Zeitschrift: Technische Mitteilungen / Schweizerische Post-, Telefon- und Telegrafenbetriebe = Bulletin technique / Entreprise des postes, téléphones et télégraphes suisses = Bollettino tecnico / Azienda delle poste, dei telefoni e dei telegrafi svizzeri

Herausgeber: Schweizerische Post-, Telefon- und Telegrafenbetriebe

Band: 64 (1986)

Heft: 7

Artikel: Was tragen die PTT zur Datensicherheit bei? = Quel est l'apport des PTT à la sécurité des données?

Autor: Lutz, Hans Peter W.

DOI: https://doi.org/10.5169/seals-875034

Was tragen die PTT zur Datensicherheit bei?[1]

Quel est l'apport des PTT à la sécurité des données?[1]

Hans Peter W. LUTZ, Bern

Zusammenfassung. *Der Einsatz der modernen EDV- und Prozessortechnik wird mehr und mehr mit der Anwendung verschiedenster Kommunikationsmittel verknüpft. In diesem Zusammenhang stellt sich – aus den verschiedensten Gründen – auch die Frage nach der Sicherheit und der Sicherung der über die Fernmeldenetze übermittelten Informationen. Dieser Artikel soll dazu beitragen, vor allem im Anwendungsbereich des Datennetzes Telepac allfällig vorhandene falsche Vorstellungen und Erwartungen aus dem Wege zu räumen bzw. bisher allenfalls unbeachtet gebliebene Möglichkeiten und Massnahmen für die Gewährleistung der Datensicherheit aufzuzeigen.*

Résumé. *Les techniques modernes de l'informatique et des processeurs sont de plus en plus étroitement liées aux applications des moyens de communication modernes. C'est à ce propos – et pour diverses raisons – que se pose aussi la question de la sécurité et de la sauvegarde des données transmises par les réseaux de télécommunications. Par cet article, l'auteur souhaite contribuer à corriger les idées erronées et les espoirs trompeurs que l'on se fait notamment au sujet du réseau de données Télépac. Il montre aussi certaines possibilités et mesures éventuellement inédites en matière de protection des données.*

Qual è il contributo delle PTT alla sicurezza dei dati?
Riassunto. *La moderna tecnica di elaborazione elettronica di dati è sempre più impiegata per i più diversi mezzi di comunicazione. Sorge pertanto il problema della sicurezza e della protezione delle informazioni trasmesse attraverso le reti delle telecomunicazioni. Con questo articolo, l'autore vuole contribuire a eliminare, soprattutto riguardo alla rete di dati Telepac, opinioni e aspettative sbagliate e indicare possibilità e provvedimenti non ancora considerati in materia di sicurezza dei dati.*

1 Grundlagen und Vorgaben

Im Zusammenhang mit der Problematik Sicherheitsaspekte in Datennetzen ist eine Rückbesinnung auf die rechtlichen Grundlagen sowie ein Blick auf die unternehmenspolitische Grundeinstellung der PTT-Betriebe nötig, innerhalb derer sich diese bewegen und ihre Tätigkeiten im Bereich der Teleinformatik entwickeln. Die folgenden Grundlagen finden hierbei Verwendung:

- Bundesverfassung
- Telefon- und Telegrafenverkehrsgesetz (TVG)
- Verordnungen zum TVG
- Kommunikationsleitbild PTT
- Unternehmenspolitische Grundsätze und Richtlinien PTT.

Der Wortlaut der relevanten Artikel der Bundesverfassung und des Telefon- und Telegrafenverkehrsgesetzes sind im *Kasten 1* zusammengefasst, jene des Kommunikationsleitbildes PTT im *Kasten 2*, die der unternehmenspolitischen Grundsätze PTT, insbesondere über die Dienstleistungspolitik, im *Kasten 3*.

Besondere Beachtung verdient hierbei der *Grundsatz 5 des Kommunikationsleitbildes PTT*.:

> *Die PTT-Betriebe befassen sich im Kommunikationsbereich mit der Übermittlung von Informationen und nicht mit Inhalten.*

Aus dieser Formulierung ist die Rollenverteilung bzw. die Abgrenzung der Verantwortlichkeiten zwischen den PTT-Betrieben und den Kunden bzw. den Lieferanten von Informatikmaterial klar erkennbar. Diese Abgrenzung hat übrigens auch zum heute realisierten Betriebskonzept des Dienstes Videotex geführt: Im Normalfall sind die Informationen, die irgendwelche Informationsanbieter für diesen Dienst zur Verfügung stellen wollen,

[1] Nach einem Vortrag an der SVD-Herbsttagung 1985

1 Principes et normes

Lorsqu'on s'interroge sur la problématique de tous les aspects touchant à la sécurité des réseaux de données, tant au point de vue des bases légales qu'à celui de la politique d'entreprise des PTT, on s'aperçoit que les activités du domaine de la téléinformatique se situent dans ce cadre. En l'occurrence, les bases légales et les principes suivants sont applicables:

- Constitution fédérale
- Loi réglant la correspondance télégraphique et téléphonique (LTT)
- Ordonnances afférentes à la LTT
- Plan directeur de la communication pour les PTT
- Principes et directives régissant la politique d'entreprise des PTT.

