

E: 22. 6. 09 (8-9)

1487

3

2 V. 3 / 22.6.09

EINGEGANGEN
14. JULI 2009
Erled.

Zur Nutzung von Verkehrsdaten im Rahmen der
Vorratsdatenspeicherung

Felix C. Freiling
Universität Mannheim

Sachkundige Stellungnahme im Rahmen der Verfassungsbeschwerden
1 BvR 256/08, 263/08, 586/08
20. Juni 2009

Inhaltsverzeichnis

1	Einführung	3
2	Technische Hintergründe	3
2.1	Schichtung von Telekommunikationssystemen	3
2.1.1	Physische Schicht	3
2.1.2	Netzwerkschicht	5
2.1.3	Transportschicht und darüber liegende Schichten	5
2.1.4	Dynamische und lokale IP-Adressen	6
2.2	Drahtgebundene lokale Netze	6
2.3	Drahtlose lokale Netze (WLAN)	7
2.4	Mobilfunktechnologie	8
2.4.1	Telefonie im GSM-Netz	8
2.4.2	Authentifizierung im GSM-Netz	9
2.4.3	SMS im GSM-Netz	9
2.4.4	GPRS im GSM-Netz	10
2.4.5	MMS im GSM-Netz	11
2.5	LKW-Mautsystem der Firma TollCollect	11
3	Zur Begriffsbildung	11
3.1	Inhaltsdaten	11
3.1.1	Legaldefinition und Beispiele	12
3.1.2	Technische Betrachtung der Definition	12
3.2	Verkehrsdaten	12
3.2.1	Legaldefinition und Beispiele	12
3.2.2	Technische Betrachtung der Definition	12
3.2.3	Bildung von Bewegungsprofilen	13
3.3	Bestandsdaten	14
4	Entstehung und Speicherung von Verkehrsdaten	14
4.1	Durch § 113a TKG erfasste Daten	14
4.2	In der Praxis anfallende Daten ohne Bezug zu § 113a TKG	15
4.3	Probleme bei extern angebotenen Datendiensten	15
4.4	Extern initiierte Datenkommunikation	16
4.5	Entstehungsorte der Verkehrsdaten und alternative Zugriffsmöglichkeiten	16
4.6	Sorgfaltspflichten des Speichernden	17
4.7	Kosten der Speicherung	17
5	Notwendigkeit der Speicherung von Verkehrsdaten	18
5.1	Zu Abrechnungszwecken	18
5.2	Zur Verfolgung von Straftaten	18
5.2.1	Ablauf einer Verkehrsdatenabfrage	18
5.2.2	Nutzen von Verkehrsdatenabfragen in der Praxis	19
5.2.3	Mittels Telekommunikation begangene Straftaten	19
6	Zusammenfassende Diskussion des § 113a TKG	20
6.1	Verkehrsdaten vs. Inhaltsdaten	20
6.2	Nutzen von Verkehrsdaten für die Praxis	20
6.3	Offener Zugriff auf Verkehrsdaten	21
6.4	Kostensatz bei Vorratsdatenspeicherung	21
A	Bezüge des Artikels zu den Fragen aus dem Fragenkatalog	23

1 Einführung

Die nachfolgenden Ausführungen entstanden aus Anlass einer Anfrage des Bundesverfassungsgerichts im Rahmen der Verfassungsbeschwerden 1 BvR 256/08, 263/08, 586/08. Teil der Anfrage war ein Fragenkatalog, zu dem ich als sachkundiger Dritter Stellung nehmen sollte. Statt einer listenhaften Beantwortung der Fragen habe ich mir erlaubt, die technischen Hintergründe in einer zusammenhängenden Diskussion darzustellen. Der Bezug zu den Fragen aus dem Fragenkatalog, zu denen ich mich sachkundig fühlte, wird im Anhang explizit hergestellt.

Bei der Darstellung sind vor allem zwei Aspekte wichtig für mich gewesen: zum einen die Betrachtung der aktuellen technischen Umstände, mit denen sowohl Anbieter von Telekommunikationsdiensten als auch die Ermittlungsbehörden leben müssen, und zum anderen die Berücksichtigung der zukünftigen technischen Entwicklung.

