DuD

Datenschutz und Datensicherung
Recht und Sicherheit der Informations- und Kommunikationssysteme

# Reprint

Das unentbehrliche Informationsorgan
und Kommunikationsmedium in allen
Fragen des Datenschutzes und der Datensicherung

vieweg

**Zitiervorschlag:**
*Bizer, J. / Hammer, V. / Pordesch, U. / Roßnagel, A.:* Ein Bundesamt für die Sicherheit in der Informationstechnik – Kritische Bemerkungen zum Gesetzentwurf der Bundesregierung, DuD 4/1990, 178 ff.

Der Text entstand im Rahmen von Arbeiten der Projektgruppe verfassungsverträgliche Technikgestaltung - provet - e.V. (www.provet.org). Die Open-Access-Version wird mit freundlicher Genehmigung der Springer Fachmedien Wiesbaden GmbH bereitgestellt.

**Hinweis zum OCR-Text:**
Das AP40s ist die gescannte Fassung des entsprechenden Arbeitspapiers von provet.
Durch eine OCR-Software wurden das Scan-Ergebnis automatisch in Text umgewandelt und zusätzlich zu den Bildern in dieser Datei hinterlegt. Bitte beachten Sie, dass wir die Qualität der OCR-Umwandlung nicht überprüft haben.

Stand der elektronischen Fassung: Version 1.0 vom 11.05.2020

# Ein Bundesamt für die Sicherheit in der Informationstechnik – Kritische Bemerkungen zum Gesetzentwurf der Bundesregierung[1]

*Johann Bizer, Volker Hammer, Ulrich Pordesch, Alexander Roßnagel*

*Mit Datum vom 23. Februar 1990 hat die Bundesregierung dem Bundesrat den Entwurf eines „Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)" zugeleitet[2], der noch in dieser Legislaturperiode verabschiedet werden und zum 1.1.1991 in Kraft treten soll (§ 8).[3] Dieser Gesetzentwurf ist ein Ausdruck für die Aufmerksamkeit, die die Bundesregierung der Sicherheit in der Informationstechnik neuerdings zukommen läßt. Ihre politischen Handlungsabsichten hat sie in ihrem am 23. November 1989 gebilligten „Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik (IT)" zusammengestellt.[4] Die Errichtung des neuen Bundesamts ist die wichtigste Maßnahme im Rahmen dieses Handlungskonzepts. Der Gesetzentwurf kann daher nur im Kontext der Zielsetzungen und Handlungsvorschläge dieses Rahmenkonzepts adäquat beurteilt werden. Daher beschränkt sich die folgende Bewertung dieses Gesetzentwurfs nicht auf eine kurze Beschreibung der historischen Genese des geplanten Bundesamtes (1) sowie auf die Darstellung (2) und die Erörterung rechtlicher Probleme des Gesetzentwurfs (3), sondern stellt ihn in den Kontext der umfassenderen Zielsetzungen (4) und entwickelt aus deren Kritik (5) und einer Kritik der vorgesehenen Maßnahmen (6) ein neues Aufgabenverständnis (7), aus dem konstruktive Vorschläge für die Aufgabenbestimmung und Befugniszuweisung des geplanten Amtes abgeleitet werden (8).*

## 1 Von der Zentralstelle für das Chiffrierwesen zum Bundesamt für die Sicherheit in der Informationstechnik

Aufbau und Konzept des geplanten BSI stützen sich auf die in den 50er Jahren gegründete Zentralstelle für das Chiffrierwesen (ZfCH)[5], die mit erweitertem Aufgabenbereich zum 1. Juni 1989 in eine „Zentralstelle für die Sicherheit in der Informationstechnik (ZSI) umbenannt wurde.[6] Die ZfCH war dem Bundesnachrichtendienst (BND)[7] zugeordnet, unterstand dem für die Koordination der Geheimdienste zuständigen Staatssekretär des Bundeskanzleramtes und zählte damit zum Geschäftsbereich des Bundeskanzlers. Ihre Aufgabe war neben dem Ver- und Entschlüsseln von Nachrichten der eigenen „Dienste" auch die Sicherung der Kommunikation der Bundesverwaltung – wie beispielsweise des auswärtigen Amtes mit den eigenen Botschaften im Ausland – sowie das Entschlüsseln von Nachrichten, die im Rahmen der Auslandsaufklärung und Spionageabwehr abgefangen und abgehört worden sind.[8] Anfang der 70er Jahre wurde der ZfCH die Überprüfung der für die Verarbeitung oder Übertragung von Verschlußsachen eingesetzten Computerhardware auf die Abstrahlsicherheit übertragen. 1987 wurden die Aufgaben der ZfCH um den Bereich „Computersicherheit" erweitert.[9]

Mit der zunehmenden Aufgabenerweiterung im Bereich Computersicherheit wurde die ZfCH zum 1. Juni 1989 in „Zentralstelle für Sicherheit in der Informationstechnik" (ZSI) umbenannt. Sie befindet sich weiterhin im Geschäftsbereich des Bundeskanzleramtes.[10] Ihre Aufgaben wurden in dem Rahmenkonzept der Bundesregierung nun aber über den Bereich des staatlichen Geheimschutzes hinaus auch auf Sicherheitsaspekte der ‚zivilen' Anwendung der Informationstechnik ausgedehnt.[11]

Mit dem nun vorliegenden Gesetzentwurf wird die Umwandlung der ZSI in eine Bundesoberbehörde betrieben. Diese soll nicht mehr dem Bundeskanzleramt zugeordnet sein, sondern dem Bundesminister des Innern unterstehen (§ 1).[12] Nur der Aufgabenbereich „Entzifferung" soll beim Bundeskanzleramt und damit beim BND verbleiben.[13] Damit ist das BSI zumindest organisatorisch aus dem Geheimdienstbereich herausgenommen. Allerdings besteht nun mit der Zuordnung zum Bundesminister des Innern (BMI) eine Nähe zu den Sicherheitsbehörden des Bundes, insbesondere dem Bundesamt für Verfassungsschutz und dem Bundeskriminalamt.[14] Personelle Bezüge werden aufgrund des Mangels an qualifiziertem Personal auch zur alten ZfCH bestehen.[15] Der designierte Leiter des BSI ist der langjährige Leiter der ZfCH und der ZSI. Der Gründungsstamm von 153 Mitarbeitern wird aus dem BND übernommen. Bis 1994 soll sich dann die Zahl der Mitarbeiter auf 270 erhöhen.[16]

## 2 Der Gesetzentwurf der Bundesregierung

Der Gesetzentwurf beschränkt sich auf einige wenige Regelungen. Er enthält eine weite Begriffsbestimmung der Informationstechnik („alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen")[17] sowie eine Definition der „Sicherheit in der Informationstechnik" (§ 2). Diese beschränkt sich auf die „Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen oder Komponenten oder bei der Anwendung dieser Systeme und Komponenten".

Zu den gesetzlich bestimmten Aufgaben des BSI (§ 3) zählt die Untersuchung von Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie die Entwicklung von Sicherheitsvorkehrungen. Allerdings beschränkt sich diese Aufgabe auf die Anwendung der Informationstechnik zur Aufgabenerfüllung des Bundes (§ 3 Nr. 1). Das BSI soll Maßstäbe[18] für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten entwickeln (§ 3 Nr. 2), derartige Prüfungen und Bewertungen selbst vornehmen sowie auf Antrag der Hersteller oder Vertreiber Sicherheitszertifikate erteilen (§ 3 Nr. 3). Das Verfahren und die Voraussetzungen der Zertifikatserteilung sowie die Möglichkeiten, die Sicherheitszertifikate anderer Prüfstellen anerkennen zu lassen, werden in § 4 geregelt.[19] Schließlich soll das BSI Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik beraten (§ 3 Nr. 7).

