Berliner
Datenschutzbeauftragter

BERLIN

Landesbeauftragter für den Datenschutz
Freie Hansestadt Bremen

Der Hamburgische
Datenschutzbeauftragte

Mobilfunk und Datenschutz

Materialien zum

20

Impressum:

Herausgeber: Berliner Datenschutzbeauftragter
verantwortlich: Claudia Schmid
Pallasstraße 25–26, 10781 Berlin
Telefon: (0 30) 7 83 88 44
Telefax: (0 30) 2 16 99 27
Bildschirmtext: * 92 67 90 #

Redaktion: Volker Brozio

Druck: Verwaltungsdruckerei Berlin
gedruckt auf Umwelt-Recycling-Papier
1. Dezember 1994

Mobilfunk und Datenschutz

Franz Werner Hülsmann
Sven Mörs
Peter Schaar

Inhaltsverzeichnis

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer 45. Sitzung am 16./17. Februar 1993 den Arbeitskreis Medien beauftragt, die Netzsicherheit des Mobilfunks zu untersuchen und der Konferenz über die Ergebnisse bei der nächsten Konferenz zu berichten. Aus diesem Bericht ist diese Broschüre entstanden.

1. Netzsicherheit im Mobilfunk – Grundsatzprobleme

1.1 Einführung

Die Übertragung personenbezogener oder sonstiger vertraulicher Daten mittels mobiler Kommunikationsdienste unterliegt besonderen Risiken, die sich aus den Spezifika des eingesetzten Übertragungsmediums „Luft“ ergeben. Anders als bei leitungsgebundener Kommunikation können die übertragenen Signale auf der „Luftschnittstelle“ nicht physikalisch gegen unbefugtes Mithören und Aufzeichnung abgeschirmt werden; dies gilt auch für solche Übertragungen, die „punktgenau“ erfolgen sollen (z. B. über Richtfunkstrecken) und für nur zum lokalen Gebrauch bestimmte Übertragungsnetze (Funk-LAN).

Ein zweites generell bei den meisten Funkdiensten auftretendes Problem besteht darin, daß die mobilen Kommunikationspartner geortet werden müssen, um erreichbar zu sein. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls – im Zuge des Verbindungsaufbaus – Informationen über ihren Standort ab. Diese Standortinformationen könnten durch den Netz- oder Dienstbetreiber – aber auch von Dritten – zur Bildung sogenannter „Bewegungsprofile“ mißbraucht werden.

Bei satellitengestützten Kommunikationsdiensten ist eine genaue Ortung zum Teil nicht erforderlich, aber gleichwohl möglich. Besonders problematisch ist hier, daß die Kommunikationsinhalte im gesamten Abstrahlbereich des Satelliten empfangen und ausgewertet werden können.

Die folgenden Ausführungen konzentrieren sich auf die oben genannten Problemfelder, wobei jeweils konkrete Dienste betrachtet werden.

1.2 Arten personenbezogener Daten

Die bei der Telekommunikation anfallenden Datenarten lassen sich grob in drei Gruppen untergliedern:

Bestandsdaten (oder auch Stammdaten) sind diejenigen Daten, die in einem Dienst oder Netz dauerhaft gespeichert und bereitgehalten werden. Hierzu gehören die Rufnummer und gegebenenfalls der Name und die Anschrift des Teilnehmers, Informationen über die Art des Endgerätes (analoges oder digitales Telefon, Telefaxgerät, Datensichtstation usw.), gegebenenfalls für den Anschluß jeweils verfügbare Leistungsmerkmale und Berechtigungen und Daten über die Zuordnung zu Teilnehmergruppen (z. B. zu einer Sammelanschlußgruppe).

Inhaltsdaten sind die eigentlichen „Nutzdaten“, d. h. die übertragenen Informationen und Nachrichten (gesprochene oder kodierte Texte, Bilder und im Wege der Fernverarbeitung übertragene Daten).

Verbindungsdaten geben Auskunft über die näheren Umstände von Kommunikationsvorgängen. Hierzu gehören Angaben über Kommunikationspartner (z. B. Rufnummern des rufenden und des angerufenen Anschlusses), Zeitpunkt und Dauer der Verbindung, in Anspruch genommene Systemleistungen, benutzte Anschlüsse, Leitungen und sonstige technischen Einrichtungen, Dienste und – bei mobilen Diensten – die Standortkennungen der mobilen Endgeräte.

Neben diesen Datenarten fallen in Telekommunikationsnetzen weitere Daten an, z. B. interne Systemdaten, die jedoch in der Regel nicht personenbezogen sind (z. B. interne Systemtabellen für die Leitungswegführung) oder jedenfalls keinen Bezug zu den Kommunikationspartnern haben (z. B. Paßwörter für die Systemwartung). Diese Daten werden bei der weiteren Darstellung nicht berücksichtigt.

Aus diesen grundlegenden Datenarten können weitere Datenarten abgeleitet werden, was jedoch zusätzliche Verarbeitungsschritte voraussetzt, z. B. Entgeltdaten für die teil-

nehmerspezifische Abrechnung und Verkehrsdaten (Daten über die Auslastung des Systems) für Planungs- und Servicezwecke.

1.3 Fernmeldegeheimnis

Das Fernmeldegeheimnis steht unter dem Schutz des Grundgesetzes (Artikel 10 GG). Während dieser grundrechtliche Schutz direkt nur gegenüber staatlichen Stellen gilt und somit nur öffentliche Betreiber von Telekommunikationseinrichtungen unmittelbar bindet, werden durch § 10 Fernmeldeanlagengesetz (FAG) alle Personen und Stellen, die für den öffentlichen Verkehr bestimmte Fernmeldeanlagen betreiben, beaufsichtigen oder sonst bei ihrem Betrieb tätig sind, ebenfalls zur Wahrung des Fernmeldegeheimnisses verpflichtet, also auch private Betreiber von Netzen und Anbieter von Diensten.

Das Fernmeldegeheimnis erstreckt sich sowohl auf die Inhaltsdaten als auch auf die „näheren Umstände des Fernmeldeverkehrs, insbesondere darauf, ob und zwischen welchen Personen ein Fernmeldeverkehr stattgefunden hat“ (§ 10 FAG). Geschützt sind also auch die Verbindungsdaten, wie das Bundesverfassungsgericht in seinem Fangschaltungs-Beschluß vom 25. Februar 1992 festgestellt hat. Daten über Art und Zeitpunkt der Kommunikation sind ebenso geschützt wie die Angaben über das Kommunikationsziel.

Nach den Feststellungen des Bundesverfassungsgerichts greift jegliche Registrierung von Telefon-Verbindungsdaten in das Fernmeldegeheimnis ein und bedarf folglich – zumindest soweit staatliche Stellen beteiligt sind – einer verfassungskonformen gesetzlichen Grundlage. Dies gilt auch für die Registrierung von Telefonnummern bei Fangschaltungen.

Das Fernmeldegeheimnis ist immer dann gefährdet, wenn Dritte, die nicht Urheber oder Adressat des Fernmeldeverkehrs sind, Kenntnis von der Tatsache erhalten, daß eine Kommunikation zwischen Teilnehmern stattfindet oder stattgefunden hat und unter welchen näheren Umständen sie abgewickelt wurde (hierzu gehört z. B. der Standort eines Mobiltelefons) und welche Informationen dabei übertragen wurden.

Verletzungen des Fernmeldegeheimnisses durch Personen, die beim Betrieb von Fernmeldeanlagen beschäftigt sind, werden gemäß § 354 Strafgesetzbuch (StGB) mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Andere Privatpersonen, die einen Kommunikationsvorgang gezielt oder zufällig mithören, unterliegen nicht den Strafandrohungen des § 354 StGB; unter Umständen kommen jedoch andere Straftatbestände in Betracht, etwa § 201 (Verletzung der Vertraulichkeit des Wortes) oder § 202 a StGB (Ausspähen von Daten).

Gemäß § 201 StGB wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer unbefugt das nichtöffentlich gesprochene Wort eines anderen auf Tonträger aufnimmt oder wer es unbefugt mit einem Abhörgerät abhört.

Nach § 202 a StGB wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer unbefugt Daten, die nicht für ihn bestimmt sind und die gegen einen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft. Der Tatbestand dürfte insbesondere dann erfüllt sein, wenn die Daten verschlüsselt übertragen werden (besondere Sicherung) und der Abhörer es schafft, die Daten wieder zu entschlüsseln und somit im Klartext zur Kenntnis zu nehmen.

Angesichts des nur unvollkommenen strafrechtlichen und technischen Schutzes von unverschlüsselt über die Luftschnittstelle übertragenen Informationen ist es dringend erforderlich, bei Nutzung derartiger Dienste technisch – d. h. im wesentlichen durch Verschlüsselung – sicherzustellen, daß eine unbefugte Kenntnisnahme bei der Übertragung unterbleibt.

1.4 Datenschutz

§ 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) definiert personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“. Der Schutz der personenbezogenen Daten ergibt sich – wie das Bundesverfassungsgericht bereits in seinem Volkszählungsurteil 1983 festgestellt hat aus dem Grundgesetz. Das informationelle Selbstbestimmungsrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (BVerfGE 65,1).

Für die Verarbeitung dieser Daten durch die Betreiber von Telekommunikationsnetzen und -diensten gibt es bereichsspezifische Regelungen, die den allgemeinen Bestimmungen des Bundesdatenschutzgesetzes vorgehen. Diese bereichsspezifischen Bestimmungen befinden sich zur Zeit in stetiger Veränderung. Zum einen hat das Bundesverfassungsgericht in dem oben zitierten Fangschaltungs-Beschluß entschieden, daß das Postverfassungsgesetz und die Datenschutzverordnung für die Deutsche Bundespost Telekom (Telekom-Datenschutzverordnung – TDSV) keine ausreichende verfassungskonforme Rechtsgrundlage für die Verarbeitung von Verbindungsdaten darstellen. Andererseits ergibt sich die Notwendigkeit zur Neufassung der entsprechenden Regelungen aus den durch II-Recht resultierenden Vorgaben zur Deregulierung bzw. Privatisierung des Telekommunikationswesens.

Zu den weiterhin geltenden Vorschriften gehört § 14 a Abs. 1 FAG bezüglich des Schutzes von Inhaltsdaten. Danach dürfen beim Erbringen von Telekommunikationsdienstleistungen Nachrichteninhalte nur aufgezeichnet, Dritten zugänglich gemacht oder sonst verarbeitet werden, soweit dies Gegenstand oder aus verarbeitungstechnischen Gründen Bestandteil der Dienstleistung ist. Damit soll sichergestellt werden, daß die Betreiber nur in eng umschriebenen Fällen berechtigt sind, übertragene Informationen zu speichern. Dies betrifft z. B. elektronische Postdienste oder auch Sprachmailbox-Systeme, bei denen Daten als Bestandteil der Dienstleistung gespeichert werden. Ferner sind solche Dienste betroffen, bei denen aus der besonderen Art der Datenübertragung – etwa bei paketorientierten Diensten gemäß CCITT X.25 – die einzelnen Datenpakete in den Vermittlungsrechnern für sehr kurze Zeiträume zwischengespeichert werden müssen. Diese Daten sind nach der „Zustellung“ an die Empfänger zu löschen.

Am 1. Januar 1995 ist das Gesetz zur Neuordnung des Postwesens und der Telekommunikation in Kraft getreten. Mit diesem Artikelgesetz wird das Fernmeldeanlagengesetz ergänzt und geändert. Eine neue Bestimmung (§ 10 a FAG-neu) verpflichtet die Betreiber von Fernmeldeanlagen zu technischen Vorkehrungen und sonstigen Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten, der programmgesteuerten Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Eingriffe, gegen äußere Angriffe und Katastrophen. Das FAG enthielt bislang keine derartigen bereichsspezifischen Datensicherungsregelungen, so daß bis dahin nur die einschlägigen Bestimmungen des BDSG (§ 9 – technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes) anzuwenden waren. § 10 a FAG-neu tritt nicht etwa völlig an Stelle der BDSG-Regelungen, sondern ergänzt und präzisiert teilweise die dort enthaltenen Vorgaben.