2 Technische Hintergründe

In heutigen Kommunikationssystemen wird die weitaus größte Menge an Daten digital übertragen. Kommunikationsinhalte werden demnach beim Sender als Folge von binären Symbolen (Bits) in das Kommunikationssystem eingebracht und beim Empfänger ebenso aus dem System entnommen. Es ist zu erwarten, dass in Zukunft alle Kommunikationstechnologien (also etwa auch Fernsehen, Radio) ihre Daten digital übertragen werden. Digitale Daten werden in Form von kurzen Datenpaketen über zwischengeschaltete Computer (*multi hop*-Betrieb) verschickt (so genannte *Paketvermittlung*). Kommunikationsverbindungen, wie sie etwa in der Internettelefonie oder beim Anschauen von Videos entstehen, werden durch Kettung einer Vielzahl an Datenpaketen simuliert.

In der Praxis hat sich das Internet Protokoll (IP) als de facto Standard für die weltweite Vermittlung von digitalen Datenpaketen etabliert. Im folgenden gebe ich einen kurzen Überblick über die technischen Hintergründe dieser digitalen Kommunikationssysteme. Da die Darstellung der Funktionsweise der klassischen Internet-Technologien auch in der rechtswissenschaftlichen Literatur schon gut ausgearbeitet ist (siehe etwa Seitz), beschränken sich meine Ausführungen auf die Wiederholung von für mich wesentlichen Aspekten, insbesondere die der Mobilkommunikation.

2.1 Schichtung von Telekommunikationssystemen

In digitalen Kommunikationssystemen, die auf IP basieren, hat sich eine hierarchische Schichtenstruktur durchgesetzt, nach denen Daten verarbeitet werden. Ich möchte im folgenden die aus meiner Sicht wesentlichen drei Schichten erläutern. Abbildung 1 stellt die Schichten im Zusammenhang dar.

2.1.1 Physische Schicht

Datenkommunikation funktioniert letztendlich dadurch, dass digitale Informationseinheiten (Bits) über ein physisches Medium von einem Computer über eine räumliche Distanz zu einem zweiten Computer übertragen werden. Das einfachste Beispiel sind zwei Computer, die als Medium ein zwischen ihnen angebrachtes Kupferkabel verwenden. Aber auch die Luft kann zum Medium werden, wenn die beiden Computer Antennen haben und sie sich in Funkreichweite voneinander befinden. Auch wenn es in globalen Datennetzen so aussieht, als würden Informationen unmittelbar von einem Rechner zu einem weit entfernten anderen Rechner übertragen werden, so erfolgt letztendlich die Übertragung immer über Zwischenstationen, die jeweils über ein gemeinsames Medium verbunden sind.

Die konkreten Vorgänge zur Datenübertragung über ein Kabel unterscheiden sich stark von denen zur Datenübertragung etwa über Funk. Ihnen allen ist aber gemeinsam, dass man

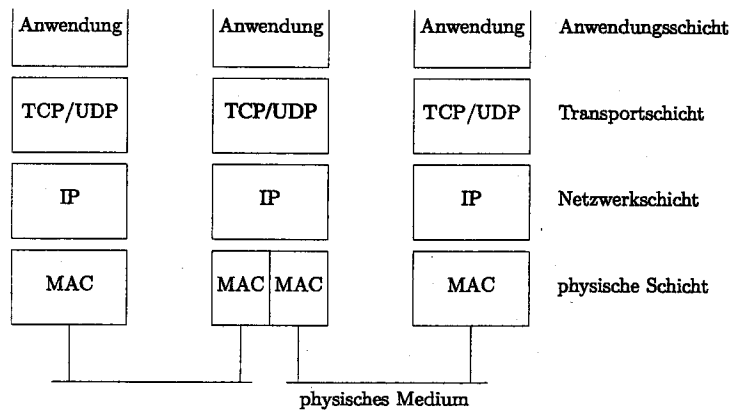


Abbildung 1: Schichtenstruktur IP-basierter Kommunikationssysteme

mit ihrer Hilfe einzelne Bits von einem Rechner zu einem (an einem gemeinsamen Medium angeschlossenen) anderen Rechner übertragen kann. In der Informatik kapselt man darum die Details der Übertragung in einer Schicht aus Software und Hardware. Die Hardware besteht aus der so genannten *Netzwerkkarte*, an die das Kabel angeschlossen wird oder die die Antenne enthält. Die Software besteht aus so genannten *Treibern*. Wegen ihres Bezuges zu einem gemeinsamen physischen Medium wird diese Schicht *physische Schicht* genannt. Eine Schicht kann man sich immer wie einen Dienstleister der Privatwirtschaft vorstellen, der ein genau beschriebenes Angebot macht. Die physische Schicht ist demnach ein Dienstleister, der Bits über ein (beliebiges) gemeinsames Medium von Rechner zu Rechner transportiert.