Darüber hinaus soll das BSI die bisher schon der ZfCH bzw. der ZSI übertragene Funktion einer Zulassungsbehörde für informationstechnische Systeme oder Komponenten übernehmen, die im Bereich des Bundes für die Verarbeitung oder Übertragung von Verschlußsachen eingesetzt werden. Dazu gehört auch die Herstellung der Schlüsseldaten, die für den Betrieb zugelassener Verschlüsselungsgeräte benötigt werden (§ 3 Nr. 4).[20]

Weiterhin soll das BSI andere für die Sicherheit in der Informationstechnik zuständige Stellen des Bundes, insbesondere soweit sie Beratungs- und Kontrollaufgaben wahrnehmen, unterstützen (§ 3 Nr. 5).[21] Hierzu zählt auch die Unterstützung des Bundesbeauftragten für den Datenschutz unter Wahrung seiner nach dem BDSG vorgesehenen Unabhängigkeit. Unterstützen soll das BSI außerdem die zuständigen Behörden des Bundes bei der Verhütung und Verfolgung von Straftaten sowie den Verfassungsschutz bei der Beobachtung von Bestrebungen und Tätigkeiten nach § 3 Abs. 1 des BVerfSchG[22], soweit es sich um strafbare Handlungen bzw. Bestrebungen oder Tätigkeiten gegen die Sicherheit der bzw. unter Ausnutzung der Informationstechnik handelt (§ 3 Nr. 6).

## 3 Rechtliche Bedenken

Die Vorschrift des § 3 Nr. 6 ist mißglückt, weil die Aufgaben der Verbrechensverhütung, der Strafverfolgung und des Verfassungsschutzes miteinander vermengt werden, für diese aber verschiedene Behörden mit unterschiedlichen Befugnissen zuständig sind. Es zählt beispielsweise nicht zu den Aufgaben des Verfassungsschutzes, Straftaten zu verfolgen[23], ebensowenig ist es Aufgabe des Generalbundesanwalts, geheimdienstliche Tätigkeiten im Inland zu beobachten.[24] Soweit die Formulierung des Entwurfes eine Unterstützung von Tätigkeiten nichtzuständiger Behörden durch das BSI zuläßt, ist sie rechtswidrig.

Unklar bleibt auch die Begrenzung der Unterstützung durch die Formulierung „soweit dies erforderlich ist, um strafbare Handlungen, Bestrebungen oder Tätigkeiten, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen, zu verhindern oder zu erforschen". Behörden des Bundes zur *Strafverfolgung* sind vor allem der Generalbundesanwalt sowie das BKA[25], die selbst nur in ausdrücklich im Gesetz bestimmten Fällen zur Strafverfolgung befugt sind.[26] Einmal abgesehen davon, daß ein Begriff der „Straftaten gegen die Sicherheit in der Informationstechnik" dem geltenden Strafrecht fremd ist, sind diese Bundesbehörden nicht für die Verfolgung der Straftaten gegen die sogenannte Computerkriminalität zuständig.[27] Die Unterstützung des BSI beschränkt sich damit im wesentlichen auf die Verfolgung der Straftaten, die unter Nutzung der Informationstechnologien begangen werden.[28] Im Bereich *Verhütung* von Straftaten darf das BSI im wesentlichen nur das BKA unterstützen. Das BKA selbst ist jedoch nur für die „Vorbeugungsarbeit zur Verbrechensbekämpfung" zuständig, soweit es die Polizei der Länder unterstützt.[29] Weitergehende Befugnisse zur Verhütung von Straftaten liegen bei den Ländern.[30]

Problematischer als die mißglückte Gesetzesfassung dieser Unterstützungspflicht, die durch gesetzestechnische Präzisierungen korrigiert werden könnte, ist aus verfassungsrechtlicher Sicht, daß das BSI zugleich die Polizei und den Verfassungsschutz unterstützen soll. Aus den Erfahrungen mit der geheimen Staatspolizei heraus hat das Grundgesetz die Aufgaben des Verfassungsschutzes und der Polizei funktionell, instrumentell und organisatorisch getrennt.[31] Der Verfassungsschutz darf mit geheimdienstlichen Mitteln aber ohne Exekutivmöglichkeiten beobachten, die mit Zwangsmitteln ausgestattete Polizei muß dem Bürger grundsätzlich offen gegenübertreten. Dieses *Trennungsgebot* darf auch nicht durch Amtshilfeersuchen unterlaufen werden.[32] Die an sich unzulässige Amtshilfe soll nun ermöglicht werden, indem das BSI als Behörde zur Unterstützung beider Funktionen dazwischengeschaltet wird. Dies ist verfassungsrechtlich zumindest bedenklich.

Noch bedenklicher ist jedoch die Verpflichtung des BSI, zwei Herren gleichzeitig zu dienen. Es soll auf der einen Seite den Bundesbeauftragten für den Datenschutz unterstützen (§ 3 Nr. 5), also durch seine technische Kompetenz dazu beitragen, das Recht auf informationelle Selbstbestimmung besser zu *schützen*. Zugleich soll es auf der anderen Seite das Bundeskriminalamt, den Militärischen Abschirmdienst und den Verfassungsschutz unterstützen (§ 3 Nr. 6). Sein technischer Sachverstand soll mithelfen, als riskant definierte Verhaltensweisen und Absichten effektiver auszuforschen – und damit das Recht auf informationelle Selbstbestimmung zu *beschneiden*. Das BSI kann aber nicht zugleich Techniksysteme entwickeln, die etwa die Vertraulichkeit von Kommunikation sicherstellt, und diejenigen unterstützen, die sie aufheben wollen, ohne eine der Aufgaben zu Gunsten der anderen zu verletzen.

Diese Bedenken fordern eine veränderte organisatorische Strukturierung der im Gesetzentwurf angesprochenen Sicherheitsaufgaben: Das BSI sollte als rein ‚zivile' Behörde konzipiert werden und lediglich die für Informationstechnik zuständigen Stellen des Bundes beraten und den Bundesbeauftragten für den Datenschutz unterstützen. Dagegen sollten technische Abteilungen, die zur Unterstützung der Arbeit des Verfassungsschutzes und des BKA für erforderlich gehalten werden, bei diesen selbst – und zwar getrennt – aufgebaut werden. Für ein rein ‚ziviles' BSI stellt sich dann die Frage, warum es vom BMI weisungsabhängig sein sollte. Seinen Aufgaben der Begutachtung und Zertifizierung sowie der Verbesserung der Bürgersicherheit dürfte ein unabhängiger Status eher entsprechen. Daher sollte der BMI auf die Rechtsaufsicht beschränkt werden. Die Freiheit von sachlichen Weisungen müßte allerdings im Errichtungsgesetz ausdrücklich festgeschrieben werden.[33]

## 4 Die Zielsetzungen der Bundesregierung

Die Kritik und die Suche nach konstruktiven Verbesserungen dürfen sich aber nicht darin erschöpfen, einige rechtliche Probleme des *vorliegenden* Gesetzentwurfs zu erörtern. Viel entscheidender ist die Frage, ob er denn dem gesellschaftlichen Problem gerecht wird, auf das er eine Antwort sein soll. Zu fragen ist daher, welchen Zielsetzungen er dienen soll und in welchem Grad er sie zu erfüllen vermag.

Das Problem beschreibt die Bundesregierung knapp aber zutreffend in den ersten beiden Sätzen ihrer Gesetzesbegründung als die „Verletzlichkeit der modernen Informationsgesellschaft": „Viele Bereiche von Wirtschaft und Verwaltung sind bereits heute von dem einwandfreien Funktionieren der Informationstechnik abhängig. Mit dem zunehmenden Einsatz der Informationstechnik steigen auch die damit verbundenen Risiken durch unrichtige, unbefugt gesteuerte, fehlende oder rechtsgutgefährdende Informationen."[34]

Dieser Gefahr setzt die Bundesregierung ihr Konzept der „Sicherheit in der Informationstechnik" und die Errichtung eines Bundesamtes entgegen. Sie präzisiert die Sicherheit, die sie durch diese Maßnahmen erreichen will, insbesondere durch folgende Zielsetzungen:

- Betriebssicherheit
  Durch Anforderungen an informationstechnische Systeme sowie deren Überprüfung und Zertifizierung soll die Betriebssicherheit von IT-Produkten erhöht werden.[35] IT-Anwender sollen in die Lage versetzt werden, system- und anwendungsbezogene Risikoanalysen zu erstellen und angemessene Sicherheitskonzepte zu entwickeln und zu realisieren. Umgekehrt soll für die Hersteller ein Markt für sichere IT-Systeme geschaffen werden, so daß IT-Systeme und -Komponenten mit einem ausreichenden Sicherheitsstandard zur Verfügung stehen.[36]
- Sicherung der internationalen Wettbewerbsfähigkeit
  Mit Hilfe eines eigenen Sicherheitsstandards sowie insbesondere der Erteilung von Sicherheitszertifikaten soll die Exportfähigkeit der bundesdeutschen Industrie auf internationalen Märkten vor allem aber dem US-Markt, der eigene behördliche Zertifizierungen kennt, gesichert werden.[37] Um die Durchsetzbarkeit der eigenen Zertifikate zu erhöhen, werden darüber hinaus EG-weite bzw. internationale Kriterien zur Bewertung, Prüfung und Zertifizierung von IT-Systemen und Komponenten angestrebt, die auch mit der NATO abgestimmt werden sollen.[38]
- Innere Sicherheit
  Mit der Einrichtung des BSI soll insbesondere auf Gefahren für die innere Sicherheit reagiert werden.[39] Als Risiken werden zum einen die gestiegene Computerkriminalität, Sabotage durch extremistische oder terroristische Gruppierungen sowie die organisierte Kriminalität gesehen.[40] Zum anderen wird auf die Arbeit gegnerischer Nachrichtendienste, insbesondere auf die feindliche „Fernmeldeaufklärung", verwiesen.[41]