Entfallen sind die Ermächtigungen aus § 14 a Abs. 2 FAG und aus § 34 Abs. 3 Nr. 3 Postverfassungsgesetz zum Erlaß von Datenschutzverordnungen. An ihre Stelle ist eine neue Verordnungsermächtigung aus § 10 Postregulierungsgesetz (PTRegG) getreten. Darin werden datenschutzrechtliche Grundsätze (Verhältnismäßigkeit und insbesondere Beschränkung bei der Erhebung, Verarbeitung und Nutzung von Daten und der Grundsatz der Zweckbindung) vorgeschrieben. Daten über juristische Personen stehen

ausdrücklich den personenbezogenen Daten gleich. Ferner werden die folgenden zulässigen Verarbeitungszwecke aufgeführt:

— Begründen, inhaltliche Ausgestaltung und Änderung eines Vertragsverhältnisses,
— Herstellen und Aufrechterhalten einer Telekommunikationsverbindung,
— Entgeltermittlung (für den Nachweis der Entgelte und die Speicherungsdauer und den Umfang der Speicherung sind dem Kunden Wahlmöglichkeiten einzuräumen),
— Erkennen und Beseitigen von Störungen und
— Aufklärung von Leistungserschleichungen.

Für bestimmte weitere Zwecke (z. B. zur Gestaltung von Telekommunikations- und Informationsdienstleistungen) dürfen Daten nur mit ausdrücklicher Einwilligung verarbeitet werden. Weitere Vorschriften des § 10 PTRegG beziehen sich auf die Gewährleistung des Datenschutzes bei Einzelentgeltnachweisen und auf das Identifizieren von Anschlüssen bei Belästigungen (Fangschaltungen), wobei es ausdrücklicher schriftlicher Anträge der Kunden bedarf.

Die vorgenannten Verarbeitungsermächtigungen beziehen sich ausschließlich auf die näheren Umstände des Fernmeldeverkehrs, d. h. auf die Verarbeitung von Verbindungsdaten. Dagegen ist die Verarbeitung von Nachrichteninhalten außer unter den Voraussetzungen nach § 14 a Abs. 1 FAG nur unter sehr restriktiven Bedingungen zulässig, namentlich für das Aufklären und Unterbinden unzulässiger Nutzungen, wenn hierzu die Speicherung unerläßlich ist. In diesen Fällen sind das Bundesministerium für Post und Telekommunikation und die zuständige Datenschutzkontrollbehörde zu informieren; auch der Betroffene ist zu unterrichten, sobald dies ohne Gefährdung des verfolgten Zwecks möglich ist.

2. Terrestrische Dienste

Terrestrisch sind diejenigen Dienste, die grundsätzlich ohne Einsatz von Satellitenanlagen abgewickelt werden, z. B. das herkömmliche Telefon und Mobilfunkdienste. Dabei kann zwischen Mobiltelefonen zum Austausch von Sprache und mobilem Datenaustausch unterschieden werden. Die Funktionsprinzipien sind bei beiden Dienstarten gleich.

Bei Verbindungen von und zu bzw. zwischen Mobilfunkstationen muß zwischen unterschiedlichen Teilen des Verbindungsweges unterschieden werden (vgl. Abbildung 1):

— Der Verbindungsweg zwischen Mobil- und Basisstation: Hier werden sowohl die Informationen für den Verbindungsauf- und -abbau als auch die Gesprächsinhalte per Funk übertragen.
— Der Verbindungsweg zwischen den Basisstationen: Hier werden Festnetze benutzt; beim Mobiltelefon sind es bisher das ISDN der Deutschen Bundespost TELEKOM bzw. Standleitungen auf der Basis der ISDN-Technologie, bei mobilen Datendiensten können es z. B. das DATEX-P-Netz oder ein anderes X.25-Netz sein. Dieser Teil der Übertragung ist damit so (un)-sicher wie das Telefonieren bei der Benutzung von „normalen“ Telefonanschlüssen.

Alle Verbindungen – auch die zwischen zwei nebeneinander im Stau stehenden Autotelefonen – werden über die Basisstationen und das sie verbindende Festnetz abgewikkelt. D. h. insbesondere, daß alle datenschutzrechtlichen Aussagen zum Festnetztelefon auch für die Mobiltelefonnetze gelten. Auf die spezifische Gefährdung des Festnetzes wird hier nicht näher eingegangen.

2.1 Mobiltelefon

In diesem Kapitel sollen die speziellen datenschutzrechtlichen Risiken, die sich aus der Nutzung der schnurlosen Telefone sowie der Mobiltelefonnetze (B-, C-, D 1- und D 2-Netze sowie dem E-Netz) ergeben, dargestellt werden. Auf andere Risiken – wie z. B. negative Auswirkungen der Funkwellen auf den Menschen (Elektrosmog), Verkehrsgefährdung durch Ablenkung beim Autofahren oder Probleme, die sich aus dem Zwang der dauernden Erreichbarkeit ergeben – kann in dieser Broschüre nicht eingegangen werden.

2.1.1 Schnurlose Telefone

Schnurlose Telefone sind eigentlich keine Mobiltelefone, da der Anschluß direkt am Festnetz geschieht. Nur der Telefonhörer – mit entsprechend erweiterten Funktionen, wie z. B. einem Tastenfeld zum Wählen – ist in einem begrenzten Umfeld – zwischen 200 und 500 Metern – mobil. Statt einer Schnur gibt es eine Funkverbindung zwischen der direkt am Festnetz angeschlossenen Feststation und dem Mobilteil.

Die am weitestens verbreitete Technik benutzt analoge Funksignale nach dem CT 1-Standard (die Sprache wird unverschlüsselt und unverschleiert übertragen) bzw. dem CT 2-Standard (die Sprache wird verschleiert). In beiden Fällen können die Signale mit – inzwischen fachhandelsüblichen – Funkscannern abgehört werden, wobei für den CT 2-Standard ein – ebenfalls im Fachhandel erhältlicher – Inverter erforderlich ist. Somit können die über das Mobilteil geführten Gespräche in der Nachbarschaft mitgehört werden.

Es gibt aber auch bereits schnurlose Telefone, bei denen die Übertragung auf der Funkstrecke zwischen Mobilteil und Festnetzanschluß digitalisiert wird. Dazu wird der sogenannte DECT-Standard verwendet. Dieser Standard erlaubt auch eine Verschlüsselung der digitalisierten Signale. Von dieser Möglichkeit wird allerdings bei den meisten im Handel erhältlichen Geräten kein Gebrauch gemacht.

2.1.2 B- und C-Netz

Auf diese beiden Mobiltelefonnetze wird nur kurz eingegangen, da sie – insbesondere aber das B-Netz – technisch überholt sind. Neuanschlüsse beim B-Netz sind nicht mehr möglich.

2.1.2.1 Technik

Die Übertragung der Inhaltsdaten und der für den Verbindungsauf- und -abbau erforderlichen Daten erfolgt analog.

Beim B-Netz muß der/die Anrufende den gegenwärtigen Ort des angerufenen Mobiltelefons kennen, da im Netz nicht gespeichert wird, wo sich dieses zur Zeit befindet. Neben der Rufnummer des angerufenen Mobiltelefons muß daher die Kennzahl des Funkvermittlungsbereiches, in dem sich das angerufene Mobiltelefon befindet, bekannt sein.

Beim C-Netz gibt es eine bundeseinheitliche Rufnummer, unter der das Mobiltelefon unabhängig von seinem jeweiligen Standort erreicht werden kann – sofern es eingeschaltet ist und sich nicht gerade in einem Funkschatten befindet. Hierzu wird der momentane Standort des Mobiltelefons im C-Netz gespeichert.

2.1.2.2 Verbindungsdaten

Bei Gesprächen von Mobiltelefonen werden die Verbindungsdaten inklusive der Standortkennung von der DeTeMobil gespeichert und bis zu 80 Tage nach Rechnungsstellung aufbewahrt.

2.1.2.3 Inhaltsdaten

Die Übertragung der über Funktelefone des B- bzw. C-Netzes geführten Gespräche erfolgt analog. Daher ist ein Abhören solcher Gespräche auf der Funkstrecke mit inzwischen frei verkäuflichen Scannern relativ leicht möglich.

2.1.3 D-Netze

2.1.3.1 Technik

Bei den D-Netzen (D 1- und D 2-Netz) werden die Sprachsignale digitalisiert übertragen. Dies gilt sowohl für die Funkstrecke als auch im Festnetz. Hierzu sind die D-Netze an digitale Stand- bzw. Miet-Leitungen der Deutschen Bundespost TELEKOM angeschlossen. So können die Vorteile der Digitalisierung auch für die Verbindung im Festnetz genutzt werden. Jedes der beiden D-Netze besitzt eine eigene – vom anderen D-Netz getrennte – Infrastruktur.

Die für den Verbindungsaufbau notwendigen Daten – insbesondere die Wählinformationen – liegen in den D-Netzen ebenfalls in digitalisierter Form vor.

Mehrere Basisstationen (FuFSt – FunkFestStationen oder BSS – Base Station Systems) sind über eine Funkvermittlungsstelle (FuVSt oder Mobile Switching Center – MSC) an das Festnetz angeschlossen. Der von einem BSS erfaßte Bereich wird auch als Funkzelle bezeichnet und hat in Abhängigkeit von den örtlichen Gegebenheiten einen Radius von durchschnittlich 35 Kilometern.

In den MSC findet der wesentliche Teil der Verwaltung der D-Netze statt. Um eine Verbindung zu einem Mobiltelefon aufbauen zu können, muß der Netzbetreiber den momentanen Standort dieses Mobiltelefons kennen. Hierzu wird eine für jeden Mobilanschluß eindeutige Kennung verwendet, die auf einer Chipkarte gespeichert ist. Diese Chipkarte ist zum Betrieb des Mobiltelefons erforderlich. Beim Einschalten des Gerätes meldet es sich mit der Chipkarten-Kennung bei der nächsten Basisstation an. Diese schickt (über das Festnetz) die Information über den Aufenthaltsort des Mobiltelefons an das zuständige MSC, bei dem die Kennung der Chipkarte registriert ist. Dort befindet sich das zu dieser Chipkarte gehörende Home Location Register (HLR). In diesem wird auch die jeweilige Basisstation gespeichert, in deren Bereich das Mobiltelefon sich gerade befindet, sowie festgehalten, ob das Mobiltelefon ein- oder ausgeschaltet ist.

Neben dem HLR ist in jedem MSC ein Visitor Location Register (VLR) vorhanden, in dem alle Mobiltelefone, die sich im Bereich dieser MSC aufhalten, registriert sind.

Als weitere Komponente enthält jedes MSC noch ein Authentication Center (AC). Hier wird der Zugang des Mobiltelefons zum D-Netz unter Verwendung der auf der Chipkarte gespeicherten Daten geprüft und der Schlüssel zur Verschlüsselung der Verbindung zwischen dem Mobiltelefon und der BSS generiert.

Bei einem Verbindungswunsch wird anhand der gewählten Rufnummer das zuständige MSC ausgesucht, bei dem die Chipkarte registriert ist. Dort wird aufgrund der im HLR eingetragenen Daten das MSC herausgefunden, in dessen Bereich sich das Mobiltelefon befindet. Der Ruf wird zu diesem MSC gelenkt, von wo aus er über das zuständige BSS ausgestrahlt wird. Das Mobiltelefon reagiert auf den Ruf, indem es sich gegenüber dem MSC authentifiziert. Wird während einer laufenden Verbindung der Bereich eines BSS verlassen, so wird die Verbindung automatisch vom nächsten BSS übernommen. Hierbei kann auch ein Wechsel des MSC erfolgen. Dies wird an das MSC in dem das Mobiltelefon registriert ist, übermittelt und in das dortige HLR eingetragen. Dieser Vorgang wird Roaming genannt.

