Johann Bizer/Alexander Roßnagel
Sicherheit in der Informationstechnik – Aufgabe für ein neues Bundesamt

1. Die Verletzlichkeit der »Informationsgesellschaft«

Seit dem 1. Januar 1991 gibt es das Bundesamt für die Sicherheit in der Informationstechnik (BSI). Das Amt soll mit 270 Mitarbeitern die Sicherheit in der Informationstechnik erhöhen. »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.«[1]

Knapp, aber zutreffend beschreibt die Bundesregierung mit diesen Worten die steigende »Verletzlichkeit der modernen Informationsgesellschaft«[2] und damit das Problem, für das das neue Amt die Lösung sein soll. In der Tat werden Fehler der Informations- und Kommunikationstechnik, Fehlbedienungen und böswillige Mißbrauchshandlungen erheblich bedrohlicher, wenn die Abhängigkeit der Gesellschaft vom Funktionieren der automatischen Informationsverarbeitung und -übermittlung und damit das potentielle Schadenspotential gegenüber heute noch beträchtlich ansteigen werden. Dem Bild der »Informationsgesellschaft« entsprechend, das man hierzulande hoffnungs-[3] oder besorgnisvoll[4] zeichnet, werden Informationsverarbeitung und Telekommunikation in Umfang, Verbreitung und Bedeutung zunehmen, noch stärker in die Gesellschaft eindringen und zu einem vernetzten System zusammenwachsen. Dabei werden sie andere Formen der Informationssammlung, -verarbeitung und Kommunikation verdrängen und schließlich weitgehend ohne Alternative und Substitutionsmöglichkeit sein. Störungen in einem Bereich werden sich dann schnell auf andere Bereiche übertragen. Eine IuK-gestützte Warenwirtschaft wird auf der völligen Vernetzung von Lieferanten, Zulieferern, Produzenten, Händlern, Kunden und Banken beruhen. Vom Funktionieren der IuK-Systeme werden auch die Energieversorgung, die medizinische Versorgung, das gesamte Zahlungssystem, die wichtigsten Dienstleistungen, wissenschaftliche Organisationen, das Verkehrssystem, die Medien, der Umweltschutz sowie die staatliche Verwaltung und die politische Steuerung abhängig sein.[5]

1 Einleitung zur amtlichen Begründung des BSIG, BR-Drs. 134/90, S. 1 = BT-Drs. 11/7029.

2 BR-Drs. 134/90, S. 1; s. auch Bundesinnenminister Schäuble, BT-Sten.Ber. 11/16794; Staatssekretär Neusel, Aktivitäten der Bundesregierung zur IT-Sicherheit, Vortrag auf der 1. Deutschen Konferenz über Computersicherheit 15./16. Mai 1990, RDV 1990, S. 161 ff.

3 S. z. B. Bundesminister für Forschung und Technologie/Bundesminister für Wirtschaft, Zukunftskonzept Informationstechnik, Bonn 1989.

4 S. z. B. Kubicek/Rolf, Mikropolis, Hamburg 2. Aufl. 1986; Roßnagel/Wedde/Hammer/Pordesch, Digitalisierung der Grundrechte. Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen 1990.

5 S. hierzu näher das ›Zukunftsbild‹ in Roßnagel/Wedde/Hammer/Pordesch, Die Verletzlichkeit der ›Informationsgesellschaft‹, Opladen 2. Aufl. 1990, 18 ff.

Bereits in der Vergangenheit haben eine Vielzahl von Vorfällen die Verletzlichkeit der »Informationsgesellschaft« angedeutet. So fielen beispielsweise am 21. Januar 1990 in den USA alle 114 Fernvermittlungsstellen im landesweiten Telekommunikationsnetz von AT&T gleichzeitig aus. Ein identischer Softwarefehler im Routingsystem führte für neun Stunden zu einer Überlastung aller Vermittlungscomputer. Schätzungsweise 75 Millionen Telekommunikationsverbindungen konnten durch diesen Ausfall nicht vermittelt werden. Durch einen Brand in der Vermittlungszentrale der Illinois Bell Telephone Company wurden 1988 Tausende von Unternehmen und Haushalten für Wochen von jeder Telekommunikation abgeschnitten. 1987 gingen »Oldsmobil« die kompletten Designdaten eines neuen Automodells durch einen Computerfehler verloren. Bundesdeutschen Hackern gelang es im September 1987, über Fehler im Betriebssystem zweier NASA-Rechner das Space Physics Analysis Network zu erreichen und von diesem aus in 136 Computer einzudringen, die Daten sowohl aus zivilen als auch militärischen Projekten verarbeiteten. Im Herbst 1988 legte ein Computervirus, den ein Student in zwei Computernetze implantiert hatte, über 6000 Rechner lahm und zerstörte etliche tausend Dateien und Programme in der US-Bundesverwaltung.
Vorfälle dieser Art[6] gefährden den Weg in die »Informationsgesellschaft«. Um ihrer Verletzlichkeit entgegen zu wirken, hat der Bundestag am 24. Oktober 1990 das »Gesetz über die Errichtung des Bundesamts für die Sicherheit in der Informationstechnik« (BSIG) verabschiedet.[7] Im folgenden werden Geschichte des BSI (2.) und der Inhalt seines Errichtungsgesetzes (3.) kurz beschrieben, das Amt von seinen Aufgaben und Befugnissen her kritisch beleuchtet (4. und 5.) und an notwendigen und möglichen Alternativen gemessen (6.).

