durch die Datenverarbeitung bei der Polizei, Datenschutz und Datensicherung 1989, 487 ff.

Raubold, Eckart: Sicherheit ist mehr als Schutz vor Angriffen, GMD-Spiegel 2/3'1989, S. 16-21.

Rihaczek, K.: Datensicherheit amerikanisch, Datenschutz und Datensicherung Heft 5/1987, S. 240ff.

Rihaczek, K.: Ein Kompromißvorschlag zur Datenverschlüsselung, Datenschutz und Datensicherung Heft 6/1987, S. 299ff.

Roller, Gerhard: Haftung für Umweltschäden in der EG, Studie für das Europäische Umweltbüro (EEB), Brüssel/Frankfurt, 1989, S. 37 ff., demnächst Brüssel, 1990.

Roßnagel, Alexander: Bedroht die Kernenergie unsere Freiheit? Das künftige Sicherungssystem kerntechnischer Anlagen, 2. Aufl. München 1983.

Roßnagel, Alexander: Radioaktiver Zerfall der Grundrechte? Zur Verfassungsverträglichkeit der Kernenergie, München 1984.

Roßnagel, Alexander: Die unfriedliche Nutzung der Kernenergie. Gefahren der Plutoniumwirtschaft, Hamburg 1987.

Roßnagel, Alexander: Großtechnik und Bürgerfreiheit, Referat zum 6. Rechtspolitischen Kongreß der SPD, Essen 20.-22.6.1986, in: Däubler-Gmelin, H. / Adlerstein, W. (Hrsg.): Menschengerecht, Heidelberg 1986, 337 ff.

Roßnagel, Alexander: Bedroht Großtechnik unsere Freiheit? Universitas 1986, 800 ff.

Roßnagel, Alexander (Hrsg.): Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989.

Roßnagel, Alexander: Das Recht auf (tele-)kommunikative Selbstbestimmung, erscheint in: Kritische Justiz, Heft 2/1990.

Roßnagel, Alexander: Möglichkeiten einer verfassungsverträglichen Gestaltung der Informations- und Kommunikations-Technik, erscheint in: Wechselwirkung 44 (Februar 1990).

Roßnagel, A.: Technik und die Gefahr für das Individuum, in: Bundeskriminalamt (Hrsg.), Technik im Dienst der Straftatenbekämpfung, Wiesbaden, 1990.

Roßnagel, Alexander / **Pordesch**, Ulrich: Informationstechnische Vernetzung und Verteidigungsfähigkeit, erscheint in: Sicherheit und Frieden, 1990.

Roßnagel, Alexander / **Wedde**, Peter: Die Reform der Deutschen Bundespost im Licht des Demokratieprinzips, Deutsches Verwaltungsblatt 1988, 562 ff.

Roßnagel, Alexander / **Wedde**, Peter / **Hammer**, Volker / **Pordesch**, Ulrich: Die Verletzlichkeit der 'Informationsgesellschaft', Opladen 1989.

Roßnagel, Alexander / **Wedde**, Peter / **Hammer**, Volker / **Pordesch**, Ulrich: Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen 1990.

Schmidt, Werner: Kompromittierende Abstrahlung, Datenschutz und Datensicherung 6/1987, S. 276 ff.

Schmidt, Werner: Hintergrundpapier Wissenschafts-Pressekonferenz vom 6.2.1990 zum Thema: Computersicherheit: Risiken ausschalten und neue Standards entwickeln.

Schneider, Wolfgang: Änderung des Betriebsverfassungsgesetzes: verbesserte Arbeitnehmerrechte bei der Informationstechnik?, Recht der Datenverarbeitung 1989, S. 113.

SPD-Entwurf zum BDSG, 1989, Bundestags-Drucksache Nr. 11/3730.

Steinmüller, Wilhelm: Datenschutz und Mitbestimmung, Computer und Recht 1989, S. 606 ff.

