Berliner
Datenschutzbeauftragter

BERLIN

Datenschutz bei Telekommunikation und Medien

Materialien zum

14

Datenschutz bei Telekommunikation und Medien

3., überarbeitete und ergänzte Auflage
Juli 1993

Herausgeber:

Berliner Datenschutzbeauftragter
Hildegardstraße 29/30, 10715 Berlin
ab 1. Oktober 1993: Pallasstraße 25, 10781 Berlin
Telefon: (0 30) 7 83 88 44
Telefax: 8 53 60 44
Bildschirmtext: *679#
Redaktion: Dr. Alexander Dix
Satz und Druck: Verwaltungsdruckerei Berlin

Inhalt

B. Beschlüsse der Internationalen Konferenz der Datenschutzbeauftragten
Resolutions of the International Conference of Data Protection Commissioners

5. Konferenz, 18. 10. 1983, Stockholm

Neue Medien
New Media

7. Konferenz, 26. 9. 1985, Luxemburg

Datenschutz und Neue Medien
Data Protection and New Media

9. Konferenz, 24. 9. 1987, Oslo

Neue Medien
New Media

11. Konferenz, 30. 8. 1989, Berlin

Berliner Resolution/Berlin Resolution

Zusatzerklärung der Datenschutzbeauftragten der EG-Länder
Additional Statement by the Data Protection Commissioners of EC-Nations

Entschließung über die Arbeitsgruppe Telekommunikation und Medien
Resolution about the Working Group on Telecommunications and Media

ISDN

12. Konferenz, 19. 9. 1990, Paris

Datenschutz und die Europäische Gemeinschaft
Data Protection and the European Community

Probleme öffentlicher Telekommunikationsnetze und des Kabelfernsehens
Problems relating to Public Telecommunication Networks and Cable Television

13. Konferenz, 4. 10. 1991, Straßburg

Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Telemarketing, der Kartentelefone und der elektronischen Directories und Beschluß der Internationalen Konferenz der Datenschutzbeauftragten

Report of the Working Group on Telecommunications and Media on problems relating to telemarketing, card telephones and electronic directories and Resolution of the International Conference of Data Protection Commissioners

14. Konferenz, 29. 10. 1992, Sydney

Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und Gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Report of the Working Group on Telecommunications and Media on problems relating to the secrecy of telecommunications and satellite communications and Common Statement of the International Conference of Data Protection and Privacy Commissioners

C. Stellungnahmen der Arbeitsgruppe Telekommunikation und Medien der Internationalen Konferenz der Datenschutzbeauftragten
Memorandum and Statement of the Working Group on Telecommunications and Media of the International Conference of Data Protection Commissioners

Memorandum vom 12. 11. 1990 zum Vorschlag der EG-Kommission für eine ISDN-Richtlinie

Memorandum of 12th November 1990 on the Proposal of the EC Commission for a Council Directive on ISDN

Stellungnahme vom 6. 2. 1991 zum Artikel 19 des Vorschlags der EG-Kommission für eine allgemeine Datenschutzrichtlinie

Statement of 6th February 1991 on Article 19 of the Proposal of the EC Commission for a general Data Protection Directive

Vorwort

Wer Dienstleistungen in modernen und komfortablen Telekommunikationsnetzen in Anspruch nehmen will, hinterläßt zwangsläufig elektronische Spuren, ohne daß die Diensteanbieter und Netzbetreiber ihn darauf hinweisen. Zu selten werden auch (wie bei der vorab bezahlten Telefonkarte auf Guthabenbasis) datenschutzgerechte, „spurlose“ Formen der Telekommunikation oder Abrechnung zumindest als Alternative angeboten. Der Europäische Binnenmarkt löst auch im Bereich der Telekommunikation grenzüberschreitende Datenflüsse in bisher nicht gekanntem Ausmaß aus. Die Struktur dieser modernen Netze entspricht bisher in keiner Weise dem Prinzip der Datensparsamkeit, zumal der immer kleiner und billiger werdende Speicherplatz den einzigen bisher wirksamen Anreiz, den der Kostensenkung, insofern an Bedeutung verlieren läßt.

Die Datenschutzbeauftragten haben sich bereits sehr früh auf nationaler und internationaler Ebene mit den wachsenden Datenschutzproblemen bei Telekommunikation und Medien auseinandergesetzt und Forderungen zur datenschutzgerechten Gestaltung von Telekommunikationsnetzen und -diensten erhoben. Die entsprechenden Beschlüsse der nationalen und internationalen Datenschutzkonferenzen sind bisher nicht zusammengefaßt veröffentlicht worden. Dies soll mit den vorliegenden Materialien nachgeholt werden. Die Konferenzbeschlüsse werden ergänzt durch Stellungnahmen der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz, die sich seit 1985 unter dem Vorsitz des Berliner Datenschutzbeauftragten mit der Frage auseinandergesetzt hat, wie der Datenschutz mit Hilfe technischer Standards und rechtlicher Regelungen zu einem notwendigen Bestandteil jedes Netzes und Diensteangebots werden kann.

Dr. Hansjürgen Garstka

Berliner Datenschutzbeauftragter

A. Beschlüsse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

7. Konferenz, 11. Dezember 1980, Berlin

Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen)

Übersicht

Vorbemerkung

Die nachstehenden Grundsätze für den Datenschutz bei den Neuen Medien sollen sicherstellen, daß die anlaufenden Erprobungen und die ihnen zugrundeliegenden Vorschriften den Datenschutz von vornherein berücksichtigen und dieser dem Einsatz neuer Technologien nicht nachfolgt.

Die Grundsätze können dem Stand der Vorhaben und der technischen Entwicklung entsprechend nicht abschließend sein.

1 Informationssammlung über Teilnehmer

1.1 Bei der Einführung Neuer Medien ist der Datenschutz sicherzustellen. Dies gilt auch für die Versuchsphase. Bereits hierfür sollten gesetzliche Regelungen getroffen werden.

1.2 Personenbezogene Benutzerdaten dürfen nur erhoben, gespeichert oder übermittelt werden, soweit ihre Verarbeitung für den Betrieb unumgänglich ist und ohne sie eine der gesetzlich zugelassenen Kommunikationsformen der Neuen Medien nicht durchgeführt werden kann.

1.3 Der Schutz der in den Neuen Medien anfallenden personenbezogenen Teilnehmerdaten kann nicht auf deren Verarbeitung in Dateien beschränkt werden.

1.4 Sofern bei bestimmten Diensten eine unmittelbare Teilnehmer-Anbieter-Kommunikation vorgesehen ist, dürfen Daten nur in dem Umfang festgehalten und übermittelt werden, wie dies zur Durchführung des jeweiligen Dienstes erforderlich und aufgrund der einschlägigen gesetzlichen Regelung zulässig ist.

1.5 Gebühren und Entgelte sind in anonymer Form zu berechnen und abzurechnen, soweit eine individualisierbare Registrierung von einzelnen Kommunikationsvorgängen zur Abwicklung von Vertragsverhältnissen nicht erforderlich ist. Sollte eine zusätzliche Kontrolle erforderlich werden, so könnte beim Benutzer eine Zähleinrichtung installiert werden.

2 Bedeutung des Versuchsstadiums (Pilotprojekte)

2.1 Bereits in der Versuchsphase ist ein möglichst wirksamer Datenschutz sicherzustellen, da diese Phase die spätere Nutzung der Neuen Medien prägt.

2.2 In der Versuchsphase ist zu prüfen, ob weitere Datenschutzregelungen auf dem Gebiet der Neuen Medien nötig sind oder ob vorhandene Vorschriften modifiziert werden müssen.

2.3 Im Rahmen wissenschaftlicher Begleituntersuchungen ist dafür zu sorgen, daß auch die Datenschutzfragen besonders geprüft werden.

2.4 Im Rahmen einer wissenschaftlichen Begleituntersuchung ist der Zugriff auf gespeicherte Datenbestände nur gestattet, sofern diese Daten anonymisiert worden sind. Darüber hinausgehende Daten dürfen nur von den Teilnehmern direkt erfragt werden.

Die Datenverarbeitung sollte in allen Phasen nur mit Einwilligung des Teilnehmers erfolgen (vgl. dazu Ziff. 3).

3 Die Bedeutung der „Einwilligung“ bei der Speicherung von Teilnehmerdaten

3.1 Die Speicherung von Teilnehmerdaten in einer Form, die die Erstellung individueller Persönlichkeitsprofile gestattet, ist zu verbieten. Darüber hinaus kann in einzelnen Diensten die Speicherung besonders sensibler Daten aus dem „unantastbaren Bereich privater Lebensgestaltung“ (vgl. BVerfGE 27, 1, 7; s. a. § 27 Abs. 3 Satz 3 BDSG) grundsätzlich verboten werden. Eine Einwilligung des Teilnehmers hebt das Verbot nicht auf.

3.2 Im übrigen ist eine Speicherung von Teilnehmerdaten erlaubt

a) wenn eine gesetzliche Regelung dies zuläßt;

b) wenn der Teilnehmer seine Einwilligung gibt.

Diese Einwilligung ist nur wirksam, wenn der Teilnehmer zuvor sorgfältig über ihre Konsequenzen aufgeklärt worden ist (informed consent). Dies gilt auch für die Abwicklung von Vertragsverhältnissen.

4 Rückkanal und sonstige technische Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgegeben werden können

4.1 Nutzungsmöglichkeiten des Rückkanals und aller sonstigen technischen Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgetan werden können, sollen nach Möglichkeit gesetzlich eingegrenzt und festgeschrieben werden. Soweit Teilnehmerdaten gespeichert werden können, dürfen Sie nur zu dem Zweck verwertet werden, zu dem sie übermittelt wurden.

4.2 Persönlichkeitsprofile der Teilnehmer dürfen anhand der in der Betriebszentrale anlaufenden Kommunikationsdaten nicht erstellt werden.

Dies gilt für jede Betriebszentrale, unabhängig von der angewendeten Technologie.

4.3 Abstimmungen und Wahlen über den Rückkanal dürfen nicht durchgeführt werden.

5 Medienprivileg

5.1 Das Verhältnis des Medienprivilegs zu den Neuen Medien bedarf insgesamt einer eingehenden Untersuchung.

5.2 Dabei muß insbesondere geprüft werden,

— ob die einzelnen Neuen Medien als Presse bzw. Rundfunk anzusehen sind oder ob es sich um Medien sui generis handelt,

— in welchen Fällen nach geltendem Recht personenbezogene Daten ausschließlich zu publizistischen Zwecken verarbeitet werden,

— ob der Geltungsbereich des Medienprivilegs im Hinblick auf die für die Benutzer bestehenden Gefahren sachgerecht geregelt ist,

— falls dies bejaht wird:
Ob der Geltungsbereich zur Klarstellung gesetzlich geregelt werden soll,

— falls dies verneint wird:
Inwieweit der Geltungsbereich neu geregelt werden sollte.

Schließlich bedarf besonderer Erörterung die Gefahr, daß in Medienarchiven gespeicherte, personenbezogene Daten in die Speicherzentralen eingegeben werden und unter Berufung auf das Medienprivileg (§ 1 Abs. 3 BDSG und entsprechende Regelungen in den Ländergesetzen) frei zugänglich gemacht werden. Unter diesem Gesichtspunkt verdienen auch die im Urteil des Bundesverfassungsgerichts vom 5. Juni 1973 – 1 BvR 536/72 – (BVerfGE 35, S. 202 ff. [219 ff.] „Lebach“) aufgestellten Grundsätze zum Schutze der Persönlichkeit vor dem Zugriff der Öffentlichkeit besondere Berücksichtigung.

6 Fernmeldegeheimnis und Neue Medien

6.1 Im gesamten Netzbereich werden die zentralen Einrichtungen der Neuen Medien ebenso wie die Übertragungswege vom Fernmeldegeheimnis im Sinne von Art. 10 GG umfaßt, sofern es sich dabei um juristische Personen des öffentlichen Rechts handelt.

6.2 Folgt man der Auffassung, daß die zentralen Einrichtungen der Neuen Medien keine Fernmeldeanlagen sind, ist ein dem Fernmeldegeheimnis vergleichbares Amtsgeheimnis für den Nutzungsbereich – unter Umständen in Verfassungsrang – zu schaffen.

6.3 Die Einblicknahme in und die Übermittlung von personenbezogenen Daten aus Speichereinrichtungen einer Bildschirmtext- bzw. Kabelfernsehzentrale sind nur aufgrund gesetzlicher Regelungen unter engen, genau bestimmten Voraussetzungen zulässig. Unter Datenschutzgesichtspunkten ist es bedenklich, die Regelungen des Gesetzes zu Art. 10 GG uneingeschränkt anzuwenden.

7 Datenschutzkontrolle und Datensicherung

7.1 Die Kontrolle des Datenschutzes bei Neuen Medien sollte Aufgabe der Datenschutzbeauftragten des Bundes und der Länder sein.

7.2 Beim Anschluß von EDV-Einrichtungen durch Teilnehmer sind hinreichende technische und organisatorische Maßnahmen zu fordern, sowohl hardware- als auch softwaremäßig, z. B. Schlüsselschalter, Paßwortroutinen usw.

---

12. Konferenz, 21. Juni 1982, Stuttgart

Datenschutzrechtliche Regelungen im Staatsvertrag über Btx (Bildschirmtext)

Die Datenschutzbeauftragten der Länder und des Bundes halten auf der Grundlage ihres Beschlusses vom 11. Dezember 1980 („Grundsätze für den Datenschutz bei den Neuen Medien“) bereichsspezifische Regelungen über den Datenschutz bei Bildschirmtext für erforderlich.

Die Datenschutzbeauftragten der Länder schlagen vor, in den Entwurf eines Staatsvertrages über Bildschirmtext (Stand: 1. Juni 1982) folgende Vorschriften über den Datenschutz aufzunehmen:

1. Artikel 9 erhält folgende Fassung:

Artikel 9

(1) Soweit in diesem Staatsvertrag nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden.

(2) Wer zur Nutzung von Bildschirmtext technische Einrichtungen für andere bereitstellt (Betreiber), darf personenbezogene Daten über die Inanspruchnahme einzelner Angebote nur erheben und speichern, soweit und solange diese erforderlich sind, um

1. den Abruf von Angeboten zu übermitteln (Verbindungsdaten)
2. die Abrechnung der für die Inanspruchnahme der technischen Einrichtungen und der Angebote seitens des Teilnehmers zu erbringenden Leistungen zu ermöglichen (Abrechnungsdaten).

(3) Abrechnungsdaten nach Absatz 2 Nr. 2 sind so zu speichern, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter, von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennbar sind, es sei denn, der Teilnehmer beantragt eine andere Art und Weise der Speicherung.

(3 a) Die Übermittlung von Abrechnungs- und Verbindungsdaten an Dritte ist unzulässig.

(3 b) Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Verbindungsdaten nach Absatz 2 Nr. 1 sind nach Ende der jeweiligen Verbindung zu löschen.

(4) Absätze 2, 3, 3 a, und 3 b gelten entsprechend für Einzelmitteilungen.

(5) Für das Bereithalten personenbezogener Daten als Inhalt von Angeboten sind ohne Rücksicht darauf, ob die Daten in einer Datei verarbeitet werden, die für den Anbieter geltenden Vorschriften über den Datenschutz anzuwenden.

(6) Der Anbieter darf vom Teilnehmer personenbezogene Daten nur erheben und diese verarbeiten, wenn das Erbringen der Leistung oder die Abwicklung des Vertragsverhältnisses anderenfalls unmöglich wäre. Werden Daten des Teilnehmers vom Anbieter gespeichert oder übermittelt, ist der Teilnehmer hierauf vor der Erhebung besonders hinzuweisen. Diese Daten dürfen ohne Einwilligung des Betroffenen nur im Rahmen der Zweckbestimmung der vereinbarten Leistung verarbeitet werden. Das Erbringen der Leistung darf nicht davon abhängig gemacht werden; daß der Betroffene in die Verarbeitung seiner Daten außerhalb der in Satz 3 genannten Zweckbestimmung einwilligt. Die Einwilligung kann auch über Bildschirmtext abgegeben werden.

(7) Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsansprüche nach Datenschutzrecht richten sich gegen den Anbieter, soweit personenbezogene Daten den Inhalt von Angeboten betreffen, im übrigen gegen den Betreiber.

(8) Betreiber und Anbieter haben die technischen und organisatorischen Maßnahmen zu treffen, die über die Vorschriften der Datenschutzgesetze hinaus erforderlich sind, um sicherzustellen, daß

- die Verbindungsdaten unmittelbar nach Ende der Verbindung gem. Abs. 3 b Satz 2 gelöscht werden,
- der Teilnehmer personenbezogene Daten nur durch eine eindeutige und bewußte Handlung übermitteln kann und
- die zu Zwecken der Datensicherung vergebenen Codes einen dem Stand der Technik entsprechenden Schutz vor unbefugter Kenntnisnahme und Verwendung bieten.

(9) Die jeweils zuständigen Landesbeauftragten für den Datenschutz überwachen die Einhaltung der Vorschriften über den Datenschutz bei dem Betreiber. Die Kontrollbefugnisse sonstiger Stellen bleiben unberührt.“

2. Nach Artikel 9 wird folgender Artikel 9 a eingefügt:

„Artikel 9 a
Geheimhaltung

Die bei den Bereitstellungseinrichtung tätigen Personen sind zur Geheimhaltung der bei ihrer Tätigkeit bekanntgewordenen Tatsachen verpflichtet.“

3. In Artikel 10 wird folgender Satz angefügt:

   „Das Erheben personenbezogener Daten bei sonstigen Meinungsumfragen ist verboten."

4. Artikel 13 ist hinsichtlich der Verstöße gegen Datenschutzrecht zu ergänzen.

Im Interesse der Rechtsklarheit würden die Datenschutzbeauftragten eine eindeutige Regelung über die Trägerschaft der Bildschirmtextzentrale begrüßen, da die Anwendung der in Artikel 9 Abs. 1 genannten Datenschutzbestimmungen davon abhängt.

Ausnahmen für die Bundespost sind nur akzeptabel, wenn für sie durch Bundesrecht gleichwertige Regelungen geschaffen werden.

---

19. Konferenz, 28. März 1984, Hamburg

Zur Kabelkommunikation

In mehreren Bundesländern werden in nächster Zeit Projekte zur Einführung von Kabelrundfunk und Kabelkommunikation auf Breitbandkabel geplant oder teilweise beginnen. Angesichts der Gefahren, die für den Persönlichkeitsschutz der Teilnehmer aus dem Betrieb dieser Systeme entstehen können, haben die Datenschutzbeauftragten des Bundes und der Länder Vorstellungen über eine gesetzliche Regelung des Datenschutzes bei der Kabelkommunikation entwickelt. Sie sind dabei von den Grundsätzen für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen) ausgegangen, die auf der 7. Konferenz am 11. Dezember 1980 in Berlin beschlossen wurden.

Zur Sicherung des Datenschutzes halten sie eine gesetzliche Regelung für erforderlich, die vorbehaltlich der bei den einzelnen Projekten in den Ländern entstehenden Gestaltungsunterschiede nach dem gegenwärtigen Erkenntnisstand zumindest folgende Regelungen enthalten muß:

A
Datenschutz

Abs. 1:

Für die Erhebung, Verarbeitung und sonstige Nutzung personenbezogener Daten sind, soweit nichts anderes bestimmt ist, die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden, unabhängig davon, ob die Daten in einer Datei verarbeitet werden.

Abs. 2:

Personenbezogene Daten über die Inanspruchnahme einzelner Angebote dürfen nur erhoben und gespeichert werden, soweit und solange diese erforderlich sind, um

1. den Abruf von Angeboten zu vermitteln (Verbindungsdaten),

2. die Abrechnung der für die Inanspruchnahme der technischen Einrichtungen und der Angebote seitens des Teilnehmers zu erbringenden Leistungen zu ermöglichen (Abrechnungsdaten).

Abs. 3:

Die Speicherung der Abrechnungsdaten (Abs. 2 Nr. 2) darf Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter vom einzelnen Teilnehmer in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine andere Art und Weise der Speicherung. Die Übermittlung (Bekanntgabe) von Abrechnungs- und Verbindungsdaten an Anbieter und Dritte ist unzulässig. Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Verbindungsdaten nach Abs. 2 Nr. 1 im übrigen sind nach Ende der jeweiligen Verbindung zu löschen.

Abs. 4:

Die Abs. 2 und 3 gelten entsprechend für Einzelmitteilungen.

Abs. 5:

Für das Bereithalten personenbezogener Daten als Inhalt von Angeboten sind auf den Anbieter die für die Übermittlung geltenden Vorschriften über den Datenschutz anzuwenden und vom Anbieter zu beachten.