2. Vorgeschichte des BSI

Aufbau und Konzept des BSI stützen sich auf die in den 50er Jahren gegründete Zentralstelle für das Chiffrierwesen (ZfCH).[8] Die ZfCH war dem Bundesnachrichtendienst (BND)[9] 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 oder abgehört worden sind.[10] 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.[11]

6 S. zu ihnen und vielen anderen Roßnagel/Wedde/Hammer/Pordesch (Fn. 5), 69 ff., 106 ff., 129 ff. sowie den Bericht des Bundesrechnungshofs BT-Drs. 11/7691.
7 S. BT-Sten. Ber. 11/18247 ff.
8 Zur Geschichte siehe auch das Hintergrundpapier von Staatssekretär Hans Neusel auf der Wissenschaftspressekonferenz vom 6. 2. 1990 sowie ders. (Fn. 2), S. 164 ff.
9 FR v. 29. 11. 1989; Referatsleiter beim BfD W. Schmidt, Hintergrundpapier auf der Wissenschaftspressekonferenz vom 6. 2. 1990, S. 2.
10 Neusel (Fn. 8), 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.
11 Neusel (Fn. 8), S. 2; ders. (Fn. 2) S. 164 f., s. zur Geschichte der ZSI und ähnlichen Entwicklungen in den USA, die zu vielen Befürchtungen in der kritischen Beurteilung dieses Gesetzesvorhabens geführt haben,

Ihre politischen Handlungsabsichten in diesem Feld hat die Bundesregierung in ihrem am 23. November 1989 gebilligten »Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik (IT)« zusammengestellt.[12] Die Errichtung des neuen Bundesamts ist das »Kernstück« im Rahmen dieses Handlungskonzepts.[13] Der Gesetzentwurf ist daher im Kontext der Zielsetzungen und Handlungsvorschläge dieses Rahmenkonzepts zu beurteilen.

Mit der zunehmenden Aufgabenerweiterung im Bereich Computersicherheit wurde die ZfCH zum 1. Juni 1989 in »Zentralstelle für Sicherheit in der Informationstechnik« (ZSI) umbenannt. Sie befand sich weiterhin im Geschäftsbereich des Bundeskanzleramtes.[14] 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.[15]

Mit dem BSIG wurde nun die ZSI in eine Bundesoberbehörde umgewandelt. Sie soll allerdings nicht mehr dem Bundeskanzleramt zugeordnet sein, sondern als »zivile Behörde«[16] dem Bundesminister des Innern unterstehen (§ 1).[17] Nur der Aufgabenbereich »Entzifferung« soll beim Bundeskanzleramt und damit beim BND verbleiben.[18] 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.[19] Personelle Bezüge werden aufgrund des Mangels an qualifiziertem Personal auch zur alten ZfCH bestehen.[20] Der 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.[21]

Die parlamentarischen Beratungen verliefen ohne besondere Komplikationen. Der Bundesrat empfahl in seiner Stellungnahme im wesentlichen nur Änderungen zu den beamtenrechtlichen Regelungen. Ansonsten schlug er vor, auch Länderbehörden von dem künftigen Sicherheitswesen des BSI profitieren zu lassen.[22] Die SPD unterstützte die Errichtung des neuen Bundesamtes, kritisierte jedoch die Ressortie-

auch Bizer/Hammer/Pordesch/Roßnagel, Das neue Bundesamt für Sicherheit in der Informationstechnik. Planungen – Kritik – Vorschläge, Provet-Projektbericht 4, Darmstadt Februar 1990, 3 ff., 17 ff.

12 Zit. als IT-Sicherheitsrahmenkonzept. Eine vorläufige Version dieses Rahmenkonzepts vom 27. 9. 1989 wurde in DuD 1989, S. 291 ff. veröffentlicht.

13 S. Neusel (Fn. 2), S. 165.

14 Vgl. Präsident der ZSI O. Leibenich, Hintergrundpapier auf der Wissenschaftspressekonferenz vom 6. 2. 1990, S. 1.

15 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; Neusel (Fn. 2), S. 16 ff. Ein nationaler Kriterienkatalog zur Evaluation von vertrauenswürdigen IT-Systemen ist bereits erstellt – GMBl. v. 1. 6. 1989. Ein erster Entwurf der EG-Kommission der Information Technology Security Evaluation Criteria, der unter Leitung der ZSI in einem internationalen Arbeitskreis erarbeitet worden ist, liegt ebenfalls bereits vor – Version 01 vom 2. 5. 1990, hrsg. vom Bundesinnenministerium.

16 Neusel (Fn. 2), S. 165.

17 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. 2).

18 Neusel (Fn. 2).

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

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

21 BR-Drs. 134/90, S. 3. Inwieweit der Mangel an Kryptographen durch Übernahme ehemaliger Mitarbeiter des Zentralen Chiffrierorgans der DDR gedeckt wird, ist noch ungewiß – s. Abg. Such, BT-Sten. Ber. 11/18252.

