Weitere Aspekte fernmeldetechnischer Alternativen zum ISDN

Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner
Institut für Rechnerentwurf und Fehlertoleranz
(früher Institut für Informatik IV)
Fakultät für Informatik der Universität Karlsruhe
Postfach 6980, D 7500 Karlsruhe 1
Telefon (0721) 608-4218

In seinem Artikel „Für fernmeldetechnische Alternativen zum ISDN" (in PIK 10/2 (1987) 87-92, im folgenden [Kubi_87] genannt) setzt sich Herr Prof. Herbert Kubicek kritisch mit den Plänen der Deutschen Bundespost auseinander, die von ihr betriebenen Fernmeldenetze zu einem zunächst schmalbandigen, später breitbandigen ISDN sowie einem auch die Verteilnetze ersetzenden IBFN auszubauen.

Seine Hauptforderung lautet, bei staatlich gelenkten und gesellschaftlich genutzten großtechnologischen Systemen die soziale Beherrschbarkeit in den Vordergrund zu rücken und Einfluß auf die Technikgestaltung nehmen zu lassen.

Diese Forderung sieht Prof. Kubicek in den Planungen der Deutschen Bundspost in keiner Weise berücksichtigt: die Einführung des ISDN werde tiefgreifende Auswirkungen auf die Arbeitswelt, auf die Medienlandschaft und auf das informationelle Selbstbestimmungsrecht der Bürger (Datenschutz) haben. Zur Beherrschung der drohenden Probleme unternehme die Post keinerlei Schritte, und dies, obwohl es geeignete technische Alternativen zu den Postplänen gebe.

Der Ist-Analyse von Prof. Kubicek stimmen wir uneingeschränkt zu. Die Deutsche Bundespost steht – so scheint es zumindest – auf dem Standpunkt, daß für „harmlose" Techniken wie das ISDN eine aufwendige Folgenabschätzung oder gar eine staatliche Regulierung nicht notwendig ist. Diese Betrachtungsweise geht davon aus, daß

- die Telekommunikationstechnik keine existentielle Bedrohung darstellt – wie dies etwa für die Kern- oder Gentechnik der Fall ist – und daher der Zustand vor Einführung der neuen Technik im technischen Sinne notfalls wiederhergestellt werden kann und
- genau die Techniken und Dienste gesellschaftlich erwünscht sind, die von einer hinreichend großen Zahl von Bürgern genutzt und damit positiv bewertet werden und gesellschaftlich unerwünschte Techniken mangels Nachfrage nicht überleben; individuelle soziale Härten muß die Gesellschaft notfalls ausgleichen.

Diese Haltung ist insbesondere in Technikerkreisen häufig anzutreffen. Sie verkennt jedoch zumindest, daß das geplante ISDN neben den geplanten auch ungeplante Dienste ermöglichen wird, z.B. die Massenüberwachung der ISDN-Teilnehmer durch (eigene oder fremde) Geheimdienste, Fernmeldefirmen – oder auch „nur" die Angst der Bürger vor dieser Möglichkeit. Ebenfalls unbeachtet bleibt bei dieser Haltung die Trägheit großtechnischer Systeme: mit der Einführung des ISDN sind enorme Investitionen an Arbeitszeit und Geld verbunden, die bei einem „Ausstieg" aus dem ISDN nach Einführung desselben teilweise verloren wären. Da dies volkswirtschaftlich und damit politisch nicht akzeptabel wäre, ist die Möglichkeit, nach Einführung des ISDN durch Entscheidung des Regelkreises „Gesellschaft" in kurzer Zeit wieder zum alten oder einem alternativen Zustand zu gelangen, eine reine Illusion.

Aus dieser Erkenntnis muß man – wie Prof. Kubicek sehr detailliert begründete – folgern, daß vor Einführung des ISDN die möglichen Folgen für die Gesellschaft umfassend und hinreichend genau abgeschätzt werden müssen. Ein System darf nur dann realisiert werden, wenn seine Folgen von den Betroffenen überwiegend positiv bewertet werden.