Wird von einem Mobiltelefon aus eine Verbindung aufgebaut, muß sich das Mobiltelefon zuerst gegenüber dem Netz authentifizieren. Hierzu fordert das MSC, in dessen Bereich sich das Mobiltelefon gerade befindet, von dem MSC, in dem dessen Chipkarte

registriert ist, die Authentifizierungsparameter an. Nach der Authentifizierung wird dem Mobiltelefon der Schlüssel mitgeteilt, mit dem diese Verbindung zwischen BSS und Mobiltelefon verschlüsselt wird. Für jede neue Verbindung wird ein anderer Schlüssel zwischen BSS und Mobiltelefon verwendet.

2.1.3.2 Organisatorisches

Mobiltelefondienste unterschieden sich organisatorisch von den bisherigen Telefonnetzen in mehrfacher Hinsicht:

— Erstmals bieten private Netzbetreiber Übertragungsdienste an. Für die Übermittlung im Festnetz sind sie allerdings zur Zeit noch auf Leitungen der TELEKOM angewiesen. Mit der bis 1998 zu erwartenden EU-weiten Aufhebung des Telefondienst- und des Netzmonopols können Netzbetreiber ein eigenes Festnetz oder andere private Netze zur Verbindung der MSC nutzen.

— Die Teilnehmer und Teilnehmerinnen sind nicht darauf angewiesen, die Dienstleistung direkt von einem Netzbetreiber zu beziehen. Vielmehr werden Mobiltelefondienste auch von sogenannten Service-Providern angeboten. Die Serviceprovider stellen auf der Grundlage der durch die Netzbetreiber übermittelten Verbindungsdaten die in Anspruch genommenen Leistungen in Rechnung.

2.1.3.3 Welche Daten fallen an?

Es sind verschiedene Arten von Daten zu unterscheiden, die bei der Anmeldung zu einem der D-Netze bzw. bei der Nutzung dieser Netze verarbeitet werden.

Die Verarbeitung dieser Daten kann, je nach Vertragsgestaltung sowohl bei den Netzbetreibern als auch bei den Serviceprovidern erfolgen.

2.1.3.3.1 Bestandsdaten

Hierzu gehören vor allem Namen oder Firma, Anschrift, Zahlungsart und je nach Zahlungsart Bankverbindung oder Daten der Kreditkarte. Ebenfalls erhoben wird, ob ein Eintrag in die Kundenverzeichnisse (Telefonbücher, CD-ROM etc.) gewünscht wird und wie mit den Verbindungsdaten nach Rechnungsstellung verfahren werden soll (siehe dort). Mittlerweise ist es üblich, daß bei der Antragstellung eine Schufa-Auskunft eingeholt wird. Dabei werden personenbezogene Daten an die Schufa übermittelt. In Einzelfällen werden darüber hinaus Bonitätsdaten bei Wirtschaftsauskunfteien abgefragt.

2.1.3.3.2 Verbindungsdaten

Von den Netzbetreibern werden folgende Verbindungsdaten erhoben:

— Art der Verbindung (abgehender oder ankommender Anruf, Notruf),
— Kennung des rufenden und des gerufenen Anschlusses,
— Kennung des Ursprungs- und Zielstandortes (MSC und BSS),
— Verbindungsbeginn und -ende,
— Dienstekennung (z. B. Telefon, FAX, etc.),
— aktivierte Zusatzdienste und
— Datenaufkommen.

Die Verbindungsdaten werden von den MSC an das Abrechnungszentrum des jeweiligen Netzbetreibers geschickt. Dort werden die Entgeltdaten ermittelt und zusammen mit den Verbindungsdaten zur Rechnungserstellung verwendet oder an den zuständigen Serviceprovider übermittelt.

Nach Wahl des Kunden/der Kundin werden die Verbindungsdaten nach Rechnungsstellung entweder sofort gelöscht oder 80 Tage verkürzt oder komplett gespeichert. Ein

vollständige Speicherung wird von der DeTeMobil – soweit es die eigene Rechnungsstellung betrifft – zur Zeit nicht angeboten.

Die vollständige Speicherung der Zielrufnummern ist für den Fall vorgesehen, daß ein vollständiger Einzelentgeltnachweis beantragt wurde. Allerdings wird im D 1-Netz bislang aus Datenschutzgründen nur ein Einzelentgeltnachweis angeboten, bei dem die Zielnummern um die letzten drei Ziffern verkürzt sind. In diesem Fall werden die Zielnummern bei der DeTeMobil auch nur entsprechend verkürzt gespeichert. Hingegen sind bei verschiedenen privaten Service-Providern unverkürzte Einzelentgeltnachweise erhältlich.

2.1.3.3.3 Inhaltsdaten

Im Gegensatz zum B- und C-Netz, bei denen die Sprache analog übertragen wird, erfolgt in den D-Netzen eine digitalisierte Übertragung.

Das Abhören der Inhaltsdaten ist wegen der Digitalisierung nicht ganz so einfach wie bei den analogen Netzen, aber prinzipiell möglich. Mit einfachen Scannern können die Funkstrecken nicht abgehört werden. Eine Verschlüsselung der Daten auf der Funkstrecke nach dem GSM-Standard soll verhindern, daß – selbst mit entsprechender DV-Unterstützung – Gespräche auf den Funkstrecken abgehört werden. Dabei ist anzumerken, daß der Schutz u. a. auf der Geheimhaltung der Verschlüsselungsalgorithmen beruht. Diese Algorithmen sind allerdings zwangsläufig allen Herstellern von Mobiltelefonen und Basisstationen bekannt.

2.1.4 E-Netz

Für das E-Netz gelten grundsätzlich die im Abschnitt D-Netze enthaltenen Aussagen. Der Unterschied zu den D-Netzen ist ein technischer: Die Trägerfrequenzen liegen in einem anderen Bereich und die Mobiltelefone im E-Netz arbeiten im Vergleich zu den D-Netzen mit einer geringeren Sendeleistung. Wegen der prinzipiell kleineren Funkzellen ist eine genauere Ortung der Teilnehmer und Teilnehmerinnen möglich.

2.2 Funkruf

Mit Hilfe von Funkrufsystemen (auch paging-Dienste genannt) ist es möglich, einer Person ein Signal oder auch eine Nachricht zukommen zu lasssen. Die Art der übertragenen Nachricht und der Umfang der übertragenen Inhaltsdaten hängt von der eingesetzten Technik ab. Die Möglichkeiten reichen von einer rein akustischen Signalisierung (vier verschiedene Töne), deren Bedeutung vorher zwischen den Beteiligten entsprechend abgestimmt sein muß, z. B. „zu Hause melden“ oder „im Büro melden“, über numerischer Signalisierung (bis zu 15 numerische Zeichen), bei der dann z. B. die anzurufende Telefonnummer übermittelt werden kann, bis zur alphanumerischen Anzeige (bis zu 80 Zeichen), bei der dann auch eine Information wie z. B. „Termin von 14 Uhr verschoben auf 16 Uhr“ übermittelt werden können.

2.2.1 Eurosignal

Seit 1974 gibt es in der Bundesrepublik den Funkrufdienst Eurosignal. Außer in Deutschland wird dieser Dienst nur in Frankreich und der Schweiz angeboten. Der Dienst ermöglicht die Übermittlung eines Rufsignals an kleine tragbare Funkrufempfänger unter Verwendung eines beliebigen Telefonanschlusses, von DATEX-J, Telex oder Teletex. Die Bundesrepublik ist in drei Funkbereiche aufgeteilt (Nord, Mitte und Süd), die jeweils eine eigene Funkrufzentrale haben. An diese sind die Funkrufsender angeschlossen. Über Eurosignal ist eine Übermittlung von Zeichen oder Ziffern nicht möglich.

Da jedem Eurosignalempfangsgerät bis zu vier Eurosignalnummern zugeordnet werden können und am Empfangsgerät signalisiert wird, welche der vier Nummern „angepiepst“ wurde, können – bei entsprechender vorheriger Vereinbarung – vier verschiedene Informationen übermittelt werden.

Unbefugte können allein durch Abhören des Funkverkehrs deshalb keine inhaltlichen Daten erhalten.

2.2.2 Cityruf

Dieser Funkrufdienst wurde 1989 in Betrieb genommen. Hierbei ist die Übermittlung von Nur-Ton-Signalen, numerischen oder alphanumerischen Nachrichten möglich.

Es gibt vielfältige Möglichkeiten, einen Cityruf abzusetzen. Dies kann telefonisch, per DATEX-J, über Telex oder via Teletex erfolgen. Die telefonische Auftragserteilung kann entweder direkt – durch Anwahl der entsprechenden Funkrufnummer – oder über einen Auftragsdienst der Deutschen Bundespost TELEKOM erfolgen. Dort nimmt eine Platzkraft den Anruf entgegen und trägt die Daten des Funkrufs zur Aussendung in den Auftragsdienstrechner ein. Diese Daten werden nach der Aussendung des Funkrufes gelöscht. Bei der direkten Anwahl der Funkrufnummer können über die MFV-Signalisierung (Multifrequenzverfahren, bei dem den einzelnen Ziffern verschiedene Töne zugeordnet sind) sowohl Nur-Ton als auch numerische Nachrichten übermittelt werden. Bei Verwendung von PC und Modem können auch alphanumerische Nachrichten übertragen werden. Unabhängig von der Art der Auftragserteilung werden die Daten nach Aussendung des Funkrufes Im Auftragsrechner der DeTeMobil gelöscht.

Die Aussendung des Funkrufes selbst erfolgt in unverschlüsselter Form, so daß die Nachrichten mit Hilfe handelsüblicher Scanner abgehört werden können. Eine Zuordnung der Nachrichten zu den Empfängerinnen und Empfängern ist aber sehr schwierig, da die Funkrufnummern vor der Aussendung in eine nur dem jeweiligen Cityrufempfangsgerät und der Funkrufzentrale bekannten „Identifikationsnummer“ umgesetzt werden.

2.3 Mobile Datenübertragung – MODACOM

In den kommenden Jahren ist mit einer verhältnismäßig weiten Verbreitung von Diensten zur mobilen Datenübertragung zu rechnen. Dabei handelt es sich zum einen um spezielle für diesen Zweck konzipierte Dienste wie Modacom; zum anderen können in Zukunft auch digitale Netze nach dem GSM-Standard (z. B. D 1 und D 2) und andere digitale Kommunikationsnetze wie IRIDIUM und INMARSAT zur Datenübertragung eingesetzt werden (die diesbezüglichen Darstellungen erfolgen in den Abschnitten 2.1 und 3.).

Seit dem 1993 betreibt die Telekom-Tochter DeTeMobil den öffentlichen mobilen zellularen Datenübertragungsdienst „Modacom“ im Regelbetrieb. Dem vorangegangen ist eine einjährige Erprobungsphase in Nordrhein-Westfalen. Bis Ende 1995 soll Modacom mit etwa 900 Basisstationen eine bundesweite Flächendeckung von 80 Prozent erreichen, wobei vorhandene Basisstationen für das C- und D 1-Netz nach geringfügiger Modifikation mitgenutzt werden sollen.

Der Modacom-Dienst ist bislang auf Deutschland begrenzt; in anderen Ländern betriebene ähnliche Dienste sind mit Modacom nur teilweise kompatibel.

Eine zweite Lizenz für den Betrieb eines entsprechenden Dienstes ist 1994 an die Gesellschaft für Datenfunk (GfD) erteilt worden.