22 BR-Drs. 134/90 (Beschluß).

rung des Bundesamts beim Bundesinnenminister, fehlende Haftungsregelungen und den rein technischen Sicherheitsbegriff des Gesetzes. Außerdem monierte sie, daß eine Technikfolgenabschätzung und -bewertung der künftigen Risikopotentiale im Aufgabenkatalog des Amtes fehle.[23] Die GRÜNEN machten darüberhinaus rechtliche Bedenken gegen die Zusammenarbeit zwischen BSI einerseits und Bundeskriminalamt, Verfassungsschutz und Geheimdiensten andererseits geltend und kritisierten die Aufgaben- und Befugniszuweisung als probleminadäquat.[24] Sie legten eine Fülle von Änderungsvorschlägen vor, die das Ziel verfolgten, dem Amt einen unabhängigen Status zu verschaffen, seine Zielsetzungen auf die Gewährleistung von Bürgersicherheit zu konzentrieren und ihm Befugnisse einzuräumen, eine Reduzierung der Verletzlichkeit der Gesellschaft auch tatsächlich zu erreichen.[25] Die Vorschläge der Opposition fanden inhaltlich ihren Niederschlag in der Stellungnahme des Ausschusses für Forschung, Technologie und Technikfolgenabschätzung, wurden aber vom federführenden Innenausschuß zurückgewiesen.[26]

In der Öffentlichkeit stieß das Gesetzesvorhaben auf wenig Interesse.[27] Die Auseinandersetzungen beschränkten sich vorwiegend auf Fachkongresse[28] und die Fachliteratur[29]. Kritische Stellungnahmen wurden vom Deutschen Gewerkschaftsbund[30], dem Forum der Informatiker und Informatikerinnen für Frieden und gesellschaftliche Verantwortung (FiFF)[31] und der Gesellschaft für Informatik (GI)[32] vorgelegt. Die Kritik wurde – in unterschiedlicher Stringenz – von der Opposition aufgegriffen und in die parlamentarischen Beratungen eingeführt. Dadurch wurde erreicht, daß die Aufgaben des BSI um die Technikfolgenabschätzung erweitert[33] und die Beratungspflichten für BKA und Verfassungsschutz präzisiert wurden.

23 S. der Abg. Paterna, BT-Sten.Ber. 11/16795 f. und 18248 ff.; die auf eine SPD-Initiative zurückgehende Stellungnahme des Ausschusses für Forschung, Technologie und Technikfolgenabschätzung des Bundestages zum Entwurf des BSIG vom 12. 9. 1990 – BT-Drs. 11/8177, 10 ff.

24 S. die Abg. Rust, BT-Sten.Ber. 11/16796 f.; Abg. Such, BT-Sten. Ber. 11/18251 f.

25 S. BT-Drs. 11/7246; 11/8177 und 11/8197.

26 S. zu beiden BT-Drs. 11/8177.

27 Eine Ausnahme bildet der Artikel von Gunhild Lütge, Alles unter Kontrolle? in der Zeit Nr. 20 vom 11. 5. 1990.

28 Z. B. die 1. Deutsche Konferenz über Computersicherheit in Bad Godesberg am 15./16. 5. 1990 oder die Tagung »Zukunftskonzept Informationstechnik« der Gesellschaft für Informatik vom 14.–17. 6. 1990.

29 Bizer/Hammer/Pordesch/Roßnagel, Ein Bundesamt für die Sicherheit in der Informationstechnik – Kritische Bemerkungen zum Gesetzentwurf der Bundesregierung, DuD 1990, 178 ff.; Bernhardt/Ruhmann, Wie ein Geheimdienst zur obersten Bundesbehörde für Computersicherheit gemacht wird, FiFF-Kommunikation 2/90, 29 ff.; Roßnagel, BSI: Kein Beitrag zur Verringerung der Verletzlichkeit, Computerwoche 12 vom 23. 3. 1990, 8; Kersten, ZSI/BSI: Eine staatliche Initiative zur IT-Sicherheit, Computerwoche 12 vom 23. 3. 1990, 40 ff.; Bernhard/Ruhmann, Mutation einer Geheimdienststelle, Computerwoche 12 vom 23. 3. 1990, 44 ff.; Schäuble, Wider Kriminalität und Akzeptanzverlust, Sieg Tech 4/90, 18 ff.; Beth, Zur Sicherheit der Informationstechnik, Informatik-Spektrum 1990, S. 204 ff.; Wortmann, Konzepte der Bundesregierung zur Sicherheit in der Informationstechnik, DuD 1990, S. 453 ff.

30 Richert, Neue »Philosophie« muß her, Sieg Tech 4/90, 21 ff.

31 FiFF-Kommunikation 1/1990, S. 8; Computerwoche vom 22. 12. 1989, S. 6.

32 Stellungnahme der Arbeitsgruppe 10 des FB 8 der GI zum Entwurf des Errichtungsgesetzes der Bundesregierung für ein Bundesamt für Sicherheit in der Informationstechnik auf der GI-Fachtagung »Informatik und Gesellschaft« vom 14. bis 17. 6. 1990.

33 S. hierzu bereits Bundesinnenminister Schäuble in der ersten Lesung im Bundestag am 31. 5. 1990, BT-Sten.Ber. 11/16794 sowie Neusel (Fn. 2), S. 164 ff. Diese Aufgabe wurde nach § 3 Abs. 1 Nr. 7 BSIG allerdings auf die Beratung der Hersteller, Vertreiber und Anwender beschränkt.

Als Errichtungsgesetz beschränkt sich das BSIG in § 1 auf die Schaffung einer neuen Bundesoberbehörde. Eine Ziel- oder Zweckbestimmung fehlt.[34] § 2 beschränkt sich auf eine Begriffsbestimmung der Informationstechnik als »alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen« und auf eine Definition der »Sicherheit in der Informationstechnik«. Unter diesem Begriff versteht der Gesetzentwurf die

»Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen oder
2. Komponenten oder bei der Anwendung dieser Systeme und Komponenten« (§ 2 Abs. 2).