L'*encadré 1* récapitule la teneur des articles significatifs de la Constitution fédérale et de la loi réglant la correspondance télégraphique et téléphonique, l'*encadré 2* celle du plan directeur de la communication pour les PTT et l'*encadré 3* les principes régissant la politique d'entreprise des PTT, notamment ce qui concerne la politique en matière de prestations.

Le *principe 5 du plan directeur de la communication pour les PTT* mérite une attention particulière:

> *les PTT se chargent, dans le secteur de la communication, de la transmission des informations et non de leur contenu.*

En se fondant sur cet énoncé, il est possible de délimiter clairement les rôles et les responsabilités entre l'Entreprise des PTT et les clients ou les fournisseurs de matériel informatique. La conception de l'exploitation du service Vidéotex, telle qu'elle est aujourd'hui réalisée, se fonde aussi sur cette délimitation des tâches: habituelle-

[1] Selon un exposé présenté à l'assemblée d'automne 1985 de la SVD

Kasten 1

Bundesverfassung

Art. 36 Das Post- und Telegrafenwesen im ganzen Gebiet im ganzen Umfang der Eidgenossenschaft ist Bundessache

Die heutige Rechtsprechung schliesst das Telefon, den Telex sowie den technischen Teil von Radio und Fernsehen hierbei mit ein

Telefon- und Telegrafenverkehrsgesetz

Art. 1 Fernmelderegal

Die PTT-Betriebe haben das ausschliessliche Recht, Sende- und Empfangseinrichtungen sowie Anlagen jeder Art, die der elektrischen oder radioelektrischen Zeichen-, Bild- oder Lautübertragung dienen, zu erstellen und zu betreiben

Art. 4 Leistungspflicht

Wo sie die erforderlichen Einrichtungen besitzen oder dieses Gesetz deren Schaffung vorsieht, sind die PTT-Betriebe unter den Bedingungen dieses Gesetzes, der Telegrafen- und Telefonordnung sowie der Ausführungsbestimmungen zu den darin vorgesehenen Leistungen gegenüber jedermann verpflichtet

Art. 6 Amtsgeheimnis

Die mit telegrafen- oder telefondienstlichen Verrichtungen betrauten Personen dürfen über den Telegrafen- oder Telefonverkehr einer Person sowie über den Inhalt der telegrafendienstlichen Aufzeichnungen und der vermittelten Telefongespräche keine Mitteilungen an Dritte machen

Encadré 1

Constitution fédérale

Art. 36 Dans toute la Suisse, les postes et les télégraphes sont du domaine fédéral. Selon la jurisprudence actuelle, la notion de téléphone englobe les services tels que le télex ainsi que les équipements techniques de la radio et de la télévision.

Loi réglant la correspondance télégraphique et téléphonique

Art. 1 Régale des télécommunications

L'Entreprise des PTT a le droit exclusif d'établir et d'exploiter des installations expéditrices et réceptrices, ou des installations de n'importe quelle nature servant à la transmission électrique ou radioélectrique de signaux, d'images ou de sons.

Art. 4 Obligation de fournir des prestations

En tant qu'elle dispose des installations nécessaires ou que la présente loi en admet la réalisation, l'Entreprise des PTT est tenue envers chacun aux prestations inscrites dans la présente loi, dans l'ordonnance sur les télégraphes et les téléphones et dans les règlements qui en découlent.

Art. 6 Secret de fonction

Il est interdit aux personnes chargées d'assurer le service télégraphique ou téléphonique de faire à des tiers des communications sur les relations télégraphiques ou téléphoniques d'une personne, sur le contenu des inscriptions de service relatives à la correspondance télégraphique et des conversations téléphoniques. Il leur est également interdit de donner à qui que ce soit l'occasion de commettre un tel acte.

Kasten 2

Kommunikationsleitbild PTT

Das Kommunikationsleitbild soll eine Konzentration der Kräfte zur sinnvollen Nutzung und Förderung bestehender und zukünftiger Kommunikationsformen bewirken, mögliche interne und externe Konflikte lösen helfen und periodisch angepasst werden. Das Kommunikationsleitbild dient in erster Linie als Grundlage des unternehmerischen Handelns der PTT-Betriebe. Es stützt sich auf die nachfolgenden zehn Grundsätze, welche die Aufgaben und die Haltung der PTT-Betriebe in der Gesellschaft verdeutlichen und abgrenzen sollen:

Grundsatz 1 Die PTT-Betriebe sind dem Gemeinwohl verpflichtet

Grundsatz 2 Die PTT-Betriebe stellen die Versorgung des ganzen Landes mit einwandfreien Post- und Fernmeldeleistungen zu gleichen Bedingungen und auf wirtschaftliche Weise sicher

Grundsatz 3 Die PTT-Betriebe erbringen ihre Leistungen auf der Basis des gesetzlichen Auftrages

Grundsatz 4 Die PTT-Betriebe bewahren ihre organisatorische und wirtschaftliche Einheit