Das Modacom-System besteht aus folgenden Komponenten:

— einem terrestrischen Festsender-Kleinzellennetz mit Basisstationen (BS) zur Bereitstellung der Funkstrecke. Die BS sind über Festverbindungen (Base Station Link – BSL) mit einer Funkvermittlungseinrichtung (Area Communication Controller – ACC) als zweite Netzebene verbunden;
— den ACC selbst, die in örtlicher Nähe zum zentralen Netzkontrollzentrum (Network Management Center – NMC) untergebracht und mit diesem verbunden sind. Die ACC vermitteln ferner Verbindungen in das Datex-P-Netz der TELEKOM und in andere X.25-Dienste;
— dem NMC, das neben der betrieblichen Überwachung der Netzkomponenten die Erfassung und Verarbeitung aller Verbindungsdaten einschließlich Erstellung von Entgeltrechnungen übernimmt;
— den mobilen Terminals (spezielle Einbau- und Handgeräte, Laptops mit eingebautem Funkmodem oder sonstige mit einem Funkmodem verbundene Rechner).

Die Funkmodems buchen sich nach dem Anschalten im Netz ein, d. h. sie senden ein Signal aus, das von der nächsten Basisstation empfangen und an das NMC weitergeleitet wird. Dadurch wird der Standort der mobilen Terminals dem Netz bekanntgegeben. Die Terminals werden in eine Art Standby-Modus versetzt und können die für sie bestimmten Nachrichten empfangen.

Die Übertragung erfolgt mit einer technischen Übertragungsrate von 9 600 Bit/s. Die effektive Übertragungsrate (übertragene Nutzdaten) liegt allerdings – je nach Sende- und Empfangsbedingungen – deutlich niedriger.

Die Teilnehmerauthentifikation erfolgt mittels einer eindeutigen hardwarekodierten achtstelligen hexadezimalen Kennung (ID) der Funkmodems. Die ID wird von den Herstellern so in das Funkmodem integriert, daß jeder Versuch der Veränderung eine irreversible Zerstörung des Geräts zur Folge hätte (Herstellerangaben).

Die ID’s werden im Zentralrechner im NMC verwaltet. Beim Einbuchen wird geprüft, ob die übertragene ID zu den zugelassenen Dienstteilnehmern gehört. Auf diese Weise soll sichergestellt werden, daß nur autorisierte Teilnehmer den Dienst nutzen können. Bei Diebstahl bzw. Nichtbegleichung von Entgelten wird die jeweilige ID gesperrt. Ferner dient die ID als eindeutige Adresse des jeweiligen Senders/Empfängers.

Neben der eindeutigen ID können in den Funkmodems noch zusätzlichen „FlottenID’s“ (FID) gespeichert werden, die es – ähnlich wie geschlossene Benutzergruppen (GBG) bei anderen Diensten – ermöglichen, an einen definierten weiteren Empfängerkreis („Flotte“) gerichtete Nachrichten zu empfangen. Die FID werden ebenfalls in den NMC gespeichert. Anders als die ID können die FID durch Software durch den Hersteller auch nachträglich im Funkmodem geändert werden.

Die Daten werden auf der Luftschnittstelle – anders als bei D 1 und D 2 – nicht kryptographisch verschlüsselt übertragen. Allerdings erfolgt die Übertragung – aus Gründen der Übertragungssicherheit (Reduzierung der Bitfehlerrate) – verwürfelt nach einer Trellis-Kodierung. Die Daten können zusätzlich auf der Anwendungsebene, d. h. durch die Benutzer selbst, kryptographisch verschlüsselt werden. Die Anwendungsverschlüsselung kann jedoch nicht die zur Abwicklung der Kommunikation übertragenen Steuerungs und Vermittlungsinformationen umfassen.

Wie in broadcast-orientierten leitungsgebundenen Netzen (z. B. Ethernet) fischen sich die Funkmodems die für sie bestimmten Informationen aus dem übertragenen Datenstrom heraus. Dabei wird das Modem jeweils nur dann aktiviert, wenn eine Nachricht mit der jeweiligen Modem-ID oder einer im Modem gespeicherten FID übertragen wird.

Sowohl der genaue Authentifikationsmechanismus als auch das für die Datenübertragung verwendete Protokoll werden vom Betreiber und von den Herstellern geheimgehalten. Die Lizenznehmer (alle Hersteller außer dem Lizenzgeber Motorola) mußten sich zu strikter Geheimhaltung verpflichten.

Für Modacom ergibt sich folgende datenschutzrechtliche Beurteilung:

Eine Bewertung der Systemsicherheit von Modacom wird durch die Tatsache erschwert, daß die wesentlichen Systemfeatures nicht öffentlich gemacht werden. Die Systemsicherheit beruht offenbar zum großen Teil auf der Geheimhaltung der genauen Funktionsweise des Dienstes und der dabei verwendeten Protokolle („security by obscurity“).

Die ausschließliche Authentifikation der Teilnehmer gegenüber dem Netz mittels hardware-kodierter Kennungen ist deshalb problematisch, weil durch Manipulation der Hardware (-Änderung der Hardware-Adresse oder softwaremäßige Emulation derselben) bzw. durch unautorisierten Nachbau Maskeraden möglich werden könnten.

Da die Datenübermittlung per Funk unverschlüsselt erfolgt, könnten die übertragenen Informationen abgehört, aufgezeichnet und ausgewertet werden. Die Kodierung nach einem stets gleichen aber noch geheimgehaltenen Verfahren bietet zwar noch einen gewissen Schutz gegen „Gelegenheitshacker“, kann jedoch professionellen Angreifern schwerlich widerstehen. Diese Schwachstelle erscheint als besonders problematisch, wenn per Modacom die Authentifizierung bei stationären Rechnern erfolgt und Kennungen, Paßwörter oder sonstige sensible Informationen übertragen werden sollen. Die Nutzung des Dienstes für die Übertragung sensibler Daten kann deshalb nur dann vertreten werden, wenn auf der Anwendungsebene eine kryptographische Verschlüsselung implementiert wird.

Durch die Sendung und Registrierung von Informationen über den Standort könnten die Teilnehmer zwar auch von unautorisierten Abhörern lokalisiert und somit sowohl vom Dienstbetreiber als auch durch Dritte grundsätzlich Bewegungsprofile erstellt werden. Da die Funkzellen bei Modacom jedoch zur Zeit noch wesentlich größer sind als in den D-Netzen, sind die Standorte in derartigen Profilen allerdings nur verhältnismäßig grob abzubilden.

3. Satellitenkommunikation

Dem Einsatz von Satelliten kommt in der Telekommunikation eine ständig wachsende Bedeutung zu. Während Satelliten traditionell vor allem für Zwecke der Fernerkundung, der Verteilung von Radio- und Fernsehprogrammen und zum Herstellen von Telefonverbindungen über große Entfernungen hinweg benutzt wurden, dringen sie jetzt zunehmend auch in Bereiche vor, die bislang durch terrestrische Festnetz- oder Funkanlagen abgedeckt wurden, z. B. Mobiltelefonie und -datenübertragung. Zusätzlich wird das Angebot kontinuierlich um neue Dienste erweitert, die ohne Satelliteneinsatz bisher nicht möglich waren. Dazu gehören gegenwärtig vor allem Flottenmanagement-, Positionsbestimmungs- und Fernortungssysteme. Diese Dienste decken so unterschiedliche Bedürfnisse wie die Ortung gestohlener Fahrzeuge, Rationalisierung im Speditionsgewerbe und die Überwachung von Subventionsmaßnahmen auf EG-/EU-Ebene ab. Die Anzahl der Satellitenbetreiber, insbesondere aber die der Diensteanbieter vergrößert sich nach wie vor ständig.

Nach den vorliegenden Materialien haben die Belange des Datenschutzes in den Überlegungen von Satellitenbetreibern und Diensteanbietern bisher keine wesentliche Rolle gespielt. In dieser Broschüre wird zunächst eine Bestandsaufnahme der verschiedenen Einsatzfelder für Satelliten versucht. Gleichzeitig werden die wichtigsten Datenschutzrisiken herausgearbeitet.

3.1 Satellitentechnik

Die bisher gebräuchlichen Fernmeldesatellitensysteme bestehen in der Regel aus folgenden Komponenten:

über die Aufwärtsstrecke („uplink“) werden Informationen von leistungsstarken Erdfunkstationen (sogenannte „Hub-Stationen“) zum Satelliten abgestrahlt. Bei der Erdfunkstation kann es sich je nach Anwendung auch um eine Mobilanlage handeln.

Das „Raumsegment“ („space segment“) besteht aus sogen. „Transpondern“, die von der Erde empfangene Informationen in eine andere Frequenz umsetzen, verstärken und zur Erde zurückstrahlen.

Die Abwärtsstrecke („downlink“) besteht je nach Betriebsart des Satelliten aus einer fest definierten Punkt-zu-Punkt-Verbindung, einer Punkt-zu-Mehrpunkt-Verbindung oder einer Verbindung zu einer mobilen Empfangsstation. Dabei kann es sich z. B. um ein mobiles Satellitentelefon, aber auch um einen Lastkraftwagen mit einer mobilen Empfangsanlage handeln (Flottenmanagement).

Aus technischen Gründen werden für die Auf- und die Abwärtsstrecke unterschiedliche Frequenzbereiche genutzt: Gebräuchliche Kombinationen sind hier die Bereiche 4/6 GHz („C-Band“), 11/14 oder 12/14 GHz („Ku-Band“), infolge der fortschreitenden Überlastung dieser Frequenzbereiche aber auch zunehmend der Bereich 20/30 GHz. Für die Abwärtsstrecke wird dabei jeweils das niedrigere Frequenzband genutzt.

Es lassen sich zwei Typen von Satelliten unterscheiden: Geostationäre Satelliten sind in einer Umlaufbahn über dem Äquator mit ca. 36 000 km Entfernung zur Erde positioniert. Da ihre Umlaufgeschwindigkeit der der Erde entspricht, erscheinen sie von der Erde aus betrachtet wie „am Himmel aufgehängt“, als ortsfest. Da der 36 000 km-Orbit mittlerweile vollständig von Satelliten belegt ist – zwischen den Geräten muß ein Sicherheitsabstand von 2 bis 3 Grad eingehalten werden, damit sie sich nicht gegenseitig stören – werden Satelliten zunehmend auch auf niedrigeren Umlaufbahnen betrieben („low earth orbit“-Satelliten – LEO). Diese Satelliten sind von der Erde aus betrachtet nicht ortsfest, sondern umkreisen sie.

Bei der Datenübertragung via Satellit lassen sich verschiedene Prinzipien unterscheiden: Geostationäre Kommunikationssatelliten strahlen die von einer festen Erdfunk-

stelle oder einer mobilen Sendeanlage gesendeten Signale nach der Umsetzung in einen anderen Frequenzbereich verstärkt zu anderen ortsfesten Erdfunkstellen oder mobilen Empfangsanlagen zurück. Bei bereits in Planung befindlichen Satellitennetzen werden die empfangenen Daten unter Umständen vor der Zurückstrahlung zur Erde noch an andere Satelliten übermittelt. Weiterhin existieren Satelliten, deren regelmäßige Bewegung um den Erdball zum Transport von Daten genutzt wird. In diesem Fall werden die Daten in den Satelliten während des Transports im Orbit zwischengespeichert.

Gegenwärtig umkreisen allein ca. 500 Kommunikationssatelliten die Erde (Stand: Ende 1992). Diese Angabe berücksichtigt nicht die zahlreichen zivilen Fernerkundungssatelliten sowie militärische Satellitensysteme. Die Gesamtanzahl der im Orbit befindlichen Satelliten nimmt nach wie vor beständig zu.