Es folgt in § 3 Abs. 1 ein umfangreicher Katalog der Aufgaben des BSI, der Forschungs- und Entwicklungsaufgaben beschreibt (Nr. 1 und 2), die Erteilung von Sicherheitszertifikaten vorsieht (Nr. 3), dem BSI die Zulassung von informationstechnischen Produkten für den Geheimschutzbereich überträgt (Nr. 4) und es zur Unterstützung anderer Behörden verpflichtet (Nr. 5 bis 7). § 4 regelt das Verfahren und die Voraussetzungen der Zertifikatserteilung und § 5 enthält eine Verordnungsermächtigung für den Bundesminister des Innern. In §§ 6 bis 6c folgen schließlich beamtenrechtliche Vorschriften.

4. *Staats- und Marktsicherheit statt Bürgersicherheit*

Wer das Gesetz mit der Problembeschreibung seiner Begründung vergleicht, dem fällt vor allem auf, daß das Problem der »Verletzlichkeit der modernen Informationsgesellschaft« in der Aufgabenbeschreibung des Amtes auf die Unterstützung der deutschen IuK-Industrie und Hilfestellungen zur Gewährleistung der inneren Sicherheit reduziert wird. Befugnisse zur Verringerung der Verletzlichkeit fehlen völlig.

Vielmehr soll die deutsche *IuK-Industrie unterstützt* werden durch die Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen und Komponenten, die Prüfung und Bewertung von IuK-Produkten sowie die Erteilung von Sicherheitszertifikaten (§ 3 Abs. 1, Nr. 2–4). Die Sicherheit in der Informationstechnik soll dadurch erhöht werden, daß die Nachfrage nach »sicheren« IuK-Produkten durch den amtlichen Nachweis von Sicherheitsstandards erleichtert wird. Betreibern, Anwendern und Nutzern von Informations- und Kommunikationstechniken sollen die Zertifikate Orientierungshilfen für die Sicherheitsqualität bestimmter Produkte liefern. Allerdings ist für kein IuK-Produkt – vom PC bis zum Großrechner – der Nachweis der Sicherheit als Zulassungsvoraussetzung vorgeschrieben. Über die sozial gewünschte Sicherheit in der Informationstechnik wird allein der Markt entscheiden.

Auch strebt das BSI für die Zertifizierung keine Monopolstellung an. Vielmehr soll es jedem frei stehen, ob er das Zertifikat einer anderen Institution dem des BSI vorzieht.[35] Die Marktorientierung des Gesetzes zeigt sich auch darin, daß Prüfung

34 Alle Paragraphen ohne Gesetzesangaben sind solche des Entwurfs eines »Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnologie (BSI)«.

35 Neusel (Fn. 8), S. 4; Leibenich (Fn. 15), S. 2.

und Bewertung auch von anderen »sachverständigen Stellen«, die vom Bundesamt hierzu beauftragt werden (§ 4 Abs. 2), vorgenommen und daß Sicherheitszertifikate anderer anerkannter Prüfstellen aus dem Bereich der Europäischen Gemeinschaft bei gleichwertiger Sicherheit anerkannt werden können (§ 4 Abs. 4).

Durch eigene Sicherheitsstandards und die Erteilung von Sicherheitszertifikaten soll insbesondere gegenüber dem US-Markt, der eine eigene behördliche Zertifizierung kennt, die Exportfähigkeit der bundesdeutschen Industrie gesichert werden.[36] Um eine internationale Anerkennung der deutschen Zertifikate zu erreichen, wird eine Abstimmung mit europäischen bzw. internationalen Kriterien zur Bewertung, Prüfung und Zertifizierung von IT-Systemen und Komponenten angestrebt, die auch mit der NATO abgestimmt werden sollen.[37] Die ausschließliche Orientierung auf den nationalen und internationalen Markt verengt die ursprüngliche Zielsetzung des Gesetzes, die »Verletzlichkeit der modernen Informationsgesellschaft« zu verringern, auf die Sicherung der internationalen Wettbewerbsfähigkeit.

Für den *Bereich der Inneren Sicherheit* soll das Bundesamt aus dem Dunkel seiner Vorgänger, den Geheimdiensten, heraustreten und als technische Fachbehörde die staatlichen Stellen, »insbesondere soweit sie Beratungs- und Kontrollaufgaben wahrnehmen« (§ 3 Abs. 1 Nr. 5), unterstützen. Ausdrücklich nennt der Gesetzentwurf den Bundesbeauftragten für den Datenschutz, »dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht«. Erst aus der Begründung ist zu entnehmen, daß hierzu auch die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesinnenministerium (KBSt) sowie vor allem das Bundesamt für Verfassungsschutz und der Militärische Abschirmdienst sowie das Bundesministerium für Wirtschaft, soweit es Unternehmen mit Verschlußsachen-Aufträgen des Bundes betreut, gezählt werden.[38]

Neben dem Geheimschutz erstreckt sich der Aufgabenbereich des BSI aber auch auf die Unterstützung »der Polizei und der Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben« sowie der Verfassungsschutzbehörden bei ihrer Tätigkeit.[39] Das BSI soll seine Fachkenntnisse aus der Sicherung der Informations- und Kommunikationsdienste zur Analyse, Bewertung und Beweisführung von »allgemein kriminell(en), extremistisch(en) oder nachrichtendienstlich motivierte(n) Einbrüche(n) in informationstechnische Systeme« den genannten Sicherheitsbehörden zur Verfügung stellen[40] und wird damit unmittelbar im Zusammenhang mit Grundrechtseingriffen tätig. Um die Kontrolle des BSI zu erleichtern, hat es die Unterstützungsersuchen aktenkundig zu machen.