Grundsatz 5 Die PTT-Betriebe befassen sich im Kommunikationsbereich mit der Übermittlung von Informationen und nicht mit Inhalten

Grundsatz 6 Die PTT-Betriebe behalten die öffentlichen Netzwerke für die Übermittlung von Informationen in ihrer Verantwortung

Grundsatz 7 Die PTT-Betriebe stellen den freien Zugang zu allen von ihnen angebotenen Kommunikationsmöglichkeiten sicher

Grundsatz 8 Die PTT-Betriebe gewährleisten in ihrem Aufgabenbereich den Persönlichkeitsschutz

Grundsatz 9 Die PTT-Betriebe betreiben eine fortschrittliche und soziale Personalpolitik

Grundsatz 10 Die PTT-Betriebe sind sich bewusst, dass nicht alles, was technisch möglich und wirtschaftlich tragbar ist, auch gesellschaftlich erwünscht ist, und beurteilen daher die Entwicklung im Kommunikationsbereich ganzheitlich

Encadré 2

Plan directeur de la communication pour les PTT

Le plan directeur de la communication a pour effet d'obtenir une concentration des forces en vue d'utiliser rationnellement et de favoriser les formes de communication existantes et futures, de contribuer à la solution d'éventuels conflits internes et externes; il doit être adapté périodiquement. Le plan directeur de la communication sert en premier lieu de fil conducteur pour l'activité de l'Entreprise des PTT. Il se fonde sur les dix principes généraux énumérés ci-après, qui définissent et délimitent les tâches et le rôle des PTT dans la société.

Principe 1 Les PTT sont tenus d'œuvrer pour le bien de la collectivité

Principe 2 Les PTT assurent dans l'ensemble du pays des services postaux et des services des télécommunications donnant toute satisfaction, aux mêmes conditions et selon des principes économiques

Principe 3 Les PTT fournissent leurs prestations en vertu du mandat que leur confère la loi

Principe 4 Les PTT entendent demeurer une unité organique et économique

Principe 5 Les PTT se chargent, dans le secteur de la communication, de la transmission des informations et non de leur contenu

Principe 6 Les PTT conservent la responsabilité des réseaux publics servant à transmettre les informations

Principe 7 Les PTT assurent le libre accès à toutes les possibilités de communication qu'ils offrent

Principe 8 Les PTT garantissent, dans leur champ d'activité, la protection de la personnalité

Principe 9 Les PTT pratiquent une politique de personnel moderne et sociale

Principe 10 Les PTT sont conscients que tout ce qui est techniquement réalisable et économiquement supportable n'est pas forcément souhaitable pour la société, raison pour laquelle ils étudient le développement dans le secteur de la communication dans son ensemble

in privatwirtschaftlich betriebenen Datenbanken gespeichert, und die PTT-Betriebe verbinden den Informationsbezüger über ihre Fernmeldenetze mit der entsprechenden Datenbank des gewünschten Anbieters. Diese Auf-

ment, les données que les fournisseurs d'information proposent pour ce service sont mémorisées dans des banques de données de caractère privé et l'Entreprise des PTT relie les demandeurs d'information aux banques

Kasten 3

Unternehmenspolitische Grundsätze und Richtlinien der PTT-Betriebe

Dienstleistungsangebot:
Die PTT-Betriebe wollen ein auf die allgemeinen Bedürfnisse ausgerichtetes Dienstleistungsprogramm erfüllen; sie überprüfen dabei periodisch alle ihre Leistungen, um festzustellen, ob sie hinsichtlich Bedürfnis und Ausmass noch dem tatsächlichen Interesse der Allgemeinheit entsprechen.

Als öffentlicher Dienstleistungsbetrieb sind die PTT-Betriebe darauf bedacht, im Rahmen der gesetzlichen Leistungspflicht und unter Beachtung der staatspolitischen und volkswirtschaftlichen Bedeutung das Dienstleistungsangebot auf die allgemeinen Bedürfnisse auszurichten, indem sie

- im Rahmen der verfügbaren Mittel die Nachfrage nach Dienstleistungen bestmöglich erfüllen
- neue Dienstleistungen einführen, wenn sie einem ausgewiesenen Bedürfnis entsprechen und für längere Dauer eine angemessene Rendite versprechen
- für jede einzelne Dienstleistung die Entwicklung der Nachfrage verfolgen und den gesamten Dienstleistungsfächer nach betriebswirtschaftlichen Kriterien periodisch überprüfen
- für jede einzelne Dienstleistung die Entwicklung des Kostendekkungsgrades verfolgen und defizitäre Dienstleistungen gegebenenfalls tariflich sanieren oder aufheben; dabei sind Möglichkeiten des Ausweichens auf andere Dienstleistungen zu berücksichtigen

Encadré 3

Principes et directives régissant la politique d'entreprise des PTT

Offre de prestations
Les PTT entendent se conformer à un programme de prestations répondant aux besoins généraux. Ils vérifient périodiquement toutes leurs prestations, afin de s'assurer qu'elles correspondent encore — par leur caractère et par leur volume — à la demande de la collectivité.