Abs. 6:

Der Anbieter darf vom Teilnehmer personenbezogene Daten nur erheben, wenn die Inanspruchnahme von Angeboten anderenfalls unmöglich wäre. Werden Daten des Teilnehmers vom Anbieter gespeichert oder übermittelt, ist der Teilnehmer hierauf vor der Erhebung besonders hinzuweisen. Diese Daten dürfen ohne Einwilligung des Betroffenen nur im Rahmen der Zweckbestimmung des Angebots verarbeitet werden. Der Teilnehmer ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Die Leistung darf nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung seiner Daten außerhalb der Zweckbestimmung des Angebots einwilligt. Wird die Einwilligung über den Rückkanal gegeben, so wird sie nach Bestätigung durch den Betroffenen wirksam.

Abs. 7:

Zu Zwecken der wissenschaftlichen Begleitforschung sowie zur Feststellung der Akzeptanz der Kabelkommunikation und von anderen Diensten dürfen personenbezogene Daten nur erhoben und gespeichert werden, wenn der Betroffene eingewilligt hat; über die Bedeutung der Einwilligung ist er vorher in geeigneter Weise aufzuklären. Eine weitere Datenverarbeitung ist nur zulässig, wenn die Einzelangaben so anonymisiert werden, daß sie dem Betroffenen nicht mehr zuzuordnen sind.

Abs. 8:

Personenbezogene Daten, die über Abs. 2 bis 7 hinaus im Zusammenhang mit der Kabelkommunikation erhoben und gespeichert werden, dürfen an Dritte nur übermittelt werden, wenn der Betroffene eingewilligt hat. Abs. 7 Satz 1, 2. Halbsatz findet Anwendung.

Abs. 9:

Die Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsansprüche der Teilnehmer nach Datenschutzrecht bleiben unberührt. Die Auskunftsansprüche gelten entsprechend für die gem. Abs. 5 gespeicherten Daten. Die Ansprüche nach Sätzen 1 und 2 richten sich

gegen den Anbieter, soweit personenbezogene Daten den Inhalt von Angeboten betreffen oder vom Anbieter gespeichert werden, im übrigen gegen den Betreiber. Der Teilnehmer hat ferner einen Anspruch auf Löschung der Abrechnungs- oder Verbindungsdaten, soweit der Betreiber zur Löschung gem. Abs. 3 Satz 3 und 4 verpflichtet ist.

Abs. 10:

Die bei dem Betreiber tätigen Personen sind zur Geheimhaltung der bei ihrer Tätigkeit bekannt gewordenen Tatsachen verpflichtet, soweit sie nicht offenkundig sind oder ihrer Natur nach der Geheimhaltung nicht bedürfen.

B
Fernwirkdienste

Abs. 1:

Angebote, die ferngesteuert in der Wohnung von Teilnehmern Messungen vornehmen oder andere Wirkungen auslösen (Fernwirkdienste), dürfen nur mit schriftlicher Einwilligung des Betroffenen eingesetzt werden. Dieser ist zuvor über den Verwendungszweck sowie über Art, Umfang und den Zeitpunkt des Einsatzes der Dienste zu unterrichten. Verweigert ein Betroffener seine Einwilligung, dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Kosten der Verweigerung hinausgehen. Der Betroffene kann seine Einwilligung jederzeit widerrufen.

Abs. 2:

Soweit im Rahmen von Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, wenn sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind. Im übrigen gelten die Vorschriften über den Datenschutz und über technisch-organisatorische Maßnahmen entsprechend.

Abs. 3:

Die Einrichtung von Fernwirkdiensten ist nur zulässig, wenn beim Betroffenen ein Anzeigengerät installiert ist, das jederzeit erkennen läßt, wann ein Dienst in Anspruch genommen wird und welcher Art der Dienst ist und wenn der Betroffene jederzeit den Dienst abschalten kann. Im Zweifel gilt das Abschalten eines Dienstes durch den Betroffenen als Widerruf der Einwilligung.

C
Technische und organisatorische Maßnahmen

Abs. 1:

Betreiber und Anbieter haben die technischen und organisatorischen Maßnahmen zu treffen, die über die Vorschriften der Datenschutzgesetze hinaus erforderlich sind, um die Ausführung der datenschutzrechtlichen Bestimmungen zu gewährleisten. Das Kabelnetz und seine Zusatzeinrichtungen sind nach dem Stand der Technik und Organisation so auszugestalten und zu betreiben, daß personenbezogene Daten nicht verfälscht, gestört und nicht über den in A und B genannten Umfang hinaus oder durch eine andere als die dort genannte Stelle erhoben, gespeichert oder auf sonstige Weise verarbeitet werden können.

Abs. 2:

Betreiber haben sicherzustellen, daß

1. die Verbindungsdaten unmittelbar nach Ende der Verbindung gelöscht werden,
2. der Teilnehmer personenbezogener Daten nur durch eine eindeutige und bewußte Handlung übermitteln kann,
3. die zu Zwecken der Datensicherung vergebenen Codes einen dem Stand der Technik entsprechenden Schutz vor unbefugter Verwendung bieten,
4. der Teilnehmer seine Verbindung mit dem Veranstalter jederzeit abbrechen kann. In diesem Fall sind alle bereits übermittelten Daten beim Veranstalter sofort zu löschen.

D
Meinungsumfragen

Abs. 1:

Meinungsumfragen mittels Kabelkommunikation über Angelegenheiten, die in den gesetzgebenden Organen des Bundes, der Länder, in den entsprechenden Organen der Gemeinden, der sonstigen kommunalen Gebietskörperschaften, in den Bezirksverordnetenversammlungen oder Bezirksversammlungen behandelt werden, sind unzulässig. Die Ergebnisse von Meinungsumfragen mittels Rückkanal bei den einzelnen Teilnehmern über deren Wahl- oder Stimmverhalten, die sechs Wochen vor der Wahl oder Abstimmung nicht veröffentlicht sind, dürfen vor der Wahl oder Abstimmung nicht bekannt gemacht werden.

Abs. 2:

Bei Meinungsfragen mittels Rückkanal dürfen personenbezogene Daten nur in anonymisierter Form verarbeitet werden.

E
Kontrolle

Abs. 1:

Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften über den Datenschutz.

Abs. 2:

Betreiber und Anbieter sind verpflichtet, dem Datenschutzbeauftragten zur Erfüllung seiner Aufgaben

1. die erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der ZPO bezeichneten Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde;
2. jederzeit den kostenlosen Abruf von Angeboten zuzulassen, Zutritt zu Grundstücken und Geschäftsräumen zu gewähren, dort Prüfungen und Besichtigungen zu gestatten und Einsicht in die geschäftlichen Unterlagen, in die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme nehmen zu lassen. Der Auskunftspflichtige hat die Maßnahmen zu dulden. Das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 GG, Art. 19 Abs. 2 der Verfassung von Berlin) wird insoweit eingeschränkt.

19. Konferenz, 28. März 1984, Hamburg

Zur Einführung von Bildschirmtext

Die Datenschutzbeauftragten beobachten mit Besorgnis die Entwicklung und Einführung von Bildschirmtext. Sie betonen, daß nach ihrer Ansicht den Problemen des Datenschutzes nicht genügend Aufmerksamkeit geschenkt wird. Sie haben begründeten Anlaß anzunehmen, daß die Deutsche Bundespost den von der Rundfunkkommission der Länder und den Datenschutzbeauftragten entwickelten Datenschutzbestimmungen des Bildschirmtext-Staatsvertrages nicht hinreichend Rechnung trägt.

1. Die Ministerpräsidenten der Länder haben am 18. März 1983 den Staatsvertrag über Bildschirmtext unterzeichnet. Bis auf wenige Ausnahmen sind die Zustimmungsgesetze in den Ländern in Kraft getreten.

   Die Zustimmung der Länder war abhängig von einer zufriedenstellenden Regelung des Datenschutzes.

   Die unmittelbar bevorstehende bundesweite Einführung von Bildschirmtext zwingt zur Prüfung, ob die Deutsche Bundespost die Forderungen erfüllt hat, die Grundlage der Zustimmung waren.

2. Die Deutsche Bundespost hat in ihrer Zusage offen gelassen, in welchem Umfang sie die Bestimmungen des Staatsvertrages in Bundesrecht umsetzen will. Die Ministerpräsidenten der Länder hatten eine Regelung in Form von Rechtsvorschriften erwartet. Dies ist wegen der Sensitivität der anfallenden Daten – umsomehr nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 geboten.

   Die bisher vorgenommenen Ergänzungen der Fernmeldeordnung bleiben weit hinter dem Erforderlichen zurück. Gegenüber dem Staatsvertrag fehlen insbesondere klare Regelungen zur Verarbeitung der Verbindungsdaten (Umfang der Speicherung, Zeitpunkt der Löschung).

   Darüber hinaus sollten die Bestimmungen festlegen, welche Abrechnungsdaten im Streitfall dem Anbieter übermittelt werden. Die jetzige Formulierung „im Rahmen der technischen und betrieblichen Möglichkeiten“ ist zu allgemein.

3. Die Datenschutzbeauftragten kritisieren mit Nachdruck, daß sich die Deutsche Bundespost bisher nicht in der Lage gesehen hat, ihnen das vollständige Systemkonzept für Bildschirmtext vorzulegen.

   Die zur Zeit bekannt gewordenen Elemente des Bildschirmtextsystems wecken begründete Zweifel daran, ob die Deutsche Bundespost den materiellen Bestimmungen des Staatsvertrages gerecht wird. Dies gilt insbesondere für das Verbot, Abrechnungsdaten so zu speichern, daß die Art und der Zeitpunkt des in Anspruch genommenen Angebots erkennbar sind.

20. Konferenz, 6./7. Juni 1984, Hamburg

Zur Einführung des Telefon-Fernwirksystems „TEMEX“

Bei der Deutschen Bundespost wird zur Zeit ein sogenanntes Telefon-Fernwirksystem mit der Bezeichnung „TEMEX“ vorbereitet.

Weil Fernwirksysteme erlauben, von außen in einer Wohnung Wirkungen auszulösen, Messungen vorzunehmen und Beobachtungen anzustellen, berühren sie maßgeblich die durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützte Privatsphäre und das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 GG). In diese Grundrechte darf nur in engen gesetzlichen Grenzen unter strikter Wahrung des Grundsatzes der Verhältnismäßigkeit bzw. mit ausdrücklicher Einwilligung des Betroffenen eingegriffen werden.

Um eine Verletzung dieser Grundrechte auszuschließen und ausreichenden Datenschutz zu gewährleisten, müssen vor Einführung von Fernwirkdiensten daher eindeutige gesetzliche Regelungen geschaffen werden, die auch die von der Verfassung vorgesehene Kompetenzverteilung zwischen Ländern und Bund berücksichtigt. Solange derartige bereichspezifische Regelungen fehlen, dürfen Telefon-Fernwirkdienste nicht eingeführt werden.

20. Konferenz, 6./7. Juni 1984, Hamburg

Zum Datenschutz bei Bildschirmtext

Eine effektiver Datenschutz bei Bildschirmtext ist abhängig von dem medienpolitischen Modus vivendi zwischen Bund und Ländern, der auf Konsens und gegenseitiges Vertrauen angelegt ist. Die Unterzeichnung des Staatsvertrages und dessen Ratifikation durch die Länderparlamente waren davon abhängig, daß die Deutsche Bundespost den im Staatsvertrag geregelten Datenschutz einhalten und für ihren Bereich entsprechende Vorschriften erlassen werden. Die Deutsche Bundespost hat dies schriftlich zugesagt. Die Reaktion der Deutschen Bundespost auf die Erklärung der Datenschutzbeauftragten, die an die Einlösung der Verpflichtung der Deutschen Bundespost erinnert, läßt befürchten, daß die Deutsche Bundespost sich von dieser gemeinsamen Geschäftsgrundlage für die Einführung von Bildschirmtext lösen will. Im Gegensatz zur einheitlichen Auffassung der Ministerpräsidenten vertritt die Deutsche Bundespost nunmehr die Ansicht, daß Bildschirmtext als Fernmeldedienstleistung bundesrechtlich verordnet sei und damit nach Art. 87 GG in der ausschließlichen Verwaltungskompetenz des Bundes stehe.

Die Datenschutzbeauftragten sind nach wie vor der Ansicht, daß die Länder für die gesamte Nutzung des neuen Mediums Bildschirmtext die Regelungskompetenz haben. Die Länder haben demzufolge den Datenschutz im Bildschirmtext-Staatsvertrag für

diesen Bereich abschließend geregelt. Die Auffassung der Deutschen Bundespost, Bildschirmtext sei ausschließlich ein Fernmeldedienst (vgl. Antwort des Parlamentarischen Staatssekretärs Spranger vom Bundesministerium des Innern in der Fragestunde des Deutschen Bundestages vom 14. März 1984 auf eine entsprechende Frage des Abgeordneten Dr. Hirsch F.D.P.), stimmt in mehrfacher Hinsicht mit der Bildschirmtextkonzeption nicht überein. So steht sie beispielsweise im Gegensatz zu der Tatsache, daß die Deutsche Bundespost nie ein Monopol für das Betreiben von Bildschirmtextdiensten in Anspruch genommen und entsprechenden Regelungen im Staatsvertrag nicht widersprochen hat.

Die Gefahren des neuen Kommunikationssystems für die Privatsphäre liegen in erster Linie in den technisch grundsätzlich möglichen umfassenden Sammlungen personenbezogener Daten in den technischen Einrichtungen, die zur Nutzung von Bildschirmtext bereitgestellt werden. Über diese technischen Einrichtungen wird die vollständige Kommunikation zwischen den Anbietern und Teilnehmern abgewickelt. Über diese Einrichtungen gehen alle Abrufe von Angeboten, fließen alle ausgetauschten Daten und wird die Gebührenabrechnung abgewickelt. Nutzbarkeit und Verwendungsmöglichkeit dieser Daten hängen hierbei von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab.

Angesichts dieser Gefährdung sind nach der Rechtsprechung des Bundesverfassungsgerichts durch Gesetz die organisatorischen und verfahrensrechtlichen Vorkehrungen zu treffen, um der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenzuwirken. Daher ist es unverständlich, daß die Deutsche Bundespost derzeit offenbar nicht bereit ist, entweder den Staatsvertrag für sich gelten zu lassen oder entsprechende bundesgesetzliche Regelungen zu schaffen. Spätestens seit dem Urteil des Bundesverfassungsgerichts zur Volkszählung ist die Erklärung der Deutschen Bundespost, daß sie neben Verwaltungsanweisungen auch Vorschriften erlassen werden, in verfassungskonformer Weise nur als Verpflichtung zu verstehen, Rechtsnormen zu schaffen. Da die Deutsche Bundespost den Staatsvertrag nicht unmittelbar für sich gelten läßt, bestehen Regelungslücken im Bundesrecht. Die Bundespost würdigt nicht in ausreichendem Maße, daß die verschärfte Datenschutzregelung im Staatsvertrag den erhöhten Gefahren begegnen und den eventuell vorhandenen Ängsten der Bevölkerung Rechnung tragen sollte.

Eine Regelung des Datenschutzes bei Bildschirmtext kann sich nicht in einer einseitigen Verpflichtungserklärung der Deutschen Bundespost gegenüber den Ländern, in Verwaltungsanweisungen oder in Vorkehrungen im technisch-betrieblichen System erschöpfen. Selbst das Fernmeldegeheimnis – dessen Reichweite bei Bildschirmtext nicht unbeschritten ist – befreit nicht von der Notwendigkeit, zusätzliche grundrechtssichernde gesetzliche Regelungen zu schaffen, die den besonderen Gefahren begegnen. Aus der Mitwirkung der Datenschutzbeauftragten bei der Schaffung der Datenschutzvorschrift im Staatsvertrag folgt eine Verantwortung gegenüber Landesregierungen und Landesparlamenten für eine ausreichende Berücksichtigung des Persönlichkeitsschutzes bei der Einführung von Bildschirmtext. Die Datenschutzbeauftragten mußten darauf vertrauen, daß die Deutsche Bundespost die den Ministerpräsidenten gegenüber abgegebene Verpflichtung einhält und ungeachtet kompetenzrechtlicher Meinungsverschiedenheiten alles tut, was für eine effektive Umsetzung der Bestimmungen des Staatsvertrages notwendig ist. Hierzu gehören eine umfassende Information über die technischen Komponenten des Bildschirmtextsystems, die vollständige Umsetzung der Datenschutzvorschriften des Staatsvertrages für die Einrichtungen der Deutschen Bundespost und die Ermöglichung einer effektiven Datenschutzkontrolle durch die zuständigen Verwaltungsbehörden der Länder. Dabei verlangt die enge Verflechtung von Netz- und Nutzungsbereich, daß alle Kontrollinstitutionen fortlaufend, unmittelbar und umfassend über die technische Ausgestaltung und Wirkungsweise des Bildschirmtextsystems unterrichtet werden.

Mit einer Information aus zweiter Hand können die Datenschutzinstanzen der Länder ihrer Verpflichtung nicht nachkommen. Die Kontrolle durch unabhängige Datenschutzinstanzen ist eine wesentliche Voraussetzung eines wirksamen Grundrechtsschutzes.

Zu den nach Ansicht der Deutschen Bundespost bereits verwirklichten technisch-organisatorischen Vorkehrungen zum Schutze des Persönlichkeitsrechts der Bürger kann noch nicht abschließend Stellung genommen werden. Zwar hat die Deutsche Bundespost inzwischen mündlich die Datenschutzbeauftragten über das technische System Bildschirmtext unterrichtet, eine schriftliche Verfahrensbeschreibung einschließlich alle Datensätze steht noch aus. Erst wenn diese vorliegt, können die Datenschutzbeauftragten zum technischen System Bildschirmtext abschließend Stellung nehmen. Die Datenschutzbeauftragten sind jederzeit bereit, Datenschutzfragen des Bildschirmtextsystems mit der Deutschen Bundespost zu erörtern.

---

35. Konferenz, 10./11. Oktober 1988, Mainz

Aktuelle Probleme des Datenschutzes in der Telekommunikation

Mit Inkrafttreten der Telekommunikationsordnung am 1. Januar 1988 hat die Deutsche Bundespost den Übergang von bisher getrennten Fernmeldenetzen zu einem einzigen, diensteintegrierten digitalen Telekommunikationsnetz für die Übermittlung aller Nachrichtenarten eingeleitet; künftig fallen an zentralen Stellen erheblich mehr und leichter auswertbare personenbezogene Daten an als bisher, die je nach Dienstart mehr oder weniger präzise Rückschlüsse auf das Verhalten der Teilnehmer erlauben. In der Telekommunikationsordnung wurden die Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Verbesserung des Datenschutzes und zur Beherrschung der möglichen Risiken bisher leider nur zum Teil befolgt.

Auch das Bundesdatenschutzgesetz kann mit seinen allgemeinen Vorschriften die Risiken nicht auffangen; dies gilt auch für die bisher bekanntgewordenen Novellierungsentwürfe. Hier bedarf es weiterer spezieller Regelungen. Bei der Novellierung des Bundesdatenschutzgesetzes muß vor allem sichergestellt werden, daß sämtliche beim Einsatz neuer Telekommunikationstechniken und -dienste anfallenden Daten in den Geltungsbereich des Gesetzes fallen. Deshalb muß z. B. selbstverständlich sein, daß alle personenbezogenen Daten aus der Bild-, Sprach-, Text- und Datenübertragung geschützt werden. Die Regelung der Zulässigkeit der Verarbeitung personenbezogener Daten, deren Kontrolle und der erforderlichen technisch-organisatorischen Maßnahmen müssen an die neuen technischen Gegebenheiten angepaßt werden.

Das Grünbuch der europäischen Gemeinschaften über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte zeigt, daß der Datenschutz bei der geplanten Liberalisierung des Angebots von

Dienstleistungen und Geräten nur unzureichend berücksichtigt wird. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist nachdrücklich darauf hin, daß der nationale Datenschutz nicht durch ein Gemeinschaftsrecht überlagert werden darf, das im Ergebnis zu weniger Datenschutz führt als das nationale Recht. Die frühzeitige Einbindung des Datenschutzes in die jetzt folgenden Beratungen – auch auf EG-Ebene – ist daher dringend erforderlich.

Die Länder sind im Rahmen ihrer Zuständigkeit zum Erlaß von Regelungen zur Nutzung der Telekommunikation verpflichtet, auch die notwendigen Datenschutzvorschriften zu erlassen. Der Bildschirmtext-Staatsvertrag kann hierzu als Vorbild dienen. In einem derartigen Staatsvertrag müssen auch die materiellen Voraussetzungen zum Betrieb privater Telekommunikationsdienste und deren Zulassung geregelt werden.