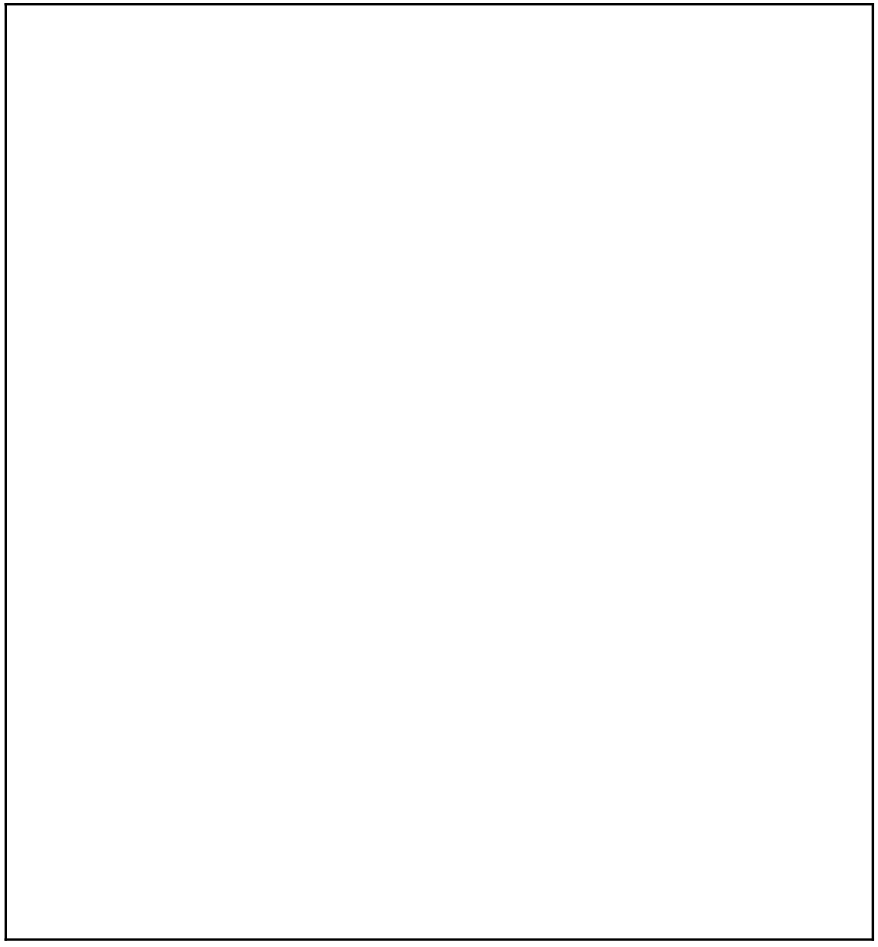

Abbildung: Prinzip der Satellitenkommunikation am Beispiel von INMARSAT (Quelle: Satellite Business, März 1993, S. 9)

3.2 Satellitenbetreiber

Das kontinuierliche Auftreten neuer Anbieter im Bereich der Satellitenkommunikation führt zu einer großen Unübersichtlichkeit des Angebots. Bei genauer Betrachtung sind die meisten Anbieter von Satellitendiensten jedoch keineswegs selbst Betreiber von Satelliten, sondern sie haben die Übertragungskapazitäten ihrerseits von anderen Unternehmern gemietet. Aufgrund des erheblichen Investitionsbedarfs für die Entwicklung und den Betrieb eines Satelliten sowie vor allem den Transport in die Orbitposition gibt es nur relativ wenige Organisationen, die selbst Satelliten betreiben. Dabei handelt es sich meist um internationale Konsortien oder um nationale Fernmeldebehörden. Diese vermieten dann Transponderkapazität ihrer Satelliten an andere Unternehmen oder Behörden („Signatare“), die darauf aufbauend Satellitenkommunikationsdienste am Markt anbieten.

Zu den für die Bundesrepublik wichtigsten kommerziellen Betreibern von Satelliten gehören

INTELSAT (International Telecommunications Satellite Organisation), eine internationale Organisation mit mehr als 100 Mitgliedsländern, die in 172 Ländern Kommunikationsdienste ihrer INTELSAT-Satelliten anbietet,

INMARSAT (International Maritime Satellite Organisation), eine 1975 gegründete internationale Organisation mit gegenwärtig ca. 70 Mitgliedern (Stand: April 1994), die sich zunächst vornehmlich mit dem Aufbau von Kommunikationsverbindungen zu Schiffen beschäftigte, ihr Geschäftsfeld aber mittlerweile auch auf Kommunikationsverbindungen zu Flugzeugen und mobilen Landfahrzeugen ausgedehnt hat,

EUTELSAT (European Telecommunications Satellite Organization), die 1977 von 26 europäischen Fernmeldeverwaltungen zur Verbesserung der innereuropäischen Satellitenverbindungen gegründet wurde und heute 38 Mitglieder hat. Neben TV-Übertragung, Telefon- und Datenübertragungsdiensten wird auch das Flottenmanagementsystem EUTELTRACS über EUTELSAT-Satelliten betrieben,

sowie die TELEKOM AG (ehemals Deutsche Bundespost TELEKOM), die im Augenblick drei DFS-KopernikusSatelliten unterhält, die zur Übertragung von TV-Programmen, für Fernmeldeverbindungen (vor der Vereinigung der beiden deutschen Staaten insbesondere solche zwischen der BRD und West-Berlin) und Datenübertragungsdienste genutzt werden.

Daneben betreiben zahlreiche weitere Einzelstaaten Satelliten zu zivilen und militärischen Zwecken, wobei früher ausschließlich militärisch genutzte Anlagen zunehmend auch für zivile Zwecke vermarktet werden.

3.3 Einzelne Satellitendienste

Satelliten werden für alle denkbaren Telekommunikationsdienste genutzt. Nutzer sind dabei zunächst staatliche Einrichtungen für Post und Telekommunikation oder deren privatisierte Nachfolgeorganisationen, wie z. B. die Deutsche Bundespost TELEKOM, die als Signatar an mehreren internationalen Satellitenorganisationen (INTELSAT, EUTELSAT, INMARSAT, INTERSPUTNIK) beteiligt ist.

Daneben nutzen auch Privatunternehmen zum Beispiel für die Verbindung von Konzernzentralen mit den verschiedenen Zweigstellen zunehmend Satellitentechnik für Telekommunikationszwecke. Hierbei kommt insbesondere die VSAT-Technologie zum Einsatz, die weiter unten gesondert erläutert wird.

Im folgenden werden einzelne spezielle Satellitendienste beispielhaft genauer beschrieben.

3.3.1 Satellitengestützte Ortung

3.3.1.1 Positionsbestimmungssysteme – zum Beispiel GPS

Das „Global Positioning System“ (GPS) erlaubt die satellitengestützte Bestimmung der eigenen Position an einem beliebigen Ort auf der Erde bis auf wenige Meter genau. Es besteht aus 21 „NavStar“-Satelliten, die die Erde in einer Höhe von 20200 km umkreisen. Mit einem GPS-Empfangsgerät werden die vier dem Standort am nächsten befindlichen Satelliten angepeilt. Auf der Grundlage der Signallaufzeiten wird der Standort berechnet.

GPS wurde im Auftrag des amerikanischen Verteidigungsministeriums entwickelt und im Golfkrieg erfolgreich getestet. GPS-Empfänger sind auf dem freien Markt erhältlich und werden gegenwärtig vor allem im Bereich der Schiffahrt, aber auch für die Positionsbestimmung im Autoverkehr genutzt. Auch die Anwendung für den instrumentengesteuerten Flugbetrieb ist bereits erprobt worden.

GPS selbst ist ein „passives“ System; die Positionsdaten werden zunächst nur an das abfragende Empfangsgerät gesandt. Dies geschieht nicht ständig, sondern nur auf Anforderung durch das Empfangsgerät. Personenbezogene oder -beziehbare Daten, die ohne eine Kontrolle des Betroffenen erhoben oder verarbeitet werden, fallen daher zunächst nicht an. Das System wird jedoch im Rahmen von anderen Diensten (Ortung gestohlener Fahrzeuge, Flottenmanagement) zur Positionsbestimmung genutzt. Die mit GPS gewonnenen Informationen können in diesen Systemen zur Erzeugung von Bewegungsbildern genutzt werden.

Rußland betreibt ein GPS-ähnliches, ursprünglich ebenfalls militärischen Zwecken gewidmetes System unter dem Namen „GLONASS“. Funktionsweise und Leistungsumfang entsprechen in etwa denen des GPS-Systems. Mit einer zukünftigen kommerziellen Vermarktung auch dieses Systems ist zu rechnen.

3.3.1.2 Flottenmanagementsysteme – zum Beispiel EUTELTRACS

EUTELTRACS ist ein Duplex-Satellitendienst für Standortbestimmung und Nachrichtenaustausch. Das System wird überwiegend von Speditionen im Bereich des Flottenmanagements eingesetzt. Für EUTELTRACS werden zwei geostationäre EUTELSAT-Satelliten genutzt, deren Ausleuchtungszone ganz Europa, aber auch Teile des mittleren Ostens und Nordafrikas umfaßt.

EUTELTRACS wird gegenwärtig in 11 europäischen Ländern von sieben verschiedenen Diensteanbietern vermarktet. Jeder nationale Diensteanbieter betreibt ein Network Management Center (NMC), mit dem die Feststationen der Kunden kommunizieren. Jedes NMC ist wiederum mit der zentralen Hub-Station in der Nähe von Paris verbunden, über die die Verbindung zu den Satelliten hergestellt wird.

Die Positionsbestimmung einer Mobileinheit erfolgt, indem durch eine zentrale Hub-Station ein Signal über die beiden Satelliten an die Mobileinheit gesandt wird. Die Mobileinheit berechnet aus den unterschiedlichen Signallaufzeiten den Standort und sendet diesen zurück an die Hub-Station. Die Ortungsgenauigkeit beträgt dabei ca. 300 m. Die Position läßt sich in der Speditionszentrale auf digitalisierten Landkarten abbilden. Die Positionsermittlung erfolgt automatisch in frei einstellbaren Intervallen; dadurch kann der Weg der Mobileinheit in der Zentrale kontinuierlich mitverfolgt werden. Auch das Abrufen von technischen Fahrzeug- und Frachtdaten wie Öldruck oder Frachttemperatur ist möglich. Zusätzlich können mit dem zur Mobileinheit gehörigen Terminal mit LCD-Display auch Nachrichten ausgetauscht werden.

Ähnliche Systeme werden in der Bundesrepublik auch von der NUKEM GmbH („NuLoc“) und von Dantronic („MODIS“) angeboten. Diese Systeme nutzen jedoch das GPS zur Positionsbestimmung und Mobiltelefone des C-/D-Netzes für die Datenübertragung. Verschiedene Unternehmen (z. B. MAN und die TELEKOM AG) bieten auf dem INMARSAT-C-Dienst aufsetzende Flottenmanagement-Systeme an. Auch hier wird GPS zur Positionsbestimmung genutzt.

Aus Datenschutzsicht sind derartige Systeme als bedenklich einzustufen. Es ist offensichtlich, daß hier ein elektronisches Bewegungsprofil des Einzelnen ohne dessen Einwilligung erzeugt werden kann. Dadurch werden auch arbeitsrechtliche Fragen aufgeworfen, da das System eine Überwachung von Arbeitnehmern im Transportgewerbe in bisher nicht bekanntem Ausmaß gestattet. Hier sollte eine verbindliche Festlegung der Verwendungszwecke der erhobenen Daten auf die Disposition erfolgen und jede weitere Verwendung z. B. zu einer Leistungskontrolle ausgeschlossen werden.

3.3.1.3 Fernortung

Im Bereich der Fernortung haben satellitengestützte Systeme zur Lokalisierung gestohlener Fahrzeuge in letzter Zeit eine zunehmende Publizität erlangt. Solche Systeme werden sowohl von politischer Seite propagiert als auch in der Privatwirtschaft erprobt. Von einem deutschen Automobilhersteller ist bekannt, daß dort zur Zeit diesbezügliche Versuche durchgeführt werden.

Das bereits oben beschriebene EUTELTRACS-System kann ebenfalls zur Ortung gestohlener Fahrzeuge eingesetzt werden. Die debis-Tochter „Charterway“ hat ein System zur satellitengestützten Entdeckung gestohlener LKW-Anhänger entwickelt, daß allerdings noch nicht vermarktet wird.

Ob solche Systeme überhaupt geeignet sind, den zunehmenden Diebstahl von Fahrzeugen einzudämmen, ist umstritten. Kritiker weisen darauf hin, daß die auf einer drahtlosen Übermittlung von Positionsdaten mittels elektromagnetischer Wellen basierende Systeme relativ leicht ausgeschaltet werden können, indem das Fahrzeug in einem Behälter mit reflektierenden Innenwänden transportiert wird.