## 5 Kritik der Zielsetzungen

Die im Gesetzentwurf dem BSI zugewiesenen Aufgaben lassen ein nur reduziertes Problemverständnis der Verletzlichkeit der Informationsgesellschaft erkennen. Das Problem der Verletzlichkeit, nämlich die Möglichkeit großer Schäden für einzelne oder die Gesellschaft, entsteht vor allem dadurch, daß soziale Funktionen von Menschen auf Informations- und Kommunikationssysteme übertragen werden. Informationsverarbeitung und Kommunikation werden dadurch vom Funktionieren einer Technik abhängig, auf die sich die Menschen verlassen. Im Vertrauen auf die Technik erhöhen sie deren Leistungsfähigkeit – und damit zugleich das Schadenspotential. Durch diese Übertragung werden zudem Informationsverarbeitungs- und Kommunikationsprozesse für Dritte zugänglich. Sie können diese leichtfertig oder mißbräuchlich ausforschen, manipulieren, unterbinden, beschädigen oder zerstören. Fehler und Manipulationen können so die Erfüllung der dem technischen System übertragenen gesellschaftlichen Funktionen beeinträchtigen.[42] Diese Erkenntnis führt zu zwei Folgerungen:

Zum einen ist nicht nur ein technisches System (Computer) zu analysieren und zu bewerten, sondern auch dessen soziale Funktion im Rahmen einer konkreten Anwendung. Denn nur so kommen die Abhängigkeit des einzelnen oder der Gesellschaft von der Technik und die mit einem Funktionsversagen verbundenen Schadenspotentiale in den Blick. Daher ist es notwendig, die IuK-Systeme auch in Sicherheitsanalysen als sozio-technische Systeme zu betrachten.

Zum anderen ist nicht nur die Sicherheit von Geräten und Softwareprodukten zu verbessern. Vielmehr sind vor allem Handlungskonzepte zu entwerfen,

- um die gesellschaftliche Abhängigkeit von Systemen der IuK-Technik zu verringern,
- um die potentiellen Schäden eines Mißbrauchs oder Fehlers der IuK-Systeme und die sozialen Folgen eingetretener Schäden zu vermindern,
- um zu verhindern, daß durch die Techniknutzung neue Mißbrauchsmotive hervorgerufen werden,
- um auszuschließen, daß die IuK-Technik neue Mißbrauchsmöglichkeiten und Fehlerquellen eröffnet, und zu erreichen, daß sie bestehende reduziert,
- um zu verhindern, daß die unvermeidlichen Sicherungsmaßnahmen negative Folgen für die Grundrechtsausübung des einzelnen und das soziale und politische System insgesamt hervorrufen.

In den Blick zu fassen, sind daher nicht nur die Risiken, die aus Sicherheitsmängeln technischer Produkte entstehen, sondern auch die Risiken, die von den sozialen Bedingungen und Folgen der IuK-Technik-Nutzung und -Sicherung im betrieblichen und gesellschaftlichen Kontext hervorgerufen werden.[43] Und als Risiken dürfen nicht nur die Ausfallkosten eines defekten Techniksystems, der Verrat militärischer Geheimnisse, die finanziellen Verluste durch Computerkriminalität oder verminderte Exportchancen verstanden werden. Als Risiken sind auch und vorwiegend die Nachteile zu betrachten, die dem einzelnen Bürger sowie der Gesellschaft durch den Ausfall der auf die IuK-Technik übertragenen sozialen Funktionen (Verkehr, Energieversorgung, Prozeßsteuerung, Handel, Zahlungsverkehr, usw.) entstehen. Ausserdem sind die negativen Folgen zu begreifen, die sowohl durch die möglichen Schäden als auch durch die Sicherungsmaßnahmen zu ihrer Verhinderung für die Ausübung von Grundrechten und einen freien Prozeß politischer Willensbildung entstehen können.[44]

## 6 Kritik des Handlungskonzepts

Diese Erkenntnis erfordert Zielsetzungen, die dieser Problembeschreibung gerecht werden, und Maßnahmen, die

durch eine präventive Gestaltung der IuK-Technik diese Risiken vermeiden oder zumindest verringern. Mit ihrem Handlungskonzept wird die Bundesregierung aber weder ihrer eigenen Problemerkenntnis noch ihren eingeschränkten Sicherheitszielen gerecht. Im Detail ist an den Handlungsvorschlägen zu kritisieren:

- die fehlende Zukunftsorientierung

  Der Gesetzentwurf und das Rahmenkonzept behandeln zwar zukünftig einsetzbare Sicherungstechniken, nicht aber die Frage, wo, wozu und in welcher Form IuK-Techniken künftig eingesetzt werden könnten und sollten oder wo und unter welchen Bedingungen aus Risikogesichtspunkten auf einen Einsatz verzichtet werden sollte.

- die Problemverschiebung zur Mißbrauchsverhinderung

  Das zentrale Problem der Verletzlichkeit der Gesellschaft wird in der Verhinderung von Fehlern und Mißbrauchsaktionen gesehen, anstatt in der Abhängigkeit von der IuK-Technik.[45] Das mögliche Schadensausmaß durch den Ausfall oder die Manipulation von IuK-Systemen wird ausschließlich als Problem der Technikanwender betrachtet, nicht aber in seinen Auswirkungen auf die Menschen in den sozialen oder politischen Systemen.[46]

- unzureichende Bedrohungsanalysen

  Dem zu engen Ansatz „Sicherheit der Informationstechnik" entsprechend werden die heutigen und künftigen Motive und Möglichkeiten potentieller Angreifer nicht detailliert untersucht.[47] Ohne derartige Untersuchungen kann aber nicht erkannt werden, wo das heute beobachtbare (meist noch begrenzte) Ausmaß von Schäden einem hohen Sicherungsniveau zu verdanken ist oder nur dem Fehlen entsprechend motivierter Angreifer.

- mangelnde Problematisierung der Verläßlichkeit von Sicherungsmaßnahmen

  Technische und administrative Sicherungsmöglichkeiten werden nicht hinsichtlich ihrer immer nur begrenzten Verläßlichkeit problematisiert. Der Erfolg von Sicherungsmaßnahmen hängt jedoch vorwiegend von der Zuverlässigkeit organisatorischer, menschlicher und sozialer Voraussetzungen ab.[48] Nur wenn auch diese Grenzen der Verläßlichkeit von Sicherungsmaßnahmen berücksichtigt werden, kann das verbleibende Restrisiko realistisch beurteilt werden.

- keine Betrachtung von Technikalternativen

  Die IuK-technische Entwicklung wird als unbeeinflußbar hingenommen. Ihre Risiken sollen allein durch ergänzende Maßnahmen abgewendet werden. Als mögliche Strategie zur Erhöhung der Datensicherheit wird folglich die Option einer nichttechnischen Problemlösung (auch Datenvermeidung) oder die Suche nach sozio-technischen Alternativlösungen nicht berücksichtigt.