En tant qu'entreprise publique de services, l'Entreprise des PTT doit tendre, dans le cadre de l'obligation légale de fournir des prestations et en tenant compte de leur importance politique et économique, à ce que son offre de prestations corresponde aux besoins généraux

- en satisfaisant au mieux la demande de prestations, dans les limites des moyens à disposition;
- en n'introduisant de nouvelles prestations que lorsqu'elles répondent à un besoin reconnu de la clientèle et qu'elles laissent prévoir un rendement convenable de longue durée;
- en suivant, pour chaque prestation, l'évolution de la demande, et en examinant périodiquement selon les critères de l'économie d'entreprise tout l'éventail des prestations;
- en observant l'évolution du degré de couverture des frais de chaque prestation, en assainissant le cas échéant les tarifs des prestations déficitaires ou en supprimant celles-ci; il y aura lieu de tenir compte des possibilités de recourir à d'autres prestations.

gabenteilung hat sich sehr gut bewährt, und zwar sowohl in technischer als auch in betrieblicher oder politischer Hinsicht.

Nebst diesen rechtlichen und operativen Vorgaben bestehen im technischen Bereich eine ganze Reihe weiterer Vorgaben in der Form von Grundforderungen, Pflichtenheften und Spezifikationen für Systeme und einzelne Komponenten in den Bereichen Vermittlung, Übertragung und (PTT-)Endgeräte, in denen die Aspekte der Datensicherheit gebührende Beachtung finden. Als Beispiel diene das damalige «Rahmenpflichtenheft für ein Datennetz mit Paketvermittlung EDWP» aus dem Jahre 1978, das die Grundlage für die Beschaffung der heutigen Hardware und Software für Telepac war und worin konkrete Anforderungen bezüglich Ausfallwahrscheinlichkeiten, Fehlerhäufigkeiten und Dienstqualität dieses Datennetzes festgeschrieben worden sind.

2 Datenschutz und Datensicherheit

Bei der Problematik Sicherheitsaspekte in Datennetzen sind grundsätzlich zwei Bereiche klar voneinander zu unterscheiden, nämlich Daten*schutz* und Daten*sicherheit*.

Der *Datenschutz* hat als Zielsetzung, jeden Missbrauch – ob beabsichtigt oder unbeabsichtigt – von manuellen und maschinellen Datenverarbeitungsmitteln zu verhindern und eine ordnungsgemässe Datenverarbeitung sicherzustellen.

Im Zentrum der Datenschutzproblematik steht heute der Persönlichkeitsschutz, d. h. der Schutz der durch die Daten ausgedrückten Sachverhalte des realen Lebens, insbesondere bei Daten über Personen und deren Privatsphäre.

Die Zielsetzungen für eine ordnungsgemässe Datenverarbeitung sind von den jeweils hierfür verantwortlichen Stellen bzw. Benutzern festzulegen und in die Tat umzu-

de données voulues au moyen de ses réseaux de télécommunication. Cette répartition des tâches a donné de très bons résultats, tant sur le plan technique que sur celui de l'exploitation ou de la politique.

Outre ces dispositions légales et structurelles, il existe techniquement parlant toute une série d'autres prescriptions, notamment des exigences fondamentales, des cahiers des charges pour des systèmes entiers ou des composants discrets, dans les domaines de la commutation, de la transmission, des terminaux PTT, prescriptions dans lesquelles toute l'attention voulue a été accordée à la sécurité des données. On peut citer comme exemple le «Cahier des charges-cadre pour un réseau de données à commutation de paquets EDWP» de 1978, qui a servi de base à l'acquisition des matériels et des logiciels actuels du réseau Télépac et dans lequel étaient formulées des exigences concrètes concernant la probabilité des défaillances, la fréquence des défauts et la qualité de service exigée de ce réseau de données.

2 Protection des données et sécurité des données

En ce qui concerne la sécurité, les problèmes afférents au réseau de données peuvent en principe être clairement scindés en deux domaines, à savoir la *protection* des données et la *sécurité* des données. La *protection* des données englobe toutes les mesures permettant d'éviter un usage abusif, qu'il soit intentionnel ou non, de moyens de traitement manuels ou mécaniques, et assurant un traitement régulier des données.

Aujourd'hui, la protection de la personnalité est le problème crucial que pose la protection des données, c'est-à-dire la protection à l'égard de toute indiscrétion se rapportant à la vie de tous les jours et qui pourrait être révélée par les données, en particulier par les informations se rapportant à des personnes physiques et à leur sphère privée.

setzen. Allen Datenschutzregelungen liegen naturgemäss einige Grundsätze zugrunde, wie:

- Zweckbestimmung der Datensammlungen
- öffentliche und bekannte Grundlagen für die Führung von Datensammlungen
- Auskunfts- und Einsichtsrecht für direkt Betroffene
- Berichtigungsrecht bei falsch oder unvollständig gespeicherten Daten
- Datenverkehrsregelung (Regelung der Weitergabe geschützter Daten).

Die Methoden zur Gewährleistung des Datenschutzes werden *Datensicherung* genannt; sie umfassen alle Massnahmen technischer und organisatorischer Art, um Daten vor Verfälschung, Fehlverarbeitung, Zerstörung, Entwendung oder unzulässiger Verwendung zu schützen. Der kombinierte Einsatz von Datensicherungsmassnahmen führt dann zur *Datensicherheit*, die unabdingbare Voraussetzung für die Gewährleistung eines realen Datenschutzes ist.