Innerhalb dieser Schicht müssen vielfältige Aufgaben gelöst werden, etwa die Adressierung der angeschlossenen Rechner. Werden beispielsweise Daten über Funk übertragen, muss klar sein, für welchen Rechner sie bestimmt sind. Hierfür besitzen die angeschlossenen Rechner innerhalb dieser Schicht eine *physische Adresse*. Meist spricht man hier von der Adresse für den physischen Medienzugriff (*media access control*, MAC), also der MAC-Adresse.

Computer können zeitgleich über verschiedene Medien kommunizieren, zum Beispiel über Funk und über ein Kabel. Diese Rechner können Daten auf dem einen Medium empfangen und sie dann auf dem anderen Medium weiterversenden. Da es sich aber um unterschiedliche Medien handelt, benötigt ein und derselbe Rechner zwei verschiedene Netzwerkkarten. Entsprechend besitzt der Rechner auch verschiedene MAC-Adressen, jeweils eine pro Medium, an das er angeschlossen ist. Derartige Konfigurationen treten etwa im Heimbereich auf, wo es häufig einen Rechner (WLAN-Router) gibt, der zwischen einer Datenübertragung über Funk (WLAN) und einer Datenübertragung über Kabel (DSL) vermittelt.

Die MAC-Adresse wird vom Hersteller der Netzwerkkarte gewählt und ist in der Regel fest mit der Karte verbunden. Damit nicht zufällig zwei Netzwerkkarten dieselbe MAC-Adresse haben, gibt es ein weltweit verwendetes Codierungsschema für MAC-Adressen (in das ein Code für den Hersteller und eine Seriennummer der Karte eingeht). Die MAC-Adresse muss aber genau genommen nur für das jeweils verwendete Medium eindeutig sein. Bei manchen Netzwerkkarten kann man die MAC-Adresse auch durch Software auf einen beliebigen Wert setzen.

2.1.2 Netzwerkschicht

Während die physische Schicht die *lokale* Vernetzung über gemeinsame Medien regelt, bestimmt die *Netzwerkschicht* die Regeln für die *globale* Vernetzung im Internet. Charakteristisch für die Netzwerkschicht ist die Verwendung des *Internet Protocol (IP)* und die Adressierung über IP-Adressen.

Eine weltweite Adressierung von Rechnern über (physische) MAC-Adressen wäre zwar möglich, ist aber aus praktischen Erwägungen nicht sinnvoll, da MAC-Adressen ursprünglich allein für die lokale Vernetzung konzipiert wurden. Werden mehrere lokale Netze (mit gemeinsamen Medium) über Zwischenrechner (*router*) zu größeren Netzen zusammengeschlossen, dann benötigt man geeignete Mechanismen, damit die Daten ihren Weg von einem Rechner zum anderen über einen oder mehrere solcher Zwischenrechner finden können (die so genannte *Wegwahl, routing*). Hierbei sind *IP-Adressen* von zentraler Bedeutung.

Mit einer IP-Adresse wird ein einzelner Rechner weltweit eindeutig identifiziert. Vereinfacht gesprochen teilt sich die IP-Adresse in zwei Teile auf: Der erste Teil identifiziert das lokale Netzwerk, in dem sich der Rechner befindet; der zweite Teil identifiziert dann den Rechner selbst innerhalb des lokalen Netzwerkes. Dieser Trick ermöglicht eine schnelle Wegwahl und erlaubt es, Daten weltweit zu verschicken. Wie eingangs erwähnt, werden die verschickten Datenmengen dabei in kleine Portionen zerteilt und in Form von Paketen, den so genannten *IP-Paketen*, von Rechner zu Rechner weitergeleitet. Vor dem Versand wird dem Datenpaket ein "Kopf" vorangestellt, der unter anderem die IP-Adresse des Zielrechners sowie die IP-Adresse des Absenders enthält (*Protokollkopf*). Dies ist vergleichbar mit der Briefpost: Die zu sendenden Daten (zum Beispiel eine Rechnung) werden in einen Umschlag gesteckt und mit Informationen zur Wegwahl (Absender- und Zieladresse) versehen.