Auf die rechtliche Fragwürdigkeit dieser Regelungen ist schon an anderer Stelle hingewiesen worden.[41] Hervorzuheben ist hier die Konsequenz dieser Verquickung widerstreitender Interessen. Das BSI kann nicht, wenn es seine Zielvorgabe adäquat erfüllen will, Diener zweier Herren sein. Nach dem BSIG soll es auf der einen Seite

36 BR-Drs. 134/90, S. 2; IT-Sicherheitsrahmenkonzept, Pkt. 1.2; 3.1; nach § 3 Abs. 2 bedürfen die Entscheidungen des BSI über Kriterien und Verfahren der Zertifikatserteilung des Einvernehmens mit dem Bundesminister für Wirtschaft.

37 § 4 Abs. 4; 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. Zum Verfahren der Zertifikatserteilung s. ZSI, IT-Evaluationshandbuch, Bonn 1990, S. 68 ff.

38 BR-Drs. 134/90, S. 22.

39 Entgegen dem Wortlaut der Vorschrift führt die Begründung – BR-Drs. 134/90, S. 23 – auch den Militärischen Abschirmdienst an.

40 BR-Drs. 134/90, S. 23.

41 Bizer/Hammer/Pordesch/Roßnagel (Fn. 29), DuD 1990, S. 179.

den Bundesbeauftragten für den Datenschutz unterstützen (§ 3 Abs. 1 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 Abs. 1 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.

Ebenfalls in den Bereich der inneren Sicherheit fallen die Unterstützungsaufgaben für die staatliche Geheimhaltung, die das BSI von seinen Vorgängern ZfCH und ZSI übernimmt. Zum einen soll das BSI die informationstechnischen Systeme oder Komponenten zulassen, die im Bereich des Bundes für die Verarbeitung oder Übertragung von Verschlußsachen eingesetzt werden, und zum anderen die für den Betrieb zugelassener Verschlüsselungsgeräte benötigten Schlüsseldaten herstellen (§ 3 Abs. 1, Nr. 4).[42]

Auch der zweite Schwerpunkt des Gesetzes, die Unterstützung der Staatssicherheit, wird jedoch dem selbstgesteckten Zweck, die »Verletzlichkeit der modernen Informationsgesellschaft« zu reduzieren, nicht gerecht. Denn ein Bundesamt darf nicht nur die Sicherheitsinteressen großer Institutionen oder der staatlichen Behörden verfolgen oder die Gewährleistung der inneren 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.[43] Der Gesetzentwurf sieht in diesem Sinne jedoch nur die widersprüchliche Unterstützung sowohl des Datenschutzbeauftragten als auch der Sicherheitsbehörden vor.

Für den Bürger bestehen drei zentrale Schutzziele:[44] 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[45] und kommunikative Selbstbestimmung[46] 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 die *Verbrauchersicherheit* allerdings erst, wenn strenge Haftungsregelungen an die zertifizierten Eigenschaften geknüpft würden.[47]

Durch die immer größeren Sammlungen personenbezogener Daten und die verbesserten Möglichkeiten der Übermittlung und Auswertung wird es immer dringlicher,

42 Siehe im einzelnen die Begründung, BR-Drs. 134/90, S. 21.
43 Vgl. hierzu z. B. Roßnagel u. a. (Fn. 4), S. 118 ff.
44 Im Gesetzentwurf ist von diesen allein der Datenschutz berücksichtigt.
45 S. BVerfGE 65, 1 (42 ff.).
46 S. hierzu Roßnagel, Das Recht auf (tele)kommunikative Selbstbestimmung, Kritische Justiz 3/1990.
47 S. hierzu näher Bizer/Hammer/Pordesch/Roßnagel (Fn. 12), S. 26 ff.

die *Sicherheit der Betroffenen* vor ungewünschten Informationstechnik-Anwendungen zu gewährleisten. Beispielsweise wird die Transparenz des Kundenverhaltens durch die »Informatisierung der Kundenschnittstelle« etwa bei elektronischen Bestellungen, Kreditanträgen oder der Kundenidentifizierung beim elektronischen Zahlungsverkehr stetig erhöht. Marketingstrategen versuchen mit den gewonnenen Profilen, das Verbraucherverhalten zu beeinflussen. 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.
Bürgersicherheit kann in der Informationsgesellschaft nur gewährleistet werden, wenn der Bürger selbst in ausreichendem Maße seine Anonymität wahren und für ihn wichtige Nachrichten vor dem Zugriff Dritter verbergen kann.[48] 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 ist 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.[49] Allerdings müssen die geheimen Schlüssel wirklich geheim gehalten werden, sonst können Nachrichten manipuliert, Identitäten vorgetäuscht oder verschlüsselte Nachrichten in den Klartext übersetzt werden.[50]