Allen unzähligen Datensicherungsverfahren liegen ebenfalls einige Grundsätze zugrunde, wie:

- sinnvolle Redundanz gegen Datenverlust und -verfälschung
- Abschirmung und Kontrolle gegen unzulässigen Datenzugriff
- Trennung der Kompetenzen gegen Missbräuche durch Fachleute.

An technischen Möglichkeiten für die Datensicherung seien etwa folgende erwähnt, ohne dass hierbei auf die jeweilige technische Ausgestaltung im einzelnen eingegangen werden kann:

- Kanalcodierung
- Fehlererkennungs- und Fehlerkorrektursysteme (Redundanzanreicherung)
- Informationsrückkopplung (Echoplex)
- Entscheidungsrückkopplung (ACK/NAK-Technik)
- zeichenweise Informationssicherung
- blockweise Informationssicherung
- zyklische Blocksicherung.

Alle diese technischen Massnahmen sind in der Regel durch den Benutzer in dessen Anwendungsprozeduren zu verwirklichen, wofür dieser auch die alleinige Verantwortung über deren Erfolg bzw. Misserfolg trägt.

3 Problematik Teilnehmeranschluss

Für die Datenübermittlung bieten die PTT-Betriebe ihren Kunden heute drei verschiedene Transportnetze mit entsprechenden Dienstleistungen an, nämlich:

- das Telefonnetz (Wählnetz, Mietleitungen)
- das Telexnetz
- das Datennetz Telepac.

Bezüglich Sicherheitsaspekte sind alle drei Transportnetze einander ähnlich; sie lassen sich grundsätzlich gemäss *Figur 1* darstellen.

Im Netzbereich wird in allen drei Transportnetzen durch die jeweils eingesetzte Übertragungstechnik (Analogtechnik mit Trägerfrequenzsystemen oder Digitaltechnik mit Pulscode-Modulationssystemen) mit ihrer weitgehenden Multiplexierung eine sehr grosse Sicherheit ge-

Les services responsables ou les utilisateurs des données sont donc tenus de mettre en pratique toutes les mesures conduisant à un traitement correct des données. De par la nature des choses, un certain nombre de principes fondamentaux réglementent la protection des données, notamment:

- le motif pour lequel des fichiers de données sont établis
- les bases connues, de nature officielle, concernant la tenue de fichiers de données
- le droit, pour la personne directement touchée, de se renseigner sur les données qui la concerne et d'en prendre connaissance
- le droit de rectifier des données erronées ou mémorisées de manière incomplète
- la réglementation en matière de communication de données protégées.

Les méthodes visant à assurer la protection des données sont appelées *sauvegarde des données ou mise en sûreté des données*; elles comprennent les mesures techniques et les mesures d'organisation propres à garantir la protection des données personnelles contre la falsification, le traitement incorrect, la destruction, le vol ou un emploi non autorisé. Par la combinaison de ces mesures de sauvegarde des données, on parvient à assurer la *sécurité des données*, condition indispensable à une protection des données efficace.

Les innombrables méthodes de sauvegarde des données se fondent toutes sur un certain nombre de principes, à savoir:

- assurer une redondance judicieuse des données pour prévenir leur vol ou leur falsification
- protéger les données contre un accès illicite au moyen de contrôles
- délimiter les compétences, de manière à prévenir les abus de la part de spécialistes.

Parmi les nombreuses possibilités techniques d'assurer la sécurité des données, les méthodes suivantes méritent d'être évoquées, abstraction faite des détails qui les caractérisent:

- codage des canaux
- système de reconnaissance et de correction d'erreurs (redondance accrue)
- feed-bak de l'information (Echoplex)
- feed-bak de décision (technique ACK/NAK)
- mise en sûreté des informations caractère par caractère
- mise en sûreté des informations par blocs
- mise en sûreté cyclique des blocs.

En règle générale, il appartient à l'usager de mettre en œuvre ces mesures techniques en fonction des procédures d'application qui lui sont propres, étant entendu qu'il est seul responsable du succès ou de l'insuccès de ces méthodes.

3 Problématique des raccordements d'abonnés

Aujourd'hui, les PTT offrent à leurs clients trois réseaux de transport distincts pour transmettre des données,