- Die Verkennung der gesellschaftspolitischen Dimension

  Mögliche nachteilige Effekte von Sicherungsmaßnahmen auf die Grundrechte von Arbeitnehmern, Netzteilnehmern oder sonstigen Betroffenen werden nicht thematisiert (z.B. Personenüberwachung im Zusammenhang mit Zugangs- und Zugriffskontrollen und Protokollierungen). Die möglichen Freiheits- und Demokratiekosten der je nach Informatisierungsgrad der Gesellschaft unterschiedlich notwendigen Sicherungssysteme werden nicht vorausschauend abgeschätzt und politisch bewertet. Durch das unkontrollierte Schaffen von Sicherungszwängen, entsteht die Gefahr, daß die Gesellschaft in das Dilemma getrieben wird, künftig nur noch zwischen Freiheit und Sicherheit entscheiden zu können.[49]

- die Ablehnung aktiver Steuerungsmaßnahmen

  Die Aufgabe der Bundesregierung und der Bundesverwaltung wird lediglich in der entwicklungsbegleitenden Herstellung einheitlicher Sicherheitsstandards, in der Erforschung und Entwicklung von IT-Sicherheitskomponenten und -systemen sowie in der Beratung der Anwender und Hersteller von IT-Produkten gesehen. Die technische Entwicklung selbst bleibt jedoch außerhalb des Blickfeldes. Ein steuernder oder auch nur korrigierender Eingriff aus Sicherheitsgesichtspunkten ist nicht vorgesehen.

Insgesamt erscheint der Gesetzentwurf und ebenso das ihm zugrundeliegende Rahmenkonzept als ein halbherziger Versuch der Bundesregierung, einem von ihr mitverursachten Dilemma entgehen zu wollen. Auf der einen Seite forciert sie den Wettlauf in die ‚Informationsgesellschaft'[50], auf der anderen Seite muß sie aber die Sicherheitsgefahren und Sicherungszwänge erkennen, die sie damit setzt. Diese Risiken gefährden nun die Akzeptanz des eingeschlagenen Weges in die ‚Informationsgesellschaft' und zwingen die Bundesregierung zum Handeln. Da sie aber offensichtlich keineswegs bereit ist, ihre Politik einer forcierten Informatisierung der Gesellschaft zu verändern oder zu modifizieren, versucht sie in ihrem Konzept diese Risiken so zu definieren, daß sie durch die Errichtung eines Bundesamtes und seiner im wesentlichen auf die Verbesserungen der Sicherheitstechnik begrenzten Aufgabenstellung lösbar erscheinen.

Im Ergebnis wird eine Politik, die Sicherheit ausschließlich durch nachträgliche und ergänzende Verbesserung der als gegeben unterstellten Technik erreichen will, weder die Verletzlichkeit der Gesellschaft verringern noch den bereits auf die Belange der Wirtschaft und des Staates begrenzten Zielsetzungen des Rahmenkonzepts gerecht werden können. Ohne vorbeugende Begrenzung der technischen Abhängigkeit der Gesellschaft und einer gezielten Reduzierung der Schadenspotentiale könnte es zu einem gefährlichen Wettlauf zwischen ‚Angreifern' und technischer Sicherung kommen, den letztere kaum gewinnen kann. Dies aber hätte zum einen einen unvertretbaren Anstieg des „Restrisikos" der Informationstechnik und zum anderen einen sozialunverträglich hohen Zwang zur Sicherung zur Folge.[51]

## 7 Verletzlichkeit der Gesellschaft – Neue Ziele für die Technikbewertung

Wird jedoch die Problembeschreibung der Bundesregierung ernst genommen und eine Verringerung der Verletzlichkeit der Gesellschaft als zentrale Aufgabe des zu schaffenden Bundesamtes angesehen, dann besteht ein wesentlich erweiterter Handlungsbedarf mit anderen Schwerpunktsetzungen. Hierfür ist die technische Sicherung von IuK-Systemen ein wichtiger, aber keineswegs ausreichender Beitrag.[52]

### 7.1 Verminderung der Verletzlichkeit der Gesellschaft

Die Verletzlichkeit der Gesellschaft ergibt sich aus ihrer Abhängigkeit von IuK-Technik und den daraus erwachsenden Risiken großer Schäden. Das Ziel eines Bundesamtes, das die Verletzlichkeit vermindern soll, muß es daher sein, gleichermaßen große Schadenspotentiale durch eine hohe Abhängigkeit von Technik-Systemen zu vermeiden und die Wahr-

scheinlichkeit eines Ausfalls der auf die Technik übertragenen sozialen Funktionen zu vermindern.

Der Ausfall von Informationstechnik, der zur Störung von Abläufen und in der Folge zu großen gesellschaftlichen Schäden führt, kann zum einen durch versehentliche Fehler in der Produktion von Hardware und Software, bei der Bedienung der Systeme oder durch mutwilligen Mißbrauch entstehen. Zur *Begrenzung der Schadenshäufigkeit* trägt es deshalb bei, wenn Fehler vermieden und Angriffe verhindert werden können. Dies kann zum Teil durch die im derzeitigen Gesetzentwurf und dem Rahmenkonzept vorgegebene Aufgabenstellung des BSI erreicht werden. Denn die Entwicklung von Prüfkriterien und -verfahren sowie Sicherheitsstandards kann zur Funktionssicherheit von IT-Produkten beitragen, wenn sie eine entsprechende Marktnachfrage stimuliert. Allerdings müßten hierbei auch Fragen der Beherrschbarkeit berücksichtigt werden. Gleichzeitig könnte durch deren Veröffentlichung und Diskussion das Sicherheitsbewußtsein von Anwendern und Herstellern geschärft werden und mittelfristig eine Anpassung der Systeme an die so erkannten Sicherheitsprobleme erfolgen.

Dennoch werden diese Maßnahmen nicht alle Fehler- und Angriffsmöglichkeiten ausschließen. Denn insbesondere gegen Insider werden rein technische Vorkehrungen unzureichend sein und die technische Verhinderung von externen Angriffen setzt eine organisatorische und technische Lückenlosigkeit des Sicherungssystems voraus, die in den meisten Fällen in der Praxis nicht zu gewährleisten ist.[53] Für eine umfassende Bewertung der Technik und ihrer Folgen ist deshalb auch die Verläßlichkeit von technischen Sicherungsvorkehrungen und die aus Defiziten folgenden ergänzenden personenbezogenen Sicherungsmaßnahmen zu berücksichtigen. Die aus dem Sicherungszwang resultierenden sozialen Kosten in Form von Grundrechtseinschränkungen müssen in die Bewertung einbezogen werden.

Die Arbeit des Bundesamtes sollte weiter darauf gerichtet sein, Motive für Angriffe gegen umstrittene IuK-Technik zu vermindern, und deshalb eine konsensorientierte Technikeinführung anstreben. Dies ist aber nur auf der Basis breiter Bürgerbeteiligung an Planungs- und Einführungsprozessen möglich.

Als vorrangige Aufgabe muß jedoch die *Begrenzung des Schadenspotentials* angesehen werden. Denn nur dann werden hohe Sicherungszwänge vermieden und kann auf die Einschränkung der Freiheitsgrundrechte von Bedienern und Bürgern zur organisatorischen Sicherung der Technik verzichtet werden. Für die verschiedenen Anwendungen von Informationstechnik sollte demnach das Bundesamt jeweils prüfen, welche Abhängigkeiten durch den Technikeinsatz entstehen. Im konkreten Fall sind dazu verschiedene Alternativen des Technikeinsatzes zu vergleichen und hinsichtlich der Folgen für die Gesellschaft und ihres Schadenspotentials zu bewerten. Insbesondere ist zur Schadensbegrenzung darauf zu achten, daß Substitutionsmöglichkeiten erhalten bleiben, die bei einem Technikausfall zumindest einen „Notbetrieb" gewährleisten. Eine ähnliche Wirkung wird erreicht, wenn die Diversifikation von eingesetzten IuK-Systemen garantiert ist. Durch Softwarefehler oder Manipulation sind dann immer nur einige und nicht alle Anwender betroffen.

### 7.2 Daseinsvorsorge

Die Vorkehrungen zur Schadensbegrenzung und Sicherung müssen – neben den genannten grundsätzlichen Strategien – immer für den spezifischen Anwendungsbereich und das verfolgte Schutzziel konkretisiert werden. Im folgenden sollen exemplarisch einige Anwendungsfehler der IuK-Technik mit den Problemen für die Verletzlichkeit aufgezeigt werden. Das BSI hätte jeweils die erforderlichen *Steuerungsmaßnahmen* zu ergreifen, um die Technikgestaltung sicherzustellen, die zur Begrenzung der Verletzlichkeit erforderlich ist.