5. Betriebssicherheit statt Verletzlichkeit

Aber nicht nur in der Beschränkung der Schutzobjekte verdient das Gesetz Kritik, sondern auch in der Begrenzung des Handlungsziels auf die Betriebssicherheit informationstechnischer Systeme.[51] Die technische Sicherung von IuK-Systemen ist zwar ein wichtiger, aber keineswegs ausreichender Beitrag.[52] Indem das Gesetz die Aufmerksamkeit allein auf die technische Verringerung der Wahrscheinlichkeit von Schadenseintritten lenkt, berücksichtigt es nur die eine Hälfte des Problems der Verletzlichkeit der Informationsgesellschaft. Um sie zu verringern, sind darüberhinaus jedoch die Schadenspotentiale, die durch die Abhängigkeit von der Informationstechnik für die Gesellschaft und den einzelnen Bürger geschaffen werden, die konkreten Anwendungsbedingungen und die durch sie verursachten sozialen Folgen zu berücksichtigen. Zwar wurde auf entsprechende Kritik hin die Beratungspflicht des § 3 Abs. 1, Nr. 7 um eine begrenzte Folgenabschätzung ergänzt. Doch kann eine Einzelfallberatung auf Anforderung, die neben der Betriebssicherheit

48 Vgl. hierzu Pfitzmann/Pfitzmann/Waidner, Datenschutz garantierende offene Kommunikationsnetze, InformatikSpektrum 1988, S. 118 ff.
49 Zur Beschreibung beispielsweise des TeletrustKonzeptes der GMD vgl. die 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.
50 Zu Aspekten der Verletzlichkeit s. Hammer (Fn. 49), S. 398 ff.
51 BR-Drs. 134/90, S. 1 f., 9 ff.; § 3 Nr. 14 BSIG; Leiberich (Fn. 15), S. 2.
52 Vgl. zum folgenden ausführlicher Bizer/Hammer/Pordesch/Roßnagel (Fn. 12), S. 21 ff.

auch »mögliche Folgen fehlender oder unzureichender Sicherheitsvorkehrungen« berücksichtigt, die erforderliche Verletzlichkeitsanalyse nicht ersetzen.

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.[53]

Existentielle Voraussetzung für das Überleben in einer hochindustrialisierten Gesellschaft ist die Bereitstellung von Nahrung, Energiedienstleistungen, Kleidung, Fortbewegungs- und Zahlungsmitteln sowie anderen Gütern 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. Hohe Schadenspotentiale können durch die Abhängigkeit von IuK-Systemen vor allem zu erwarten sein in den gesellschaftlichen Bereichen des Verkehrswesens, der Steuerung komplexer industrieller Prozesse, des Zahlungsverkehrs und der staatlichen und privaten Verwaltung.

Um diese Risiken zu verringern, genügt es nicht, lediglich entwicklungsbegleitend einheitliche Sicherheitsstandards herzustellen, informationstechnische Sicherheitskomponenten und -systeme zu erforschen und zu entwickeln sowie die Anwender und Hersteller von informationstechnischen Produkten zu beraten, die informationstechnische Entwicklung aber als unbeeinflußbar hinzunehmen. Vielmehr ist es erforderlich, die Schadenspotentiale, die durch die steigende Abhängigkeit von der Informationstechnik anwachsen, in den Blick zu bekommen und gestaltend zu beeinflussen. Notwendig ist, die Schadenspotentiale zu verringern, indem die Abhängigkeit der Gesellschaft von der IuK-Technik reduziert wird.

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 Informationstechnik-Nutzung und -Sicherung im betrieblichen und gesellschaftlichen Kontext hervorgerufen werden. 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.

Eine Gesellschaft, die – um mögliche Katastrophen auszuschließen – darauf ange-

53 S. zum Begriff der Verletzlichkeit näher Roßnagel u. a. (Fn. 5), S. 5 ff. sowie zur Verletzlichkeit der im folgenden angesprochenen einzelnen Anwendungsbereiche 81 ff., 92 ff., 98 ff. und 199 ff.

wiesen ist, Sicherheit gegenüber menschlicher Böswilligkeit zu gewährleisten, ist auf präventive gesellschaftliche Kontrolle angewiesen. Will sie im Interesse von Freiheit und Demokratie diesen *Sicherungszwang* vermeiden, muß sie ihre Abhängigkeit von Technik-Systemen und damit deren Schadenspotential reduzieren.[54] Der Gesetzentwurf läßt jedoch in seiner Technikfixierung auch die negativen sozialen Folgen unberücksichtigt, die der Sicherungszwang verursacht. Statt ihn zu verringern, strebt er an, ihn bestmöglich zu erfüllen.

6. *Vertane Chancen*

Das BSIG ist lediglich ein Organisationsgesetz. Geregelt werden Errichtung, Aufgaben und Befugnisse einer neuen Bundesoberbehörde. Zugleich aber ist dieses Gesetz der erste Schritt zu einer rechtlichen Regulierung der Informationstechnik.[55] Mit ihm werden Weichen gestellt, die weit über den eigentlichen Regelungsgegenstand – eine neue Bundesbürokratie – hinausweisen – und zwar vor allem dadurch, daß vieles bewußt ungeregelt bleibt.

