Deutscher Bundestag
11. Wahlperiode

Drucksache 11/7246

29. 05. 90

Sachgebiet 204

Antrag

der Abgeordneten Frau Rust, Such und der Fraktion DIE GRÜNEN

Sicherheitsprobleme der Informations- und Kommunikationstechniken – Schutz von Individuum und Gesellschaft

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

1. Viele Bereiche der Wirtschaft, Wissenschaft und Verwaltung, des öffentlichen und privaten Lebens sind bereits heute vom einwandfreien Funktionieren der Informations- und Kommunikationstechniken (IuK-Techniken) abhängig. Mit dem zunehmenden Einsatz von IuK-Techniksystemen steigen auch die damit verbundenen Risiken. Das Problem der Verletzlichkeit der „Informationsgesellschaft" – die Möglichkeit großer Schäden für Individuum und Gesellschaft – entsteht vor allem dadurch, daß soziale Funktionen von Menschen auf IuK-technische Systeme übertragen werden. Im Vertrauen auf die Technik wird deren Leistungsfähigkeit und damit zugleich das Schadenspotential erhöht. Durch diese Übertragung werden zudem Informationsverarbeitungs- und Kommunikationsprozesse für Dritte zugänglich, die diese leichtfertig oder mißbräuchlich ausforschen, manipulieren, unterbinden, beschädigen oder zerstören können. Fehler und Manipulationen können so die Erfüllung der dem technischen System übertragenen gesellschaftlichen Funktionen beeinträchtigen.

   Als Risiken der „Informationsgesellschaft" müssen deshalb nicht nur die Sicherheitsmängel technischer Produkte, die Ausfallkosten defekter technischer Systeme, der Verrat militärischer Geheimnisse, die finanziellen Verluste durch Computerkriminalität oder verminderte Exportchancen in den Blick genommen werden, sondern insbesondere die Nachteile, die dem/der einzelnen Bürger/in sowie der Gesellschaft durch den Ausfall der auf die IuK-Technik übertragenen sozialen Funktionen (Verkehr, Energieversorgung, Prozeßsteuerung, Handel, Zahlungsverkehr, Verwaltungen, Kommunikation usw.) entstehen.

   Eine entscheidende Betriebsbedingung ist z. B. der Frieden, da eine hochinformatisierte Gesellschaft weder kriegstaug-

lich noch verteidigungsfähig ist (A. Roßnagel, Anhörung des Ausschusses für Forschung, Technologie und Technikfolgenabschätzung, 7. März 1990).

Außerdem können durch die möglichen Schäden wie auch durch die Sicherungsmaßnahmen zu ihrer Verhinderung erhebliche Beeinträchtigungen für die Ausübung der Grundrechte und den freien Prozeß politischer Willensbildung auftreten, d. h. die „Informationsgesellschaft" setzt sich einem Sicherungszwang aus, den sie nicht mehr beherrschen kann und dessen Dynamik in sozial unverträgliche politische und soziale Verhältnisse zu führen droht.

2. Der Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz – BSIG, Drucksache 11/7029) ist schon in seiner Problembeschreibung zu eng gefaßt: Um das auch von der Bundesregierung benannte Problem „der Verletzlichkeit der modernen Informationsgesellschaft zu begrenzen", beschränkt sich der Gesetzentwurf auf Probleme der Sicherheit des technischen Systems (Betriebssicherheit), der internationalen Wettbewerbsfähigkeit und der inneren Sicherheit. Diese reduzierte Definition der Risiken macht die Gesellschaft zum einen davon abhängig, daß es den Sicherheitssystemen – in einem noch völlig offenen Entwicklungsprozeß – gelingt, das Restrisiko der Informatisierung für jeden Entwicklungsschritt ausreichend gering zu halten. Zum anderen wird die Gesellschaft einem Zwang zur Sicherung ausgesetzt, dessen externe Kosten an Freiheits- und Demokratieeinbußen die Bürger zu tragen haben.

II. Der Deutsche Bundestag fordert deshalb die Bundesregierung auf, einen Gesetzentwurf vorzulegen, der sowohl die Sicherheitsprobleme der IuK-Technik als auch die Verletzlichkeit von Individuum und Gesellschaft als Folge des Einsatzes von IuK-Technik verringern hilft.