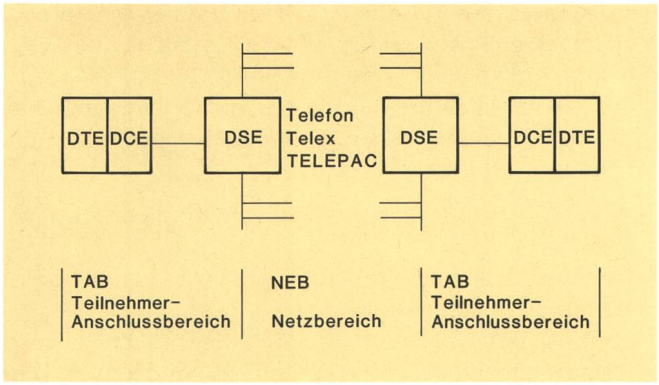

Fig. 1
Grundzüge der Telekommunikationsnetze – Caractéristiques des voies de communication
DTE Datenendeinrichtung – Equipement terminal de traitement de données
DCE Datenübertragungseinrichtung – Equipement de terminaison du circuit de données
DSE Datenvermittlungseinrichtung – Equipement de commutation de données
TAB Secteur de raccordement d'abonnés
NEB Secteur du réseau
Telefon – Téléphone
Telex – Télex
Telepac – Télépac

gen allfällige Beeinflussung des Leitungssignales durch Unbefugte geboten. Ein möglicher Missetäter müsste demnach zunächst einmal dieselben Übertragungsausrüstungen einsetzen, um überhaupt an einen bestimmten Datenkanal heranzukommen; anschliessend müsste er Kenntnisse über Art und zeitlichen Ablauf der auf diesem Datenkanal abgewickelten Anwendung besitzen, um diesen Informationsfluss gezielt stören oder verändern zu können, und dies alles in Echtzeit. Dies erfordert einen ganz erheblichen materiellen und finanziellen Aufwand dar, der wohl kaum so leicht und unbemerkt erbracht werden dürfte.

Der *Teilnehmeranschlussbereich* hingegen ist heute sicherheitsmässig als das schwächste Glied in allen drei Netzen zu bezeichnen, wird doch jeder einzelne Anschluss dienstspezifisch zwei- oder vierdrähtig bis zum Teilnehmer geführt. Innerhalb der Hausinstallationen, die weitverzweigt sein können, bestehen naturgemäss mannigfaltige Möglichkeiten der missbräuchlichen Anzapfung eines Datenkanals, auf die hier aber im einzelnen nicht näher eingegangen werden kann und die in der Regel nicht die PTT-Betriebe betreffen.

4 Massnahmen zur Gewährleistung der Datensicherheit (bei Telepac)

Die PTT-Betriebe haben in ihrem Datennetz Telepac zahlreiche Massnahmen technischer und organisatorischer Art eingeplant, um die Datensicherheit innerhalb ihres Einflussbereiches zu gewährleisten. Nachstehend sind vor allem jene Massnahmen summarisch aufgeführt, die gegenüber Mietleitungen und deren Anwendungen von einiger Bedeutung sind:

41 Virtuelle Verbindungen, dynamische Multiplexierung

Anwendung der Technik der virtuellen Verbindungen und der dynamischen Multiplexierung gemäss den inter-

chacun d'eux étant à même de fournir des prestations spécifiques:

- le réseau téléphonique (réseau commuté, circuits loués)
- le réseau télex
- le réseau de données Télépac.

En ce qui concerne la sécurité, les trois réseaux de transport se ressemblent; leurs traits caractéristiques ressortent de la *figure 1:*

En ce qui concerne le *secteur du réseau*, la technique de transmission utilisée dans les trois réseaux de transport considérés (technique analogique pour les systèmes à courants porteurs ou technique numérique pour les systèmes de modulation par impulsions et codage), associée à des techniques de multiplexage, assure un haut degré de sécurité à l'égard de toute personne qui tenterait d'influer sur les signaux de ligne. Pour accéder à un canal de données déterminé, un éventuel «pirate» devrait tout d'abord disposer des mêmes équipements de transmission; en outre, il devrait connaître le genre d'application et la répartition temporelle des données transmises sur ce canal et opérer de plus en temps réel, s'il voulait perturber systématiquement ou modifier le flux des informations. Cela supposerait la mise en œuvre de moyens matériels et financiers importants, de sorte qu'une telle opération pourrait difficilement passer inaperçue.

En revanche, le *secteur de raccordement d'abonnés* est certainement aujourd'hui l'élément le plus vulnérable dans les trois réseaux, chaque abonné étant raccordé au service spécifique considéré en 2 ou en 4 fils. Il existe donc de nombreuses possibilités de se greffer illicitement sur un canal de données, au sein d'une installation intérieure, vu qu'elle peut être très finement ramifiée. Ce cas ne concernant en règle générale pas les PTT, il ne sera pas examiné plus en détail dans ce qui suit.

4 Mesures propres à assurer la sécurité des données dans le réseau Télépac

En ce qui concerne le réseau de données Télépac, les PTT ont pris de nombreuses mesures d'ordre technique et structurel pour assurer la sécurité des données dans le secteur dont ils sont responsables. Ce sont donc sur-

Tabelle I. Multiplexer-Hierarchie
Tableau I. Hiérarchie des multiplexeurs

Typ Type	Einzelkanal Canal individuel	Vielfachkanal Canal multiple	Telefonkanäle Canal téléphonique
MUX C	50 bit/s 300 bit/s	2,4 kbit/s	
MUX B	2400 bit/s 4800 bit/s 9600 bit/s	64 kbit/s	1
MUX A	64 kbit/s	2048 kbit/s	30
DMX-2	64 kbit/s	2,048 Mbit/s	30
DMX-8	2,048 Mbit/s	8,448 Mbit/s	120
DMX-34	8,448 Mbit/s	34,368 Mbit/s	480
DMX-140	34,368 Mbit/s	139,264 Mbit/s	1920
DMX-565	139,264 Mbit/s	565,992 Mbit/s	7680