Unter anderem nennt Prof. Kubicek zwei Folgen, die er eindeutig negativ bewertet, und auf deren Betrachtung wir uns im folgenden beschränken werden:

- die Erleichterung von Telearbeit durch ein Netz, das digital arbeitet, eine relativ hohe Übertragungsrate anbietet und dessen Gebührenstruktur die Datenkommunikation mit dem Fernsprechen gleichsetzt, und

- die Erleichterung der Individual- und Massenüberwachung der Teilnehmer eines Netzes, das Inhalts- und Verkehrsdaten (wer kommuniziert wann wieviel mit wem?) ungeschützt und unnötig umfangreich in den Vermittlungseinrichtungen verarbeitet.

Die beiden Folgen unterscheiden sich unter anderem in der Stabilität ihrer Einschätzung: gilt Telearbeit z.B. in Gewerkschaftskreisen heute als eher negativ, so könnte sie doch in wenigen Jahren für viele als erstrebenswert gelten; demgegenüber ist Datenschutz eine auf Dauer erwünschte Eigenschaft und durch die Datenschutzgesetze und das Recht auf informationelle Selbstbestimmung [Bund_83] in unserem Rechtssystem verankert.

Zur Lösung des Problems schlägt Prof. Kubicek vor, statt der von der Bundespost verfolgten Pläne zum Aufbau eines im Prinzip völlig neuen Telekommunikationssystems ein Konzept des bedarfsorientierten (und damit diensteorientierten) und langsamen Ausbaus der heutigen dienstespezifischen Netze zu verfolgen, wobei vor jedem Ausbauschritt dessen Folgen abgeschätzt werden (was einfacher sein dürfte, als die Folgen eines „großen" Schrittes wie die der Einführung des ISDN abzuschätzen).

Hieraus abzuleiten ist sein konkreter Moratoriumsvorschlag: Das Fernsprechnetz und das IDN bleiben voneinander getrennt erhalten. Die Übertragung auf den Teilnehmeranschlußleitungen des Telefonnetzes bleibt analog; die bisherigen mechanischen Vermittlungseinrichtungen werden beibehalten oder durch festverschaltete elektronische statt den von der Post geplanten und zum Teil schon eingesetzten frei programmierbaren ersetzt. Das Fernnetz und das digitale IDN werden den Anforderungen der Wirtschaft entsprechend ausgebaut, wobei aber jeder Teilnehmer die Freiheit haben soll, ob er sich des analogen Fernsprechnetzes bedienen möchte oder des IDN und eines möglicherweise vorhandenen Sprachkommunikationsdienstes im IDN [Kubi_87 Abschnitt 4.2, ausführlicher KuRo_86].

Ein bedarfsorientierter Ausbau des IDN hat natürlich je nach Bedarfsabschätzung verschiedene Auswirkungen: Stimmen die Abschätzungen der Bundespost, so wird das IDN schrittweise solange ausgebaut, bis es den für das ISDN prognostizierten Bedarf an Datenkommunikation abdeckt und dann vermutlich aus Kostengründen das zumindest im Ortsnetzbereich davon getrennte Fernsprechnetz verdrängt, denn andernfalls müßten für das IDN in großem Umfang neue Teilnehmeranschlußleitungen verlegt werden. Stimmt hingegen die Einschätzung von Prof. Kubicek, der die Postprognosen stark anzweifelt, so bleibt das IDN ein relativ weitmaschiges und teures Spezialnetz, was aber, da nur relativ wenige neue IDN-Vermittlungsstellen installiert werden müßten, zu einer insgesamt kostengünstigeren Lösung führen würde als das von der Post geplante ISDN oder ein voll ausgebautes, aber ungenutztes IDN.

Grundidee des Moratoriumsvorschlages ist, daß die gegenwärtige Situation zumindest für die private Telekommunikation noch für längere Zeit sozial akzeptabel ist und Änderungen an dieser Situation sich im wesentlichen nur aus Änderungen der Telekommunikationstechnik ergeben.