A. Folgende Zielsetzungen sind dabei zu berücksichtigen:

1. a) Orientierung der Entwicklung und des Einsatzes von IuK-Technik an der Sicherheit der Bürger und der Gesellschaft. Neben Datensicherungsmaßnahmen bedeutet dies

   — einen breiten gesellschaftlichen Konsens für die künftige Techniknutzung zu suchen, weil nur so Angriffsmotive reduziert werden können;

   — die gesellschaftliche Abhängigkeit von Techniksystemen dadurch zu verringern, daß Substitutionsmöglichkeiten erhalten bzw. geschaffen werden oder auch der Verzicht auf eine bestimmte Technik in Betracht gezogen wird;

   — die Technik selbst so zu gestalten, daß Angriffsmöglichkeiten und Beherrschbarkeitsprobleme verringert werden;

   — ausreichende Notfallmaßnahmen vorzusehen.

b) Gewährleistung der Versorgungssicherheit der Bevölkerung durch Vorkehrungen zur Schadensbegrenzung bzw. -vermeidung beim Einsatz von IuK-Techniken

- in den besonders wichtigen gesellschaftlichen Bereichen der Verkehrssysteme, der Prozeßsteuerung, der Geldwirtschaft und den Verwaltungen und Dienstleistungen,
- in Infrastruktursystemen der Telekommunikationsdienste und der Teletransaktionen,
- in Basissystemen (z. B. Betriebssysteme, Datenbanken).

c) Gewährleistung von Bürgersicherheit gegenüber möglichem Mißbrauch von IuK-Technik durch Staat und Wirtschaft

- Schutz der Konsumenten vor erhöhter Transparenz des Kundenverhaltens (z. B. Kunden-, Vermögens-, Ausgaben und Risikoprofile) und Verbraucher durch verschärfte Haftungsregelungen zur Erhöhung der Produktsicherheit,
- Schutz des/der Arbeitnehmers/in vor Eignungs- und Leistungsprofilen,
- Schutz der Privatsphäre vor Überwachung der Verhaltensweisen und Lebensgewohnheiten (z. B. durch Auswertung von Nutzdaten der Telekommunikation im ISDN-System),
- Sicherung der Bürger vor dem Ausforschungsinteresse der Behörden der inneren Sicherheit, der Nachrichtendienste und des Militärs,
- Förderung der Entwicklung von Verschlüsselungsverfahren, die eine vertrauenswürdige Identifikation, Manipulationskontrolle und eine anonyme Kommunikation elektronischer Nachrichten und Dokumente gewährleisten, wie z. B. bestimmte Public-Key-Systeme.

d) Verbesserung der Funktionssicherheit technischer Systeme und Bewertung dieser Sicherheit durch unabhängige Instanzen. Zur Vermeidung von Interessenkonflikten zwischen Bürger- und Staatssicherheit bei Verschlüsselungsverfahren

- dürfen Validierungs- und Revisionsinstanzen kein Interesse an den Daten haben, deren ordnungsgemäße und sichere Verarbeitung sie kontrollieren sollen,
- dürfen sie nicht der Geheimhaltung unterliegen und damit gezwungen sein, der Öffentlichkeit gegenüber erkannte Sicherungslücken und praktische Sicherungsverfahren zu verheimlichen.

e) Herstellung von Bedingungen der Möglichkeit einer sozialen Beherrschbarkeit von IuK-Technik

Zwingend notwendig sind die Gewinnung von

- Erkenntnisfähigkeit: Staat und Gesellschaft müssen in der Lage sein, künftige Risiken so früh zu erkennen, daß ihnen rechtzeitig durch Technikauswahl und -gestaltung begegnet werden kann.
- Lernfähigkeit: Technische Entwicklungen müssen dadurch korrigierbar bleiben, daß technische sowie nichttechnische Alternativen offengehalten oder hergestellt werden; das erforderliche Zukunftswissen muß in organisierten Verfahren erworben und der Öffentlichkeit vermittelt werden; Technikfolgenabschätzung muß verantwortlich durchgeführt werden.
- Steuerungsfähigkeit: Gegenüber widerstreitenden Macht- und Gewinninteressen müssen Staat und Gesellschaft befähigt werden, die Technikentwicklung und den Technikeinsatz nach selbstgesetzten Zielen zu steuern. Sie benötigen dazu Steuerungskriterien und -instrumente, Steuerungszugriff und -macht und schließlich die Fähigkeit und Zeit, diese Bedingungen zu kontrollieren, um ggfs. eine bestimmte Technikentwicklung zu verlangsamen oder anzuhalten.