Existenzielle Voraussetzung für das Überleben in einer hochindustrialisierten Gesellschaft ist die Bereitstellung von Nahrung, Energiedienstleistungen, Kleidung, Fortbewegungs- und Zahlungsmitteln sowie anderer Güter und Dienstleistungen zur Befriedigung der Grundbedürfnisse. Bereits heute, jedenfalls aber in Zukunft werden gerade diese sozialen Funktionen ausnahmslos mit Hilfe von IuK-Technik gesteuert und sind von ihrem Funktionieren vollständig abhängig. 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 den bereichsspezifischen Einsatz von IuK-Technik auf ein vertretbares Maß zu verringern. Hohe Schadenspotentiale können durch die Abhängigkeit von IuK-Systemen unter anderen in folgenden wichtigen gesellschaftlichen Bereichen entstehen:

- Die Anforderungen an die Zuverlässigkeit, Schnelligkeit und Pünktlichkeit aller *Verkehrssysteme* nehmen aufgrund von Mobilitätsanforderungen, Just-In-Time-Produktionskonzepten und eng geplanten Vertriebsstrukturen in Warenwirtschaftssystemen zu. Der Ausfall der dort zunehmend eingesetzten IuK-Systeme kann sehr große volkswirtschaftliche Schäden zur Folge haben und die Versorgung der Bevölkerung beeinträchtigen.
- Der Einsatz von Informationstechnik in der *Prozeßsteuerung* kann durch Automatisierung einerseits Risiken vermindern. Gleichzeitig kann durch engere Kopplung oder größere Produktionsanlagen das Schadenspotential vergrößert werden.[54]
- Manipulationen oder Ausfälle von elektronischen *Zahlungssystemen* können zu großen volkswirtschaftlichen Schäden führen, einzelne Menschen oder Unternehmen ruinieren und zu Versorgungsengpässen führen.[55]
- Die Gesellschaft ist auf eine stetige, wirksame und kalkulierbare *Verwaltung* existentiell angewiesen. Ihr Ausfall durch das Versagen von Informationstechnik kann leicht zu großen Schäden für gesellschaftliche Gruppen führen.[56]

Eine weitere Ursache für das Entstehen großer Schäden können Wechselwirkungen zwischen verschiedenen Anwendungsbereichen oder die gemeinsame Nutzung von *Basistechniken* oder *IuK-Infrastrukturen* sein. Eine solche enge Kopplung, wie sie beispielsweise durch die fast ausschließliche Verwendung eines Telekommunikationsnetzes[57] entstehen könnte, muß durch entsprechende bereichsübergreifende Planungen vermieden werden. Das künftige Bundesamt könnte in diesem Sinne die Abhängigkeiten, die weder vom Netzbetreiber noch von den Nutzern erkannt werden, analysieren und für eine ausreichende Diversifikation Sorge tragen.

### 7.3 Bürgersicherheit

Ein Bundesamt darf nicht nur die Sicherheitsinteressen großer Institutionen oder der staatlichen Behörden verfolgen oder die Gewährleistung der inneren und äußeren Sicherheit des Staates in den Vordergrund stellen. Damit würde die Bewältigung der Risiken, die für jeden einzelnen Bürger aus der allgegenwärtigen Anwendung der Informationstechnik erwachsen, diesem selbst überlassen. Er müßte der Durchsetzungsmacht „der Großen" erliegen, wenn nicht auch seine Ziele institutionalisiert gegenüber Exekutive und Wirtschaft

vertreten würden. Die Gewährleistung von IT-Sicherheit muß daher vor allem darauf zielen, die Freiheitsgrundrechte der Bürger zu sichern.[58] Der Gesetzentwurf sieht in diesem Sinne jedoch nur die widersprüchliche Unterstützung sowohl des Datenschutzbeauftragten als auch der Sicherheitsbehörden vor.[59]

Für den Bürger bestehen drei zentrale Schutzziele:[60] Er soll zum ersten als Nutzer der Informationstechnik für seine Bedürfnisse keine Risiken in Kauf nehmen müssen. Zum zweiten ist eine gegen seine Interessen gerichtete Nutzung der Technik oder seiner Daten durch staatliche oder private Organisationen zu verhindern. Drittens sind seine Rechte auf informationelle[61] und kommunikative Selbstbestimmung[62] sowie sein Fernmeldegeheimnis gegen das steigende Ausforschungsinteresse staatlicher Sicherheitsbehörden zu schützen:

Das Vorhaben, Softwareprodukte hinsichtlich ihrer Sicherheit und Verfügbarkeit zu bewerten und die Prüfergebnisse durch Zertifikate bekanntzumachen, kann die Markttransparenz im Sinne des *Konsumentenschutzes* verbessern. Nachhaltig verbessert würde der Verbraucherschutz allerdings erst, wenn etwa strenge Haftungsregelungen an die zertifizierten Eigenschaften geknüpft würden.

Durch die immer größeren Sammlungen personenbezogener Daten und die verbesserten Möglichkeiten der Übermittlung und Auswertung wird es immer dringlicher, den *Betroffenen* vor IuK-Anwendungen zu *schützen*. Die Transparenz des Kundenverhaltens wird durch die „Informatisierung der Kundenschnittstelle" z.B. bei elektronischen Bestellungen, Kreditanträgen oder der Kundenidentifizierung beim elektronischen Zahlungsverkehr stetig weiter erhöht. Marketingstrategen versuchen mit den gewonnenen Profilen, das Verbraucherverhalten zu beeinflussen.[63] Über die im Gesetz vorgesehene technische Unterstützung des Datenschutzbeauftragten hinaus müßte gerade das BSI die Entwicklung technischer Komponenten vorantreiben und sicherstellen, die – wie auf dem Wochenmarkt – anonyme Teletransaktionen ermöglichen.

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

Der Gesetzentwurf betont jedoch einseitig die Sicherung der Datenverarbeitung bei staatlichen Stellen und die Verfolgung und Verhütung von ‚Computerdelikten'. Der mögliche Mißbrauch von IuK-Systemen durch staatliche Stellen oder Machtverschiebungen zwischen Bürger und Staat durch Technik-Nutzung werden nicht zum Bedrohungspotential gerechnet, gegen das Vorkehrungen zu treffen sind. 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.[64] Bürgersicherheit kann in der Informationsgesellschaft jedoch nur gewährleistet werden, wenn der Bürger selbst in ausreichendem Maße seine Anonymität wahren und für ihn wichtige Nachrichten vor dem Zugriff Dritter verbergen kann.[65] Prototypische Entwicklungen zeigen, daß dies mit Verschlüsselungssystemen gelingen kann. Voraussetzung für eine solche Verbesserung des Grundrechtsschutzes mit Hilfe der Informationstechnik ist ein Verschlüsselungsverfahren, das für jedermann verfügbar und für das jeder die benötigten Schlüssel für seine gewünschten Kommunikationspartner erhalten kann. Public-Key-Systeme erfüllen diese Bedingungen, denn die beiden Schlüssel zum Ver- und Entschlüsseln sind verschieden und ohne Zusatzwissen praktisch nicht gegenseitig ableitbar. Ein Schlüssel des Paares wird dem Teilnehmer „privat" und geheim in einer Chipkarte zur Verfügung gestellt, während der andere in einem Directory, dem „Schlüssel-Telefonbuch", veröffentlicht wird.

Ein Public-Key-System soll im *TeleTrusT*-Konzept der GMD[66] Anonymität bei Erhalt der Rechtssicherheit garantieren: Klartexte können mit einer unfälschbaren elektronischen Unterschrift versehen und dadurch „rechtssicher" werden. Die gleiche Verschlüsselungsfunktion kann aber auch ganze Nachrichten vor unerwünschten Einsichtnahmen schützen. Die Anonymität von Teletransaktionen kann dadurch gewährleistet werden, daß Bürger mit Hilfe der Chip-Karte unter Pseudonymen handeln können.