Szagunn / Neumann / Wohlschieß: Gesetz über das Kreditwesen, Kommentar, 3. Aufl, Stuttgart 1976.

Thompson, Ken: Reflecting on Trusting Trust, Communications of the ACM, August 1984, Vol. 27, No. 8, S. 761-763.

Waidner, M. / Pfitzmann, B. / Pfitzmann, A.: Über die Notwendigkeit genormter kryptographischer Verfahren, Datenschutz und Datensiche-rung 6/1987, S.293 ff.

Weck, Gerhard: Datensicherung - Konzepte und Bewertung, Datenschutz und Datensicherung 8/1989, S. 386-392.

Zukunftskonzept Informationstechnik, hrsg. vom Bundesminister für Forschung und Technologie und dem Bundesminister für Wirtschaft, Bonn, August 1989.

ABKÜRZUNGSVERZEICHNIS

BAG	Bundesarbeitsgericht
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des BGH in Zivilsachen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichts-Entscheid
CEN	Commité Européen de Normalisation
CENELEC	Commité Européen de Normalisation Electronique
DES	Data Encryption Standard (Ein symmetrisches Krypto-system, 1977 vom NBS standardisiert)
DoD	Department of Defense
EEB	Europeen Environmental Bureau (Europäisches Umweltbüro)
EG	Europäische Gemeinschaft
f.	folgende
ff.	fortfolgende
Fn.	Fußnote
IABG	Industrie Anlagen Betriebsgesellschaft
ISIT	Interministerieller Ausschuß für die Sicherheit in der Informationstechnik
IT	Informationstechnik
IuK-	Informations- und Kommunikations-(Technik)
ISDN	Integrated Services Digital Network
mwN.	mit weiteren Nachweisen
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology
NRPL	NATO-Recommended Products-List
NSA	National Security Agency
NSDD	National Security Decision Directive
OTA	Office of Technology Assessment
PKS	Public-Key-System
RSA	(Ein asymmetrisches Kryptosystem, benannt nach den Entwicklern Rivest, Shamir und Adleman, 1977)
S.	Seite
SECAN	(NATO-Behörde)
TÜV	Technischer Überwachungsverein
usw.	und so weiter
VGH	Verwaltungsgerichtshof
Vgl.	Vergleiche
ZfCh	Zentralstelle für Chiffrierwesen
ZSI	Zentralstelle für Sicherheit in der Informationstechnik

Zeitschriften

AuR	Arbeit und Recht
CR	Computer und Recht
DuD	Datenschutz und Datensicherung
GVBl	Gesetz- und Verwaltungsblatt
KJ	Kritische Justiz
NJW	Neue juristische Wochenzeitung
NZA	Neue Zeitschrift für Arbeitsrecht
RDV	Recht der Datenverarbeitung

Gesetze

AMG	Arzneimittelgesetz
AtG	Atomgesetz
BayDSG	Bayerisches Datenschutzgesetz
BDSG	Bundesdatenschutzgesetz
BerlDSG	Berliner Datenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BImSchG	Bundesimmisionsschutzgesetz
BImSchV	Bundesimmisionsschutzverordnung
BSIG	BSI-Errichtungsgesetz
BSIG-E	BSI-Errichtungsgesetz, Entwurf vom 9.2.1990
BStatG	Bundesstatistikgesetz
GFD NW	Gesetz für Datenschutz, Nordrhein-Westfalen
H(ess)DSG	Hessisches Datenschutzgesetz
HmbgDSG	Hamburgisches Datenschutzgesetz
KWG	Kreditwesengesetz
LuftVG	Luftverkehrsgesetz
NdsDSG	Niedersächsisches Datenschutzgesetz
ProdhaftG	Produkthaftungsgesetz
RlPfDSG	Rheinland-Pfälzisches Datenschutzgesetz
StörfallVwV	Störfallverwaltungsverordnung
STVG	Straßenverkehrsgesetz
WHG	Wasserhaushaltsgesetz