40. Konferenz, 4./5. Oktober 1990, Kiel

Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes

Wegen der dynamischen technischen Entwicklung auf dem Gebiet der Telekommunikation ist es dringlich, das Grundrecht auf freie Entfaltung der Persönlichkeit gegen neue Gefährdung zu schützen. Den Risiken für das Recht auf unbeobachtete Kommunikation muß rechtzeitig begegnet werden:

- Die Einführung von ISDN macht es möglich, daß auch nach Beendigung von Telefongesprächen über einen bestimmten Zeitraum gespeichert wird, wer wann mit wem wie lange telefoniert hat.
- Der zunehmende Einsatz von Funkdiensten im Telekommunikationsverkehr (z. B. mobile Telefone, Satellitenkommunikation) ist mit der Speicherung von noch mehr Daten über die Telefonverbindungen verbunden und erleichtert die Möglichkeit des Abhörens und Aufzeichnens der Gesprächsinhalte.
- Zunehmend stehen Abhöranlagen zur Verfügung, mit denen aus der Masse der geführten Telefongespräche bestimmte Telefonate gezielt herausgegriffen, aufgezeichnet und nach bestimmten Gesichtspunkten ausgewertet und gespeichert werden können.

Das Grundgesetz läßt Einschränkungen des Fernmeldegeheimnisses unter gewissen Voraussetzungen auf gesetzlicher Grundlage zu. In den vergangenen Jahren hat der Gesetzgeber diese Eingriffsmöglichkeiten mehrmals erweitert und hierbei alle Telekommunikationsdienste (wie z. B. Telefax und Btx) einbezogen. Zudem hat die Rechtsprechung den Anwendungsbereich extensiv ausgelegt. Vor diesem Hintergrund ist es erforderlich:

- Die gesetzlichen Regelungen präziser und enger zu fassen,
- bei Entwicklung, Auswahl und Einsatz von Telekommunikationstechniken darauf zu achten, daß bei deren Betrieb die Speicherung personenbezogener Daten nach Dauer und Umfang auf das wirklich Notwendige beschränkt wird,
- erlaubte Eingriffe in das Grundrecht nach Artikel 10 auf das unerläßliche Maß zu beschränken und eine strenge Zweckbindung der dabei gewonnenen Daten sicherzustellen,
- eine wirksame Kontrolle solcher Eingriffe durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.

Neben die Ausweitung der Möglichkeit der Überwachung der Telekommunikation treten zunehmend weitere Techniken der heimlichen Datenerhebung (z. B. durch Videoaufnahmen, Abhörgeräte, Richtmikrofone), durch die das Recht auf ungestörte Kommunikation auch außerhalb des Fernmeldebereiches gefährdet ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, daß der Gesetzgeber diesen Gefährdungen des Rechts auf informationelle Selbstbestimmung seine Aufmerksamkeit zuwendet. Sie unterstützt in diesem Zusammenhang die Einwände der Bundesregierung in deren Stellungsnahme zum Gesetzentwurf des Bundesrates zur Bekämpfung der organisierten Kriminalität. Die Datenschutzbeauftragten sehen in der Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes einen Schwerpunkt ihrer weiteren Arbeit.

41. Konferenz, 8. März 1991, Bonn

Telekommunikation und Datenschutz

I.

Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutsche Telefone werden monatlich rund drei Milliarden Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderungen des Datenschutzes, das „Grundrecht auf unbeobachtete Kommunikation“ zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 1. Juli 1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, „Rechtsverordnungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten“ zu erlassen. Der Ausschuß für Post und Telekommunikation und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnisses angemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV) und über den Datenschutz für Unternehmen, die Telekommunika-

tionsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.

Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindungsdaten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost TELEKOM festgehalten werden, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) sollen Kunden – auch Arbeitgeber – auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.

Die Datenschutzbeauftragten fordern:

1. Alle – durch die computergesteuerte Vermittlungstechnik entstehenden – Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe unverzüglich zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind. Auf Antrag des Kunden darf zur Prüfung der Richtigkeit des in Rechnung gestellten Entgelts oder zur Erstellung eines Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

   Die Entscheidung des Kunden über die Form der Abrechnung muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von „Kommunikationsprofilen“, die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige der Rufnummer des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall „auf Knopfdruck“ zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen – zum Beispiel zur Aufklärung telefonischer Bedrohungen oder in Notfällen – müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigt ihre Forderung (Beschluß vom 4./5. Oktober 1990), Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Art. 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung – schon aus Gründen der Normenklarheit – in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

---

44. Konferenz, 1./2. Oktober 1992, Stuttgart

„Lauschangriff“

Die Datenschutzbeauftragten des Bundes und der Länder erklären (bei Gegenstimme des LfD Bayern):

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sogenannter „Lauschangriff“) zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum“ verbleiben, in dem er „sich selbst besitzt“ und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt“ (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung – insbesondere heimlicher – entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlich-

keitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.

3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z. B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

44. Konferenz, 1. / 2. Oktober 1992, Stuttgart

Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen – auch wenn sie von einem Dienstapparat aus geführt werden – unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen – insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind – umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

— Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.

— Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z. B. bei Feuerwehr und Rettungsdiensten).

— Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.

— Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.

— Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.

— Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

B. Beschlüsse der Internationalen Konferenz der Datenschutzbeauftragten

Resolutions of the International Conference of Data Protection Commissioners

5. Konferenz, 18. Oktober 1983, Stockholm

Neue Medien

Die Internationale Konferenz der Datenschutzbeauftragten geht übereinstimmend davon aus, daß der Einsatz Neuer Medien, die über Kabelnetze verbreitet werden, eine erhebliche Gefährdung für die Persönlichkeitsrechte mit sich bringen kann.

Soweit bei den Neuen Medien die Kommunikation zwischen Informationsanbietern und Teilnehmern durch elektronische Datenverarbeitungsanlagen gesteuert wird, ist – im Gegensatz zu herkömmlichen Medien – die Speicherung personenbezogener Daten in einem gewissen Umfang erforderlich.

So werden beim Medium „Bildschirmtext“ (Videotex) Verbindungs- und Abrechnungsdaten gespeichert. Bei manchen Diensten werden die vom Teilnehmer abgerufenen Sendungen registriert. Das Recht der Unverletzlichkeit der Wohnung wird berührt, wenn mit neuen Diensten von außen in den Wohnungen Wirkungen ausgelöst und Messungen vorgenommen werden.

Über die auf diese Weise an zentralen Stellen automatisiert entstehenden Sammlungen personenbezogener Daten könnten Persönlichkeitsprofile aller Benutzer erstellt werden. Deren soziale Beziehungen und Verhaltensweisen können damit zum Gegenstand von Maßnahmen gemacht werden.

Darüber hinaus können mit Hilfe der neuen Medien personenbezogener Daten jeglicher Art mit geringem Aufwand und in großem Umfang verbreitet werden. Erfahrungen mit Bildschirmtext haben gezeigt, daß Anbieter und Benutzer mißbräuchlich sensible Daten über die Neuen Medien veröffentlichen.

5th Conference, 18th October 1983, Stockholm

New Media

There was consensus at the International Conference of Data Protection Commissioners that the application of the new media, which will be circulated by cable networks, might well be accompanied by considerable danger to the individual’s rights to privacy.

As far as communication between information providers and subscribers is controlled by electronic data processing systems, a certain amount of personal data needs to be stored, which is not the case with traditional media.

Videotex is a good example of this where call and accounting data are stored. Some services register transmissions called up by subscribers. The right to inviolability of an individual’s privacy at home is infringed upon if the new services are able to induce effects in the home from any remote location and whenever measurements are made.

Personal data which automatically collected at central places in this manner can be used to draw up individual profiles of all users. Users’ social relations and patterns of behaviour can in this way be made object of other measures.

In addition to the above, the new media can be used to circulate at little expense copious quantities of all kinds of private data. Experience with videotex has indicated that providers and users misuse sentitive data making it public over the new media.

7. Konferenz, 26. September 1985, Luxemburg

Datenschutz und Neue Medien

1. Die Internationale Konferenz der Datenschutzbeauftragten hat am 18. Oktober 1983 auf ihrer Sitzung in Stockholm einen Beschluß zum Thema Neue Medien gefaßt, in dem gefordert wurde, daß durch geeignete Maßnahmen, insbesondere der Gesetzgebung, in jedem Land die Betriebsbedingungen so gestaltet werden, daß durch den Einsatz der Neuen Medien Persönlichkeitsrechte nicht beeinträchtigt werden.
2. Die Weiterentwicklung der Neuen Medien in den einzelnen Staaten bestätigt einerseits die Notwendigkeit der Forderungen, zeigt aber andererseits auch zusätzliche Gefährdungen auf.
   - —Die internationale Standardisierung der Telekommunikationsdienste und die zunehmende grenzüberschreitende Vernetzung der Systeme machen internationale Vereinbarungen auch über den Datenschutz bei neuen Informations- und Kommunikationsdiensten dringlich.
   - —Der beginnende Aufbau von Glasfasernetzen, die anstehende Einführung der Breitbandkommunikation und die Integration der einzelnen Telekommunikationsdienste, verbunden mit der Digitalisierung von schmal- und breitbandigen Übertragungsnetzen werden zu einer erheblichen Zunahme der Informationsströme führen. Gleichzeitig werden Integration und Digitalisierung zu einer besseren Auswertbarkeit mit Hilfe automatischer Anlagen führen und damit die Gefahr des unbefugten Aufzeichnens und Auswertens der übermittelten Informationen erhöhen.
   - —Der Einsatz von Satelliten zur Kommunikation schafft im Hinblick auf die Datenintegrität und den Schutz von unbefugtem Abhören ebenfalls Risiken.
3. Die anläßlich des Erfahrungsaustausches versammelten Vertreter der nationalen Datenschutzinstitutionen appellieren daher an die internationale Konferenz der Datenschutzbeauftragten, den in ihrem Beschluß vom 18. Oktober 1983 enthaltenen Forderungen gegenüber den nationalen Regierungen Nachdruck zu verleihen und auf eine Verstärkung der internationalen Zusammenarbeit bei der Überwachung Neuer Medien hinzuwirken.

7th Conference, 26th September 1985, Luxembourg

Data Protection and New Media

1. At its meeting in Stockholm on 18th October 1983, the International Conference of Data Protection Commissioners passed a resolution on the subject of the new media. This resolution demands that suitable measures, in particular, legislation, be taken in each country to ensure that operating conditions be organised in such a way that the application of the new media in no way encroaches upon the individual's rights to privacy.
2. The further development of the new media in individual countries confirms the need for such demands; it also indicates additional dangers, however:
   - —International standardisation of telecommunications services and increasing transnational networking of systems make international agreements on data protection, too, with regard to new information and communication services a matter of utmost urgency.
   - —The beginning construction of optical fibre networks, the imminent introduction of broadband communication, and the integration of individual telecommunication services in conjunction with the digitalisation of narrow- and broadband transmission networks will lead to a considerable increase in information streams. At the same time, integration and digitalisation will lead to an improved ability to evaluate with the help of automatic systems. This will be accompanied by the increased danger of unauthorised recording and evaluating of transmitted information.
   - —The use of satellites for communication likewise induces risks with regard to data integrity and protection against unauthorised monitoring.
3. The representatives of the national data protection organisations, convened to exchange experience, therefore appeal to the International Conference of Data Protection Commissioners to draw the attention of national governments to the demands contained in their resolution of 18 October 1983, and to do all in their power to increase international cooperation in monitoring the new media.

9. Konferenz, 24. September 1987, Oslo

Neue Medien

1. Die Internationale Konferenz der Datenschutzbeauftragten beobachtet seit Jahren die Entwicklung der Neuen Medien und die damit verbundenen Probleme des Datenschutzes. Sie hat mit ihren Entschließungen vom 18. Oktober 1983 in Stockholm und vom 26. September 1985 in Luxemburg Forderungen zur Verbesserung des Datenschutzes erhoben.
2. Der Stand der Massenmedien und Telekommunikation im Jahre 1987 ist durch folgende Merkmale gekennzeichnet:
   - —Die verschiedenen für die Telekommunikation genutzten analogen und digitalen Einzelnetze streben nach einer Vereinheitlichung der technischen Normen; zunehmend entstehen einheitliche nationale Infrastrukturen für die Telekommunikationsnetze.
   - —Dienste für die Verbreitung von Massenmedien und für andere Telekommunikationsformen verschiedenster Art werden auf diesen Netzen national und international angeboten.
3. Die Internationale Konferenz der Datenschutzbeauftragten ist besorgt über die Sammlung einer zunehmend größeren Anzahl von personenbezogenen Daten durch Massenmedien und Telekommunikationsdienst. Die Risiken sind offensichtlich, die in einer derartigen Kumulation von Daten und deren möglichen Gebrauch zu Zwecken liegen, die nicht mit den Zwecken übereinstimmen, für die sie erhoben wurden. Soweit keine anonymen Nutzungsformen eingeführt werden, ermöglicht die über die ursprünglichen Kommunikationszwecke hinausgehende Verarbeitung derartiger Informationen den Aufbau von Daten über die Lebensführung und Interessen von Einzelindividuen und Familien. Eine solche Entwicklung wird als keineswegs wünschenswert angesehen.

   Die Informationen konzentrieren sich letztlich bei wenigen öffentlichen und privaten Netzbetreibern und Kommunikationsanbietern (Post, Teleports, internationale Serviceunternehmen). Die Risiken des Mißbrauchs, der Sabotage und Spionage sowie der Manipulation bürden diesen Institutionen eine erhebliche Verantwortung auf, ohne daß in den meisten Ländern die nationalen Gesetze hinreichende rechtliche Regelungen hierfür vorsehen.
4. Die Internationale Konferenz der Datenschutzbeauftragten fordert deshalb nachdrücklich die Entwicklung von Regelungswerken auf nationaler und internationaler Ebene. Für die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung sind internationale Normen anzustreben. Die Zusammenarbeit der nationalen Kontrollinstanzen ist zu verbessern.

New Media

1. For several years the International Conference of Data Protection Commissioners have been following the development of the New Media and the data protection problems it entails. In its resolutions of 18 October 1983 in Stockholm and of 26th September 1985 in Luxembourg it raised demands for the improvement of data protection in this connection.

2. The state of mass media and telecommunications in 1987 is marked by the following features:
   — The various analogous and digital individual networks used for telecommunications tend towards uniformity of technical standards; there is an trend towards national telecommunication network infrastructures.
   — The services of the mass media and other forms of telecommunication services of different kinds are offered nationally and internationally by these networks.

3. The International Conference of Data Protection Commissioners is concerned about the collection of an inscreasingly greater quantity of personalized data by the mass media and telecommunication services. The risks inherent in such an accumulation of data and its potential use for purposes other than those for which the data were obtained are obvious. Unless anonymous procedures for the use of such services will be introduced, the processing of such information beyond its original purposes could enable the building up of files of life styles and interests of individuals and families. Such a development is considered entirely undesirable.

   Informations is ultimately concentrated within the control of a few public and private network operators and providers of communication services (the postal administration, teleports, international service providers). The risks of abuse, sabotage and espionage, etc., as well as manipulation, constitute a considerable burden of responsibility for these institutions without there being national legislation containing sufficient legal provisions in most countries.

4. The International Conference of Data Protection Commissioners, therefore, emphatically demands the development of regulatory systems on a national and international level. International standards should be sought for the technical and organisational measures required to provide data protection. Cooperation between national control institutions should be further improved.

Berliner Resolution

Die Telekommunikation befindet sich weltweit in einer raschen Entwicklung. Über internationale Datennetze werden in wachsendem Umfang auch personenbezogene Daten transferiert, etwa im Zusammenhang mit der Verwendung von Kreditkarten, bei Reise-Buchungs-Systemen und innerhalb multinationaler Unternehmen. Die Nutzung dieser Technologie kann bedeutende Vorteile mit sich bringen. Aber zugleich wird es schwieriger, die Rechte derer zu schützen, deren persönliche Daten rund um die Welt übermittelt werden.

Der Europarat, die OECD, die Vereinten Nationen und weitere internationale Organisationen haben Empfehlungen und Leitlinien zum Datenschutz verabschiedet. Sie enthalten einen gemeinsamen Bestand von Grundsätzen für eine faire Praxis, wie sie etwa in der Konvention des Europarats (Konvention Nr. 108) und in den OECD-Leitlinien zum Ausdruck kommen. Sie bezwecken den Schutz der Privatheit des einzelnen.

Bisher haben sich acht Staaten durch Beitritt zur Konvention des Europarats international verpflichtet, einen bestimmten Datenschutzstandard einzuhalten. Die Datenschutz-Kontrollinstanzen dieser Länder haben in gewissem Umfang die Befugnis, den grenzüberschreitenden Datenfluß zu kontrollieren, wenn dies zum Schutz einzelner nötig ist. Bei dieser Kontrolle ergeben sich allerdings schwerwiegende praktische Probleme. Datenübermittlung ins Ausland bedeutet deshalb für den einzelnen in der Mehrzahl der Fälle, daß er nicht mehr die Gewißheit haben kann, daß die Grundsätze, die in nationalen Gesetzen und in den verschiedenen internationalen Übereinkommen festgelegt sind, auf seine oder ihre Daten angewandt werden. Zum Beispiel kann es dann keine Garantie geben, daß die Daten auf dem neuesten Stand und genau sind und nur für bestimmte Zwecke verwendet werden. Der einzelne kann auch sein Recht, einen Datenschutzbeauftragten anzurufen, nicht wahrnehmen.

Das Problem eines wirksamen internationalen Datenschutzes läßt sich nur durch gleichwertige gesetzliche Sicherungen in den übermittelnden und empfangenden Ländern lösen. Diese Lösung wird auch von den oben genannten Empfehlungen und Leitlinien vorgezeichnet.

Nach Auffassung der Datenschutzbeauftragten muß bei der Entwicklung und Nutzung internationaler Datendienste dem Datenschutz die gleiche Priorität gegeben werden wie der Förderung der Datenverarbeitung und der Telekommunikation. Sie empfehlen deshalb:

— Die Regierungen sollten sowohl einzeln als auch im Rahmen internationaler Organisationen darauf hinarbeiten, daß so bald wie möglich gleichwertige gesetzliche Sicherungen geschaffen werden.

— Wer personenbezogene Daten über die Grenzen vermittelt, muß den Schutz beim Empfänger prüfen, daß die Beachtung der Rechte der Betroffenen tatsächlich sichergestellt wird.

Das Ziel dieser Maßnahmen muß sein:

— Die Datenschutzgrundsätze der Konvention Nr. 108 und der OECD-Leitlinien werden unabhängig von einer grenzüberschreitenden Übermittlung gewährleistet;

— International operierende Datenverarbeitungssysteme müssen so aufgebaut sein, daß der Einzelne ohne unzumutbare Schwierigkeiten seine Datenschutzrechte wahrnehmen kann;

— Berichtigungen, Aktualisierungen und Löschungen von Daten müssen auch im Ausland nachvollzogen werden, wenn die Daten zuvor dorthin übermittelt worden sind;

— Die durch den internationalen Datenaustausch erhöhten Gefahren für das Recht des einzelnen, über die Verwendung ihrer Daten zu bestimmen, müssen durch internationale Zusammenarbeit der Datenschutzbeauftragten ausgeglichen werden.

11th Conference, 30th August 1989, Berlin

Berlin Resolution

World-wide telecommunications are evolving rapidly. International data networks are increasingly used for transfers of personal data, for instance in the use of credit cards, for the purposes of travel booking systems and within multinational enterprises. The use of this new technology can bring significant benefits. But it also increases the problem of safeguarding the position of those individuals whose details are transmitted around the world.

The Council of Europe, the OECD, the United Nations and other international organisations have adopted recommendations and guidelines on data protection. A common feature is a set of principles of good practice such as those in the Council of Europe Convention (Treaty 108) and in the OECD guidelines. These good practices are designed to safeguard the privacy of individuals.

So far, eight states have acceded to the Council of Europe Convention and so committed themselves internationally to legally established data protection standards. Data protection authorities in those countries have some authority to control the transborder flow of personal data when this is necessary to protect individuals. However, controlling transborder data flows in this way presents severe practical problems. In most cases, therefore, data transmission across national borders implies that the individual can no longer ensure that the principles laid down by national laws and the various international agreements will be applied to his or her data.

For example there can be no guarantee that the data are up to date, accurate, and used only for proper purposes; and the individual loses the opportunity to appeal to any data protection commissioner.

The solution to giving effective international protection to personal data lies in equivalent legal safeguards in the transmitting and receiving countries. This solution is consistent with the international recommendations and guidelines referred to above.