Für die eigentliche Übertragung der Daten von Rechner zu Rechner wird jeweils auf die Dienstleistungen der physischen Schicht zurückgegriffen.

2.1.3 Transportschicht und darüber liegende Schichten

Die Netzwerkschicht übernimmt für den weltweiten Versand von IP-Paketen keinerlei Garantien. Pakete können verloren gehen oder sie können mehrfach beim Empfänger zugestellt werden. Eine Funktion der *Transportschicht* ist es, bestimmte Formen von Zuverlässigkeit beim Datenverkehr zu erreichen. Dies geschieht mit ganz unterschiedlichen Techniken, etwa dadurch, dass mit eingebauten Sequenznummern der Verlust eines IP-Paketes entdeckt werden kann. Mit Hilfe dieser Techniken kann man auf Ebene der Transportschicht wieder so etwas wie eine stehende "Datenverbindung" realisieren. Die Transportschicht bedient sich dabei der Dienstleistung der Netzwerkschicht.

Die zweite wesentliche Funktion der Transportschicht ist eine verfeinerte Adressierung. Für viele praktische Anwendungen ist nämlich die Adressierung eines einzelnen Rechners zu grob. Man möchte spezielle "Teile" des Rechners ansprechen, etwa analog zu unterschiedlichen Sachbearbeitern bei der Briefpost. Dies geschieht durch Nennung eines *Anschlusses (port)*, einer Nummer zwischen 0 und 65535. Der Anschluss identifiziert meist eine bestimmte Anwendung, etwa den auf dem Rechner laufenden Webbrowser. Auf Ebene der Transportschicht besteht eine Adresse also aus einer IP-Adresse und einer Anschlussnummer (*port number*).

Moderne Anwendungen wie E-Mail, Chat, WWW werden in höheren Schichten ("oberhalb" der Transportschicht) angesiedelt und verwenden die Transportschicht zum weltweiten Versand von Daten. Die Transportschicht wiederum verpackt diese Daten in IP-Pakete und verwendet die Dienste der Netzwerkschicht. Die *Inhalte* einer Datenübertragung werden also in vollem Umfang erst oberhalb der Transportschicht verarbeitet. Allerdings enthält auch die Transportschicht selbst schon viele Informationen über die Art der übertragenen Daten, beispielsweise die Anschlussnummer.

2.1.4 Dynamische und lokale IP-Adressen

Das Wachstum des Internet hat zu einer Verknappung von IP-Adressen geführt, so dass heute nicht mehr jeder am Internet angeschlossene Rechner notwendigerweise eine weltweit eindeutige IP-Adresse hat. In vielen Bereichen verwendet man heute *dynamische IP-Adressen*. Hierbei wird einem am Internet angeschlossenen Rechner zwar eine weltweit eindeutige IP-Adresse zugewiesen, allerdings nur für die Dauer der Internetbenutzung. Nach dem "Trennen" der Verbindung zum Internet kann die IP-Adresse einem anderen Benutzer zugewiesen werden. Dynamische IP-Adressen bilden ein starkes Hindernis bei der Strafverfolgung, da sie eine Zuordnung von IP-Adresse zu einem konkreten Computer erschweren.

Bestimmte IP-Adressen sind außerdem für Netze vorbehalten, die nicht mit dem Internet verbunden sein müssen. Diese IP-Adressen werden im globalen Internet nicht verwendet (so genannte *lokale IP-Adressen*). Dies sind zum Beispiel IP-Adressen, die mit "192.168." oder "10." beginnen. Viele Firmen organisieren ihre lokalen Netzwerke mit Hilfe dieser IP-Adressen. Wird das Netzwerk dann mit dem globalen Internet verbunden, muss es einen Zwischenrechner geben, der zwischen "internen" (lokalen) IP-Adressen und "externen" (weltweit gültigen) IP-Adressen vermittelt (*network address translation, NAT*). Diese Zuordnung ist relativ flüchtig und im nachhinein schwer nachvollziehbar, da sie in der Regel von Kommunikationsvorgängen auf der Transportschicht abhängt.

In vielen Privathaushalten wird heute eine Kombination aus dynamischen und lokalen IP-Adressen verwendet. Der Zugangspunkt zum Internet (meist ein WLAN-Router, siehe Abschnitt 2.3) erhält vom Internetprovider eine weltweit eindeutige (dynamische) IP-Adresse. Im internen (lokalen) Netz vergibt der Zugangspunkt dann wiederum lokale IP-Adressen.