Tabelle II. Anschlussklassen im Datennetz Telepac
Tableau II. Classes de raccordement dans le réseau de données Télépac

Basisdienste **Services de base**		
Übertragungs-geschwindigkeit Vitesse de transmission	Übertragungs-verfahren Procédés de transmission	Betriebsverfahren Procédés d'exploitation
2 400 bit/s	seriell, synchron sérielles, synchrones	duplex
4 800 bit/s	seriell, synchron sérielles, synchrones	duplex
9 600 bit/s	seriell, synchron sérielles, synchrones	duplex
48 000 bit/s	seriell, sychron sérielles, synchrones	duplex
Zusatzdienste **Services complémentaires**		
Übertragungs-geschwindigkeit Vitesse de transmission	Übertragungs-verfahren Procédés de transmission	Bertriebsverfahren Procédés d'exploitation
bis 300 bit/s jusqu'à 300 bit/s	seriell, asynchron sérielles, asynchrones	duplex
bis 1200 bit/s jusqu'à 1200 bit/s	seriell, asynchron sérielles, asynchrones	duplex

nationalen Normen für die Paketvermittlungstechnik *(Tab. I)*.

42 Steuerung und Kontrolle des Datenflusses

Netzinterne Steuerung, Überwachung und nötigenfalls auch Korrektur des Datenflusses, und zwar getrennt für die beiden Netzbereiche Teilnehmeranschluss und interzentrale Verbindungen.

43 Anschlussklassen

Anwendung bestimmter Anschlussklassen mit definierten Bitraten und Zugangsprozeduren für X.25-Anschlüsse (Paketmodus) und für X.28-Anschlüsse (Zeichenmodus) gemäss *Tabellen II* und *III*.

44 Geschlossene Teilnehmergruppen

Möglichkeit der Bildung von Teilnehmergruppen mit einzeln festgelegten oder gar keinen Verkehrsbeziehungen zu anderen Teilnehmern.

45 Anschlussidentifikation

Möglichkeit für den Rufenden bzw. den Gerufenen, die Teilnehmernummer seines Partners übermittelt zu erhalten und zu überprüfen.

46 NUI und Passwort

Anwendung eines Sicherheitsmechanismus mit *N*etwork *U*ser *I*dentification (NUI) und Passwort; keine Speicherung von Passworten im Netz, sondern fallweise Berechnung mit Algorithmus und Vergleich mit Eingabe.

tout les mesures ayant une certaine importance dans le domaine des circuits loués et de leurs applications qui sont sommairement récapitulées ci-après:

41 Liaisons virtuelles, multiplexage dynamique

Uilisation de la technique des liaisons virtuelles et d'un multiplexage dynamique selon les normes internationales applicables à la technique de la commutation par paquets *(tab. I)*.

42 Commande et contrôle du flux de données

Commande interne du réseau, surveillance et correction éventuelle du flux de données, les secteurs du réseau «raccordement d'abonné» et «communications intercentrales» étant traités séparément.

43 Classes de raccordement

Utilisation de classes de raccordements spécifiques avec débits binaires définis et procédures d'accès pour raccordements X.25 (mode paquet) ainsi que raccordements X.28 (mode caractère) selon les *tableaux II* et *III*.

44 Groupes fermés d'usagers

Possibilités de former des groupes d'usagers ne pouvant pas communiquer avec les autres usagers ou ne le pouvant que de manière limitée.

45 Identification du raccordement

Possibilités pour l'appelant ou l'appelé d'obtenir et de vérifier le numéro d'abonné de son correspondant.

46 NUI et mot de passe

Recours à un mécanisme de sécurité par association du numéro d'identification d'abonné (*N*etwork *U*ser *I*dentification = NUI) et du mot de passe; pas de mémorisation de mots de passe dans le réseau mais calcul de ceux-ci dans chaque cas particulier à l'aide d'un algorythme et d'une comparaison avec le critère entré.

Tabelle III. Bitfehlerraten auf den Fernmeldenetzen
Tableau III. Taux d'erreurs sur les bits dans les réseaux de télécommunication

Netz Réseau		Bitfehlerraten Taux d'erreurs sur les bits
Telefonnetz Réseau téléphonique	Wählnetz Réseau commuté	$10^{-6} \ldots 10^{-4}$
	Mietleitungen analog Lignes louées analogiques	$10^{-7} \ldots 10^{-5}$
	Mietleitungen digital Lignes louées numériques	$10^{-8} \ldots 10^{-6}$
Telexnetz/Réseau télex		$10^{-6} \ldots 10^{-5}$
Telepac Télépac	X.25 (Paketmodus) X.25 (Mode paquets)	$10^{-8} \ldots 10^{-6}$
	X.28 (Zeichenmodus) X.28 (Mode caractères)	$10^{-6} \ldots 10^{-4}$

47 Transparentes Benutzerdatenfeld

Möglichkeit der Verwendung des transparenten Benutzerdatenfeldes für die Verschlüsselung der Daten sowie der Verwendung geeigneter Prozeduren nach den Anforderungen des Benutzers.