The Data Protection Commissioners believe that data protection should be given the same priority as the promotion of data processing and telecommunications in the development and use of international data services. They therefore recommend that:

— Governments should move rapidly both individually and through international bodies towards establishing equivalent legal safeguards as soon as possible.

— Those transmitting personal data across national boundaries should check and monitor the protection given to such data by those receiving them, with a view to ensuring that proper regard will be given to the position of individuals.

The objective of these actions should be to ensure that:

— The Basic Principles for Data Protection contained in Treaty 108 and in the OECD guidelines are guaranteed to an individual notwithstanding the transfer of his data across national boundaries;

— Internationally operated data processing systems are structured in such a way that the individual can safeguard his data protection rights without undue difficulty;

— Any correction, up-dating and erasure applied to data which have previously been transmitted abroad will also be applied to the transferred data in any foreign country concerned;

— The greater risks, entailed by international exchanges of data, to the rights of individuals to decide on the use to be made of their data are counterbalanced by international co-operation among data protection commissioners.

11. Konferenz, 30. August 1989, Berlin

Zusatzerklärung der Datenschutzbeauftragten der EG-Länder

Die Datenschutzbeauftragten der Länder der Europäischen Gemeinschaft sind der Überzeugung, daß die Existenz und die Aktivitäten der Gemeinschaft einerseits besondere Vorkehrungen des Datenschutzes erforderlich machen, andererseits aber auch verbesserte Möglichkeiten bieten, den Datenschutz über nationale Grenzen hinaus wirksam zu machen.

— Der für Ende 1992 angestrebte EG-Binnenmarkt ist auf den freien Austausch von auch personenbezogenen Informationen gerichtet, etwa in den Bereichen Direktmarketing/Adressenhandel und Kreditinformation.

— Entscheidungen der Europäischen Gemeinschaft verpflichten in zunehmendem Umfang die Mitgliedsländer zur Erhebung und Verarbeitung personenbezogener Daten – so etwa im Bereich der Landwirtschaftsstatistik – und zur grenzüberschreitenden Datenübermittlung – so beispielsweise im Umwelt-, Gesundheits- und Sozialbereich.

— Einige Länder der Europäischen Gemeinschaft arbeiten an einem Pilot-Projekt für gemeinsame polizeiliche Fahndungsdateien (Schengener Informationssystem) – gewissermaßen als Ersatz für die wegfallenden Kontrollen an den Binnengrenzen.

— Die Einrichtungen der EG selbst führen zunehmend personenbezogene Datenbanken. Diese Einrichtungen unterliegen jedoch keinem Datenschutzgesetz und sind daher nicht an die Grundsätze des Datenschutzes gebunden.

Die Europäische Gemeinschaft und ihre Mitgliedstaaten werden aufgefordert, in ihre Planungen für „Europa '92" die Notwendigkeit eines umfassenden und konsistenten Ansatzes zur Verwirklichung der Grundsätze des Datenschutzes in den Mitgliedsländern und in bezug auf die Aktivitäten der Gemeinschaft selbst einzubeziehen.

Im einzelnen schlägt die Konferenz vor:

— Durch entsprechende Rechtsakte der Europäischen Gemeinschaft sollten die Grundsätze der Europaratskonvention 108 für alle Mitgliedsstaaten ebenso wie für die Institutionen der EG selbst verbindlich gemacht werden.

— Eine unabhängige Datenschutzkontrollinstanz sollte eingerichtet werden. Sie sollte die Einrichtungen der EG in allen Datenschutzfragen beraten, die Verarbeitung personenbezogener Daten innerhalb der Einrichtungen der EG kontrollieren, Eingaben von Betroffenen entgegennehmen und mit den nationalen Datenschutzorganen zusammenarbeiten.

Die Commission Nationale de l'Informatique et des Libertés (die französische Datenschutzkommission) wird gebeten, diese Vorschläge alsbald dem Vorsitzenden des Ministerrats sowie den Präsidenten des Europaparlaments und der EG-Kommission zu unterbreiten und um Unterstützung zu werben.

11th Conference, 30th August 1989, Berlin

Additional Statement by the Data Protection Commissioners of the European Community (EC) Nations

The Data Protection Commissioners of the European Community Nations believe that the existence and the activities of the Community give rise both to particular requirements for data protection and to increased opportunities for making data protection effective across national boundaries.

— The EC internal market to be achieved by the end of 1992 is oriented towards the free exchange of information, including personal information, for instance in the fields of direct marketing/address trading and credit reporting.

— European Community decisions increasingly call for the collection and processing of personal data to be carried out by member nations, for instance in the field of agricultural statistics. They also call for transborder data transmission, for instance in the environmental, health-care and social fields.

— Some Community nations are already working on a pilot project to establish common police „wanted persons" files (the Schengen Information System) to provide a substitute, as it were, where controls at internal frontiers are to be abolished.

— On a growing scale, personal information data bases are maintained by the European Community institutions themselves. However, these institutions are not subject to data protection legislation and hence to any requirement to meet the Basic Principles for Data Protection.

The European Community and its member nations are therefore urged to take full account, in their planning for "Europe 1992", of the need for a complete and consistent approach to implementation of the Basic Principles for Data Protection across Community nations and within community activities.

The detailed proposals put forward by the European Community Commissioners are as follows:

— Appropriate legal instruments should ensure that the Basic Principles of Data Protection contained in the Council of Europe Convention (Treaty 108) will be binding on all member nations and on the EC institutions themselves;

— An independent data protection authority should be established to advise the EC institutions on all data protection issues and to supervise the processing of personal data within these institutions. It should consider complaints from individual data subjects and co-operate with the national data protection bodies.

The Commission Nationale de l'Informatique et des Libertés (the French Data Protection Commission) is invited to submit these proposals to the Presidents of the Council of Ministers, of the European Parliament and of the EC Commission as soon as possible and to try to gain their support.

11. Konferenz, 30. August 1989, Berlin

Entschließung über die Arbeitsgruppe Telekommunikation und Medien

Die Ausarbeitung des Entwurfs für eine Entschließung war Anlaß zu einem sehr nützlichen Informationsaustausch zwischen den teilnehmenden Delegationen.

Die Empfehlungen und Entscheidungen, die wir in unseren jeweiligen Ländern ausgesprochen bzw. getroffen haben, sollten die internationale Dimension der Netze und Dienstleistungen berücksichtigen.

Die Informationen über die Entwicklungen, die sich jenseits unserer Grenzen vollziehen, dürfen uns nicht ausschließlich von unseren nationalen Organen übermittelt werden.

Die Netze und Dienstleistungen werden in unseren jeweiligen Ländern nicht gleichzeitig bzw. im selben Rhythmus weiterentwickelt.

Unsere Erfahrungen haben gezeigt, daß die Effizienz des Datenschutzes in diesem Bereich – über die Prinzipien hinaus – auf praktischen Maßnahmen beruht, über die von den nationalen Verwaltungsinstanzen Informationen nicht leicht zu erhalten sind.

Daher beschließt die Konferenz, daß diese Arbeitsgruppe ihre Arbeit in Berlin fortsetzt und daß nach Möglichkeit jede Delegation ihre Erfahrungen, insbesondere in folgenden Bereichen, einbringen sollte:

— detaillierte Rechnungslegung

— Modalitäten zur Aufnahme in die Teilnehmerverzeichnisse, Verwendung der Teilnehmerverzeichnisse

— verschiedene Kategorien der Telematischen Dienste (elektronische Post, Fernkäufe, Informationsdienste usw.)

— Fernmeßverfahren

— ISDN

— Zelluläres Telefon (digitaler Mobilfunk)

— automatische Anrufeinrichtungen

— Sicherheit der Netze

— Kabelnetze für Dialogfernsehen.

11th Conference, 30th August 1989, Berlin

Resolution about the Working Group on Telecommunications and Media

When drafting the resolution on ISDN the delegation had a first, fruitful exchange of information.

When we express opinions or make decisions on our countries, we have to take into account the international dimension of telecommunication networks and services.

Information on events taking place beyond our national borders can not be provided to us by our national operators only.

Networks and services do not always develop at the same time and at the same place in our countries.

Experience has shown that the efficiency of data protection in this field depends – beyond mere principles – on practical measures and this is not always easy to obtain from our national operators.

This is why the Conference agrees that this Working Group should continue its work in Berlin.

Each delegation should have the opportunity to present its experiences in detail (analysis of the problems, possible solutions, adopted solutions) particular in the following fields:

— detailed bills

— provisions regarding the listing of subscribers in directories and the use of directories

— the different categories of telematic services (electronic mail, teleshopping, information services)

— telemetry

— ISDN

— cellular telephone (digital car telephone)

— automatic prerecorded message device

— network security

— interactive TV cable networks.

11. Konferenz, 30. August 1989, Berlin

Beschluß zu ISDN auf Vorschlag der Arbeitsgruppe Telekommunikation und Medien

Die nationale und internationale Entwicklung der Telekommunikation ist derzeit gekennzeichnet durch die Einführung diensteintegrierender, digitalisierter Netze. Diese sind die Träger vielfältiger Dienste.

Die Entwicklung führt sowohl für die Netzträger als auch für die Diensteanbieter zur Verarbeitung von erheblich mehr personenbezogenen Daten, als dies bei bisherigen Netzen der Fall war. Diese Situation erfordert nationale und internationale Vorkehrungen zum Schutz personenbezogener Daten.

Die Internationale Konferenz der Datenschutzbeauftragten stellt fest, daß hierzu erhebliche Anstrengungen erforderlich sind. Insbesondere darf der Datenschutz nicht als Hindernis für die Entwicklung des Internationalen Informationsmarktes gesehen werden, sondern er stellt vielmehr eine notwendige Ergänzung der technischen Entwicklung dar, die für die Akzeptanz der neuen Telekommunikationstechnologien unerläßlich ist, er stellt vielleicht sogar ein beschleunigendes Element dieser Entwicklung dar.

Sie geht bei offenen Netzen von folgenden Grundsätzen aus:

— Abrechnungsdaten dürfen nur und nur so lange gespeichert werden, wie dies erforderlich ist, um Rechnungen zu erstellen oder auf eventuelle Anfechtungen zu reagieren; ferner zur Erstellung detaillierter Rechnungen, die ausschließlich für diejenigen Teilnehmer bestimmt sind, die sie angefordert haben. Die Vereinfachung der Tarifsysteme kommt dem Datenschutz entgegen.

— Für bestimmte Telekommunikationsdienste (Telefon, Kabelfernsehen mit Rückkanal, Datenübermittlungsdienste, Autobahngebühreneinzug usw.) müssen anonyme Zahleinrichtungen geschaffen werden. Ungeachtet der Abrechnungsprobleme macht es die Mehrwertigkeit der Netze erforderlich, diese mit den technischen Möglichkeiten eines anonymen Zugangs auszustatten.

— Daten, die für die Vermittlung erforderlich sind, sind unverzüglich zu löschen; Inhaltsdaten dürfen nur gespeichert werden, wenn sie für die Abwicklung des Dienstes erforderlich sind.

— Vorkehrungen sollten getroffen werden, die jenen Teilnehmern, die wünschen, in Teilnehmerverzeichnisse aufgenommen zu werden, garantieren, daß sie nicht Objekt unerwünschter kommerzieller Werbung werden. Das Recht, daß unentgeltlich in den Teilnehmerverzeichnissen kein Eintrag erscheint, sollte angestrebt werden. Daten, die die Erreichbarkeit von Teilnehmern sicherstellen sollen, dürfen nicht zur Erstellung von Personenprofilen führen, die eine Verhaltenskontrolle erlauben.

— Maßnahmen zur Datensicherung insbesondere gegen den Zugang nicht autorisierter Personen, die Manipulation, das Mithören oder zur Gewährleistung der Authentizität des Senders müssen auf höchstem technischen Niveau und zu akzeptablen Preisen angeboten werden.

— Angemessene Kontrollinstitutionen sind sowohl national als auch international einzurichten.

— In lokalen Netzen und bei Telekommunikationsendgeräten ist bereits bei der Normierung und Genehmigung auf den Datenschutz Rücksicht zu nehmen.

Insbesondere erfordern folgende Dienstemerkmale besondere Aufmerksamkeit:

— Die Anzeige des anrufenden Teilnehmers muß sowohl vom Anrufer als auch vom Angerufenen unterdrückt werden können; Mißbrauch muß durch Maßnahmen im Netz verhindert werden.

— Freisprecheinrichtungen müssen so gestaltet werden, daß nur mit Kenntnis der Gesprächsteilnehmer mitgehört oder aufgezeichnet werden kann.

— Beim Zugang zu Anrufbeantwortern, Voice- und Mailboxsystemen sowie Datenübermittlungsdiensten sind hinreichende Zugangssicherungen einzuführen.

11th Conference, 30th August 1989, Berlin

Resolution on Intergrated Services Digital Networks (ISDNs) Proposed by the Working Group on Telecommunications and Media

The present national and international development of telecommunications is characterized by the introduction of Integrated Services Digital Networks (ISDNs). These provide multiple services.

This development means that considerably more personal data is processed by network operators as well as by service suppliers than was the case with previous networks. This development calls für national and international measures to ensure the protection of personal data.

The International Conference of Data Protection Commissioners believes that considerable efforts are required in the light of this development. In particular, not only should data protection not be seen as an obstacle to the development of the international information market. On the contrary, it represents a necessary complement to the technical development, one which is essential to the acceptance of the new telecommunications technologies – it may even be an element that will accelerate this development.

In the case of open networks, data protection should be based on the following principles:

— Accounting data should be stored only if, and only for as long as it is essential for drawing up bills or responding to disputes about accuracy and furthermore itemised bills should be provided solely for those subscribers who request them.

— Anonymous payment procedures should be established for certain telecommunications services (telephone, cable TV with feedback channel, data transfer services, motorway toll etc.). Despite billing problems, the multi-purpose character of the networks makes it necessary for them to be provided with the technical potential for anonymous access.

— Data necessary for establishing a circuit should be deleted immediatly. Other data may be stored only if it is essential for carrying out a service.

— Precautions have to be taken so as to ensure that those subscribers who want to be recorded in directories will not be subjected to undesired commercial advertising. The right to deletion without charge from subscriber directories should be an objective. Data collected and stored so that subscribers can be reached must not be used to draw up subscriber profiles allowing behaviour to be monitored.

— Data protection measures, in particular those to prevent unauthorised access, manipulation and interception, and those to authenticate the identity of the originator of a message must be provided to the highest possible technical standards and at an acceptable cost.

— Adequate regulatory institutions should be set up on both a national and international level.

— In the case of Local Area Networks and telecommunication terminals, data protection must initially be taken into account at the stages of setting design standards and approving equipment.

The following service features require particular attention:

— It must be possible for the identity of the caller to be suppressed by either the caller or the person being called. Abuse must be forestalled by provisions in the network.

— Installations for on-hook operating must be designed in such a way as guarantee that neither interception nor recording is possible without the concerned parties knowing about it.

— Access to answering machines, Voice- and Mailbox systems must be adequately secured.

12. Konferenz, 19. September 1990, Paris

Datenschutz und die Europäische Gemeinschaft

Im Hinblick auf die von der 11. Internationalen Konferenz der Datenschutzbeauftragten am 30. August 1989 verabschiedete Berliner Entschließung und insbesondere im Hinblick auf das Zusatzkommuniqué der Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Gemeinschaften;

in Kenntnis der Tatsache, daß die Kommission der Europäischen Gemeinschaften eine Reihe von Entwurfsvorschlägen für Richtlinien hinsichtlich der automatischen Verarbeitung personenbezogener Daten und die Sicherheit von Informationssystemen verabschiedet hat, und zwar u. a.:

— einen Entwurfsvorschlag für eine Richtlinie des Rates zur Harmonisierung bestimmter Gesetzes-, Durchführungs- und Verwaltungsbestimmungen der Mitgliedstaaten zum Schutze des Einzelnen hinsichtlich der automatischen Verarbeitung personenbezogener Daten;

— einen Entwurfsvorschlag für eine Richtlinie des Rates zum Schutze personenbezogener Daten und der Privatsphäre im Zusammenhang mit öffentlichen digitalen Telekommunikationsnetzen und insbesondere im Zusammenhang mit dem „Integrated Services Digital Network“ (ISDN – Dienste integrierendes Digitales Netz) und den Mobilfunknetzen;

In Anerkenntnis der Tatsachen, daß die Entwürfe für diese Rechtsinstrumente von der Kommission der Europäischen Gemeinschaften ohne vorherige Konsultierung der Datenschutzbeauftragten der Mitgliedstaaten erarbeitet wurden;

haben die Datenschutzbeauftragten (der Mitgliedstaaten der Europäischen Gemeinschaften), die am 19. September 1990 anläßlich der 12. Internationalen Konferenz der Datenschutzbeauftragten zusammentraten,

nach Anhörung des Vortrages und der Erläuterungen des/der Vertreter/s der Kommission der Europäischen Gemeinschaften beschlossen,

— die Richtlinienentwürfe ihrerseits zu prüfen und nach dem gegenseitigen Austausch ihrer Prüfungsergebnisse noch vor Ende des Jahres 1990 erneut zusammenzutreten, um sich auf eine gemeinsame Haltung zu diesen Vorschlägen zu einigen;

— diese gemeinsame Haltung in geeigneter Weise ihrer jeweiligen Regierung zur Kenntnis zu bringen;

— diese gemeinsame Haltung gemeinsam der Kommission und dem Rat der Europäischen Gemeinschaften sowie dem Europäischen Parlament zur Kenntnis zu bringen, so daß sie bei der künftigen Prüfung der Richtlinienentwürfe Berücksichtigung finden kann;

— angesichts der zunehmenden Bedeutung europäischer Fragen die Möglichkeit zu prüfen, einmal jährlich zu einer Konferenz zusammenzutreten, um insbesondere datenschutzrelevante Fragen innerhalb der Europäischen Gemeinschaften zu erörtern.

Data Protection and the European Community

Having regard to the Berlin Resolution adopted by the 11th International Conference of Data Protection Commissioners on 30th August 1989, and more particularly the additional communique from the data protection commissioners of Member States of the European communities.

Noting the adoption by the Commission of the European communities of a series of draft proposals for directives concerning the protection of individuals with regard to automatic processing of personal data and the security of information systems and among others:

- —a draft proposal for a council directive aiming at the harmonization of certain legislative, regulatory and administrative provisions of the Member States relating to the protection of individuals with regard to automatic processing of personal data;
- —a draft proposal for a council directice concerning the protection of personal data and privacy in the context of public digital telecommunications networks and in particular the Integrated Services Digital Network and Public Digital Mobile Networks;

Acknowledging that such proposals for legal instruments have been elaborated by the Commission of the European Communities without having consulted the data protection commissioners of the Member States;

The Data Protection Commissioners (of the Member States of the European Communities) meeting in Paris on September 19, 1990 on the occasion of the 12th International Conference of Data Protection Commissioners.

After having heard the presentation and the explanations of the representative(s) of the Commission of the European Communities;

Resolve:

- —to conduct their own analyses of the draft directives and to meet, after exchanging their conclusions, before the end of 1990 with a view to adopting a common position on these proposals;
- —to inform their respective government of any such common position in such ways as may be appropriate;
- —collectively to bring any such common position to the attention of the Commission and the Council of the European Communities and the European Parlament so that it may be taken into consideration during the future examination of the draft directives;
- —to consider – given the inscreasing importance of European issues – the possibility of meeting annually in conference in order to discuss more specifically any questions relating to data protection within the European Communities.

Probleme öffentlicher Telekommunikationsnetze und des Kabelfernsehens

Nachdem die Internationale Konferenz der Datenschutzbeauftragten in ihrer Entschließung vom 31. August 1989 allgemeine Grundsätze zu dienste-integrierenden digitalen Netzen (ISDN) aufgestellt hat, begrüßt sie den zweiten Bericht der Arbeitsgruppe „Telekommunikation und Medien“, der zeigt, daß diese Grundsätze konkretisiert und auf der technischen Ebene garantiert werden sollten. Diese Grundsätze sind auf jede Form der Telekommunikation einschließlich analoger Formen und bestimmter Formen massenmedialer Kommunikation (insbesondere Kabelfernsehen) anzuwenden. Öffentliche und private Netzbetreiber sollten diese Prinzipien ebenso verwirklichen wie Anbieter von Telekommunikationsdiensten.

I.
Teilnehmerverzeichnisse

Verzeichnisse von Teilnehmern an Telekommunikationsdiensten sind inzwischen weltweit die wichtigsten öffentlich verfügbaren personenbezogenen Dateien. Die Konferenz stellt mit Sorge fest, wie schwierig es ist, die Nutzung dieser Daten weltweit zu kontrollieren. Die Risiken nehmen durch den Verkauf der Teilnehmerverzeichnisse auf elektronischen Datenträgern zu.