Bei den in der Entwicklung befindlichen Ortungssystemen entsteht – eine flächendeckende, vielleicht gar gesetzlich vorgeschriebene Nutzung vorausgesetzt – ein gravierendes Datenschutzproblem in erster Linie durch die gegebene Möglichkeit zur Erstellung von detaillierten Bewegungsbildern aller Benutzer von Kraftfahrzeugen. Selbst wenn im Augenblick die Verwendung der Daten auf die Zwecke der Bekämpfung von Kfz-Diebstählen beschränkt werden soll, so wird doch allein die entstehende Infrastruktur und das Vorhandensein solcher Datenbestände Begehrlichkeiten bei staatlichen und privaten Organisationen wecken. Allein im Bereich der allgemeinen Kriminalitätsbekämpfung lassen sich ohne viel Phantasie zahlreiche andere Nutzungszwecke denken. Weitere mögliche Anwendungsgebiete wären ohne Anspruch auf Vollständigkeit z. B. die Lenkung von Verkehrsflüssen, die Überprüfung von Zahlungen von Kilometergeld für dienstlich genutzte Fahrzeuge im Steuerrecht, Kontrolle von Geschwindigkeitsüberschreitungen und die Erhebung von Straßenbenutzungsgebühren.

Das Überwachungspotential, ganz zu schweigen von den entstehenden Mißbrauchsrisiken, muß angesichts der Verbreitung von Kraftfahrzeugen als außerordentlich hoch eingeschätzt werden. Bevor mit immensem Aufwand high-tech-Systeme zur nachträglichen Ortung gestohlener Fahrzeuge geschaffen werden, sollte die Fahrzeugindustrie zunächst die Möglichkeiten der Prävention durch entsprechende Modifikationen an den Fahrzeugen ausschöpfen. Die Durchsetzung eines verbesserten Schutzniveaus scheitert bisher an der komplizierten Interessenlage der beteiligten Instanzen, nicht etwa an einem Mangel an technischen Möglichkeiten. Aus Datenschutzsicht sind Systeme, die ohne Einflußmöglichkeit des Betroffenen ständig personenbezogene Daten ausstrahlen, insgesamt inakzeptabel. Auch in diesem Bereich muß vielmehr sichergestellt werden, daß personenbezogene Daten nur mit Wissen des und kontrollierbar durch den Betroffenen erhoben und verarbeitet werden können.

3.3.2 Telefon- und Kommunikationsdienste

Satellitensysteme werden zunächst in großem Umfang für die herkömmlichen Telekommunikationsdienste eingesetzt. Dazu gehören beispielsweise Telefon, Telefax, Telex, Datenübertragungsdienste, E-mail und Videokonferenzschaltungen. Zwar werden Satellitenverbindungen schon lange für die Herstellung von Telefonverbindungen über große Entfernungen – z. B. im Transatlantikverkehr – genutzt. Aber auch für vergleichsweise geringe Entfernungen setzt z. B. die TELEKOM AG bei Bedarf Satellitenanlagen ein: Dies betrifft zum Beispiel die Verbindung mit der deutschen Botschaft in Moskau, Telefon-, Telex- und Datex-P-Verbindungen in verschiedene Länder Osteuropas („DELOS" – Deutscher Telefonanschluß in Osteuropa), aber auch zahlreiche Verbindungen in die „fünf neuen Länder", in denen bis zur Instandsetzung der terristrischen Netze Satellitenkapazität zum Betrieb eines Overlay-Fernsprechnetzes genutzt wurde. Für den Benutzer von Telekommunikationseinrichtungen bleibt der Einsatz der Satelliten meist verborgen.

Satellitengestützte Dienste im Bereich der Sprach- und Datenübertragung werden auch von verschiedenen anderen Herstellern angeboten. Diese Dienste verfügen über Gateways in öffentliche Telefon- bzw. Datennetze, so daß von mobilen oder ortsfesten Satellitenterminals jeder Teilnehmer dieser Netze erreicht werden kann. Aufgrund der Vielzahl der angebotenen Dienste muß sich die Darstellung hier auf einige beispielhafte Dienste und Anbieter beschränken.

Dazu gehören die Satellitendienste der Inmarsat-Gruppe, die in Deutschland u. a. durch die TELEKOM AG vertrieben werden. Die Dienste umfassen

Inmarsat-A: Dieser Dienst bietet satellitengestützte Sprach- und Telexverbindungen. Datenübertragung ist bis 64 kBit/s möglich. Es können auch Telefax- oder andere Daten bis 9600 bps via Modem übertragen werden. Die mobilen Endgeräte wiegen ca. 20 bis 30 kg und arbeiten mit Antennendurchmessern von ca. 1 m. Die Datenübertragung erfolgt analog. In naher Zukunft soll der Dienst durch den digitalen Inmarsat-B-Dienst ergänzt bzw. ersetzt werden.

Inmarsat-C: Der Inmarsat-C-Dienst gestattet die Übertragung von Daten (bis 600 bps) und Textnachrichten, nicht aber von Sprache. Der Zugang ist in Deutschland von allen Telex- und Datex-P-Anschlüssen mit Selbstwahl möglich. Die Übertragung kann z. B. als Telexverbindung, im Datex-P-Netz (X.25-Modus) oder als Electronic-Mail erfolgen. Die Daten werden dann in einer Land-Erdfunkstelle temporär zwischengespeichert. Bei fehlerhafter oder unvollständiger Übermittlung werden sie solange erneut übertragen, bis der korrekte Empfang bestätigt wird. Es wird auch ein „Kurznachrichten-Modus" für die Übertragung von kleinen Datenpaketen zwischen 8 und 32 Bytes angeboten. In Verbindung mit einem Positionsbestimmungssystem kann der Inmarsat-C-Dienst auch zur Flottenbeobachtung und für das Flottenmanagement verwendet werden. Die Endgeräte haben Aktentaschen- bzw. Schuhkartonformat und wiegen ca. 5 kg.

Inmarsat-M: Der Dienst bietet Sprachverbindungen sowie Datenübertragung bis zu 2,4 kBit/s. Die Übertragung erfolgt digital. Die Endgeräte haben Aktentaschenformat und wiegen ca. 5 kg.

Datenübertragungsdienste werden auch von anderen Unternehmen angeboten:

INTELSAT Business Service – IBS ist ein Dienst zur Übertragung von z. B. Sprache, Daten und Videokonferenzen. Die Übertragungsgeschwindigkeiten liegen je nach Anwendung zwischen 64 kBit/s und 8,448 MBit/s. Typische IBS-Anwendungen sind Verbindungen zwischen den einzelnen Niederlassungen multinationaler Konzerne z. B. zur Nutzung einer gemeinsamen Entwicklungsdatenbank.

Zahlreiche Unternehmen bieten sogen. „VSAT" (Very Small Aperture Terminal)-Dienste an. Diese Dienste zeichnen sich durch relativ kleine Sende- und Empfangsanlagen (Antennendurchmesser bis 1,8 m) aus und finden in der Industrie und auf dem Dienstleistungssektor eine immer größere Verbreitung. Es werden sowohl Verbindungen zwischen einzelnen („point-to-point") als auch zwischen mehreren Kommunikationspartnern („point-to-multipoint") angeboten. Dabei sind sowohl Simplex- als auch Duplex-Übertragungen möglich. Die Datenübertragungsraten liegen je nach Anbieter und Dienst zwischen 300 Bit/s und 64 kBit/s. VSAT-Dienste werden vornehmlich für die Kommunikation zwischen einzelnen Unternehmen, z. B. der Konzernzentrale und den Tochterunternehmen genutzt. Solche Netze unterhalten z. B. die Allianz-Versicherungsgruppe und das Großversandhaus Quelle. Ein System zur Verbindung von Mineralölgesellschaften zu ihren einzelnen Tankstellen ist geplant. Auf dem Gebiet der „fünf neuen Länder" wird die Ausbreitung von VSAT-Diensten zusätzlich durch die nach wie vor mangelhafte Telekommunikationsinfrastruktur erheblich begünstigt. Es ist damit zu rechnen, daß hier massenhaft auch personenbezogene Daten von Kunden, Lieferanten und Mitarbeitern übertragen werden. In der Bundesrepublik bietet die TELEKOM AG ihren VSAT-Dienst DAVID an. Weitere Anbieter sind BOSCH ANT, Alcatel SEL und verschiedene Signatare von INTELSAT, die den VSAT-Dienst INTELNET vermarkten.

Die bisher beschriebenen Dienste werden in absehbarer Zeit um weitere satellitengestützte Telekommunikationsanwendungen ergänzt werden: Derzeit planen verschiedene Hersteller die Einführung satellitengestützter Telefonnetze, deren Endgeräte nicht wesentlich größer als die momentan im Handel befindlichen „D-Netz-Handys" sein sollen. Solche Projekte verfolgen z. B. Inmarsat (Inmarsat-P, auch „Projekt 21") und ein von Motorola geführtes Konsortium („Iridium"). Diese Systeme sollen ab 1994 erprobt werden und bis Ende des Jahrzehnts weltweit flächendeckend zur Verfügung stehen.

Da die Inhaltsdaten bei der Übertragung in der Regel in Computeranlagen der Diensteanbieter und der Systembetreiber zumindest temporär gespeichert werden, stellen sich hier zunächst die Fragen nach der Datensicherheit bei der Verarbeitung in diesen Anlagen bzw. bei der Übertragung zwischen diesen. Zur Beurteilung der Datensicherheit der Datenverarbeitungsanlagen von Netzbetreibern und Diensteanbietern liegen derzeit keine detaillierten Informationen vor. Die Datensicherheit bei der Übertragung hängt von der des benutzten Übertragungsmediums ab.

Aus Sicht des Datenschutzes sind bei der Sprach- und Datenübertragung via Satellit folgende Aspekte zu berücksichtigen: Grundsätzlich kann jeder, der über ein entsprechendes Empfangsgerät verfügt, die von einem Satelliten abgestrahlten Nachrichten empfangen. Der Bundesnachrichtendienst unterhält z. B. eine Anlage zum Abhören von Kommunikationsverbindungen via Satellit. Nach Untersuchungen des BSI ist es zwar derzeit nur professionellen Anwendern möglich, Nachrichteninhalte von Satellitenverbindungen abzuhören; die momentan im freien Handel erhältlichen Scanner erlauben dies nur für wenige Verbindungen. Durch das reine Abhören der Verbindung können die Kommunikationsinhalte in der Regel nicht in Erfahrung gebracht werden, da im allgemeinen Multiplex- und Datenkompressionsverfahren bei der Übertragung eingesetzt werden. Da die entsprechenden Protokolle und Verfahren allerdings mindestens fachöffentlich bekannt sind, kann hier nicht von einem wirksamen Schutz ausgegangen werden.

Mit dem steigenden Umfang der Datenübertragung via Satellit dürfte das Interesse am Abhören der Inhalte und den dazu notwendigen Geräten in der Zukunft jedoch zunehmen. Es wird dann nur noch eine Frage der Zeit sein, bis solche Geräte am Markt erhältlich sind. Für die Übertragung sensibler, insbesondere personenbezogener Daten sollten daher wirksame Maßnahmen zur Sicherung der Vertraulichkeit der Kommunikation, z. B. durch eine wirksame end-to-end-Verschlüsselung der Daten, getroffen werden.

3.3.3 Fernerkundung

Die Fernerkundung zählt zu den ältesten Anwendungen der Satellitenkommunikation. Die Auflösung der so gewonnenen Bilder hat sich in den letzten Jahrzehnten kontinuierlich verbessert; zivil genutzte Satelliten können heute Objekte mit einer Kantenlänge von 10 bis 20 m vom Weltraum aus identifizieren, im militärischen Bereich soll dies sogar für Objekte mit 1 bis 5 m Kantenlänge möglich sein. Die Satellitenbilder werden zunehmend in digitalisierter Form erzeugt.