Mittelbar verfolgt dieses Gesetz das Ziel, die Sicherheit einer Technik zu erhöhen. Dieses Ziel teilt es mit den vielen bestehenden Regelwerken des Technikrechts. Nun aber weist die IuK-Technik gegenüber allen bisher regulierten Techniken einige Besonderheiten auf, die es verbieten, auf sie einfach die überkommenen Regulierungsmuster ordnungsrechtlicher Gefahrenabwehr zu übertragen. Sie ist nur hinsichtlich der weniger wichtigen Elemente greifbar, überwiegend jedoch immateriell. Sie entspricht nicht dem herkömmlichen Maschinenmodell der Technik, sondern besitzt Systemcharakter. Sie ist nicht auf einen Zweck festgelegt, sondern nahezu universell verwendbar. Daher ist sie nicht auf einen Anwendungsbereich beschränkt, sondern durchdringt fast alle Gesellschaftsbereiche.[56] Aufgrund dieser Unterschiede ist es verständlich, daß das neue Gesetz nicht die alten Regelungsmuster wählt. Aber die Verletzlichkeit der Gesellschaft allein mit Klassifizierung, Beratung und Zertifikaten verringern zu wollen, ist zu wenig. Vielmehr kommt es darauf an, die Lern- und Reaktionsfähigkeit der Gesellschaft im Umgang mit dieser Technik zu ermöglichen oder zu stärken. Hierzu könnte das neue Bundesamt einen sinnvollen Beitrag leisten – allerdings nur, wenn seine Aufgaben, Befugnisse und Organisationsstruktur dieser Zielsetzung angepaßt wären.[57]

Hierfür wäre das Bundesamt für die Sicherheit in der Informationstechnik als *selbständige* und *unabhängige* Bundesoberbehörde zu errichten. Es darf nicht weisungsgebunden sein und daher nur einer Rechtsaufsicht unterliegen. Die gesellschaftlich wichtige wie für die Ausübung der Kommunikationsgrundrechte sensible

54 S. hierzu näher Roßnagel u. a. (Fn. 4), S. 171 ff.

55 Die Kommunikationstechnik ist dagegen, soweit sie durch die Deutsche Bundespost Telekom angeboten wird, stark reglementiert. Doch erstreckten sich diese Regulierungen nur auf das Nutzungsverhältnis zwischen staatlichem Monopolanbieter und Verbraucher, nicht jedoch auf die Kontrolle und Beeinflussung der technischen Entwicklung. Im Zuge der durch die Poststrukturreform eingeleiteten »Deregulierung« und »Privatisierung« der Telekommunikation werden die Möglichkeiten staatlicher Einflußnahme auf die technische Entwicklung noch stärker zurückgenommen werden. – S. hierzu kritisch Roßnagel/Wedde, Die Reform der Deutschen Bundespost im Licht des Demokratieprinzips, DVBl 1988, 562 ff.

56 Roßnagel, Möglichkeiten verfassungsvertraglicher Technikgestaltung, in: ders. (Hrsg.), Freiheit im Griff. Informationsgesellschaft und Grundgesetz, 1989, 177 ff. jeweils mwN.

57 S. zum folgenden näher Bizer/Hammer/Pordesch/Roßnagel (Fn. 12), S. 45 ff. sowie dies. (Fn. 29), DuD 1990, 184 f.

Aufgabe der Verringerung der Verletzlichkeit der Gesellschaft verträgt sich nicht mit einer weisungsgebundenen Unterstellung unter den »Polizeiminister des Bundes«.

Als vorrangige Aufgabe zur Herstellung von Sicherheit muß die *Begrenzung des Schadenspotentials* angesehen werden. Denn nur unter dieser Voraussetzung werden große Sicherungszwänge vermieden und kann auf die Einschränkung der Freiheitsgrundrechte von Bediensteten und Bürgern zur organisatorischen Sicherung der Technik verzichtet werden. Das Bundesamt sollte demnach die Aufgabe haben, für die verschiedenen Anwendungen von Informationstechnik jeweils zu 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 informationstechnischen Systemen garantiert ist.

Zu den Aufgaben des BSI sollte das Sammeln und *Dokumentieren von Schadensfällen* gehören. Nur dadurch kann das Bundesamt über das notwendige Erfahrungswissen verfügen, mit dessen Hilfe die Wahrscheinlichkeit von Schadensfällen, deren Schadensausmaß sowie mögliche Gegenmaßnahmen ermittelt und eine Verringerung der Verletzlichkeit erreicht werden kann. Dazu benötigt das BSI ausreichende Informationen über die entwickelten und eingesetzten Systeme oder Komponenten der Informationstechnik sowie Kenntnisse über Störfälle. Aus diesem Grund wäre eine Anzeigepflicht für das Herstellen, Errichten, Vertreiben und Betreiben von Informations- und Kommunikationssystemen in das BSIG aufzunehmen.

Das BSI sollte jährlich in einem zusammenfassenden *Verletzlichkeitsbericht* an den Bundestag und die Bundesregierung beschreiben, wie sich die Verletzlichkeit der Gesellschaft entwickelt hat. In diesem Bericht sollte das Bundesamt für die Sicherheit in der Informationstechnik insbesondere die Abhängigkeit der Gesellschaft von informationstechnischen Systemen und das damit verbundene Schadenspotential darstellen und allen betroffenen gesellschaftlichen und staatlichen Instanzen Vorschläge unterbreiten, wie sie durch Technikgestaltung die Verletzlichkeit der Gesellschaft reduzieren können. Insbesondere indem das BSI mögliche Alternativen und Gegenmaßnahmen skizziert, könnte der Bericht das Problembewußtsein einer breiten Öffentlichkeit anregen.

Das BSI sollte, wo Bedarf dafür besteht, Modellvorhaben anstoßen und soziale Experimente unterstützen, die Alternativen zur Trendentwicklung in die ›Informationsgesellschaft‹ darstellen, denn das rechtzeitige Erkennen und Offenhalten von *Alternativen* zu technischen Entwicklungen trägt dazu bei, die Verletzlichkeit der Gesellschaft zu verringern. In solchen Modellversuchen muß das Bundesamt immer auch versuchen, die Gegengewichte gegen die negativen Folgen einer Informationsstrategie zu stärken. Für diese Alternativen sind die Verletzlichkeitsaspekte und die von ihnen ausgehenden sozialen, rechtlichen und wirtschaftlichen Folgen abzuschätzen.