Die Verwendung lokaler IP-Adressen in Verbindung mit NAT stellt Ermittlungsbehörden vor das Problem, dass eine Datenübertragung regelmäßig nur zur IP-Adresse des Zugangspunktes zurückverfolgt werden kann. Der Computer, der die Datenübertragung ursprünglich verursachte, bleibt unbekannt. In kleinen privaten Netzen ist dies weniger problematisch, da der Kreis der Personen, die als Verursacher in Frage kommen, meist eng umgrenzt werden kann. Im Kontext kleinerer oder mittlerer Firmen oder im Kontext drahtloser Netze (siehe Abschnitt 2.3) ist das deutlich problematischer.

Das heute verwendete IP-Protokoll mit der Versionsnummer 4 wird in Zukunft abgelöst werden durch die bereits standardisierte Version 6 (*IPv6*). IPv6 zeichnet sich vor allem durch eine deutlich größere Zahl von IP-Adressen aus. Die Notwendigkeit, dynamische und/oder lokale IP-Adressen zu vergeben, wird in Zukunft abnehmen.

2.2 Drahtgebundene lokale Netze

Wie oben erwähnt, ist das gemeinsame Übertragungsmedium charakteristisch für ein lokales Netz. Darin geschieht die Adressierung über die physische MAC-Adresse, die eine konkrete Netzwerkkarte identifiziert.

Im lokalen Netz kontrolliert der so genannte *Grenzrechner* den Übergang in andere lokale Netze oder das Internet. Eine wichtige Aufgabe des Grenzrechners ist die Umsetzung von IP-Adressen in MAC-Adressen. Dies geschieht auf Ebene der physischen Schicht durch eine Adressauflösung (*address resolution protocol, ARP*). Werden also in einem lokalen Netz auch lokale IP-Adressen verwendet (siehe Abschnitt 2.1.4), kann nur mit Hilfe des Grenzrechners nachvollzogen werden, welcher Rechner für eine konkrete Anfrage im Internet verantwortlich war. Viele Privathaushalte verwenden einen Grenzrechner, der lokale IP-Adressen vergibt (zum Beispiel die in Deutschland sehr verbreitete "Fritz-Box" der Firma AVM).

Die Zuordnung von IP-Adresse zu MAC-Adresse ist im Bereich privater Haushalte relativ statisch und wird für eine bestimmte Zeit im Grenzrechner gespeichert. Diese Informationen können dann auch durch den Benutzer oder im Zuge einer Beschlagnahme

abgefragt werden. Im Bereich öffentlicher Netze, insbesondere öffentlichen Zugangspunkten, erfolgt eine solche Speicherung in der Regel nicht.

2.3 Drahtlose lokale Netze (WLAN)

Drahtlose lokale Netze (*wireless local area network*, WLAN) verwenden einen *Zugangspunkt* (*access point*), der den Übergang in das drahtgebundene Netz regelt. Viele Privathaushalte besitzen heute einen solchen Zugangspunkt, der gleichzeitig der Grenzrechner zum Internet ist (WLAN-Router).

Das lokale Netz, das durch einen Zugangspunkt verwaltet wird, ist durch einen Namen (*service set identifier*, SSID) gekennzeichnet. Dieser Name wird von den Zugangspunkten über Funk in regelmäßigen Abständen ausgestrahlt. Die Adressierung innerhalb der physischen Schicht des drahtlosen Netzes erfolgt also aus einer Kombination aus SSID und MAC-Adresse.

Der Zugang zu drahtlosen lokalen Netzen ist in der Regel durch verschiedene Techniken geschützt. Gibt es keine Zugangsbeschränkungen, spricht man auch von einem *offenen WLAN*.

Eine sehr einfache Schutzmethode liegt darin, die SSID nicht regelmäßig auszustrahlen. Auch können Zugangspunkte den Zugang zum lokalen Netz abhängig von der MAC-Adresse des Rechners machen, der den Zugang wünscht. Nur wenn der Rechner eine "erlaubte" MAC-Adresse hat, wird ihm eine lokale IP-Adresse zugewiesen.

Sicherer ist die Verwendung von Verschlüsselungstechnologien wie WEP und WPA. Hierbei wird einem Rechner der Zugang nur dann gewährt, wenn er einen geheimen kryptographischen Schlüssel kennt.