2. Der Gesetzentwurf der Bundesregierung wird hingegen weder seiner eigenen Problemdefinition noch den o. g. Zielsetzungen gerecht. Diese(r) Konzeption
   - fehlt eine Zukunftsorientierung für die künftige Form und den Einsatz von IuK-Technik,
   - verschiebt das Problem der Verletzlichkeit einseitig auf die Mißbrauchsverhinderung,
   - enthält nur unzureichende Bedrohungsanalysen,
   - vernachlässigt das Problem der begrenzten Verläßlichkeit von Sicherungsmaßnahmen,
   - bietet keine Alternativen zu der als unbeeinflußbar hingenommenen IuK-Technik,
   - mangelt es an jeglichem Problembewußtsein hinsichtlich des Sicherungszwanges und der damit verbundenen möglichen Freiheits- und Demokratiekosten,
   - lehnt jegliche Steuerungsmaßnahmen selbst risikoreicher IuK-Systeme ab, die über technische Sicherungsmaßnahmen hinausgehen.

B. 1. Zur Erfüllung der o. g. Ziele soll der verlangte Gesetzentwurf Organisationsformen vorsehen, die
   - die Unabhängigkeit vom polizeilichen, nachrichtendienstlichen und militärischen Bereich garantieren,
   - den Großteil der Aufgaben nicht an Behörden, sondern an eine/n Parlamentsbeauftragte/n und freie Träger, wie z. B. Universitäten, Stiftungen, gemeinnützige Vereine u. ä. übertragen

— und im übrigen die hoheitlichen Aufgaben möglichst in dezentrale Zuständigkeit überweisen.

2. Die im Gesetzentwurf der Bundesregierung vorgeschlagene Lösung des Bundesamtes für Sicherheit in der Informationstechnik ist rechtlich bedenklich und in manchen Fällen sogar rechtswidrig:

   a) In § 3 Nr. 6 werden die Aufgaben der Verbrechensverhütung, der Strafverfolgung und des Verfassungsschutzes miteinander vermengt, für diese sind aber unterschiedliche Behörden mit unterschiedlichen Befugnissen zuständig. Es zählt z. B. nicht zu den Aufgaben des Verfassungsschutzes, Straftaten zu verfolgen, ebensowenig ist es Aufgabe des Generalbundesanwaltes, geheimdienstliche Tätigkeiten im Inland zu beobachten. Unklar bleibt auch die Begrenzung der Unterstützungspflicht des BSI.

   b) Besonders problematisch aus verfassungsrechtlicher Sicht ist, 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. Dieses Trennungsgebot darf auch durch Amtshilfeersuchen nicht unterlaufen werden.

   c) Noch bedenklicher ist die Verpflichtung des BSI, gleichzeitig den Bundesbeauftragten für den Datenschutz zu unterstützen, also das Recht auf informationelle Selbstbestimmung zu schützen, und das Bundeskriminalamt, den Militärischen Abschirmdienst und den Verfassungsschutz zu unterstützen, die ggf. das Recht auf informationelle Selbstbestimmung beschneiden.

   d) Die Weisungsabhängigkeit des BSI von der Abteilung Innere Sicherheit des Bundesministeriums des Inneren widerspricht den „zivilen" Aufgaben des BSI. Seinen Aufgaben der Begutachtung und Zertifizierung sowie der Verbesserung der Bürgersicherheit dürfte ein unabhängiger Status weit mehr entsprechen.

C. 1. Zur Konkretisierung und Umsetzung der o. g. Ziele müßten der/die Parlamentsbeauftragte, die Bundes- oder Länderbehörden folgende Aufgaben und Befugnisse haben:

   — Studien zu Alternativentwicklungen, Implikationsanalysen und Gestaltungsvorschläge, Modellversuche, Vermittlung dieses Wissens,

   — Anzeigepflicht für jeden Anwender und Anbieter von IuK-Technik,

   — jährlicher Verletzlichkeitsbericht und die Organisation kritischer Diskurse,

- Entwicklung von Kriterien der Verletzlichkeit und öffentliche Diskussion darüber,
- Empfehlungen zur Reduzierung von Verletzlichkeit,
- Beratungen zur Reduzierung von Schadenspotentialen,
- Standardisierung in pluralistisch zusammengesetzten Gremien in öffentlichen Sitzungen,
- Zertifizierungen auf der Grundlage o. g. Zielsetzungen,
- Zulassungs- und Genehmigungsverfahren für die Sicherung von Mindeststandards an Sicherung und Schadensvorsorge für IuK-Systeme,
- öffentliche Planungsverfahren, insbesondere für Infrastruktursysteme.

2. Das BSIG enthält keine der hier genannten Aufgaben und Befugnisse, sondern beschränkt sich auf technische Datensicherung.

Bonn, den 27. Mai 1990

Frau Rust
Such
Hoss, Frau Schoppe, Frau Dr. Vollmer und Fraktion

Druck: Thenée Druck KG, 5300 Bonn, Telefon 23 19 67
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 13 63, Herderstraße 56, 5300 Bonn 2, Telefon (02 28) 36 35 51, Telefax (02 28) 36 12 75
ISSN 0722-8333