48 Zeitsperren

Notwendigkeit, bei X.28-Anschlüssen die Eingabe von NUI und Passwort innerhalb einer Minute abzuschliessen.

All dies bewirkt, zusammen mit PTT-internen betrieblichen und organisatorischen Vorkehren, dass das Datennetz Telepac als generelles Transportsystem für die Text- und Datenkommunikation bezüglich Datensicherheit einen recht hohen Standard gewährleistet, der von den beiden anderen Transportnetzen, dem Telefonnetz und dem Telexnetz, auch nicht nur annähernd erreicht wird.

5 Schlussfolgerungen

Aus den gemachten Ausführungen können die nachstehenden Schlussfolgerungen abgeleitet werden:

1. Das Datennetz Telepac bietet gegenüber dem Telefonnetz (Wählnetz und Mietleitungen) und dem Telexnetz eine erheblich grössere Sicherheit gegen missbräuchlichen Datenzugriff im Netz und bei Datenbanken.
2. Das Datennetz Telepac bietet gegenüber dem Telefonnetz (Wählnetz und Mietleitungen) und dem Telexnetz eine wesentlich bessere Unterstützung bei der Verwirklichung benutzerspezifischer Sicherheitsmassnahmen auf der Applikationsebene.
3. Ein vollumfassender Schutz der Daten bei deren Erfassung, Übermittlung und Verarbeitung ist mit vernünftigem technischem, organisatorischem und wirtschaftlichem Aufwand kaum je zu erreichen.
4. Für Anwendungen mit erhöhtem Sicherheitsbedürfnis sind unter Umständen geeignete Massnahmen zu treffen, um den unbefugten Datenzugriff auf der Teilnehmeranschlussleitung und den Hausinstallationen zu erschweren oder zu verunmöglichen.
5. Ein umfassendes Sicherheitskonzept muss sowohl Massnahmen im Bereich des Datenschutzes als auch solche im Bereich der Datensicherheit umfassen.
6. Für ein solches Sicherheitskonzept gibt es keine allgemein gültige Vorgehensweise; jeder einzelne Anwendungsfall muss unter Berücksichtigung aller Randbedingungen für sich allein betrachtet und die verschiedenen Massnahmen müssen spezifisch aufeinander abgestimmt werden, um ein optimales Ergebnis zu erhalten.
7. Ein wirkungsvolles Sicherheitskonzept stützt sich ausnahmslos auf eine ausgewogene Kombination von geeigneten Massnahmen in den Bereichen Hardware, Software und Betriebsorganisation ab.

47 Champs de données d'usagers transparents

Possibilité d'utiliser des champs de données d'usagers transparents pour le chiffrement des données et d'employer des procédures appropriées répondant aux besoins de l'usager.

48 Blocages temporels

Nécessité, pour les raccordements X.28, d'introduire le NUI et le mot de passe en l'espace d'une minute. Il en résulte que le réseau de données Télépac, compte tenu des mesures internes qu'ont prises les PTT sur le plan de l'exploitation et de l'organisation, est un système de transport de textes et de communications de données offrant un très haut niveau de fiabilité en ce qui concerne la sécurité des données, qui n'est de loin pas atteint par les deux autres réseaux de transport, à savoir le réseau téléphonique et le réseau télex.

5 Conclusions

Les explications qui précèdent conduisent aux conclusions suivantes:

1. Par rapport au réseau téléphonique (réseau commuté et circuits loués) et au réseau télex, le réseau de données Télépac offre une sécurité nettement accrue à l'égard d'un accès abusif aux données transmises sur les circuits ou stockées dans des banques de données.
2. Comparé au réseau téléphonique (réseau commuté et circuits loués) et au réseau télex, le réseau de données Télépac permet de réaliser beaucoup plus efficacement des mesures de sécurité spécifiques aux usagers au niveau des applications.
3. Il est impossible de parvenir à une protection intégrale des données, lors de leur saisie, de leur transmission et de leur traitement par la mise en œuvre de mesures techniques et d'organisation d'une ampleur raisonnable et à des frais en rapport avec le but visé.
4. Pour les applications exigeant une sécurité accrue, il est parfois nécessaire de prendre des mesures appropriées pour empêcher, si possible entièrement, les personnes non autorisées d'accéder aux données transitant sur les circuits de raccordement d'abonnés et les installations intérieures.
5. Un concept de sécurité complet doit comprendre aussi bien des mesures au niveau de la protection des données qu'à celui de leur sécurité.
6. Il n'existe aucune méthode de validité générale pour un tel concept de sécurité; chaque application spécifique doit être considérée isolément, compte tenu de toutes les conditions marginales, et les diverses mesures doivent être systématiquement harmonisées si l'on veut obtenir un résultat optimal.
7. Un concept de sécurité efficace se fonde sans exception sur une combinaison équilibrée de mesures appropriées prises au niveau des matériels, des logiciels et de l'organisation de l'exploitation.