Sowohl an das Verschlüsselungsverfahren wie an das Schlüsselmanagement sind allerdings hohe Anforderungen zu stellen. Denn die umfassende Nutzung in der Gesellschaft läßt eine hohe Abhängigkeit des Zahlungssystems und Geschäftsverkehrs von dem verwendeten Public-Key-System und sensiblen Transaktionen entstehen. Lücken im Sicherungssystem können dann zu hohen materiellen wie immateriellen Schäden für einzelne Bürger oder die gesamte Gesellschaft führen. Das Verschlüsselungsverfahren muß deshalb ausreichend sicher sein, sonst können Teletransaktionen nur noch unter einem hohen Manipulationsrisiko ausgeführt werden. Genauso müssen die geheimen Schlüssel wirklich geheim gehalten werden, sonst können Nachrichten manipuliert, Identitäten vorgetäuscht oder verschlüsselte Nachrichten in den Klartext übersetzt werden.[67]

Zu den Aufgaben der Behörden der inneren Sicherheit und der Nachrichtendienste gehört auch die Überwachung von Kommunikationsbeziehungen und -inhalten und damit das Brechen gegnerischer Codes. Sie bemühen sich daher, die technische Entwicklung von Verschlüsselungsverfahren zu beeinflussen, Verschlüsselung für den allgemeinen Gebrauch zu verhindern, dessen Normung zu hintertreiben oder sich jedenfalls den Erfolg von Brechungsbemühungen durch eine Begrenzung der Schlüssellänge zu sichern.[68] Solche Strategien verfolgte in der Vergangenheit zum Beispiel die National Security Agency (NSA) der USA. Sie erreichte, daß die Schlüssellänge des DES-Algorithmus auf 56 statt auf 128 Bit begrenzt und die vollständige Veröffentlichung der Implementierung verboten wurde.[69] Dadurch erhielt sie sich die Möglichkeit, verschlüsselte Nachrichten mit vertretbarem Aufwand zu entziffern.[70] Die NSA soll sogar ihr bekannt gewordene Fehler in dem Kryptosystem verschwiegen und sich dadurch eine Geheimtür zur Entschlüsselung im Verfahren offengehalten haben.[71] Sie wäre dann in der Lage gewesen, mühelos jede Nachricht trotz Verschlüsselung mitzuhören.[72]

Durch das geplante Gesetz werden Strukturen für die künftige ‚Informationsgesellschaft' geschaffen. Dem BSI wird nach § 3 Nr. 4 die Aufgabe übertragen, für den staatlichen Geheimschutzbereich Verschlüsselungssysteme zuzulassen

und Schlüsseldaten herzustellen. Da es zugleich für die Sicherheit in der ‚zivilen' Informationstechnik zuständig ist, könnte daran gedacht werden, wenn das BSI bereits die Schlüsseldaten für den Geheimschutzbereich herstellt, ihm diese Aufgabe auch für ein ‚ziviles' Public-Key-Verfahren zu übertragen. Jedenfalls würde die Konzentration von kryptographischer Kompetenz, die sicherheitstechnische Aufgabenstellung und das schlichte Vorhandensein einer bereits bestehenden Sicherheitsbürokratie eine solche Aufgabenerweiterung des BSI nahelegen. Sie wäre trotz der offensichtlichen Risiken, die aus der organisatorischen Nähe des BSI zu den Sicherheitsbehörden erwachsen, vermutlich nur schwer abzuwehren. Wegen der Pflicht, das Bundeskriminalamt, die Bundesanwaltschaft, den Bundesgrenzschutz, das Bundesamt für Verfassungsschutz und den Militärischen Abschirmdienst zu unterstützen, wegen der Fachaufsicht des Bundesministers des Innern und der personellen Kontinuität von BND-Mitarbeitern[73] steht sogar zu befürchten, daß das BSI eine ähnliche Rolle spielen wird wie die NSA in den USA.[74]

Allerdings könnte das BSI in einem zukunftsorientierten und an der Bürgersicherheit ausgerichteten Handlungskonzept sehr wohl wichtige Aufgaben während der Entwicklung und dem Einsatz des Public-Key-Systems übernehmen: Es könnte die Normung fördern, Fachkompetenz für die öffentliche Diskussion der Vertrauenswürdigkeit des Verfahrens bereitstellen und die verwendeten Systeme validieren. Hierfür müßte es allerdings völlig unabhängig gegenüber Ausforschungsinteressen jeder Art sein. Um die informationelle Gewaltenteilung zu verstärken und um Mißbrauchsrisiken zu vermindern, wäre das Schlüsselmanagement allerdings auch bei einem neutralen Bundesamt besser unabhängig organisiert.

## 8 Ein Bundesamt für die Verringerung der Verletzlichkeit der Gesellschaft

Das Bundesamt für Sicherheit in der Informationstechnik könnte für die Verringerung der Verletzlichkeit und für die Verbesserung der Bürgersicherheit eine zentrale Rolle übernehmen, wenn es beitragen würde, die IuK-Technik in Staat und Gesellschaft nach diesen Kriterien zu gestalten. Es könnte helfen, drei wesentliche Voraussetzungen für eine gesellschaftliche Technikgestaltung zu verbessern:

- Trotz der schnellen Entwicklung der Technik und ihrer Multifunktionalität müssen auch komplexe Risiken möglichst frühzeitig erkannt werden (Sicherung der Erkenntnisfähigkeit).
- Das erworbene Risikowissen ist in institutionalisierter Weise an die Öffentlichkeit und an Entscheidungsträger zu vermitteln. Um festgestellten Risiken oder erkannten Fehlern begegnen zu können, muß versucht werden, Sachzwänge zu vermeiden und technische Alternativen offenzuhalten (Sicherung der Lernfähigkeit).
- Steuerungskriterien und ausreichende Steuerungsinstrumente müssen die Gesellschaft in die Lage versetzen, Gestaltungsziele auch gegen widerstreitende Partikularinteressen durchzusetzen (Sicherung der Steuerungsfähigkeit).

Um diese Ziele zu erreichen, sind die vorgesehenen Aufgaben und Befugnisse des BSI zu erweitern[75]:

### 8.1 Sicherung der Erkenntnisfähigkeit

Um überhaupt die Entwicklung der Verletzlichkeit der Gesellschaft beurteilen zu können, benötigt das BSI ausreichende Informationen über die entwickelten und eingesetzten Systeme. Daher sollte vorgesehen werden, daß jeder Anbieter und jeder Anwender von IuK-Systemen mit einem bestimmten Schadenspotential diese dem BSI anzeigt. Außerdem sollte eine Pflicht eingeführt werden, Schadensfälle dem BSI zu melden, um sie dort statistisch auszuwerten. Um die Technikentwicklung überhaupt beeinflussen zu können sollte das BSI Studien zu Alternativentwicklungen vergeben, in denen Verletzlichkeitsaspekte und die von ihnen ausgehenden sozialen, rechtlichen und wirtschaftlichen Folgen abzuschätzen und gegenüberzustellen wären. Darüber hinaus sollte das BSI Modellvorhaben anstoßen und soziale Experimente unterstützen, die Alternativen zur Trendentwicklung in die ‚Informationsgesellschaft' darstellen. Ziel muß es sein, individuelle und soziale Freiräume zu schaffen und vielfältige Alternativen anzubieten.

### 8.2 Sicherung der Lernfähigkeit

Um in der Öffentlichkeit Problembewußtsein zu schaffen, die Beurteilungskompetenz zu stärken und Gestaltungswissen zu vermitteln, sollte das BSI verpflichtet werden, in einem jährlichen Bericht die Entwicklung der Verletzlichkeit der Gesellschaft zu bewerten. Darin wären die Abhängigkeit von IuK-Systemen zu beschreiben und allen involvierten gesellschaftlichen und staatlichen Instanzen Vorschläge zu unterbreiten, wie sie durch Technikgestaltung die Verletzlichkeit reduzieren können. Alle Ergebnisse der vom BSI initiierten Studien müssen breit veröffentlicht werden.

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.

Um bürokratische Formen der Techniksteuerng soweit wie möglich zu vermeiden, muß eine Hauptaufgabe des BSI 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. 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. Dazu müssen Kriteriensysteme spezifiziert werden, die über die IT-Sicherheitskriterien des ZSI hinausgehen und gesellschaftliche Schadenspotentiale einbeziehen. Darüber hinaus sollte das BSI 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.

### 8.3 Sicherung der Steuerungsfähigkeit

Verletzlichkeitsaspekte müssen schwerpunktmäßig bereits in der Planungs- und Entscheidungsphase von IuK-Systemen berücksichtigt werden. Nur wenn Technikkontrolle prä-

ventiv erfolgt, läßt sich sicherstellen, daß die Anforderungen zur Schadensbegrenzung sowie zur Fehler- und Mißbrauchsverhinderung bereits die Wahl technischer Gestaltungsoptionen beeinflussen und in der Systemauslegung gewährleistet werden. Daher sind für Systeme mit besonders großem Schadenspotential – wie in anderen Technikbereichen auch – Zulassungsverfahren oder Planungsverfahren mit Öffentlichkeitsbeteiligung vorzusehen.[76] In den anderen Fällen dürfte es genügen, wenn das BSI die Befugnis erhält, Auflagen für die technische oder organisatorische Gestaltung des IuK-Systems zu erlassen, wenn sich aus der Anzeige ergibt, daß die Auswirkungen auf die Verletzlichkeit der Gesellschaft in einem unvertretbaren Ausmaß vernachlässigt werden.