Angesichts der zunehmenden Bedeutung von *Verschlüsselungssystemen* sollten die Aufgaben der Zulassung informationstechnischer Systeme oder Komponenten auf den Bereich der Bundesbehörden bzw. auf Unternehmen, die im Rahmen von Aufträgen des Bundes tätig werden, beschränkt werden. Ebenso muß die Herstel-

58 Sie sind daher in einem weiteren Diskussionszusammenhang zu erörtern – s. hierzu z. B. Roßnagel u. a. (Fn. 4), S. 286 ff.

lung der Schlüsseldaten auf die Verarbeitung oder Übertragung von Verschlußsachen des Bundes beschränkt bleiben. Die Entwicklung selbständiger ›ziviler‹ Verschlüsselungsmechanismen darf nicht behindert werden und muß unabhängig vom BSI erfolgen.

Das BSI sollte stattdessen eine unabhängige Erforschung, Entwicklung und Anwendung von Verschlüsselungssystemen fördern, denn Verschlüsselungssystemen kommt mit der zunehmenden Entwicklung von Informationstechniken eine zentrale Bedeutung für die Reduzierung der Verletzlichkeit und der Gewährleistung der Bürgersicherheit zu. Die Erforschung, Entwicklung und Anwendung von Verschlüsselungssystemen muß aber aus Gründen der Verletzlichkeit der Gesellschaft wie der Bürgersicherheit durch unabhängige staatsfreie Einrichtungen erfolgen, bei denen der Staat keinen Einfluß auf den wissenschaftlichen Erkenntnisprozeß und das Ergebnis hat. In diesem Zusammenhang könnte dem BSI die Aufgabe zufallen, die Normung für den Einsatz von Public-Key-Systemen zu fördern, Fachkompetenz für die öffentliche Diskussion der Vertrauenswürdigkeit des Verfahrens bereitzustellen und die verwendeten Systeme zu validieren.

Informations- und Kommunikationstechnik findet in vielen gesellschaftlichen Bereichen Anwendung, für die eine Sicherheitsbewertung in Genehmigungs-, Zulassungs- und Planungsverfahren erforderlich ist. Soweit die Sicherheit in der Informationstechnik berührt ist, sollte das Bundesamt *Empfehlungen* zur Reduzierung der Verletzlichkeit abgeben können. Darüberhinaus sollte das BSI in Einzelfällen *Anordnungen* für die technische oder organisatorische Gestaltung der informationstechnischen Systeme oder Komponenten treffen können, wenn die Auswirkungen auf die Verletzlichkeit der Gesellschaft in einem unvertretbaren Ausmaß vernachlässigt werden. Die Verletzlichkeit der Gesellschaft erfordert eigentlich weitergehende Genehmigungs- und Zulassungsverfahren nach Maßgabe präventiver Kontrolle. In solchen Verfahren wären allerdings nicht nur Verletzlichkeitsprüfungen durchzuführen, sondern es wären vielmehr weitere Gesichtspunkte wie Datenschutz, Verfassungsverträglichkeit, Arbeitsschutz, Verbraucherschutz zu berücksichtigen.[8]

Die Bundesregierung hat Anregungen dieser Art nicht aufgegriffen. Ihr Gesetzentwurf ist vielmehr von einer seltsamen Mischung geistiger Ursprünge geprägt: Die Wurzeln dieses Gesetzes sind zum einen in dem Bemühen der Nachrichtendienstler zu suchen, das staatliche Geheimnis auch in das Zeitalter der ›Informationsgesellschaft‹ zu retten. Auch angesichts verblüffender Hacker-Coups, zerstörerischer Computer-Viren und kompromittierender Abstrahlung soll es künftig möglich sein, Verschlußsachen so geheim zu bearbeiten, wie dies für Geheimniskrämer mittels Papier und Tinte möglich war. Die zweite Wurzel ist die Nachfrage »sicherer« Computer und Telekommunikation insbesondere im militärischen Bereich und der internationale Wettbewerb um diese lukrativen Aufträge. Hierfür sind Standards, Produktprüfungen und Zertifikate notwendig, die die geforderte Sicherheit nachweisen. Nun soll die übrige Verwaltung von den Errungenschaften sicherer Geheimnisbearbeitung und -übertragung und die übrige Wirtschaft von der Zertifizierung »sicherer« IuK-Produkte profitieren. Schließlich atmet das Gesetz den Geist des Wirtschaftsliberalismus und ist geprägt von dem Glauben an die Allmacht des Marktes. Die technische Entwicklung selbst bleibt außerhalb des Blickfeldes. Ein steuernder oder auch nur korrigierender Eingriff aus Sicherheitsgesichtspunkten ist nicht vorgesehen. Weder im staatlichen noch im nicht-staatlichen Bereich soll die zunehmende Abhängigkeit der Gesellschaft und das Entstehen großer Schadenspotentiale in irgendeiner Weise beeinflußt noch sollen gar gezielt sozio-technische Alternativen entwickelt werden. Kein Technikgesetz hatte bisher solche Eltern: Nachrichtendienste, Protektionismus und Wirtschaftsliberalismus.

Der Gesetzentwurf erscheint 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«, 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 zum Handeln. Um aber ihre Förderpolitik nicht ändern zu müssen, versucht die Bundesregierung, 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.