Personenbezogene Daten, die von Netzbetreibern erhoben und gespeichert werden, müssen dem Zweck entsprechen, dem Betroffenen einen Telekommunikationsdienst zur Verfügung zu stellen und ihm den Zugang zum Netz zu ermöglichen; die Daten müssen für diesen Zweck erheblich sein und dürfen nicht darüber hinausgehen.

Ein Teilnehmerverzeichnis sollte nur solche personenbezogenen Daten enthalten, die unbedingt zur hinreichend sicheren Identifikation bestimmter Teilnehmer erforderlich sind. Die Teilnehmer haben auch das Recht, einen Hinweis auf ihr Geschlecht (und auf ihren Wohnort)*) auszuschließen. Andererseits schließt dies die Veröffentlichung zusätzlicher Daten auf Wunsch des Teilnehmers nicht aus.

Teilnehmer haben das Recht, gebührenfrei und ohne Begründung den Eintrag ihrer Daten in ein Teilnehmerverzeichnis auszuschließen.

Bei der Erhebung von Bestandsdaten sollte der Netzbetreiber den Betroffenen vollständig darüber aufklären, ob er zur Aufnahme seiner Daten in ein Teilnehmerverzeichnis unabhängig von der Form der Veröffentlichung verpflichtet ist oder nicht.

Bestandsdaten, die einen Mitbenutzer des Endgerätes betreffen, dürfen nur mit dessen Zustimmung in ein Teilnehmerverzeichnis aufgenommen werden.

Die Weitergabe von Bestandsdaten durch einen Netzbetreiber an Dritte zu Werbezwecken darf nur mit der freiwilligen und informierten Zustimmung des Betroffenen erfolgen, es sei denn, dieser hat nach innerstaatlichem Recht die Möglichkeit, der Weitergabe zu widersprechen.

*) bezüglich des Klammerzusatzes bestehen unterschiedliche Auffassungen

Bestandsdaten von Teilnehmern, die einen Eintrag in das Teilnehmerverzeichnis ausgeschlossen oder sich entschieden haben, ihren Namen nicht für Werbezwecke nutzen zu lassen, sollten in keinem Fall an Dritte weitergegeben werden.

Besondere Aufmerksamkeit muß der höchsten räumlichen Ebene gewidmet werden, auf der dem Verzeichnis Teilnehmerdaten entnommen werden können.

Die Konferenz betrachtet mit Sorge die wachsenden Gefahren der telefonischen Direktwerbung und wird diese Probleme eingehender untersuchen.

II.

Anzeige der vom Anrufer benutzten Rufnummer

Die Einführung einer Einrichtung, die die Anzeige der Nummer des vom Anrufer benutzten Anschlusses am Endgerät des angerufenen Teilnehmers vor der Herstellung der Verbindung ermöglicht, wirft ernste Fragen des Schutzes der Privatsphäre auf.

Es ist wichtig, den Schutz der Privatsphäre des einzelnen Teilnehmers – der anrufenden und der angerufenen Person – mit den Erfordernissen der Kommunikationsfreiheit in Einklang zu bringen. Dies wird durch die Beachtung der folgenden Grundsätze erreicht:

Der Anrufer muß die Möglichkeit haben, durch eine einfache technische Vorrichtung im Einzelfall zu entscheiden, ob er seine Rufnummer anzeigen lassen will oder nicht, auf die Gefahr hin, daß sein Anruf von der angerufenen Person nicht entgegengenommen wird.

Dieses Verfahren zur Unterdrückung der Rufnummernanzeige muß für den Teilnehmer gebührenfrei sein.

Bei der Anwendung dieser Grundsätze sollen die folgenden Maßnahmen getroffen werden:

Teilnehmer müssen das Recht haben, gebührenfrei in das Teilnehmerverzeichnis einen Hinweis darauf aufnehmen zu lassen, daß sie kein Verfahren zur Anzeige der vom Anrufer benutzten Rufnummer anwenden.

Es ist notwendig, die Offenbarung übermittelter Informationen über den Anrufer an Dritte einzuschränken.

Ausnahmsweise darf die Unterdrückung der Rufnummernanzeige entsprechend dem innerstaatlichen Recht außer Kraft gesetzt werden, wenn Personen über Notruf die Feuerwehr oder den Notarzt anrufen.

Der Netzbetreiber kann die Unterdrückung der Rufnummernanzeige auch außer Kraft setzen, um auf Antrag der angerufenen Person den Urheber belästigender Anrufe festzustellen.

Diese Grundsätze sollen bei der Abwicklung internationaler Telefongespräche in gleicher Weise beachtet werden.

III.

Mobilfunk

Netzbetreiber, die ein Mobilfunknetz betreiben und anbieten, sollten Teilnehmer über die Sicherheitsrisiken informieren, die normalerweise – insbesondere bei fehlender Verschlüsselung der übermittelten Nachrichten – mit der Benutzung eines Mobilfunknetzes verbunden sind. Der Betreiber sollte dem Teilnehmer vor allem empfehlen, das Mobilfunknetz nicht zur Übermittlung vertraulicher Nachrichten zu benutzen, solange Probleme der Datensicherheit bestehen.

Netzbetreiber sollten verpflichtet sein, den Teilnehmern am Mobilfunknetz wirksame Verschlüsselungsverfahren anzubieten.

Wirksame technische Vorkehrungen sollen getroffen werden, um den unbefugten Netzzugang über mobile Endgeräte zu verhindern.

Die Speicherung von Verbindungsdaten muß strikt auf den kurzen Zeitraum des Verbindungsaufbaus zwischen Teilnehmer und Netz beschränkt werden. Das Tarifsystem soll so gestaltet werden, daß die Orte, an denen Mobiltelefone benutzt worden sind, nicht Teil der Abrechnungsdaten sind. Besondere Beachtung verdient die Frage, inwieweit die Speicherung der vollständigen Rufnummer der angerufenen Person für Abrechnungszwecke notwendig ist.

IV.

Gebührenabrechnung

Inwieweit die Speicherung der vollständigen Nummer des angerufenen Teilnehmers für Zwecke der Gebührenabrechnung im allgemeinen erforderlich ist, sollte noch näher untersucht werden.

V.

Kabelfernsehen

Die Speicherung individueller Zuschauerprofile durch Kabelfernsehgesellschaften, die einzeln abrufbare („pay per view“) Programme anbieten, ist ein Eingriff in die Privatsphäre des Kunden.

Deshalb sollten Kabelfernsehgesellschaften „pay per view“-Programme nur dann anbieten, wenn die Kunden eine praktikable und wirtschaftliche Möglichkeit (z. B. im voraus bezahlte Karten oder Decoder) haben, die Programme zu empfangen, ohne daß zuschauerbezogene Informationen gespeichert werden.

Messungen der Sehbeteiligung und Tantiemen dürfen nicht auf der Grundlage zuschauerbezogener Daten berechnet werden.

Die Konferenz befürchtet, daß in naher Zukunft im Bereich des Kabelfernsehens zahlreiche Datenschutzprobleme entstehen werden und wird die Entwicklung deshalb eingehend überwachen.

12th Conference, 19th September 1990, Paris

Resolution on Problems related to Public Telecommunication Networks and Cable Television

Having taken account of certain general principles on Integrated Services Digital Networks (ISDNs) in its resolution of 31st August 1989, the International Conference of Data Protection Commissioners welcomes the second report of the working group on „Telecommunications and Media" which indicates that these principles should be put in concrete terms and be guaranteed at the technical level. These principles may be applicable to any kind of telecommunications including analogue forms as well as certain forms of mass media communication (especially cable television). Network operators in the public and the private sectors as well as firms offering telecommunications services should adhere to these principles.

I

Directories

Telecommunications directories happen to have become the most important publicly available personal data files in the world. The Conference notes with concern the difficulty in controlling the use of these data worldwide. The risks are enlarged by selling directory data on electronic media.

Personal data collected by a network operator should be adequate, relevant and nonexcessive with regard to the purpose of making available a telecommunications service to the data subjet and connecting him to the network.

Personal data contained in a directory should be limited to such as are strictly necessary to identify reasonably a particular subscriber. He/she also has the right not to indicate his/her sex (and the place where he/she lives)*). On the other hand this would not exclude the publication of additional data at the request of the subscriber.

Subscribers have the right, free of charge and without having to give reasons, to have no personal data included in a directory.

When collecting basic data, a network operator should fully inform the data subject of whether or not he is obliged to have his data included in a subscriber directory regardless of the medium of publication.

Basic data relating to co-users of the subscriber's terminal may only be included in a directory with their consent.

The communication of basic data by a network operator to a third party for marketing purposes may only be carried out with the free and informed consent of the data subject unless the subscriber according to national law is given the opportunity to object.

Basic data of subscribers having refused to have their data included in a directory or having decided to have their name on a no-publicity list should not, in any case, be communicated to any third party.

*) There are differing views as to the words in brackets

Regard shall be had to the highest geographic level at which one can draw subscribers' information from the directory.

The Conference is concerned about the increasing dangers of direct marketing by telephone and will look into these problems in greater detail.

II

Calling line identification

The introduction of a service feature permitting the display of the number of the line used by the caller on the called subscriber's telephone before the connection is established raises serious questions of privacy.

It is important to reconcile the privacy requirements of the individual telecommunication user-caller and person being called with the requirements for freedom of communication. This is achieved through adherence to the following two principles:

— It must be possible for the caller to decide by simple technical means on a call-by-call basis whether he wants to be identified or not even at the risk of his call not being accepted by the called person.

— This non-identification procedure must be free of charge for the subscriber.

In application of these principles the following measures shall be taken:

Subscribers must have the right, free of charge, to indicate on the directory that they will not operate a procedure for identification of the calling line.

Regard should be had to the need to restrict disclosure of transmitted information concerning the caller to third parties.

As an exception, the suppression of the calling line identification may be overridden in case of persons calling emergency services such as fire brigades or ambulances according to national law.

The operator may also override the suppression of the calling line identification in order to trace malicious calls on request of the called person.

These principles shall be equally guaranteed when operating international calls.

III

Mobile telephones

When providing and operating a mobile telephone service, network operators should inform subscribers of the security risks which usually accompany the use of the mobile telephone network, particularly in the absence of encryption of communications. The operator should advise the subscriber in particular that as long as problems of data security exist subscriber should refrain from using the mobile telephone network for the purpose of communicating confidential messages.

Network operators should be obliged to offer subscribers to the mobile telephone network effective encryption procedures.

Effective technical devices shall be introduced so as to prevent unauthorized access to the network.

The storage of traffic data must be strictly limited to the time required for connecting the subscriber to the mobile telephone network. The tariff system shall be designed in such a way that the locations where the mobile telephones have been used do not form part of the billing data.

IV

Billing

Further consideration should be given to the question as to what extent the storage of the complete number of the called person is necessary for billing purposes in general.

V

Cable television

The recording of individual viewing profiles by cable television companies offering “pay per view” programmes is an encroachment upon customers’ privacy.

Therefore, cable television companies should only operate „pay per view“ systems if a practical and economic opportunity is available to customers (e. g. pre-paid cards or decoders) allowing them to receive the programmes without such information being recorded.

Audience ratings and royalties must not be calculated on the basis of identifiable viewers’ data.

The Conference is concerned that in the field of cable television numerous data protection problems will arise in the near future and therefore will monitor developments in this area closely.

13. Konferenz, 4. Oktober 1991, Straßburg

Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Telemarketing, der Kartentelefone und der elektronischen Directories und Beschluß der Internationalen Konferenz der Datenschutzbeauftragten

Bericht

Telemarketing

Der schnell zunehmende Gebrauch des Telefons für Zwecke der Direktwerbung (Telemarketing) bedroht die Privatsphäre der Verbraucher ernsthaft.

Es gibt zwei Hauptprobleme, die durch das Telemarketing für die Privatsphäre entstehen.

Das erste hängt mit der störenden Wirkung nicht erbetener telefonischer Verkaufsangebote auf die Verbraucher zusammen: Je öfter Anrufe für Werbezwecke entgegengenommen werden, desto störender wird der Verbraucher sie empfinden. Die Störung wird sogar noch verschärft, wenn die Anrufe von Anrufautomaten ausgelöst und durchgeführt werden.

Das zweite Problem betrifft die Nutzung von personenbezogenen Dateien, die für das Telemarketing eingesetzt oder als sein Ergebnis aufgebaut werden. Derartige Dateien können die informationelle Selbstbestimmung beeinträchtigen.

Telefonische Direktwerbung kann stattfinden:

a) im Zusammenhang mit einer bestehenden Beziehung zwischen dem Werbetreibenden und dem Verbraucher

   und

b) wo keine derartige Beziehung besteht (cold calls).

Im Fall a), selbst solche Verbraucher, die im Rahmen einer bestehenden Beziehung angerufen werden, sollten das Recht haben, weiteren Anrufen zu widersprechen. Die Erfahrung in einigen europäischen Ländern hat gezeigt, daß Telefonpräferenzsysteme (Listen von Anschlußinhabern, die nicht für Werbezwecke angerufen werden wollen) nicht immer hinreichend wirksam die Privatsphäre schützen.

Im Fall b) sollten Verbraucher außerhalb einer bestehenden Geschäftsbeziehung nur angerufen werden, wenn diese Anrufe auf die Initiative des Verbrauchers zurückgehen.

Der Einsatz von Anrufautomaten sollte ohne die vorherige ausdrückliche Zustimmung des Verbrauchers nicht erlaubt sein, unabhängig davon, ob eine Geschäftsbeziehung besteht oder nicht.

Es sollten effektive Maßnahmen ergriffen werden, um unerwünschtes grenzüberschreitendes Telemarketing zu unterbinden.

Neue Techniken sollten nicht ohne Sicherungen zum Schutz der Privatsphäre eingeführt werden. Soweit diese Techniken Teilnehmerverzeichnisse benutzen, sollte den Teilnehmern an den neuen Diensten bereits bei Abschluß des Vertrages die kostenlose Möglichkeit eingeräumt werden, nicht in das Teilnehmerverzeichnis aufgenommen zu werden.

Diese Grundsätze sollten in gleicher Weise auf andere Telekommunikationstechniken wie Telefax oder Electronic Mail (elektronische Post) angewandt werden.

Die schnelle Entwicklung neuer Techniken zeigt, daß die Konferenz neue Entwicklungen sorgfältig beobachten sollte, um notwendige zusätzliche Maßnahmen zu empfehlen.

Kartentelefone

In den letzten Jahren sind elektronische Zahlungsmittel für das Telefonieren in öffentlichen Einrichtungen entwickelt worden.

Im Zusammenhang mit der Digitalisierung der Telefonnetze (bei der Einzelheiten des Anrufs im Netz gespeichert werden) ist die Möglichkeit des anonymen Zugangs zum Telefonnetz eine wichtige Sicherung der Privatsphäre.

Insofern ist die schnelle Entwicklung anonymer Telefonkarten auf Guthabenbasis, die in öffentlichen Telefonzellen benutzt werden können, sehr ermutigend.

Dennoch hat die internationale Mobilität des einzelnen – ergänzt durch Entwicklungen beim Mobiltelefon – dazu beigetragen, daß bestimmte Möglichkeiten angeboten werden, die die Anonymität herkömmlicher Telefonkarten entfallen lassen und dadurch Datenschutzprobleme erzeugen.

Diese Möglichkeiten führen dazu, daß identifizierbare Zahlungsmittel (Bankkarten, Kreditkarten, Telekarten) den Kunden vorzugsweise angeboten werden, obwohl es keine unausweichlichen technischen oder organisatorischen Gründe gibt, um diese Alternative zu wählen.

Dementsprechend sollte auf internationaler Ebene besondere Aufmerksamkeit darauf verwendet werden, die Gestaltung, das Angebot und die Anbringung von Geräten zu fördern, die eine echte Auswahl zwischen den verschiedenen – anonymen oder identifizierbaren – Zahlungsmethoden ermöglichen.

Wenn der Einsatz eines identifizierbaren elektronischen Zahlungsmittels angeboten wird, muß besondere Aufmerksamkeit darauf verwendet werden, daß durch angemessene technische Maßnahmen Mißbrauch unterbunden wird. Insbesondere sollte es die Möglichkeit der Authentifizierung des Karteninhabers geben.

Schließlich sollten nur solche personenbezogenen Daten an die Kartengesellschaft übermittelt werden, die zur Rechnungsstellung erforderlich sind. Es sollte nicht möglich sein, von diesen Daten Rückschlüsse entweder auf die Nummer des Angerufenen oder den Ort des Telefons zu ziehen, von dem aus angerufen wurde.

Karteninhaber sollten vor Zweckentfremdung ihrer personenbezogenen Daten geschützt sein und auf angemessene Weise darüber informiert werden, welche Art von Daten das Kartentelefon erhebt und welche Art von Daten dem jeweiligen Diensteanbieter übermittelt wird.

Elektronische Post und damit zusammenhängende Teilnehmerverzeichnisse

Die Entstehung und schnelle Verbreitung der elektronischen Post unterstreicht, wie wichtig es ist, den Schutz personenbezogener Daten zu gewährleisten, die in elektronischen Teilnehmerverzeichnissen in Zusammenhang mit diesen Systemen gespeichert werden.

Die 12. Internationale Datenschutzkonferenz hat in ihrem Beschluß vom 19. September 1990 auf die Probleme hingewiesen, die bei öffentlichen Telekommunikationsnetzen und beim Kabelfernsehen insbesondere in bezug auf elektronische weltweite Teilnehmerverzeichnisse bestehen.

Nach eingehenderer Prüfung der Probleme elektronischer Teilnehmerverzeichnisse weist die Arbeitsgruppe auf folgende weitere Punkte hin:

Personenbezogene Daten sollten in derartigen Verzeichnissen nur mit der informierten Einwilligung des Teilnehmers gespeichert werden.

Betroffene sollten über spezielle Datenschutzrisiken informiert werden, die sich aus einem Eintrag in das Verzeichnis ergeben.

Die Identität der für das Verzeichnis verantwortlichen Stelle und der Umfang der personenbezogenen Daten, die für das Funktionieren des Verzeichnisses notwendig sind, sollten eindeutig festgelegt werden.

Technische Maßnahmen sollten getroffen werden können, um eine Verarbeitung (z. B. Umdrehen oder Kopieren des Verzeichnisses) zu unterbinden, die dem Datenschutz widerspricht.

Zusätzliche Probleme entstehen allerdings jetzt bei den Verzeichnissen, die im Zusammenhang mit Systemen der elektronischen Post geführt werden. Diese Probleme beziehen sich auf die Entstehung eines Verzeichnistyps, der völlig andere Eigenschaften besitzt als das herkömmliche elektronische Telefonbuch. Derartige Verzeichnisse sind gewöhnlich in Systemen der elektronischen Post eingebettet. Während sie viele Jahre lang vorhanden waren, haben die technischen Schwierigkeiten des Zugangs und der Manipulation solcher Verzeichnisse auf der normalen Nutzerebene ihre Wirkung aus datenschutzrechtlicher Sicht reduziert. Jetzt jedoch ist mit der Festlegung des X.500-Standards, dessen Hauptziel die Ermöglichung von Schnittstellen für Verzeichnisse aller Systeme der elektronischen Post ist, die Schaffung großer verteilter elektronischer Verzeichnisse technisch erleichtert worden, und die damit zusammenhängenden Datenschutzprobleme müssen gelöst werden.

Diese Probleme betreffen offensichtlich:

die Entstehung eines einheitlichen Personenkennzeichens für Eintragungen in das Verzeichnis (in der Literatur als „distinguished name“ bezeichnet). Die weltweite Erstreckung der geplanten Verzeichnisse unter dem X.500-Standard unterstreicht zusätzlich die Datenschutzprobleme, die mit einheitlichen Personenkennzeichen verbunden sind;

die verstärkten benutzerfreundlichen Möglichkeiten, die zur Verfügung gestellt werden für die Durchsuchung und Verarbeitung dieser Verzeichnisse;

Probleme im Zusammenhang mit der Möglichkeit, nicht in das Verzeichnis aufgenommen zu werden, da das Verzeichnis gerade die Aufgabe hat, den aktiven Betrieb der elektronischen Post zu gewährleisten.

Beschluß

Die 13. Internationale Konferenz der Datenschutzbeauftragten begrüßt den Bericht der Arbeitsgruppe Telekommunikation und Medien und unterstreicht die Bedeutung der beschriebenen Probleme in den Bereichen des Telemarketing, der Kartentelefone und der elektronischen Verzeichnisse.