Diese Einschätzung trifft sicher für viele Bereiche zu, unserer Meinung nach aber nicht für alle. Dies sei für die Bereiche Telearbeitsplätze und Datenschutz kurz erläutert [ausführlich Pfit_86]: mit dem Beibehalten des im Teilnehmeranschlußbereich analogen Telefonnetzes werden zugleich zwei Eigenschaften bewahrt, nämlich einerseits die Möglichkeit, durch synchrone Modems digitale Daten mit einer Rate von 4800 bit/s transparent über das Telefonnetz zu übertragen [KuRo_86 Seite 94, Tane_81 Seite 95, 96] und die Unmöglichkeit, die Inhalte eines Telefongesprächs wirkungsvoll zu verschlüsseln (Ende-zu-Ende-Verschlüsselung) und damit vor unbefugter Kenntnisnahme zu schützen, ohne zugleich die Sprachqualität ganz wesentlich zu verschlechtern.

Beide Eigenschaften erscheinen zur Zeit relativ harmlos:

- Telearbeitsplätze, die ein Terminal zu Hause beim Arbeitnehmer mit einem zentralen Rechner beim Arbeitgeber verbinden, gibt es kaum; für sehr datenintensive Arbeitsplätze erscheint die Übertragungsrate zudem als zu gering.
- Mangels technischer Unterstützung ist zumindest eine Massenüberwachung durch Mithören aller oder vieler Telefongespräche noch nicht sehr ergiebig (wenn auch für besonders interessante Verbindungen, etwa für die Telefonverbindungen von West nach Ost, die Auswertung „von Hand" manchen als lohnend erscheint).

  An die Möglichkeit der Individualüberwachung einzelner Fernsprechteilnehmer hat sich die Gesellschaft „gewöhnt". Das unbefugte aber bekanntgewordene Abhören richtet sich meist gegen Personen des öffentlichen Lebens und wird eher des abgehörten Inhalts wegen als politischer

Skandal empfunden denn aus Datenschutzgründen; das befugte Abhören ist zur Verfolgung schwerer Straftaten allgemein als nützlich anerkannt.

Relativ unbeachtet in der Öffentlichkeit ist die Möglichkeit der Auswertung der Verkehrsdaten im Fernsprechnetz, die bereits heute (nach Installation von Zusatzgeräten in den Vermittlungseinrichtungen) automatisiert durchgeführt werden könnte.

Beides kann sich aber leicht ändern:

- Stößt die Telearbeit in Zukunft auf größeres Interesse, so kann die verstärkte Schaffung von Telearbeitsplätzen technisch nur wirksam verhindert werden, wenn kein Telekommunikationsnetz vorhanden ist, das die notwendige Übertragungsgeschwindigkeit unter vernünftigen Kosten erlaubt. Die Kosten der Telearbeitsplätze selbst dürften der Preisentwicklung der Mikroelektronik folgend in Zukunft kein Hinderungsgrund sein.

  Die Übertragung einer DIN A4 Seite Text dauert bei 4800 bit/s ungefähr 3 Sekunden. Stellt man sich unter einem Telearbeitsplatz nicht ein „dummes" Terminal vor, sondern einen leistungsfähigen PC mit eigenem Massenspeicher (Floppy disk, Festplatte) und Drucker, so können damit fast alle für Telearbeit zur Diskussion stehenden Arbeiten erledigt werden.

  Zudem könnten solche Firmen, die an Telearbeit großes Interesse hätten und für die der Leistungsunterschied zwischen der Übertragung mit synchronen Modems über das Fernsprechnetz und mittels des ISDN ausschlaggebend wäre, bereit sein, ihre Mitarbeiter nicht nur mit Telearbeitsplätzen, sondern auch mit IDN-Anschlüssen auszustatten, die eine vergleichbare Leistung wie ISDN-Anschlüsse erreichen.

  Ein Netzmoratorium würde damit die Telearbeit nicht, wie von Prof. Kubicek erhofft, entscheidend behindern. Dies gilt übrigens für alle Netzkonzepte, die das Fernsprechen mit zumindest derselben Sprachqualität wie heute anbieten, so daß eine technische Regelung der Telearbeit für die Zukunft generell ausscheidet.