## Anmerkungen

1 Der Aufsatz geht in Teilen auf ein Gutachten zurück, das die Projektgruppe verfassungsverträgliche Technikgestaltung (Provet), Darmstadt, im Auftrag der Fraktion ‚Die GRÜNEN im Bundestag' erarbeitet hat – s. Bizer/Hammer/Pordesch/Roßnagel, Das neue Bundesamt für Sicherheit in der Informationstechnik. Planungen – Kritik – Vorschläge, Darmstadt Februar 1990.

2 BR-Drs. 134/90 – der Gesetzentwurf ist in der Fassung vom 22.12.1989 abgedruckt in DuD 1990

3 Alle Paragraphen ohne Gesetzesangaben sind solche des Entwurfs eines „Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)".

4 Zit. als IT-Sicherheitsrahmenkonzept. Eine vorläufige Version dieses Rahmenkonzepts vom 27.9.1989 wurde in DuD 1989, S. 291 ff. veröffentlicht.

5 Zur Geschichte siehe auch das Hintergrundpapier von Staatssekretär Hans Neusel auf der Wissenschaftspressekonferenz vom 6.2.1990.

6 Neusel (Fn 5), S. 2.

7 FR v. 29.11.1989; Referatsleiter beim BfD W. Schmidt, Hintergrundpapier auf der Wissenschaftspressekonferenz vom 6.2.1990, S. 2.

8 Neusel (Fn 5), S. 1; Kersten, 6. RDV-Forum der DAFTA, 13. Tagung der DAFTA am 16. und 17.11.89; FR v. 29.11.89; s. hierzu auch die VS-Fernmelderichtlinien.

9 Neusel (Fn 5), S. 2.

10 Vgl. Präsident der ZSI O. Leiberich, Hintergrundpapier auf der Wissenschaftspressekonferenz vom 6.2.1990, S. 1.

11 Die Aufgaben der ZSI bis zum Erlaß eines Errichtungsgesetzes ergeben sich aus Anlage 3 des Sicherheitsrahmenkonzeptes, DuD 1989, S. 297 f. Zur Zeit werden von der ZSI ca. 10 IuK-Systeme evaluiert, ein IT-Evaluationshandbuch erstellt und Vorarbeiten für ein IT-Sicherheitshandbuch geleistet (Kersten, 13. DAFTA, 1989). Ein nationaler Kriterienkatalog zur Evaluation von vertrauenswürdigen IT-Systemen ist bereits erstellt (GMBl. v. 1.6.1989).

12 BR-Drs. 134/90, S. 10; Vgl. schon IT-Sicherheitsrahmenkonzept, Pkt. 9.5.1. Die Fachaufsicht wird von einem speziellen Referat „Sicherheit in der Informationstechnik" sowie der Koordinierungs- und Beratungsstelle der Bundesregierung in der Bundesverwaltung im BMI (KBSt) ausgeübt werden, vgl. Neusel (Fn 5), S. 4.

13 Neusel (Fn 5), S. 2.

14 Beide unterstehen dem BMI, vgl. § 5 Abs. 2 Nr. 2 und Abs. 3 Nr. 2 BKAG; § 2 Abs. 1 BVerfSchG.

15 BR-Drs. 134/90, S. 2.

16 BR-Drs. 134/90, S. 3.

17 BR-Drs. 134/90, S. 15: Laut Begründung beschränkt sich diese Definition nicht auf personenbezogene Daten.

18 „Kriterien, Verfahren und Werkzeuge".

19 Das BSI kann auch andere sachverständige Stellen mit der Prüfung beauftragen. Es strebt kein Monopol für die Erteilung von Sicherheitszertifikaten an. Vielmehr steht es jedem frei, ob er das Zertifikat einer anderen Institution dem des BSI vorzieht. S. hierzu auch Neusel (Fn 5), S. 4; Leiberich (Fn 10), S. 2.

20 S. im einzelnen die Begründung, BR-Drs. 134/90, S. 21.

21 BR-Drs. 134/90, S. 22: Die Begründung nennt die KBSt (Fn 12), das Bundesamt für Verfassungsschutz, den MAD und das Bundesministerium für Wirtschaft.

22 Vgl. auch den insoweit gleichlautenden Entwurf eines BVerfSchG in: BT-Drs. 11/4306, S. 24 ff.; im wesentlichen zählen zu den Aufgaben die Beobachtung von Bestrebungen gegen die freiheitlich demokratische Grundordnung sowie die Spionageabwehr.

23 § 2 BVerfSchG; § 3 Abs. 1 E-BVerfSchG, BT-Drs. 11/4306, S. 24 ff.

24 Seine Aufgabe ist die Strafverfolgung, § 142, 120 Abs. 1 GVG.

25 Zu nennen ist noch der Bundesgrenzschutz (BGS) mit der Aufgabe der Grenzfahndung, § 2 Nr. 2, b) BGS-G.

26 §§ 142 a; 120 GVG; § 5 Abs. 2 und 3 BKAG; vgl. auch Drews/Wacke/Vogel/Martens, Gefahrenabwehr, 9. Aufl. 1986, S. 64; Riegel, Bundespolizeirecht, 1985, S. 44 f.

27 Vgl. §§ 152 a, 202 a, 263 a, 266 b, 302 a, 303 b StGB.

28 Vgl. BR-Drs. 134/90, S. 23: Dort wird als Schwerpunkt der Tätigkeit des BSI die Unterstützung der Tätigkeit der Bundesbehörden in der Bekämpfung der organisierten Kriminalität, u.a. im Rauschgiftsektor, genannt.

29 § 2 Abs. 1 Nr. 7 BKAG.

30 § 5 Abs. 1 BKAG; vgl. hierzu z.B. Hessel, BKA-Gesetz, 1970, § 2, Anm. 18, § 5, Anm. 1; Riegel (Fn 26), S. 34.

31 S. hierzu z.B. Bull, in: Alternativ-Kommentar zum Grundgesetz, Art. 87 Rdn. 92 ff.

32 S. z.B. Maunz, in: Maunz/Dürig, Kommentar zum Grundgesetz, Art. 87 Rdn. 61; Bull, in: Alternativ-Kommentar zum Grundgesetz, Art. 35 Rdn. 41; Art. 87 Rdn. 95.

33 Beispiele bei Bull (Fn 31), Art. 87 Rdn. 28: Bundeskartellamt (nach § 48 f. GWB nur allgemeine Weisungen), Bundesprüfstelle, § 10 GjS und Bundesschuldenamt.

34 BR-Drs. 134/90, S. 1; vgl. auch IT-Sicherheitsrahmenkonzept, Pkt. 1.1.

35 BR-Drs. 134/90, S. 1 f., 9 ff.; § 3 Nr. 1–4 E-BSIG; Leiberich (Fn 10), S. 2.

36 IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 3.1 und Weck, G., Datensicherung – Konzepte und Bewertung, DuD 8/1989, S. 391 f.

37 BR-Drs. 134/90, S. 2; IT-Sicherheitsrahmenkonzept, Pkt. 1.2, 3.1.

38 § 4 Abs. 4 E-BSIG; BR-Drs. 134/90, S. 29. IT-Sicherheitsrahmenkonzept, Pkt. 2.1; 9.8.1; 9.8.2; 9.8.3; Zur NATO: Pkt. 6.2; 8; 9.1; 9.7.

39 BR-Drs. 134/90, S. 2, 9 ff., 11; Neusel (Fn 5), S. 1; Leiberich (Fn 10), S. 4 f.; IT-Sicherheitsrahmenkonzept, Anlage 1.

40 BR-Drs. 134/90, S. 2, 9; IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 4.3. ff., Anlage 2.

41 IT-Sicherheitsrahmenkonzept, Pkt. 2.2; 4.3; 4.6. sowie Anlage 2; Leiberich (Fn 10), S. 2.

42 S. hierzu näher Roßnagel/Wedde/Hammer/Pordesch, Die Verletzlichkeit der Informationsgesellschaft, 2. Auflage, Opladen 1990, S. 6 ff.

43 Zu einem erweiterten Verständnis von Sicherheit vgl. auch Raubold, Sicherheit ist mehr als Schutz vor Angriffen, GMD-Spiegel, 1989, S. 16 ff.