13th Conference, 4th October 1991, Strasbourg

Report of the Working Group on Telecommunications and Media on problems relating to telemarketing, card telephones and electronic directories and Resolution of the International Conference of Data Protection Commissioners

---

Report

Telemarketing

The fast growing use of the telephone for direct marketing purposes (telemarketing) poses a serious threat to privacy of consumers.

There are two main privacy problems created by telemarketing.

The first relates to the intrusive effect of unsolicited sale calls on consumers: the higher the frequency of marketing calls received, the more a consumer might estimate these calls as being intrusive. The intrusiveness is even more increased when the calls are generated and executed by automatic calling devices.

The second problem concerns the use of personal data files which are used for, or created as a result of, telemarketing. Such files may involve an encroachment upon privacy.

Telemarketing calls can arise:

a) within the context of an existing relationship between the telemarketeer and the consumer
   and
b) where no such relationship exists (cold calls).

In the case of a), even those consumers receiving calls within existing relationships should have the right to object to further calls. Experiences in some European countries have shown that telephone preference systems are not always sufficiently effective to protect privacy.

As regards b), calls to consumers where no previous relationship exists should only be made if the consumer has taken the initiative to receive such calls.

The use of automatic calling devices should not be permitted without the previous expressed consent of the consumer irrespective of the existence of a relationship.

Consideration should be given to the etablishment of effective instruments in order to prevent undesirable transborder telemarking activities.

New techniques should not be introduced without safeguards with respect to the protection of privacy. To the extent that these techniques make use of directories, ex-directory facilities should be offered free of charge to the subscribers of the new services at the time of concluding the contract.

The principles outlined above should apply equally to other telecommunication techniques such as telefax or electronic mail.

The rapid development of new techniques indicates that the conference should keep a close eye on new developments with a view to proposing appropriate additional measures.

Card Telephones

Recent years have shown the appearance of electronic means of payment for telephone calls made from equipment available in public places.

In the context of the digitalization of telephone networks (with call details being stored within the network), the facility to access the telephone network anonymously represents an important privacy safeguard.

In this regard, the rapid development of the anonymous payment cards which can be used in public telephones is very encouraging.

Nevertheless, the mobility of individuals internationally coupled With developments in mobile telephony has contributed to the emergence of certain facilities which remove the anonymity associated with conventional telephone cards and thus give rise to data protection concerns.

These facilities involve identifiable means of payment (bank cards, credit cards, telecommunications cards) being offered to individuals on a preferential basis even though there are no inevitable technical or organisational reasons for choosing this particular option.

Accordingly, particular attention should be given at the international level, to encouraging the design, promotion and installation of equipment which permits a real choice between the different methods of payment, anonymous or identifiable.

When the use of an identifiable electronic means of payment is offered, particular attention needs to be given to ensuring that appropriate techniques are put into place to prevent improper use. In particular, a means of authentication of the card user should be implemented.

Finally personal data transmitted to the card issuing company should be limited to that necessary for determining the bill. It should not be possible to deduce from such data either the called line number or the location of the telephone from which the call was made.

Card users should have safeguards against non-compatible uses of the data concerned and should be informed by appropriate means of the type of data collected by the equipment connected to the network, as well as the type of data transmitted to the service providers concerned.

Electronic Mail and Associated Directories

The emergence and rapid development of electronic mail facilities serves to underline the importance of tackling the data protection issues relating to personal data stored in the electronic directories which are associated with such systems.

The XIIth International Conference of Data Protection Commissioners, in its resolution of 19th September 1990 referred to problems related to public telecommunications networks and Cable television especially as far as electronic worldwide directories are concerned.

In developing its concerns about electronic directories, the Working Group would like to make the following further points:

- Personal data should only be stored in such directories with the informed consent of the subscriber.
- Data subjects should be informed about specific data protection risks arising out of an entry in the directory.
- The identity of the controller of the directory and the scope of personal data necessary for the functioning of the directory should be clearly defined.
- Technical measures should be available to forbid any processing (such as inversion or copying) which would contravene data protection policy.

Additional concerns now arise, however, in the area of directories associated with electronic mail systems. These relate to the emergence of a type of directory possessing characteristics quite unlike that of a conventional electronic telephone directory. Such directories are usually "embedded" in electronic mail systems. While in existence for many years, the technical difficulties in accessing and manipulating such directories at the ordinary user level has reduced their impact in data protection terms. Now, however, with the emergence of the X. 500 standard which focuses primarily on providing directory interfaces for all electronic mail systems, the establishment of large distributed electronic directories is technically facilitated and the associated data protection issues will require to be addressed.

These issues would appear to include:

- The emergence of a unique personal identifier for entries in the directory (referred to in the literature as "the distinguished name"). The global nature of the proposed directories under the X. 500 standard further underlines the data protection concerns associated with unique personal identifiers.
- The increased user-friendly facilities which will be made available for interrogation and processing of these directories.
- Problems posed by the provision of "ex-directory" facilities because of the function of the directory in actively providing the mail service.

Resolution

The XIIIth International Conference of Data Protection Commissioners welcomes the report of the Working Group on Telecommunications and Media and notes the importance of the issues raised in the areas of telemarketing, phone card facilities and electronic directories.

14. Konferenz, 29. Oktober 1992, Sydney

Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und Gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Bericht

Fernmeldegeheimnis

1.

Jeder Bürger, der ein Telefon benutzt, hat grundsätzlich die legitime Erwartung, daß sein Telefongespräch von niemandem, insbesondere von keiner staatlichen Stelle, abgehört wird.

Der Grundsatz der Vertraulichkeit von Telefongesprächen ist deshalb in den Verfassungen verschiedener Länder wie z. B. Österreichs, Deutschlands, Griechenlands, der Niederlande, Portugals und Spaniens verankert. Darüber hinaus garantiert die Europäische Menschenrechtskonvention das Recht jedes Einzelnen auf Achtung seiner Privatsphäre, seines Familienlebens, seiner Wohnung und seiner Korrespondenz. Dieser Artikel der Europäischen Menschenrechtskonvention ist vom Europäischen Menschenrechtsgerichtshof so ausgelegt worden, daß er auch das Fernmeldegeheimnis umfaßt.

In vielen Ländern ist das Abhören von Telefongesprächen sogar ein Straftatbestand. Die bloße Behauptung, daß Telefone illegal abgehört worden seien, kann auch weitreichende politische Konsequenzen haben. So mußte kürzlich ein Minister der Republik Irland auf Grund derartiger Vorwürfe zurücktreten, um nur ein Beispiel zu geben.

2.

Andererseits ist in den meisten Ländern anerkannt, daß es unter besonderen Voraussetzungen Ausnahmen vom Fernmeldegeheimnis geben muß. In Belgien, dem einzigen Land, in dem es bisher ein absolutes Verbot des Abhörens von Telefongesprächen gibt, bereitet die Regierung einen Gesetzentwurf für entsprechende Ausnahmen vor.

Die Statistik zeigt, daß Telefongespräche für Zwecke der Strafverfolgung im Jahre 1990 in 2449 Fällen in Deutschland und in 2031 Fällen in den Niederlanden abgehört wurden (Quelle: Bundesministerium für Post und Telekommunikation; Niederländisches Justizministerium).

Nach Art. 8 Abs. 2 der Europäischen Menschenrechtskonvention ist der „Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts" (auf Achtung des Post- und Fernmeldegeheimnisses) „nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum

Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist“. Dieser Katalog von Ausnahmen, die der nationale Gesetzgeber vorsehen kann, ist sehr weitreichend, und einige europäische Länder haben restriktivere Vorschriften erlassen, die das Abhören von Telefongesprächen erlauben (vgl. auch Ziffer 2.4 des Entwurfs einer Empfehlung für den Schutz von personenbezogenen Daten im Bereich der Telekommunikationsdienste, mit besonderem Bezug zu Telefondiensten, angenommen vom Ausschuß für rechtliche Zusammenarbeit des Europarats, Juni 1992).

Die Arbeitsgruppe hat die neueren Entwicklungen der Gesetzgebung in den einzelnen Ländern untersucht und dabei festgestellt, daß trotz einiger Zweifel hinsichtlich der Effektivität des Telefonabhörens als Mittel im Kampf gegen die „organisierte Kriminalität“ dennoch eine wachsende Tendenz zu beobachten ist, die Unverletzlichkeit des Fernmeldegeheimnisses mit zusätzlichen Ausnahmen zu versehen. In Deutschland trat in diesem Jahr ein neues Gesetz in Kraft, das eine Verwaltungsbehörde ermächtigt, Telefongespräche abzuhören, um illegale Waffenexporte zu verhindern (sogar bevor Straftaten begangen werden). In vielen Ländern kann das Telefonabhören in Strafverfahren angeordnet werden, die spezielle schwere Straftaten wie Drogenhandel, Mord und terroristische Verbrechen betreffen.

Allerdings wird das Abhören von Telefongesprächen neuerdings von Politikern auch als effektive Waffe im Kampf gegen Korruption und organisierte Kriminalität angesehen (Australien, Deutschland). Es ist bisher nicht gelungen, diese Kategorien von Straftatbeständen präzise zu beschreiben. Deshalb birgt jede Gesetzgebung, die mit derart ungenauen Tatbeständen arbeitet, die Gefahr, daß die Telefongespräche unverdächtiger Personen abgehört werden.

In Österreich wird andererseits über einen Gesetzentwurf diskutiert, der sogar den Geheimdienst verpflichtet, eine richterliche Anordnung zu beantragen, bevor Telefongespräche rechtmäßig abgehört werden dürfen.

Die Notwendigkeit einer Rechtsgrundlage für jeden staatlichen Eingriff in das Fernmeldegeheimnis hat der Europäische Menschenrechtsgerichtshof sehr strikt ausgelegt. In seiner neueren Rechtsprechung betont der Gerichtshof, daß Abhören und andere Formen der Registrierung von Telefongesprächen einen schwerwiegenden Eingriff in das Privatleben und die Kommunikation darstellen und deshalb auf einer Rechtsvorschrift beruhen müssen, die besonders präzise formuliert ist. Der Gerichtshof hebt hervor, daß es entscheidend ist, klare, detaillierte Vorschriften in diesem Bereich zu haben, insbesondere weil die verfügbare Technologie sich ständig weiterentwickelt (Fall Kruslin, 7/1989/167/223, Ziffer 33). Aus diesem Grund (Mangel an Präzision) wurde festgestellt, daß die Vorschriften des französischen Rechts über das Abhören von Telefongesprächen, gegen die Europäische Menschenrechtskonvention verstießen. Zwischenzeitlich ist Frankreich dem Beispiel des Vereinigten Königreichs gefolgt und hat ein neues Abhörgesetz verabschiedet, um den Anforderungen des Europäischen Menschenrechtsgerichtshofs zu entsprechen.

Das deutsche Bundesverfassungsgericht hat vor kurzem entschieden, daß eine präzise Rechtsgrundlage notwendig ist, um Fangschaltungen vorzunehmen, auch wenn der Inhalt der belästigenden Anrufe nicht aufgezeichnet wird.

Man kann drei Verfahrensstadien unterscheiden, wenn staatliche Stellen Telefone überwachen wollen:

— die Entscheidung, Telefongespräche abzuhören;

— die Durchführung dieser Entscheidung und

— die Kontrolle dieser Überwachungsmaßnahme, nachdem sie beendet worden ist.

Die Entscheidung, Telefongespräche abzuhören, kann getroffen werden von einer Verwaltungsbehörde (im Vereinigten Königreich), von einem Untersuchungsrichter (in den meisten Ländern) oder von einer Verwaltungsbehörde bzw. einem Gericht, je nachdem zu welchem Zweck abgehört werden soll (Deutschland). Beauftragte für den Datenschutz und den Schutz der Privatsphäre sind an diesen Entscheidungen nicht beteiligt und haben keine Kompetenz, sie zu überwachen. Dies bezieht sich ebenso auf die Durchführung der Anordnung, Telefongespräche abzuhören.

Sobald allerdings die Abhörmaßnahme beendet worden ist, gibt es gute Gründe dafür, daß die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die Befugnis erhalten, die Nutzung der Daten zu kontrollieren, die aus der Abhörmaßnahme stammen. In einigen Ländern wächst die Erkenntnis, daß Beauftragte für den Datenschutz und den Schutz der Privatsphäre eine wichtige Rolle in diesem Bereich zu spielen haben, obwohl sie bisher noch keine derartige Kompetenz haben mögen.

In den Niederlanden wird das Recht möglicherweise in naher Zukunft in der Weise geändert, daß die Ergebnisse einer Abhörmaßnahme in den Akten der Nachrichtendienste dokumentiert werden. Sobald dies geschieht, würden diese Akten der Kontrollkompetenz der Registratiekammer unterliegen.

In Deutschland kann der Bundesbeauftragte für den Datenschutz nicht in ein gerichtliches Verfahren eingreifen, das zu einer Abhöranordnung führt. Aber der Bundesminister für Post und Telekommunikation hat anerkannt, daß der Bundesbeauftragte für den Datenschutz zu kontrollieren hat, ob die Deutsche Bundespost TELEKOM die Abhöranordnung korrekt durchführt, welche Art personenbezogene Daten bei Durchführung der richterlichen Anordnung erhoben werden und für welchen Zweck sie genutzt werden. Es ist entscheidend, daß die Ergebnisse einer Abhörmaßnahme nur für den Zweck benutzt werden, für den die Daten ursprünglich erhoben wurden.

In mehreren Ländern wird das Recht geändert, um die Überwachung von Nachrichten zu ermöglichen, die mit anderen Telekommunikationsmitteln (Telefax, Telex, Datenübertragung etc.) übermittelt werden. Zum Teil wird diese Gesetzgebung sich auch auf private Netzbetreiber und Diensteanbieter erstrecken und sie zur Zusammenarbeit mit der Polizei verpflichten.

Man muß sich vergegenwärtigen, daß die Überwachung von Telekommunikationsverbindungen, insbesondere das Abhören von Telefongesprächen, kein gewöhnliches Überwachungsmittel ist, das automatisch gegen jeden eingesetzt werden kann, der bestimmte Verbrechen begeht oder die nationale Sicherheit bedroht. Es ist im Gegenteil in den meisten Ländern eine Ermittlungsmethode für Ausnahmesituationen und unterliegt zusätzlichen Bedingungen. In einer Reihe von Ländern kann die Überwachung von Telefongesprächen nur angeordnet werden, wenn jemand einer Straftat verdächtigt wird, zu deren Aufklärung die Abhörmaßnahme beitragen kann, und nur dann, wenn herkömmliche Ermittlungsmethoden unpraktikabel oder erfolglos sind.

Es ist entscheidend, daß die Person, deren Telefongespräche abgehört worden sind, von der verantwortlichen Behörde über die Abhörmaßnahme informiert wird, sobald dies möglich ist, ohne den Zweck der Ermittlungen zu gefährden.

Nur dann ist der Einzelne in der Lage, die Abhörmaßnahme durch einen Richter oder ein anderes unabhängiges Organ überprüfen zu lassen. Die Benachrichtigung des Betroffenen ist bisher allerdings nur in wenigen nationalen Rechtssystemen vorgesehen.

3.

Das Recht des Bürgers, das Telefon zu benutzen, ohne registriert und beobachtet zu werden, schützt ihn nicht nur gegen die Aufzeichnung der Gesprächsinhalte, sondern auch gegen die Nutzung der technischen Daten, die vom Telekommunikationsnetz für andere als Abrechnungszwecke erzeugt werden (Verbindungsdaten wie Zeit, Dauer des Gesprächs und Rufnummer des Angerufenen). Allerdings gibt es von diesem Grundsatz noch weiterreichende Ausnahmen als vom Prinzip der Vertraulichkeit des Gesprächsinhalts. In Belgien und Deutschland können Verbindungsdaten auf Grund einer strafgerichtlichen Anordnung in jedem Strafverfahren genutzt werden, während das Abhören von Telefongesprächen im eigentlichen Sinn in vielen Ländern nur bei bestimmten Katalogstraftaten zulässig ist.

Auch in dieser Beziehung lassen sich in den verschiedenen Rechtssystemen unterschiedliche Tendenzen feststellen. In Australien hat der Attorney-General vor kurzem vorgeschlagen, den Begriff der Kommunikationsüberwachung neu zu definieren, so daß er das Mithören oder Aufzeichnen von Informationen umfaßt, die eine Person einer anderen über ein Telekommunikationssystem übermittelt, ohne das beide Gesprächsteilnehmer davon wissen; die Registrierung von Verbindungsdaten sollte nicht mehr unter diesen Begriff fallen. Diesen Vorschlag hat der australische Beauftragte für den Schutz der Privatsphäre scharf kritisiert. Nach seiner Auffassung sollten Verbindungsdaten und Inhaltsdaten, die über ein Telefonnetz übermittelt werden, in der gleichen Weise geschützt werden. Aufgrund neuerer technischer Entwicklungen (insbesondere der Einrichtung von digitalen Telekommunikationsnetzen) werden Verbindungsdaten systematisch von den Netzbetreibern gespeichert und sind deshalb für eine gewisse Zeit auch für andere Zwecke wie Strafverfahren verfügbar. Es gibt keinen Grund für ein unterschiedliches Schutzniveau für Inhaltsdaten einerseits und Verbindungsdaten andererseits. Der Grundsatz der Vertraulichkeit von Telefongesprächen schützt sowohl deren Inhalt als auch deren nähere Umstände (Zeit, Dauer und die an ihnen beteiligten Personen).

Aus demselben Grund hat die deutsche Konferenz der Datenschutzbeauftragten den Bundestag aufgefordert, die alte Vorschrift aufzuheben, die die Nutzung von Verbindungsdaten für jedes Strafverfahren zuläßt. Wendet man diese Vorschrift auf digitale Netze an, so ist sie mit dem verfassungsrechtlich geschützten Fernmeldegeheimnis nicht mehr vereinbar.

4.

Da die Gesetzgebung über die Telekommunikationsüberwachung gegenwärtig in vielen Ländern, die in der Arbeitsgruppe vertreten sind, geändert wird, kann dieser Bericht nur ein Zwischenbericht sein. Es ist notwendig, daß die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die technische und rechtliche Entwicklung in diesem Bereich genau beobachten, um die Privatsphäre des Einzelnen gegen exzessive Überwachung zu schützen.

Satellitenkommunikation

Vor mehr als sechs Jahren verabschiedete die VII. Internationale Konferenz der Datenschutzbeauftragten in Luxemburg eine Entschließung über Datenschutz und Neue Medien, in der sie betonte, daß der „Einsatz von Satelliten zur Kommunikation“. . . „Im Hinblick auf die Datenintegrität und den Schutz vor unbefugtem Abhören ebenfalls Risiken“ schafft.

Seitdem scheinen diese Risiken fast vergessen, obwohl es geradezu eine Revolution am Himmel gegeben hat, was die Kapazität der Satelliten angeht. Der Kapazitätszuwachs der europäischen Satelliten von 1989 bis 1993 wird bei 215 % liegen (vgl. EG-Kommission, Grünbuch zur Satellitenkommunikation, Tabelle 5, S. 57).

Satelliten können für eine Reihe von Zwecken eingesetzt werden, deren wichtigste die Verteilung von Fernsehprogrammen und die Telekommunikation sind. Es gibt andere Einsatzmöglichkeiten wie etwa die weltweite

— Positionsbestimmung und das Flottenmanagement,

— Fernmessen und Fernwirken,

— Fernerkundung.

1. Telekommunikation

Ein Satellitensystem besteht in der Regel aus mindestens zwei Erdfunkstationen und dem Raumsegment. Informationen werden von einer leistungsstarken Erdfunkstation zum Satelliten gefunkt („Uplink“, Aufwärtsstrecke; ein fester Punkt-zu-Punkt-Dienst). Sie werden dann über Transponder im Satelliten zurück zu einer anderen Erdfunkstation oder mehreren Erdfunkstationen übermittelt („Downlink“, Abwärtsstrecke). Bei der Abwärtsstrecke sind verschiedene Dienstformen vorstellbar, wie z. B. ein fester (Punkt-zu-Punkt-Telekommunikations-)Dienst, ein Fernsehverteil-(Punkt-zu-Mehrfachpunkt-) Dienst, ein mobiler Dienst, bei dem Informationen zu beweglichen Empfangsstationen wie etwa Lastwagen mit kleinen Dachantennen gefunkt werden. Moderne Satelliten tragen bis zu 16 Transponde und jeder Transponder kann bis zu zwei Fernsehkanäle oder 1 700 Telefonsprachkanäle übertragen.