  Eine Lösung des Problems Telearbeit bzw. der von Prof. Kubicek dargestellten möglichen negativen Folgen der Telearbeit muß daher eine rein politische sein.
- Eine Massenüberwachung der Telefongespräche, gleich ob analog oder digitalisiert übertragen, wird sofort praktikabel, wenn diese durch automatische Sprechererkennung oder gar Sprachanalyse unterstützt wird.

  Durch festverschaltete Vermittlungseinrichtungen, wie von Prof. Kubicek zur Verminderung des Datenschutzproblems vorgeschlagen, wird die Situation kaum besser: zwar wird die nachträgliche Manipulation der Vermittlungseinrichtungen erschwert; kaum ausgeschlossen werden kann jedoch, daß die festverschalteten Vermittlungsstellen von Anfang an fest eingebaute „Trojanische Pferde" enthalten oder daß Telefonleitungen außerhalb der Vermittlungsstellen angezapft werden.

Darüber hinaus vernachlässigt ein im wesentlichen auf das Fernsprechnetz begrenztes Netzkonzept wie das Netzmoratorium auch die Schutzbelange der Wirtschaft: auch ein Unternehmen wird ein Interesse daran haben, daß sowohl die Inhalte seiner über das IDN ausgetauschten Daten geheim bleiben als auch seine Verkehrsdaten, die zuverlässig seine Beziehungen zu anderen Unternehmen und Behörden widerspiegeln würden. Natürlich könnten innerhalb des IDN effizientere Schutzmechanismen angewendet werden, als dies im analogen Fernsprechnetz möglich ist (s.u.), doch würde dies bei den dann hinsichtlich Datenschutz benachteiligten Benutzern des Fernsprechnetzes, also der breiten Öffentlichkeit, auf recht wenig Verständnis stoßen.

Hinsichtlich des einer technischen Lösung prinzipiell unzugänglichen Bereiches „Telearbeit" ist das Netzmoratorium damit weitgehend neutral, hinsichtlich des Bereiches „Datenschutz" schreibt es aber einen unbefriedigenden und immer schlechter werdenden technisches Zustand fest.

Zu einer gezielten Änderung dieses unbefriedigenden Zustandes wurden in den letzten Jahren alternative Netzkonzepte entwickelt, die die Unbeobachtbarkeit der Benutzer garantieren [Chau_81, Pfit_83, Chau_85], ohne hinsichtlich der üblichen Leistungsparameter (Bandbreite, Fehlerrate, Kanalaufbauzeit etc.) große Einschränkungen aufzuweisen [Pfit_85]. Sie basieren größtenteils auf dem Einsatz kryptographischer Techniken (für einen Überblick sei auf [PfPW_86] verwiesen).

Die Eigenschaft der Unbeobachtbarkeit kann für diese Netzkonzepte im mathematischen Sinne bewiesen werden, wobei allerdings zum Teil noch unbewiesene Annahmen über die verwendeten Kryptosysteme gemacht werden müssen. Die für die Unbeobachtbarkeit eines Benutzers wesentlichsten technischen Einrichtungen befinden sich in dessen eigener Teilnehmerstation. Es ist daher zu hoffen, daß die Benutzer den für sie nachprüfbaren Beweisen der Unbeobachtbarkeit der alternativen

Netzkonzepte und den unter ihrer direkten Kontrolle stehenden technischen Einrichtungen zumindest ebenso viel Vertrauen schenken wie den bisherigen Systemen, deren Fehler und Schwächen sie durch Beobachtung zwar kennen, deren positive Eigenschaften sie aber im allgemeinen nicht oder höchstens durch Inspektion zentraler Fernmeldeeinrichtungen nachprüfen können.