Im Bereich der Fischerei plant die Europäische Gemeinschaft den Einsatz von Satellitentechnik zur Kontrolle der nationalen Fangflotten. Jedes Boot von über 40 m Länge soll kontinuierlich erfaßt und daraufhin kontrolliert werden, ob in Schutzzonen oder an Tagen, an denen ein Fangverbot besteht, gefischt wird.

Auch durch Fernortung können Datenschutzrisiken entstehen. Durch die fortschreitende Verfeinerung der Erfassungs- und Auswertungstechnik für Satellitenbilder besteht die Gefahr, daß zunehmend Sammlungen personenbezogener Daten entstehen, ohne daß die Betroffenen darauf Einfluß hätten oder auch nur darüber informiert wären. Der Bereich muß daher weiter kritisch beobachtet werden.

3.4 Datenschutzrecht und Satellitenkommunikation

Für die Verarbeitung personenbezogener Daten im Weltraum existieren derzeit keinerlei spezielle Datenschutzbestimmungen. Der einschlägige Weltraumvertrag („Vertrag über die Grundsätze zur Regelung von Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschließlich des Mondes und anderer Himmelskörper“ vom 27. Januar 1967) enthält keine diesbezüglichen Regelungen. Da Einzelstaaten diesen Bereich nicht sinnvoll regeln können, wäre hierfür eine zwischenstaatliche Regelung durch völkerrechtlich bindende Verträge auf der Ebene der Vereinten Nationen erforderlich. Derartige Verträge sollten z. B. regeln, in welchem Ausmaß personenbezogene Daten vom Weltall aus erhoben bzw. im Weltall verarbeitet werden dürfen, wer der verantwortliche Datenverarbeiter ist, wenn Daten im Raumsegment gespeichert werden, welche Datensicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten im Weltall getroffen werden müssen. Entsprechende Regelungen könnten auch in die Vertragswerke über die Gründung der Satellitenorganisationen Eingang finden.

Besondere Probleme wirft die mittelfristig geplante breite Einführung von satellitengestützen Mobiltelefondiensten auf: Hier könnte ein rechtsfreier Raum entstehen, da die nationale Telekommunikationsgesetzgebung (z. B. bezüglich der Speicherung von Verbindungs-, aber auch von Inhaltsdaten) keine Anwendung findet. Gleiches gilt auch für die zu erwartenden Regelungen auf der Ebene der Europäischen Union.

Hier müßten ebenfalls weltweit gültige, völkerrechtlich bindende Regelungen geschaffen werden. Soweit dies nicht erreicht werden kann, sollten die Benutzer darauf dringen, daß ein den nationalen Regelungen entsprechender Datenschutzstandard mit dem Diensteanbieter vertraglich vereinbart wird.

4. Staatliche Eingriffe in das Fernmeldegeheimnis – Abhörmaßnahmen

4.1 Rechtsgrundlagen

Beschränkungen des Fernmeldegeheimnisses dürfen nur aufgrund eines Gesetzes angeordnet werden (Art. 10 Abs. 2 Satz 1 GG). Derartige Beschränkungen sind das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz – G 10), § 100 a Strafprozeßordnung (StPO) und § 39 Außenwirtschaftsgesetz.

4.1.1 Eingriff in das Fernmeldegeheimnis durch Nachrichtendienste

Zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik stationierten NATO-Truppen sind die Verfassungsschutzbehörden des Bundes und der Länder, das Amt für den militärischen Abschirmdienst und der Bundesnachrichtendienst berechtigt, den Fernmeldeverkehr zu überwachen und aufzuzeichnen (§ 1 Abs. 1 Nr. 1 G 10).

Voraussetzung sind tatsächliche Anhaltspunkte für den Verdacht, daß jemand bestimmte staatsgefährdende Straftaten plant, begeht oder begangen hat sowie, daß die Erforschung des Sachverhalts sonst aussichtslos oder wesentlich erschwert wäre. Die Anordnung darf sich auch gegen Personen richten, bei denen auf Grund bestimmter Tatsachen anzunehmen ist, sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder daß der Verdächtige ihren Anschluß benutzt.

Darüber hinaus dürfen zur Nachrichtensammlung zwecks Abwehr eines bewaffneten Angriffs auf die Bundesrepublik Beschränkungen durch den Bundesnachrichtendienst für Post- und Fernmeldebeziehungen angeordnet werden (sogenannte strategische Überwachung).

Personenbezogene Erkenntnisse aus strategischen Überwachungsmaßnahmen dürfen zur Verhinderung, Aufklärung oder Verfolgung von bestimmten im Gesetz genannten Straftaten verwendet werden, soweit gegen die Person eine eigene G 10-Maßnahme angeordnet ist oder wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, daß jemand eine der genannten Straftaten plant, begeht oder begangen hat.

Mit dem am 1. Dezember 1994 in Kraft getretenen „Verbrechensbekämpfungsgesetz“ wurde die Befugnis des Bundesnachrichtendienstes für die strategische Überwachung des Fernmeldeverkehrs auf das Sammeln von Erkenntnissen über künftige Straftaten, wie z. B. internationale Geldwäsche, internationale terroristische Anschläge, Einschmuggeln von Drogen, erweitert (§ 3 Abs. 1 Satz 2 Nrn. 2 bis 6 G 10). Die Erkenntnisse aus der Überwachung dürfen unter den o. g. Voraussetzungen durch den Bundesnachrichtendienst an die Strafverfolgungsbehörden weitergegeben werden. Kritiker – so auch die Herausgeber dieser Broschüre – sehen in diesen neuen Befugnissen einen entscheidenden Schnitt hin zur verfassungswidrigen Aufhebung des Trennungsgebots zwischen Geheimdiensten und Polizei.

4.1.2 Fernmeldeüberwachung durch Strafverfolgungsbehörden

Nach § 100 a Strafprozeßordnung (StPO) kann die Überwachung des Fernmeldeverkehrs angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, daß jemand eine in der Norm genannte Straftat begangen hat oder – wenn der Versuch strafbar ist – zu begehen versucht oder durch eine Straftat vorbereitet hat und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Die Straftaten, bei denen eine Fernmeldeüberwachung angeordnet werden kann, sind in einem abschließenden, allerdings recht umfangreichen Katalog in § 100 a StPO zusammengefaßt. Sie reichen von Friedens- und Hochverrat über Mord bis hin zu Verstößen gegen das Betäubungsmittelgesetz und die Verleitung zur mißbräuchlichen Asylantragsstellung. Der Umfang des Kataloges ist wiederholt Gegenstand der Kritik von Datenschützern gewesen, ohne daß dies zu einer Einschränkung geführt hätte.

Gemäß § 100 b StPO darf die Überwachung und Aufzeichnung des Fernmeldeverkehrs nur durch den Richter angeordnet werden. Allerdings reicht bei Gefahr im Verzug die Anordnung durch die Staatsanwaltschaft aus, die jedoch dann außer Kraft tritt, wenn sie nicht binnen drei Tagen von einem Richter bestätigt wird.

Aufgrund der Anordnung haben die Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, dem Richter, der Staatsanwaltschaft und ihren Hilfsbeamten bei der Polizei die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen.

Die bei der Überwachung erlangten und aufgezeichneten Informationen dürfen in anderen Strafverfahren zu Beweiszwecken nur verwandt werden, soweit sie zur Aufklärung einer der in § 100 a StPO genannten Straftaten benötigt werden. Sie sind zu vernichten, sobald sie zur Strafverfolgung nicht mehr erforderlich sind.

4.1.3 Fernmeldeüberwachung durch das Zollkriminalinstitut

Zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz oder dem Kriegswaffenkontrollgesetz ist das Zollkriminalinstitut berechtigt, den Fernmeldeverkehr zu überwachen und aufzuzeichnen (§ 39 Außenwirtschaftsgesetz).

Die Maßnahme kann angeordnet werden gegenüber Personen, bei denen Tatsachen die Annahme rechtfertigen, daß sie bestimmte schwerwiegende Straftaten nach dem Außenwirtschaftsgesetz oder dem Gesetz über die Kontrolle von Kriegswaffen planen, gegenüber anderen Personen oder Unternehmen, wenn der mögliche Tatverdächtige bei ihnen tätig ist und die Überwachung seines Fernmeldeverkehrs nicht ausreicht oder gegenüber Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, daß sie für den möglichen Tatverdächtigen bestimmte Mitteilungen entgegennehmen oder weitergeben oder daß dieser ihren Anschluß benutzt.

Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und die Maßnahme nicht außer Verhältnis zur Bedeutung des aufzukärenden Sachverhalts steht.

Die Anordnung ergeht auf Antrag des Behördenleiters oder dessen Stellvertreters nach Zustimmung des Bundesministers der Finanzen durch das Landgericht. Bei Gefahr im Verzug kann auch der Bundesfinanzminister die Überwachung anordnen. Die Eilanordnung tritt außer Kraft, wenn sie nicht binnen drei Tagen vom Landgericht bestätigt wird.

Die durch die Maßnahme erlangten personenbezogenen Daten dürfen außer zur Verhütung oder Aufklärung der oben genannten Straftaten auch zur Verhütung oder Aufklärung einer in § 138 Strafgesetzbuch genannten Straftat genutzt werden.

Mit dieser am 7. März 1992 in Kraft getretenen gesetzlichen Ermächtigung wird erstmals auch im Vorfeld strafbaren Handelns ein Eingriff in das Fernmeldegeheimnis zugelassen und damit die Eingriffsvoraussetzungen im bedenklicher Weise „heruntergezont“.

4.1.4 Erstreckung der Fernmeldeüberwachung auf digitale Datenübertragung

Bis zur ersten Postreform 1989 war es zweifelhaft gewesen, ob die Geheimdienste und die Strafverfolgungsbehörden überhaupt die Befugnis zur Überwachung der digitalen Datenkommunikation hatten.

Nach der bis dahin geltenden Fassung des G 10 und von §§ 100 a, 100 b StPO durften sie nämlich bloß den Fernsprechverkehr abhören und den Fernschreibverkehr mitlesen und auf Tonbänder aufnehmen.

Die Erweiterung der Überwachungsbefugnisse wurde 1989 in einem Schnellverfahren mit der Begründung durchgesetzt, es handele sich lediglich um eine Präzisierung geltenden Rechts. Tatsächlich handelte es sich jedoch um eine öffentlich kaum wahrgenommene Ausweitung von Befugnissen, wenn nunmehr nicht nur der Fernsprech- und Fernschreibverkehr, sondern der gesamte Fernmeldeverkehr überwacht und aufgezeichnet werden darf.

Datenschutzrechtliche Forderungen, die Anpassung an neuartige Telekommunikationstechniken zum Anlaß zu nehmen, im Gegenzug das G 10 und die StPO-Befugnisse zum Eingriff in den Fernmeldeverkehr endlich an die Anforderungen des Volkszählungsurteils von 1983 anzupassen (z. B. Präzisierung der Voraussetzungen für die Informationsverarbeitung aufgrund des G 10, Festlegung zeitlicher Obergrenzen für Überwachungsmaßnahmen, Stärkung der Rechte der Betroffenen und Verankerung der Kontrollkompetenz der Datenschutzbeauftragten), hatten keine Durchsetzungschance. Bis heute hat sich hieran nichts geändert.

Eine weitere im Zuge der Poststrukturreform 1989 vorgenommene Änderung der Überwachungsbefugnisse betrifft den Betrieb von privaten Telekommunikationsdiensten direkt: Nicht nur die Deutsche Bundespost, sondern auch jeder andere Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, haben den berechtigten Stellen Auskunft über den nach Wirksamwerden der G 10-Anordnungen oder Überwachungsmaßnahmen nach § 100 a StPO durchgeführten Fernmeldeverkehr zu erteilen sowie die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen (§ 1 Abs. 2 Satz 2 G 10, § 100 b Abs. 3 StPO). Sie haben ferner für die Durchführung der Überwachungsmaßnahmen das erforderliche Personal bereitzuhalten, das vom Verfassungsschutz überprüft wurde und zum Zugang zu Verschlußsachen ermächtigt ist.