In Europa werden nur 2 bis 3 % der internationalen Telefongespräche über Satellit abgewickelt, während Satelliten eine weit größere Rolle bei transatlantischer und interkontinentaler Telekommunikation spielen, wo sie fast 60 % des Verkehrsaufkommens übernehmen. Satellitengestützte Kommunikationsnetze sind von großer Bedeutung für den Aufbau der Telefoninfrastruktur in Ost- und Zentraleuropa. Die Entwicklung von billigen Antennen mit einem Durchmesser von weniger als einem Meter, insbesondere VSATs (Very Small Apperture Terminals, auch Mikrostationen genannt), die schon in den Vereinigten Staaten weit verbreitet sind, erleichtert neue Punkt-zu-Mehrfachpunkt-Dienste. Die Unterscheidung zwischen Individual- und Massenkommunikation verschwimmt immer mehr. Mikrostationen können reine Empfangs- oder interaktive Empfangs- und Sendeterminals sein. Diese technische Entwicklung führt zur Entstehung von weltweiten mobilen „Overlay“-Telekommunikationsnetzen. Sie werden terrestrische Mobilfunknetze, die in dicht besiedelten Gebieten bestehen, ergänzen, allerdings nicht ersetzen. Satellitenkommunikation wird besondere Bedeutung in großen, dünn besiedelten Ländern wie Australien, Kanada und Rußland haben.

Das Raumsegment eines Satellitensystems steht im Eigentum einer internationalen Organisation wie z. B INTELSAT (International Telekommunications Satellite Organisation), EUTELSAT, INMARSAT (International Maritime Satellite Organisation), American Mobile Satellite Corporation (USA), TELESAT MOBILE (Kanada) oder AUSSAT (Australien). Dabei handelt es sich um kommerzielle Organisationen auf der Grundlage von zwischenstaatlichen Verträgen, die selbst allerdings keine Völkerrechtssubjekte sind. Alle Unterzeichnerstaaten haben einen gewissen Kapitalanteil an der Organisation. Die Satellitenorganisationen verkaufen Kapazitäten im Raumsegment entweder selbst oder durch Diensteanbieter.

Neue Dienste vor allem für geschlossene Benutzergruppen umfassen:

a) INTELSAT Business Service (IBS), der Sprachübermittlung, Fax, Telex, Datenübertragung, elektronische Post und Videokonferenzen integriert,

b) INTELNET-Dienste, die auf Datenverteilung und Datensammlung beschränkt sind,

c) nationales oder weltweites satellitengestütztes Paging.

Geostationäre Telekommunikationssatelliten (also Satelliten, die sich in einer gleichzeitigen Umlaufbahn zur Erdoberfläche bewegen), die gegenwärtig in Betrieb sind, reflektieren lediglich die Daten, die zu ihnen heraufgefunkt werden, auf einer anderen Frequenz hinunter zu einer anderen Erdfunkstation.

Eine neue Satellitengeneration könnte allerdings durchaus auf andere Weise arbeiten: Nicht-geostationäre Satelliten können Informationen von einem Punkt der Erdumlaufbahn zu einem anderen transportieren, was die Speicherung von Daten im Raumsegment über eine längere Zeit erforderlich machen würde, als für das bloße Reflektieren der Daten erforderlich ist. Ein deutscher Forschungssatellit, der gegenwärtig Wissenschaftlern in der Arktis dient, funktioniert auf diese Weise (wie ein Postbote).

Sobald Daten im Raumsegment verarbeitet werden, wachsen die klassischen Risiken für die informationelle Selbstbestimmung, die mit jeder Verarbeitung von personenbezogenen Daten verbunden sind. Die EG-Kommission hat erkannt, daß satellitengestützte Kommunikation sowohl nationale wie auch EG-Gesetzgebung umgehen kann. Allerdings hat die Kommission bisher kein überzeugendes Konzept entwickelt, wie diesen Risiken zu begegnen ist.

2. Positionsbestimmung und Flottenmanagement

Satelliten werden zunehmend für Zwecke der Navigation nicht nur von Schiffen (die das INMARSAT-System nutzen), sondern auch von Lastwagen und sogar Einzelpersonen genutzt.

EUTELTRACS ist ein europäisches satellitengestütztes System für die mobile Landkommunikation zum Management von LKW-Flotten. Die Position eines Fahrers und seine Bewegungen mit dem LKW können von einer Zentralstelle zu jeder Zeit überprüft werden. Dies spart für das Unternehmen Zeit und Geld und könnte auch zur Vermeidung von Verkehrsstauungen beitragen, wenn die Zentralstelle den Fahrern alternative Routen vorschlagen kann, die weniger überfüllt sind.

Das Global-Positioning-System (GPS – globales Positionsbestimmungssystem) wurde vom Pentagon entwickelt und erfolgreich im Golfkrieg getestet. Es beruht auf gegenwärtig 16 Satelliten (Ende 1993 werden es 21 sein), von denen jeder die genaue Zeit und Position aussendet, die von jedem, der mit einem GPS-Empfänger ausgerüstet ist, empfangen werden kann. Der Empfänger wiederum berechnet seine genaue Position im Verhältnis zum Satelliten. Dieses System erlaubt z. B. einer Reederei, den Standort jedes ihrer Schiffe weltweit zu ermitteln und dann Informationen an das Schiff über INMARSAT zu übermitteln. Piloten und in naher Zukunft auch Fahrer können das System zusammen mit digitalen Landkarten benutzen, um ihren Weg in unbekannter Umgebung zu finden.

Gleichzeitig ist es offensichtlich, daß mit einem solchen System ein elektronisches Bewegungsprofil des Einzelnen ohne dessen Einwilligung erzeugt werden kann.

3. Fernmessen und Fernwirken

Satellitengestützte Netze können auch genutzt werden, um Pipelines, Eisenbahnlinien, Stromleitungen und Ölquellen zu überwachen. Mit Hilfe der Fernmeßtechnik kann sogar die Temperatur in einem Kühlwagen kontrolliert und angepaßt werden. Zugleich würde dies auch eine verstärkte Überwachung der Arbeitnehmer bedeuten.

4. Fernerkundung

Fernerkundung ist eine ältere (ursprünglich militärische) Einsatzform von Satelliten, durch die Bodenschätze, Wolkenbildungen (für die Wettervorhersage) Umweltverschmutzung und sogar die Routen von Zugvögeln vom Himmel aus beobachtet werden können.

Im Jahre 1991 startete die European Space Agency (ESA) einen modernen Satelliten (ERS-I), um Umweltveränderungen zu erkunden. Dieser Satellit verfügt über ein Radarsystem (SAR-Synthetic Aperture-Radar), das in der Lage ist, sogar nachts oder durch eine geschlossene Wolkendecke Fotografien der Erdoberfläche zu machen. Dieser Satellit speichert bestimmte Daten, bis er eine Position erreicht, von der aus er sie zu der nächsten Erdfunkstation abstrahlen kann.

Fernerkundungssatelliten, die von den alliierten Streitkräften im Golfkrieg eingesetzt wurden, waren in der Lage, Objekte (z. B. Panzer) zu erkennen, die zwischen 1 und 5 Metern Kantenlänge hatten. Es ist sehr wahrscheinlich, daß Satellitentechnologie, die von den Militärs entwickelt wurde, mit einer gewissen zeitlichen Verzögerung auch für den zivilen Einsatz verfügbar sein wird.

> Die EG-Kommission plant, über Satellit zu kontrollieren, ob Landwirte eine geringere Menge einer bestimmten Getreideart anbauen, als die, für die sie Gemeinschaftszuschüsse erhalten. Die Technik wird bald verfügbar sein, z. B. mit Hilfe eines Satelliten die Schlagzeilen einer Zeitung zu lesen, die jemand an einer Bushaltestelle liest.

5.

Die unbestrittenen Vorteile der Satellitentechnologie werden begleitet von offensichtlichen Risiken für die Privatsphäre, sobald der Einzelne ins Blickfeld des Satelliten gerät. Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre sollten sich deshalb für internationale Abkommen einsetzen, die regeln,

— in welchem Ausmaß personenbezogene Daten im Weltall verarbeitet werden dürfen,

— wer der verantwortliche Datenverarbeiter ist, wenn personenbezogene Daten im Raumsegment gespeichert werden, und wer für die Datensicherheit verantwortlich ist,

— daß besondere technische Maßnahmen ergriffen werden müssen, z. B. sollten Verschlüsselungstechniken (die bereits im militärischen Bereich angewandt werden) für die zivile Nutzung ohne zusätzliche Kosten angeboten werden.

Der internationale Normungsprozeß für weltweite Mobilkommunikation über Satellit berücksichtigt den Datenschutz noch immer nicht hinreichend.

Gemeinsame Erklärung

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre, die sich zu ihrer XIV. Internationalen Konferenz in Sydney getroffen haben,

—begrüßen den Bericht der Arbeitsgruppe Telekommunikation und Medien,

—heben die Bedeutung der beschriebenen Probleme im Bereich des Fernmeldegeheimnisses und der Satellitenkommunikation hervor und

—stimmen darin überein, daß die technische und rechtliche Entwicklung im Bereich des Fernmeldegeheimnisses sorgfältig beobachtet werden muß, um die Privatsphäre des Einzelnen vor exzessiver Überwachung zu schützen.

14th Conference, 29. Oktober 1992, Sydney

Report of the Working Group on Telecommunication and Media on problems relating to the secrecy of telecommunications and satellite communications and Common Statement of the International Conference of Data Protection and Privacy Commissioners

---

Report

Secrecy of Telecommunications

1.

Every citizen making a telephone call has in principle the legitimate expectation that his telephone conversation will not be intercepted by anybody, especially by public authorities.

The principle of the inviolability of telephone conversations is therefore guaranteed in the constitutions of several countries such as Austria, Germany, Greece, The Netherlands, Portugal and Spain. Moreover, the European Convention on Human Rights guarantees everyone's right to respect for his private and family life, his home and his correspondence. This provision of the European Convention has been interpreted by the European Court of Human Rights as covering the secrecy of telephone conversations.

In many countries the interception of telephone communications is even regarded as a criminal offence. The mere allegation of illegal telephone tapping can also have far-reaching political consequences. Recently a Minister in the Irish Republic had to step down due to such allegations, to give but one example.

2.

On the other hand, it has always been accepted in most countries that under special conditions there have to be exemptions from the principle of the secrecy of telephone conversations. In Belgium as the only country with an absolute legal prohibition to intercept telephone conversations the government is preparing a bill allowing for equivalent exemptions.

Statistics show that telephone conversations have been tapped for purposes of criminal procedure in 1990 in 2 449 cases in Germany and in 2 031 cases in the Netherlands (Source: German Federal Minister for Post and Telecommunications; Dutch Ministry of Justice).

According to Article 8, 2 of the European Convention on Human Rights "there shall be no interference by a public authority with the exercise of . . . 'the right to respect for the secrecy of correspondence and telephone conversations' . . . except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". This catalogue of legal exemptions which the national legislature may provide for is very far-reaching and some European countries have adopted more restrictive rules to allow for telephone tapping (cf. also para. 2.4 of the Draft Recommendation on the Protection of Personal Data in the Area of Telecommunications Services, with Particular Reference to Telephone Services, adopted by the Council of Europe's Committee on Legal Co-operation (CDCJ), June 1992).

When studying recent developments in the national legislation the Working Group has noticed that although there may be some doubts as to the effectiveness of telephone tapping in so far as it is related to "organized crime" there is nevertheless a growing tendency to allow for additional exemptions to the principle of the inviolability of telephone communications. In Germany new legislation came into force this year authorizing an administrative body to tap telephone conversations in order to prevent illegal arms exports (even before criminal offences have been committed). In many countries telephone tapping can be initiated in criminal proceedings concerning specific serious crimes such as drug trafficking, murder and terrorist offences.

However, recently telephone tapping is seen by politicians as an effective weapon against "official corruptions" and "organized crime" (Australia, Germany). These categories of offences have not yet been and cannot be precisely defined. Therefore any legislation incorporating these imprecise categories involves the risk that unsuspected persons have their telephone calls intercepted.

Austria on the other hand introduced legislation obliging even the Secret Service to obtain a judicial order before telephone conversations can be tapped legally.

The need for a legal basis for any interference by a public authority with the right to secrecy of telecommunications is being interpreted very restrictively by the European Court of Human Rights. In its most recent jurisprudence the Court stressed that tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. The Court stressed that it was essential to have clear, detailed rules on the subject, especially as the technology available for use was continually becoming more sophisticated (Kruslin case, 7/1989/167/223, para. 33). For this reason (lack of precision) the French law governing telephone tapping was found contravening the European Convention on Human Rights. In the meantime France has followed the example of the United Kingdom and has passed a new act governing telephone tapping in order to meet the European Court's requirements.

The German Federal Constitutional Court has recently ruled that a precise legal basis is necessary to trace malicious calls, even if their contents are not being recorded.

There are three stages to be distinguished when telephones are to be monitored:

—the decision to intercept telephone communications;

—the implementation of that decision and

—the supervision of this surveillance measure after it has ended.

The decision to intercept telephone conversations may be taken by an administrative body (in the United Kingdom), by an organ of judicial investigations (in most countries) or by an administrative or a judicial authority depending on the purpose of the tapping (Germany). Data Protection and Privacy Commissioners are not involved in these decisions and have no jurisdiction to control them. This applies equally to the implementation of the surveillance order.

However, once the interception of telephone communications has stopped, there is a strong case for Data Protection and Privacy Commissioners to be able to control the use of data stemming from the tapping of telephone calls. In some countries there is a growing consciousness that Data Protection and Privacy Commissioners have an important role to play in this field although they may not yet have jurisdiction to that effect.

In the Netherlands the law may be changed in the near future so that results from telephone tapping will be recorded by the Criminal Intelligence Services in their files. Whenever in the Netherlands results from telephone tapping should be recorded in files – for instance in files held by the Criminal Intelligence Services – they would come under the competence of the Registration Chamber.

In Germany the Federal Data Protection Commissioner cannot interfere with the judicial proceedings leading to an order to intercept telecommunications. But the Federal Ministry for Post and Telecommunications has accepted that the Data Protection Commissioner controls whether the German TELEKOM carries out the court order properly, what kind of personal data are being collected when carrying out the court order and for which purpose they are used. It is essential that results of a surveillance measure are only used for the purpose for which the data were originally collected.

In several countries the law is or will be amended to allow for the interception of messages transmitted by other means of telecommunications (telefax, telex, data transmission etc.). Some of the legislation will also cover private network operators and service providers obliging them to cooperate with the police as required.

One must keep in mind that the interception of telecommunications, especially telephone tapping is not a usual means of Surveillance, automatically available against anyone committing certain crimes or causing a threat to national security. On the contrary, in most countries it is an exceptional method of investigation and is subject to additional conditions. In a number of countries the surveillance of telephone calls may only be ordered if someone is suspected of an offence which tapping can help to investigate and only if traditional methods of inquiry are impractical or have failed.

It is essential that the person whose telephone calls have been intercepted is notified by the public authority responsible of the fact that he has been subject to surveillance as soon as practicable without prejudicing the purpose of the surveillance.

Only then is the individual in a position to apply for a review of the measure by a judicial or another independent body. This notification of the data subject is so far only provided for in a few national legal systems.

3.

The right of the citizen to use the telephone without being registered and observed does not only protect him against the interception of the contents of his conversation but also against the use of the technical data generated by the telecommunications network (traffic data such as time, duration of the call and number of the called party) for other than billing purposes. However, the exemptions to this rule are even more wide-ranging than to the rule of confidentiality of the contents of the telephone conversation. In Belgium and in Germany such technical (metering) data may be used by in order of the investigating judge in criminal proceedings of any kind whereas telephone tapping in the narrower sense is in many countries restricted to a catalogue of specific crimes.

Again in this respect diverse tendencies can be noted in different legal systems. In Australia the Attorney – General's Department recently proposed to redefine the interception of a Communication to cover the listening to or recording of messages passing from one person to another over a telecommunications system without the knowledge of either party thereby excluding personal informations generated by the system itself (traffic data). This proposal has been strongly criticized by the Australian Privacy Commissioner. In his view traffic data and Signals information should be protected in the same way as the Contents of messages conveyed across the telephone network. Due to recent technological developments (especially the installation of digital telecommunications networks) traffic data are being systematically stored by the network operators and therefore during a certain period of time available for other purposes such as criminal proceedings. There is no reason for a different level of protection of the content data as opposed to the traffic data. The principle of secrecy of telephone conversations covers both their contents and their circumstances (time, duration and persons taking part in it).

For the same reason the German Conference of Data Protection Commissioners has urged the German Federal Parlament to repeal the old provision which allows for the use of traffic data for any criminal proceedings. When applied to digital networks that provision is no longer in line with the constitutional guarantee of secrecy of telecommunications.

4.

As the legislation regarding the interception of telecommunications is currently being amended in many countries that are represented in the Working Group this report can only be an interim report. It is necessary for the Data Protection and Privacy Commissioners to keep a close eye on the technological and legal developments in this field in order to protect the privacy of the individual against excessive state surveillance.

Satellite Communications

More than six years ago the VIIth International Conference of Data Protection Commissioners in Luxembourg passed a resolution on Data Protection and New Media stressing that the "use of satellites for communication likewise induces risks with regard to data integrity and protection against unauthorised monitoring".

Since then these risks seem to have been almost forgotten although there has been a virtual revolution in the skies as far as the capacity of satellites is concerned. The increase in capacity of European satellites from 1989 to 1993 will be 215 % (cf. EC Commission, Green Paper on satellite communications, Figure 5, p. 57).

Satellites can be used for a number of purposes, the most important being broadcasting and telecommunications. There are other possible applications such as worldwide

—positioning and fleet management,

—telemetry and remote controlling,

—remote sensing.

1. Telecommunications

A satellite system usually consists of at least two earth stations and the space segment. Information is beamed up from a high-powered earth station to the satellite ("uplink", a fixed point-to-point service). It is then re-transmitted by transponders on the satellite back to another earth station or several earth stations ("downlink"). The downlink can be specified in terms of services, such as a fixed (point-to-point telecommunications) service, a broadcasting (point-to-multipoint TV distribution) service, a mobile service, which beams down to moving receiving stations, such as trucks with roof-top antenna dishes. Modern satellites carry up to 16 transponders and each transponder can transmit up to two TV-channels or 1 700 telephone voice channels.

Within Europe only 2 %– 3 % of international telephone calls are made via satellite whereas satellites play a far greater role in trans-atlantic and inter-continental telecommunications accounting for nearly 60 % of traffic. Satellite communications networks are of great importance for the build-up of the telephone infrastructure in Eastern and Central Europe.

The emergence of low-cost terminal dishes (antennas) with diameters of less than 1 metre, especially VSATs (Very Small Aperture Terminals, also called microstations), which are already Widespread in the United States, facilitates new point-to-multipoint services. The distinction between individual telecommunications and broadcasting becomes increasingly blurred, Microstations may be receivers only or receive/transmit terminals (interactive). This technological development will lead to the emergence of worldwide mobile telecommunications "overlay" networks supplementing (not replacing) terrestrial cellular networks which are concentrated on densely populated areas. Satellite telecommunications will be especially important in large thinly populated countries such as Australia, Canada and Russia.

The space segment of a satellite system is owned by an international organisation such as INTELSAT (International Telecommunication Satellite Organization), EUTELSAT, INMARSAT (International Maritime Satellite Organization), American Mobile Satellite Corporation (USA), TELESAT Mobile (Canada) or AUSSAT (Australia). They are commercial organisations based on international treaties but they are not international legal persons themselves. All signatory states have a certain capital share in the organisation. The satellite organisations sell space segment capacity either themselves or through service providers.

New services especially for closed user groups include:

a) INTELSAT business service (IBS), which integrates voice, facsimile, telex, data, electronic mail and videoconferencing,

b) INTELNET services are confined to data distribution and data collection,

c) nationwide or worldwide satellite-based paging.

Geostationary telecommunications satellites (i.e. they are in stationary [synchronous] orbit relative to the ground) operating currently only reflect data that are beamed up on a different frequency down to another earth station.

However, a new generation of satellites may well work on a different basis: satellites which are not geostationary could transport informations from one point of the orbit to another which would require the storage of data in the space segment over a longer period of time than is necessary for reflecting the data. A German research satellite serving scientists in the Arctic is operating on this basis (like a "postman").

As soon as data are processed in the space segment the classical risks to privacy linked to any form of personal data processing become even greater. The European Commission has realized that communications via satellite tend to evade and by-pass national and even EC-legislation. However, the Commission has so far not developed a convincing plan to meet these risks.

2. Positioning and fleet management

Satellites are increasingly being used for purposes of navigation not only by vessels (using the INMARSAT system) but also by trucks and even individuals.