Alle Netzkonzepte verwenden Ende-zu-Ende-Verschlüsselung, um die Kommunikationsinhalte vor unbefugter Kenntnisnahme zu schützen, so daß die Übertragung digital mit einer Rate von mindestens 64000 bit/s (zur Aufrechterhaltung der Sprachqualität beim Fernsprechen) erfolgen muß. Damit muß ein Datenschutz garantierendes Netz zumindest dieselbe technische Leistungsfähigkeit besitzen wie das von der Post geplante ISDN und wird auch in etwa dieselben Kosten verursachen – wem diese als zu hoch erscheinen, der muß zwischen garantiertem Datenschutz und geringen Kosten wählen; beides zusammen ist unvereinbar.

Auch die Einführung eines Datenschutz garantierenden Fernmeldenetzes kann auf der Basis des heutigen Fernsprechnetzes schrittweise erfolgen, eine mögliche Strategie hierzu wurde in [Pfit_86, PfPW_86] beschrieben.

Dies ermöglicht, auch bei der Einführung eines Datenschutz garantierenden Fernmeldenetzes nach dem von Prof. Kubicek vertretenen Prinzip der sozialen Beherrschbarkeit vorzugehen:

Ausgehend von den als unabdingbar angesehenen Eigenschaften des Netzes – flächendeckende Sprachkommunikation und garantierter Datenschutz – ergibt sich für die technische Gestaltung ein gewisser Freiraum. Wie dieser Freiraum ausgenutzt werden soll, ergibt sich aus den Bedürfnissen der Benutzer nach weiteren oder verbesserten Anwendungen (d.h. Diensten und deren Verwendung) und der Bewertung der Folgen eines entsprechenden Ausbaus.

Nach jedem Ausbau entstehen natürlich nicht nur die gewünschten Anwendungsmöglichkeiten, sondern jede Anwendung, die im Rahmen der nach dem Ausbau angebotenen Bandbreite und des erreichten Verbreitungsgrades ohne organisatorische Unterstützung durch die Bundespost technisch möglich ist, kann dann auch realisiert werden und entzieht sich damit einer technischen Steuerung. Insbesondere widerspricht der Ansatz, durch Überwachung der Kommunikation die Art der gerade durchgeführten Anwendungen zu kontrollieren, der Forderung nach Datenschutz. Dies gilt insbesondere für Anwendungen, z.B. Homebanking oder Telearbeit, die bereits mit Hilfe von Modems im Fernsprechnetz realisierbar sind.

Daher müssen auch hier für jede Ausbaustufe, die nach Abwägung der Vor- und Nachteile demokratisch beschlossen wurde, vor deren Realisierung die damit möglichen Anwendungen politisch reguliert werden.

Literatur

Bund_83 Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 – 1 BvR 209/83 u. a.; Datenschutz und Datensicherung DuD 4 (1984) 258-281

Chau_81 D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; CACM 24/2 (1981) 84-88

Chau_85 D. Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; CACM 28/10 (1985) 1030-1044

Kubi_87 H. Kubicek: Für fernmeldetechnische Alternativen zum ISDN; Praxis der Informationsverarbeitung und Kommunikation PIK 10/2 (1987) 87-92

KuRo_86 H. Kubicek, A. Rolf: Mikropolis; Mit Computernetzen in die „Informationsgesellschaft" (2. Aufl.); VSA-Verlag Hamburg 1986

Pfit_83 A. Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes; Interner Bericht 18/83, Fakultät für Informatik der Universität Karlsruhe 1983

Pfit_85 A. Pfitzmann: How to implement ISDNs without user observability - Some remarks; Interner Bericht 14/85, Fakultät für Informatik der Universität Karlsruhe 1985

Pfit_86 A. Pfitzmann: Die Infrastruktur der Informationsgesellschaft: Zwei getrennte Fernmeldenetze beibehalten oder ein wirklich datengeschütztes errichten?; Datenschutz und Datensicherung DuD 6 (1986) 353-359

PfPW_86 A. Pfitzmann, B. Pfitzmann, M. Waidner: Technischer Datenschutz in dienste-integrierenden Digitalnetzen - Warum und wie?; Datenschutz und Datensicherung DuD 3 (1986) 178-191