Die Tatsache der Überwachung darf anderen nicht mitgeteilt werden. Der Verstoß gegen diese Vorschrift wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Wer als Betreiber einer Fernmeldeanlage die Überwachung nicht ermöglicht oder kein entsprechend überprüftes Personal bereithält, handelt ordnungswidrig; die Ordnungswidrigkeit kann mit Geldbuße bis zu 30 000 DM geahndet werden.

4.1.5 „Auskunft über den Fernmeldeverkehr“ gemäß § 12 FAG

Eine alte, gleichwohl besonders problematische Rechtsvorschrift, die einen Eingriff in das Fernmeldegeheimnis erlaubt, ist § 12 Fernmeldeanlagengesetz. Danach kann in strafgerichtlichen Untersuchungen der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft „Auskunft über den Fernmeldeverkehr verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren“.

Anders als in §§ 100 a, b StPO wird den Strafverfolgungsbehörden durch diese Vorschrift der Zugriff auf dem Fernmeldegeheimnis unterliegende Daten auch in Verfahren ermöglicht, die der Aufklärung von Bagatelldelikten dienen: Auch wenn – wie oben erwähnt – der Straftatenkatalog von §§ 100 a, b StPO recht großzügig ist, gibt es für den Zugriff auf Daten nach § 12 FAG keine Beschränkungen durch einen Straftatenkatalog.

Anders als die Fernmeldeüberwachung nach dem G 10 und nach §§ 100 a, b StPO bezieht sich die „Auskunft“ nach § 12 FAG nur auf Daten, die gespeichert sind und auf Informationen, die dem Betreiber einer Fernmeldeanlage (bzw. dem Anbieter von Fern-

meldedienstleistungen) sonst bekannt sind. Im allgemeinen dürfte es sich bei den auf diese Weise von den Strafverfolgungsbehörden erlangten Informationen um Verbindungsdaten handeln; in bestimmten Fällen jedoch (z. B. bei Mailboxen) können jedoch auch Inhaltsdaten betroffen sein.

4.2 Durchführung von Überwachungsmaßnahmen

4.2.1 Terrestrische Dienste

Es ist nicht erforderlich – und bei recht mobilen Teilnehmern und Teilnehmerinnen auch viel zu aufwendig –, die Funkstrecken abzuhören, da alle Gespräche auch im Festnetz und dort dann auch nicht mehr verschlüsselt sondern allenfalls noch digitalisiert vermittelt werden. Über entsprechende Software in den Vermittlungsstellen – die, wenn sie noch nicht verfügbar ist, sich vielleicht schon in der Entwicklung befindet, aber zumindest entwickelbar ist – ist es technisch möglich, unter Verwendung des HLR (s. o.), in dem auch die Basisstation verzeichnet ist, in dem sich eine bestimmte Mobiltelefon-Chipkarte gerade befindet, alle Gespräche dieses Anschlusses aufzuzeichnen.

Während im analogen Netz jede Abhöraktion einen sichtbaren Eingriff in der jeweiligen Vermittlungsstelle erforderte und die Aufzeichnung der Rufnummer von Anrufenden mit erheblichem Aufwand verbunden war, kann dies durch entsprechende Softwareprogrammteile einfach realisiert werden. Die Rufnummer der Anschlüsse, die von einem zu überwachenden Anschluß aus angerufen wurden, konnten auch bisher relativ einfach durch Mitzählen der Wählimpulse festgestellt werden.

Eine weitere Vereinfachung der Überwachung ergibt die digitalisierte Übermittlung der Verbindungsdaten – insbesondere der Sende- und der Empfangsnummer. So ist es möglich, auf der gesamten Übertragungsstrecke relevante Verbindungen auszuwählen.

Die Kontrolle der Überwachungsmaßnahmen hierzu berechtigter Stellen durch die Datenschutzbeauftragten oder parlamentarische Stellen wird in digitalisierten Netzen ungleich schwieriger, da die Überwachung softwaregesteuert durchgeführt werden kann. Bei einer Kontrolle vor Ort in der zuständigen Vermittlungsstelle wäre eine Überwachungsmaßnahme dann nicht mehr augenscheinlich feststellbar. Nur durch Analyse eventuell vorhandener Systemprotokolle wäre eventuell kontrollierbar, ob und für welche Anschlüsse Überwachungen aktiviert sind.

Eine Telefonüberwachung in den D-Netzen war anfangs nicht möglich. Mittlerweile ist davon auszugehen, daß die hierzu notwendige Software inzwischen erstellt und auch im Einsatz ist. Die Ausschreibung der E-Netz-Lizenz erfolgte bereits G-10-fest, d. h. die für die Durchführung der Überwachungsmaßnahmen notwendigen Routinen standen dort bereits von Anfang an zur Verfügung.

4.2.2 Satellitengestützte Dienste

Die via Satellit abgestrahlten Signale sind – wie bereits oben erwähnt – prinzipiell im gesamten Ausstrahlungsbereich („footprint“) des benutzten Satelliten von jedermann, der über geeignete technische Einrichtungen verfügt, zu empfangen. Die bei der Übertragung verwendeten Multiplexverfahren bieten nur einen unvollständigen Schutz.

Einrichtungen zur Überwachung der Satellitenkommunikation werden in vielen Ländern auch von staatlichen Stellen betrieben, die die gesamte Satellitenkommunikation in ihrem Einzugsbereich abhören und auswerten. In der Bundesrepublik wird eine derartige Anlage vom Bundesnachrichtendienst betrieben.

Darüber hinaus ist die Existenz gleichartiger privater Einrichtungen – z. B. zum Zweck der Industriespionage – durchaus denkbar. Den Autoren liegen jedoch gegenwärtig über die Existenz solcher Anlagen keine Informationen vor.

5. Wie können sich Betroffene schützen?

5.1 Terrestrische Dienste

5.1.1 Schnurlose Telefone

Bei schnurlosen Telefonen ist ein relativ abhörsicheres Telefonieren nur möglich, wenn Geräte eingesetzt werden, bei denen die Übertragung zwischen dem Funkteil und der Feststation digitalisiert und verschlüsselt ist. Wenn aus Preisgründen noch Geräte mit analoger Übertragung angeschafft werden, sollten sich die Telefonierenden bewußt sein, daß das Gespräch mit einfachen Mitteln abgehört werden kann und bei persönlichen Inhalten auf die Verwendung des Funkteils verzichten und stattdesssen das normale Telefon verwenden.

5.1.2 B- und C-Netz

Die Neuanschaffung von Mobiltelefonen des B- und C-Netzes kann aus datenschutzrechtlichen Gesichtspunkten nicht empfohlen werden.

Sensible Gespräche sollten nicht von diesen Geräten aus, sondern besser vom nächsten erreichbaren Festnetztelefon geführt werden! Dies schützt allerdings nicht gegen Abhörangriffe auf das Festnetz. Gespräche mit sehr sensiblen Inhalten sollten daher nur persönlich – oder mit sicherer Ende-zu-Ende-Verschlüsselung – geführt werden.

5.1.3 D- und E-Netz

In den D-Netzen wird zur Zeit eine Sicherheit erreicht, die der Sicherheit von Verbindungen im Festnetz der TELEKOM entspricht. Da bei jeder Verbindung auch Festnetze benutzt werden, kann diese Sicherheit nicht größer als dort sein.

Wegen der grundsätzlichen Abhörmöglichkeiten auch im Festnetz wird empfohlen, Gespräche mit (sehr) sensiblen Inhalten nur persönlich führen.

Über die Speicherung der Verbindungsdaten ist prinzipiell die Erstellung eines Bewegungsprofil des Mobiltelefons bzw. der Mobiltelefonkarte – und damit im allgemeinen auch des Anschlußinhabers bzw. der Anschlußinhaberin – möglich.

5.1.4 MODACOM

Aufgrund der Sicherheitsprobleme, die sich aus der prinzipiellen Abhörmöglichkeit von Datenfunkdiensten ergeben, sollten die Benutzer zumindest dann anwendungsseitig für eine kryptographische Verschlüsselung sorgen, wenn sensible Daten übertragen werden sollen. Dies gilt vor allem für die Übertragung von Authentifikationsdaten (z. B. Paßwörter) bei Datenbankabfragen und bei Einbindung von Modacom-Anwendungen über spezielle Datenfunk-Server in lokale Netzwerke.

5.2 Satellitenkommunikation

Wie bereits oben ausgeführt, kann eine via Satellit übertragene Nachricht im Prinzip im gesamten Abstrahlbereich des Satelliten abgehört werden (vgl. 3.3.2). Soweit die Diensteanbieter den Benutzern keine wirksame end-to-end-Verschlüsselung anbieten, sollten die Benutzer daher – zumindest wenn sensible Daten übertragen werden sollen – selbst derartige Verschlüsselungsverfahren anwenden.

6. Ausblick auf die weitere technische Entwicklung

6.1 Mobiltelefon

Die Erreichbarkeit von Mobiltelefonen der D-Netze und des E-Netzes ist nicht auf das Gebiet der BRD beschränkt. Verträge mit anderen Netzbetreibern haben schon dazu geführt, daß auch in Teilen des europäischen Auslandes mit Mobiltelefonen, die in den D-Netzen registriert sind, telefoniert werden kann, bzw. daß solche Mobiltelefone dort auch erreicht werden können. Dies führt dann dazu, daß Abrechnungs- und Verbindungsdaten sowie der Aufenthaltsort international ausgetauscht werden. Dies ist umso bedenklicher, da verbindliche europäische Regelungen zum Schutz personenbezogener Daten vor Mißbrauch bislang fehlen.

6.2 Mobile Datenübertragung

Auch bei der mobilen Datenübertragung ist eine weitere deutliche Ausweitung der Teilnehmerzahlen zu erwarten, wobei aufgrund des noch verhältnismäßig hohen Preises der mobilen Endgeräte der Schwerpunkt bei der kommerziellen Nutzung liegen wird. Nach der inzwischen erteilten weiteren Lizenz für einen mobilen Datenübertragungsdienst durch das BMPT ist damit zu rechnen, daß sich auch in diesem Bereich wie bereits bei den Funktelefonen öffentliche und private Anbieter gegenüberstehen werden.

Ebenso wie bei digitalen Funktelefonnetzen wird es verstärkte Bemühungen zur internationalen Standardisierung geben. Aus Datenschutzsicht wird es dabei insbesondere darauf ankommen zu erreichen, daß dabei Datensicherungsmechanismen berücksichtigt werden. Dies gilt insbesondere für die Verschlüsselung der übertragenen Daten auf der Funkstrecke.

6.3 Satellitenkommunikation

Satelliten werden auch zukünftig in zunehmendem Umfang für klassische Telekommunikationsdienstleistungen eingesetzt werden. Sie ersetzen und ergänzen dabei zunehmend terrestrische Telekommunikationsnetze. Auch mit der Entwicklung weiterer satellitenspezifischer Kommunikationsdienste ist zu rechnen. Ein Ende dieser Entwicklung ist derzeit nicht abzusehen; es ist im Gegenteil zu erwarten, daß in die osteuropäischen Staaten beim Aufbau einer modernen Telekommunikations-Infrastruktur – speziell in Gebieten mit territorial schwierigen Bedingungen für den Aufbau terristrischer Netze wie z. B. in Sibirien – verstärkt auf Satellitentechnik zurückgreifen werden.

Wie oben ausgeführt, entstehen durch die verstärkte Nutzung der Satellitentechnik auch zunehmend Gefahren für das informationelle Selbstbestimmungsrecht des Einzelnen, ohne daß bisher umfassende Datenschutz- und Datensicherheitsregelungen zur Eindämmung dieser Gefährdungen entwickelt worden wären. Die Entwicklung der Satellitenkommunikation sollte daher von den Datenschutzbeauftragten stärker als bisher kritisch begleitet werden.