EUTELTRACS is a European satellite based system for land-mobile Communications to manage truck fleets. The position of a driver and his movements with the truck can be checked by a masterstation at any given time. This may save the company time and money and it may even contribute to prevent traffic jams if the masterstation can advise the drivers to take alternative routes which are less crowded.

The Global Positioning System (GPS) was developed by the Pentagon and successfully tested in the Gulf war. It relies on 16 Satellites (21 by the end of 1993) each of which sends the exact time and its position which may be received by anyone using a GPS-receiver which calculates the exact position of the satellite and the receiver. This system allows e.g. a shipping company to locate any of its vessels worldwide and then transmit informations to it via INMARSAT. Pilots and in the near future drivers may use the system together with digital maps to find their way in unknown surroundings.

At the same time it is obvious that an electronic profile of the individual's movements may be created by such a system irrespective of the individual's consent.

3. Telemetry and remote controlling

Satellite-based networks can also be used to monitor and control pipelines, railways, power lines and oil wells. By means of telemetry even the temperature in a refrigerator lorry may be checked and adjusted. At the same time that would mean an intensified surveillance of employees.

4. Remote sensing

Remote sensing is an older (originally military) application of satellites by which natural resources, cloud formations (weather forecast), environmental pollution and even passages of birds can be monitored from the sky.

In 1991 the European Space Agency (ESA) launched a modern Satellite (ERS-1) in order to explore environmental changes. This satellite operates a synthetic aperture radar (SAR) which is able to take pictures of the earth even by night or through a closed cloud cover. This satellite stores certain data until it reaches a position where it can beam them down to the nearest earth station.

Remote sensing satellites used by the allied forces in the Gulf war were able to recognize objects (e.g. tanks) which measured between 1 and 5 meters. lt is very likely that satellite technology developed by the military will be available for civilian use with a certain time lag.

The European Commission plans to control via satellite whether farmers grow less of a certain crop for which they claimed Community subsidies. The technology will soon be available e.g. to read via satellite the headlines of a newspaper which somebody is reading at a bus stop.

5.

The undisputed advantages of satellite technology are accompanied by obvious risks to privacy as soon as the individual comes into focus. Data Protection and Privacy Commissioners should therefore press for international agreements which regulate

—to what extent personal data may be processed in outer space,

—who is the controller of the file, if personal data are stored in the space segment and who is responsible for data safety,

—that special technical measures have to be taken, e.g. encryption services (already in use in military satellites) should be offered for civilian use without additional charges.

The international standardization process for worldwide mobile Communications via satellite still does not sufficiently take data protection into account.

Common Statement

The Data Protection and Privacy Commissioners meeting at their XIVth International Conference in Sydney

—welcome the report of the Working Group on Telecommunications and Media,

—underline the importance of the issues raised in the areas of secrecy of telecommunications and Satellite communications and

—agree to keep a close eye on the technological and legal developments in the field of secrecy of telecommunications in order to protect the privacy of the individual against excessive surveillance.

C. Stellungnahmen der Arbeitsgruppe Telekommunikation und Medien der Internationalen Konferenz der Datenschutzbeauftragten

Memorandum and Statement of the Working Group on Telecommunications and Media of the International Conference of Data Protection Commissioners

Memorandum

zum Vorschlag der EG-Kommission

für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen

auf der Grundlage der Beratungen der Arbeitsgruppe am 12. November 1990 in Berlin

Vor dem Hintergrund des Beschlusses der 12. Internationalen Konferenz der Datenschutzbeauftragten vom 19. September 1990 zu Problemen öffentlicher Telekommunikationsnetze und des Kabelfernsehens begrüßen die Datenschutzbeauftragten der EG-Mitgliedstaaten die Initiative der EG-Kommission, einen Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen vorzuschlagen. Ein gemeinschaftsweiter Schutz von Teilnehmerdaten und eine Beschränkung elektronischer Spuren auf das unerläßliche Minimum sind von entscheidender Bedeutung und können effektiv nur durch Gemeinschaftsrecht gewährleistet werden. Die Datenschutzbeauftragten der EG-Mitgliedstaaten unterstützen deshalb grundsätzlich den Vorschlag der Kommission. Sie regen allerdings einzelne Veränderungen des Entwurfs an, um den Datenschutz auf europäischer Ebene zu verbessern.

Während und nach der Einführung von ISDN werden analoge Netze noch für eine beträchtliche Zeit parallel zum ISDN weiterbestehen. Es ist deshalb von entscheidender Bedeutung, daß die Regelungen der Richtlinien umgesetzt werden, bevor analoge Netze aufhören zu bestehen. Art. 2 Abs. 2 des gegenwärtigen Entwurfes sollte insoweit um eine Klarstellung ergänzt werden, damit Umgehungsversuche vereitelt werden. Ohne diese Klarstellung könnte man sich auf den Standpunkt stellen, daß die Vorschriften der Richtlinie in solchen Mitgliedstaaten, die ISDN oder öffentliche digitale Mobilfunknetze bereits eingeführt haben, nicht auf Dienste in weiterbestehenden analogen Netzen anwendbar sind.

Der Entwurf verwendet die Begriffe „Telekommunikationsgeräte“ (Art. 1 Abs. 1) und „Anbieter der Dienste“ (Art. 16 Abs. 2), ohne sie zu definieren. Dies ist jedoch notwendig, um den genauen Anwendungsbereich der Richtlinie festzustellen. Es ist z. B. unklar, ob und in welchem Umfang Anbieter von Mailbox-Diensten von der Richtlinie erfaßt werden. Private Dienste-Anbieter sollten erfaßt werden, wenn sie für die Öffentlichkeit Telekommunikationsdienste erbringen unabhängig davon, ob die Mitgliedstaaten ihnen „besondere oder ausschließliche Rechte“ gewährt haben. In bestimmten Mitgliedstaaten

(z. B. in der Bundesrepublik) besteht keine Notwendigkeit, die Gewährung solcher „besonderen oder ausschließlichen Rechte“ zu beantragen, um auf privater Basis derartige Dienste erbringen zu können. Die Begriffsbestimmungen in Art. 3 des Entwurfs sollten dementsprechend geändert werden.

Die 12. Internationale Konferenz der Datenschutzbeauftragten hat betont, daß jeder Teilnehmer das Recht hat, gebührenfrei und ohne Begründung den Eintrag seiner Daten in ein Teilnehmerverzeichnis auszuschließen. Dieses Recht sollte in einem gesonderten (neuen) Artikel des Richtlinienentwurfs bekräftigt werden. Dieser könnte wie folgt lauten:

„Teilnehmerverzeichnisse

(1) Teilnehmer haben das Recht, gebührenfrei und ohne Begründung den Eintrag ihrer Daten in ein Teilnehmerverzeichnis auszuschließen.

(2) Ein Teilnehmerverzeichnis sollte nur solche personenbezogenen Daten enthalten, die unbedingt zur hinreichend sicheren Identifikation bestimmter Teilnehmer erforderlich sind. Die Teilnehmer haben auch das Recht, einen Hinweis auf ihr Geschlecht und ihren Wohnort auszuschließen. Dies schließt die Veröffentlichung zusätzlicher Daten auf Wunsch des Teilnehmers nicht aus.“

Art. 4 (1) des Entwurfs müßte entsprechend modifiziert werden.

In Art. 5 Abs. 2 des Entwurfs sollte eine klare Unterscheidung zwischen der Verantwortung der Telekommunikationsorganisationen einerseits und der Dienste-Anbieter andererseits aufgenommen werden. Sie könnte wie folgt formuliert werden:

„(2) Die Inhalte der übertragenen Information dürfen von der Telekommunikationsorganisation nur im Auftrag von Dienste-Anbietern insoweit gespeichert werden, als diese vertraglich zur Speicherung von Inhaltsdaten verpflichtet sind, es sei denn, dies ist aufgrund von Verpflichtungen erforderlich, die in den Mitgliedstaaten dem Gemeinschaftsrecht entsprechend gesetzlich vorgeschrieben sind.“

In Art. 7 Abs. 1 sollte das Wort „grundsätzlich“ gestrichen und der Satz entsprechend umgestellt werden. Folgender neuer Satz 2 sollte diesem Absatz angefügt werden:

„Jeder Mitgliedsstaat erläßt Vorschriften für strafrechtliche Sanktionen, um die Vertraulichkeit personenbezogener Daten, die bei der Bereitstellung von Telekommunikationsnetzen und -diensten verarbeitet werden, zu gewährleisten.“

In Art. 7 Abs. 2 (Sätze 1 und 3) sollte das Wort „schriftlich“, das bereits in der deutschen Entwurfsfassung enthalten ist, auch in die französischen und englischen Fassungen übernommen werden.

In Art. 8 Abs. 1 sollten die Worte „dem Stand der Technik entsprechenden, angemessenen Schutz“ ersetzt werden durch die Worte „wirksamen, hohen Standard des Schutzes“. In Abs. 2 desselben Artikels können die Worte „der Verletzung der“ ersetzt werden durch „für die“.

Die 11. Internationale Konferenz hat anonyme Zahlverfahren für bestimmte Telekommunikationsdienste wie das Telefon und Datenübertragungsdienste gefordert, um die Speicherung von Gebührendaten zu begrenzen. Dies sollte in der Formulierung des Artikels 9 des Richtlinienentwurfs zum Ausdruck kommen.

Art. 12 Abs. 3 sollte wie folgt umformuliert werden:

„(3) Bei Verbindunqen zwischen einem Teilnehmer, der mittels analoger Technik an eine Vermittlungsstelle angeschlossen ist, und einem Teilnehmer, der mittels digitaler Technik an eine Vermittlungsstelle angeschlossen ist, muß ersterer über die Möglichkeit informiert werden, daß seine Rufnummer angezeigt wird. Die Telekommunikationsorganisation muß die vorherige schriftliche Einwilligung dieses Teilnehmers einholen, bevor sie die Möglichkeit der Rufnummernanzeige schafft. Dieser Teilnehmer muß ebenfalls die Möglichkeit haben, die Rufnummernanzeige von Fall zu Fall auszuschließen.“ (letzter Satz unverändert)

Die 12. Internationale Konferenz hat betont, daß die Möglichkeit der Unterdrückung der Rufnummernanzeige von Fall zu Fall in gleicher Weise bestehen muß, wenn grenzüberschreitende Telefongespräche geführt werden. Deshalb sollte ein neuer Art. 12 Abs. 4 in den Entwurf aufgenommen werden:

„(4) Wenn ein Teilnehmer die Unterdrückung der Rufnummernanzeige bei Auslandsgesprächen mit Teilnehmern in solchen Mitgliedstaaten beantragt hat, in denen bisher keine den Absätzen 1 bis 3 dieses Artikels entsprechenden Maßnahmen ergriffen worden sind, so darf die Verbindung nur ohne Rufnummernanzeige beim angerufenen Teilnehmer hergestellt werden.“

Bisher enthält der Entwurf lediglich in Art. 13 Abs. 3 eine Regelung der gemeinschaftsweiten Aufhebung der Unterdrückung der Rufnummeranzeige in bestimmten Fällen.

Art. 16 Abs. 1 des Entwurfs sollte wie folgt präzisiert werden:

„Die Telekommunikationsorganisation darf die Telefonnummer sowie sonstige personenbezogene Daten des Teilnehmers, insbesondere Art und Länge seiner Bestellungen über einen Teleshopping-Dienst oder die über einen Videotext-Dienst angeforderten Informationen, nur im Auftrag eines Dienste-Anbieters und nur insoweit speichern, als dies unbedingt zur Erbringung des Dienstes erforderlich ist. Diese Daten dürfen nur vom Dienste-Anbieter und ausschließlich für die vom Teilnehmer gestatteten Zwecke verwendet werden.“

Angesichts der wachsenden Bedeutung der Direktwerbung über Telefon und Telefax z. B. durch automatische Wählvorrichtungen sollte Art. 17 des Entwurfs in der Weise modifiziert werden, daß jeder Teilnehmer das Recht hat, keine Telefonanrufe oder Telekopien zu Werbezwecken oder mit Angeboten von Gütern und Dienstleistungen zu erhalten, wenn er dem nicht zuvor schriftlich zugestimmt hat.

In Art. 17 Abs. 2 sollte deutlicher gemacht werden, daß nur der Dienste-Anbieter dafür verantwortlich ist, die notwendigen Maßnahmen dafür zu treffen, daß die Übermittlung von aufgedrängten Informationen (insbesondere Werbung) an den Teilnehmer unterbleibt, und eine Liste mit schriftlichen Einverständniserklärungen zu führen. Anderenfalls würde die Telekommunikationsorganisation das Fernmeldegeheimnis im Sinne des Art. 7 Abs. 1 verletzen.

Memorandum

on the Proposal of the EC Commission

for a Council Directive concerning the protection of personal data and privacy in the integrated services digital network (ISDN) and public digital mobile networks

based on the discussions of the Working Group on 12 November 1990 in Berlin

In view of the resolution on problems related to public telecommunications networks and cable television adopted by the XIIth International Conference of Data Protection Commissioners on 19 September 1990 the Data Protection Commissioners of EEC Member States welcome the initiative taken by the EC Commission to propose a Draft Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks. A Community-wide protection of subscribers' data and a reduction of electronic traces to the necessary minimum are essential and can only be ensured effectively by community legislation. The Data Protection Commissioners of EC Member States therefore support in principle the proposal put forward by the Commission. They suggest, however, specific amendments in the Draft to improve data protection on the European level.

During and after the introduction of ISDN analogue networks will Continue to exist parallel to ISDN for quite some time. It is therefore essential that the provisions of the Directive should be implemented before analogue networks have ceased to exist. Art. 2 par. 2 of the present Draft needs clarification in this respect in order to prevent circumvention. Without this clarification one could argue that the provisions of the Directive do not apply to services based on analogue networks in Member States which have implemented ISDN or public digital mobile networks.

The Draft refers to "telecommunications equipment" (Art. 1 par. 1) and "service provider" (Art. 16 par. 2) without defining these terms. This is however necessary in order to determine the exact scope of the Directive. It is e. g. not clear whether and to what extent providers of mailbox services will be covered by the Directive. Private service providers should be covered if they provide services to the public irrespective of "special or exclusive rights" granted to them. In certain Member States (e. g. the Federal Republic) there is no need to apply for special or exclusive rights in order to provide services on a private basis. The definitions in Art. 3 of the Draft should be amended accordingly.

The XIIth International Conference of Data Protection Commissioners has stressed that subscribers have the right, free of charge and without having to give reasons, to have no personal data included in a directory. Therefore a new Article should be included in the Draft dealing with directories in particular. This Article could read as follows:

"Directories

(1) Subscribers have the right, free of charge and without having to give reasons, to have no personal data included in a directory.

(2) Personal data contained in a directory should be limited to such as are strictly necessary to identify reasonably a particular subscriber. He/she also has the right not to indicate his/her sex. This does not exclude the publication of additional data at the request of the subscriber."

Art. 4 par. 1 of the Draft should be amended accordingly.

Art. 5 par. 2 of the Draft should be clarified in order to keep a clear distinction between the responsibilities of telecommunications organizations and service providers in the following way:

"(2) The contents of the information may be stored by the telecommunications organization only on behalf of service providers inasmuch as they are under a contractual obligation to store content data, except where required by obligations imposed by the law of the Member State, in conformity with Community law."

In Art. 7 par. 1 the words "In principle," should be deleted. The following new second sentence should be added to this provision:

"Each Member State shall make provision for penal sanctions in order to ensure confidentiality of personal data processed in connection with telecommunication networks and services."

In Art. 7 par. 2 (first and third sentence) the word "written" should be inserted before consent in the French and English version of the Draft. It is already contained in the German version.

In Art. 8 par. 1 the words "adequate, state-of-the-art" should be replaced by "effective, high-standard". In par. 2 of the same article the words "of a breach of" can be replaced by "to".

The XIth International Conference has called for anonymous payment procedures for certain telecommunications services such as telephone and data transfer services in order to limit the storage of billing data. This should be reflected in the wording of Art. 9 of the Draft Directive.

Art. 12 par. 3 should be redrafted in the following way:

"(3) With regard to communications between a subscriber linked to an exchange by an analogue connection and subscribers linked to an exchange by a digital connection, the former subscriber is to be informed of the possibility of the identification of his/her telephone number. The telecommunications organization is to obtain this subscriber's prior written Consent before it starts operating the possibility of identification. This subscriber must also have the possibility to eliminate the identification on a case-by-case basis." (Last phrase unchanged)

The XIIth International Conference stressed that the possibility to suppress the calling line identification on a call-by-call basis shall be equally guaranteed when operating international calls. Therefore a new Art. 12 par. 4 should be included in the Draft:

"(4) In case a subscriber has asked to eliminate the identification of his/her telephone number when making a call to a State where the provisions of Art. 12 pars. 1–3 have not been implemented the connection shall be established without identifying the calling subscriber's telephone number."

The present Draft only provides for the operation of the override function on a Community-wide basis (Art. 13 par. 3).

Art. 16 par. 1 of the Draft should be clarified as follows:

> "The telecommunications organization may only store the telephone number as well as other personal data of the subscriber, in particular concerning the quantity and nature of his/her orders when using a teleshopping service or concerning the information requested via a videotex service, on behalf of a service provider to the extent strictly necessary to supply the service. These data may only be used by the service provider for purposes authorized by this subscriber."

Bearing in mind the growing importance of direct marketing by telephone or telefax e. g. via automatic calling devices Art. 17 should be redrafted in such a way that every subscriber has the right not to receive calls for advertising purposes or for the purpose of offering the supply or provision of goods and services without his/her prior written consent.

In Art. 17 par. 2 it should be made clearer that only the service provider concerned is responsible to take the steps necessary to terminate the transmission of unsolicited messages to the subscribers and to keep a list of written consent declarations. Otherwise there was bound to be a breach of confidentiality in the sense of Art. 7 par. 1 by the telecommunications organization.

Stellungnahme

vom 6. Februar 1991 zum Artikel 19 des Vorschlags der EG-Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

Die Arbeitsgruppe Telekommunikation und Medien der Internationalen Konferenz der Datenschutzbeauftragten erörterte auch Artikel 19 des Entwurfs einer Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (COM[90]314 final-SYN 287) und die unterschiedlichen nationalen Regelungen des Verhältnisses zwischen Datenschutz und Pressefreiheit. Die Arbeitsgruppe schlägt keine bestimmte Änderung des Entwurfstexts (Art. 19) vor, regt aber an, seine Formulierung erneut zu überprüfen, um eine präzisere Abgrenzung der zulässigen Ausnahmen zu erreichen. Insbesondere sollten die folgenden Punkte berücksichtigt werden:

Das Medienprivileg sollte sich nur auf Datensammlungen für journalistische Zwecke erstrecken;

Das Privileg sollte auch für zu journalistischen Zwecken gesammelte Daten nicht gelten, wenn sie Dritten für andere Zwecke (z. B. Werbezwecke) zugänglich gemacht werden;

Wenn eine Recht zur Veröffentlichung einer Gegendarstellung oder Richtigstellung besteht, sollte ein Hinweis auf diese Gegendarstellung oder Richtigstellung zusammen mit dem ursprünglichen Text gespeichert werden;

Das Recht des Einzelnen auf Zugang zu veröffentlichten Informationen, die über ihn gespeichert sind, sollte erhalten bleiben (außer wenn dies zur Bekanntgabe der Informationsquelle führen würde);

Die Existenz des Medienprivilegs darf nicht zu einem völligen Fehlen der Datenschutzkontrolle führen. Falls personenbezogene Daten über Abonnenten einer Zeitschrift oder Nutzer eines Informationsdienstes verarbeitet werden, sollte sich das Medienprivileg nicht auf solche Daten erstrecken.

Statement

of 6th February 1991 on Article 19 of the Proposal of the EC Commission for a general Data Protection Directive

The Working Group on Telecommunications and Media of the International Data Commissioners Conference also discussed Article 19 of the Draft Directive concerning the protection of individuals in relation to the processing of personal data (COM[90]314 final-SYS 287) and the different national approaches to data protection and freedom of the press. The group does not propose any particular new formulation of the text of article 19, but suggests that it should be reexamined with a view to a more precise limitation on the derogation permitted. In particular, the following points need to be considered:

- that the media privilege should extend only to data collected for journalistic purposes;
- that the privilege should not extend to such data if they are made available to third parties for other purposes (for example marketing);
- that if there is a right to have a counter-statement or a correction published, a reference to this statement or correction should appear with the original text;
- that the right of access by an individual to published information stored about him or her (except for revealing the identity of the source) should be retained;
- that the existence of a privilege for the media should not mean a complete absence of data protection control.

In the case that personal data are collected on subscribers to a journal or users of an information service, any media privilege should not apply to such data.