44 Vgl. zur Notwendigkeit repressiver und präventiver Sicherungsmaßnahmen und ihrer Freiheits- und Demokratiekosten näher Roßnagel u.a. (Fn 42), S. 199 ff.; Hammer/Pordesch/Roßnagel, „Freiheit oder Sicherheit – ein Widerspruch informationstechnischer Vernetzung?", in: Valk, R. (Hrsg.), Vernetzte und komplexe Informatiksysteme, 18. GI-Jahrestagung Hamburg 1988, Heidelberg 1988, S. 506 ff. Hier ergeben sich auch Parallelen zur Atomtechnik. Vgl. Roßnagel, Bedroht die Kernenergie unsere Freiheit? 2. Aufl. München 1983.

45 Vgl. IT-Sicherheitsrahmenkonzept, Pkt. 1.1.

46 Vgl. im Gegensatz hierzu die Darstellung des Schadenspotentials in Roßnagel u.a. (Fn 42), S. 69 ff.

47 IT-Sicherheitsrahmenkonzept, Pkt. 4.

48 Vgl. für die Sicherung der IuK-Technik Roßnagel u.a. (Fn 42), S. 182 ff. Zur Zuverlässigkeit von derartigen Sicherungsmaßnahmen vgl. etwa für den Bereich der Nutzung der Atomenergie, Roßnagel (Fn 44), S. 224 ff.

49 Vgl. hierzu z.B. Roßnagel u.a. (Fn 42), S. 175 ff.; Hammer/Pordesch/Roßnagel (Fn 43), S. 506 ff.; Roßnagel/Wedde/Hammer/Pordesch, Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, 1990, S. 171 ff., 198 ff.

50 Vgl. z.B. Zukunftskonzept Informationstechnik, 1989.
51 Vgl. hierzu näher Roßnagel u.a. (Fn 42), S. 199 ff.
52 Vgl. zum folgenden ausführlicher Bizer/Hammer/Pordesch/Roßnagel (Fn 1), S. 21 ff.
53 Vgl. hierzu näher Roßnagel u.a. (Fn 42), S. 182 ff.
54 Vgl. hierzu z.B. Roßnagel u.a. (Fn 42), S. 81 f.
55 Vgl. hierzu z.B. Harmsen/Weiß, Aspekte der Datensicherheit und der Verletzlichkeit der Informationssysteme im Bankensektor, 1989; Roßnagel u.a. (Fn 42), S. 92 ff.
56 Vgl. hierzu z.B. Roßnagel u.a. (Fn 42), S. 98 ff.
57 Vgl. zum folgenden näher Pordesch, Katastrophenpotential der Telekommunikation, Zivilverteidigung II/1989, S. 41 ff. sowie Roßnagel/Pordesch, Informationstechnische Vernetzung und Verteidigungsunfähigkeit, Sicherheit und Frieden 4/1989, S. 220 ff.
58 Vgl. hierzu z.B. Roßnagel u.a. (Fn 49), S. 118 ff.
59 S. hierzu bereits oben 3.
60 Im Gesetzentwurf ist von diesen allein der Datenschutz berücksichtigt.
61 S. BVerfGE 65, 1 (42 ff.).
62 S. hierzu Roßnagel, Das Recht auf (tele-)kommunikative Selbstbestimmung, Kritische Justiz 2/1990.
63 Vgl. zum folgenden ausführlicher Roßnagel u.a. (Fn 49), S. 219 ff., 240 ff.
64 Vgl. hierzu z.B. Roßnagel u.a. (Fn 49), S. 118 ff.
65 Vgl. hierzu Pfitzmann/Pfitzmann/Waidner, Datenschutz garantierende offene Kommunikationsnetze, Informatik-Spektrum 1988, S. 118 ff.
66 Zur Beschreibung des Verfahrens s. z.B. verschiedene Autoren in GMD-Spiegel 1/86 und 1/88 sowie Hammer, TeleTrusT: Verletzlichkeit und Verfassungsverträglichkeit eines Konzeptes für rechtssichere Transaktionen in der Informationsgesellschaft, DuD 8/1988, S. 391 ff.
67 Zu Aspekten der Verletzlichkeit s. Hammer (Fn 66), S. 398 ff.
68 Vgl. beispielsweise Fölsing, Die hohe Schule der Kryptologie, Kursbuch 66 (1981), S. 105; Waidner/Pfitzmann/Pfitzmann, Über die Notwendigkeit genormter kryptographischer Verfahren, DuD 6/1987, S. 294.
69 Vgl. Coy, Geheime Schriften, geheime Dienste, Kursbuch 66 (1981), S. 89.
70 Vgl. Coy (Fn 69), S. 88 f. und dort auch Fn. 8.
71 Fölsing (Fn 68), S. 103.
72 Waidner/Pfitzmann/Pfitzmann (Fn 68), S. 298: Ein solches System wäre dann die offizielle Installation eines ‚großen Bruders'." S. hierzu auch näher Bizer/Hammer/Pordesch/Roßnagel (Fn 1), S. 17 ff.
73 Auch wenn die Entzifferung nicht mehr explizite Aufgabe des Bundesamtes sein wird, muß eine starke Orientierung an den Sicherheitsinteressen erwartet werden – s. hierzu z.B. die Stellungnahmen von Neusel (Fn 7), S. 3 und Leiberich (Fn 10), S. 3; s. zu ähnlichen Bedenken des Bundesbeauftragten für den Datenschutz Schmidt (Fn 7), S. 2.
74 Allerdings hat der designierte Präsident des BSI Leiberich in der Expertenanhörung vor dem Forschungsausschuß des Deutschen Bundestags am 7.3.1990 erklärt, das BSI werde sich nicht gegen Verschlüsselungsdienste im Rahmen des ISDN wenden.
75 S. hierzu näher Bizer/Hammer/Pordesch/Roßnagel (Fn 1), S. 45 ff.
76 S. hierzu näher Bizer/Hammer/Pordesch/Roßnagel (Fn 1), S. 49 ff.

# Datenschutz in der Schweizerischen Sozialversicherung

*Ulrich Meyer*

**Abstrakt:** *Zwischen Datenschutz- und Sozialversicherungsrecht gibt es Zielkonformitäten und -inkonformitäten. Das Datenschutzrecht ist neu und weniger positivrechtlich verankert. Nicht besonders klar und nicht einheitlich regelt das Sozialversicherungsrecht das Beschaffen der Daten bei Ärzten. Die von den Sozialversicherern geführten Dossiers über Versicherte gelten nicht als Datensammlungen sondern als Bearbeitungsformen im Sinne des Botschaftsentwurfs DSG. Gewisse Sozialversicherer führen Versicherten-Konten. Es werden Identifikationszahlen verwendet und Statistiken geführt. Versicherte und ausnahmsweise auch nicht beteiligte Dritte haben ein beschränktes Akteneinsichtsrecht. Ansonsten besteht ein Geheimhaltungsgrundsatz bzw. eine Schweigepflicht. In definierten Ausnahmefällen können die Daten weitergegeben werden. Es besteht eine Auskunftspflicht gegenüber einschlägig befaßten Bundesorganen. Nach dem Botschaftsentwurf DSG können Bundesorgane Name, Vorname, Adresse und Geburtstag einer Person auf Anfrage bekanntgeben. Betroffene können eine Sperrung bestimmter Personendaten verlangen, die von den Bundesorganen bedingt aufgehoben werden kann. Die einzelnen Träger der Sozialversicherungszweige leisten einander im Einzelfall auf Ersuchen Verwaltungshilfe.*

## Einleitende Bemerkungen

1. Sozialversicherungsrecht ist jener Bereich der Rechtsordnung, welcher bestimmt ist, die ganze Bevölkerung oder einzelne ihrer Schichten durch öffentlichrechtlich ausgestaltete und der Sozialversicherungsgerichtsbarkeit unterliegende Versicherungsverhältnisse gegen soziale Risiken zu sichern[1].

Datenschutzrecht soll Leitplanken für die Datenbearbeitung setzen, die garantieren, daß die Entfaltung der Persönlichkeit nicht durch unnötige und unerwünschte Informationstätigkeiten beeinträchtigt wird. Die Privatsphäre einer Person soll namentlich von Informationsbedürfnissen staatlicher Stellen abgeschirmt werden, sofern nicht ein überwiegendes Interesse an einer solchen Informationsbeschaffung besteht. Ein Datenschutzgesetz muß ferner verhindern, daß der Einzelne zu einem rechtlosen Objekt von Informationstätigkeiten wird. Er soll vielmehr Bild und Kenntnisse, die die Umwelt von ihm hat, mitbestimmen können[2].