In vielen kommerziellen Bereichen (etwa bei so genannten "Hotspots" in Hotels oder Bahnhöfen) wird schließlich ein weiterer Mechanismus verwendet. Im drahtlosen Netz wird jedem Rechner eine IP-Adresse zugewiesen. Jedoch wird der Datentransport über den Zugangspunkt hinweg zunächst blockiert. Bei diesem Vorgehen wird der Kunde beim Aufruf einer beliebigen Webseite auf eine voreingestellte Webseite umgelenkt, die zur Eingabe von Zahlungs- oder anderen Informationen auffordert. Diese Webseite wird jedoch nicht aus dem Internet geladen sondern stammt direkt vom Zugangspunkt selbst. Erst wenn die eingegebenen Informationen eine gewünschte Form haben (gültiges Passwort oder Kreditkarteninformationen etwa), wird der Zugang zum Internet freigegeben. Eine strukturell ähnliche Form der Zugangskontrolle wenden auch viele Firmen und Universitäten heute in Form so genannter *virtueller privater Netze* (VPN) an.

Aus Sicht der Strafverfolgungsbehörden sind insbesondere offene Zugangspunkte ein Problem, da erstens die Zuordnung von einer Internetkommunikation an der IP-Adresse des Zugangspunktes endet und zweitens der Benutzerkreis des Zugangspunktes nicht eingrenzbar ist. Theoretisch könnte man den konkreten Rechner, der die Datenübertragung verursachte, durch seine MAC-Adresse identifizieren. Voraussetzung hierfür ist jedoch, dass man den fraglichen Rechner bereits gefunden hat, denn eine weltweite Registrierung von MAC-Adressen gibt es, wie bereits erwähnt, nicht. Die MAC-Adresse ist zudem relativ einfach zu manipulieren. Außerdem geht, wie oben in Abschnitt 2.2 besprochen, die Zuordnung zu einer MAC-Adresse relativ schnell verloren.

Kommerzielle Zugangspunkte erlauben manchmal den legalen Zugang ohne Identifikation des Nutzers. Ähnlich einer Telefonkarte kann man gegen Bargeld Gutscheine mit Zugangscodes zum drahtlosen Netz erwerben. Wenn auf dem verwendeten Rechner die MAC-Adresse manipuliert wurde, gibt es keinerlei technische Rückverfolgungsmöglichkeit mehr. Ermittlungsbehörden sind dann auf Zeugenaussagen oder die Auswertung von Überwachungskameras angewiesen.

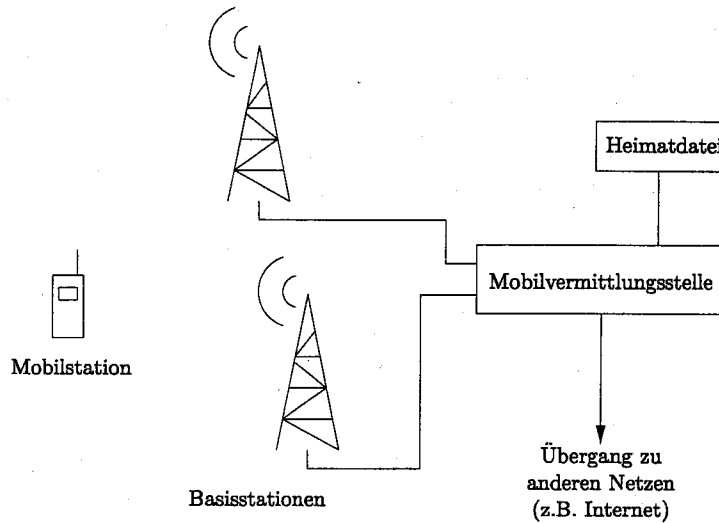


Abbildung 2: Vereinfachte Struktur des GSM-Systems.

2.4 Mobilfunktechnologie

Es folgt ein cursorischer Überblick über die heute gerbäuchliche Mobilfunktechnologie GSM mit den Diensten SMS, MMS sowie GPRS. Das UMTS-System ist strukturell ähnlich aufgebaut, so dass die Ausführungen in der Regel auch auf UMTS übertragbar sind. Mehr Details, etwa zur Verwendung von Netzen fremder Betreiber (*roaming*), finden sich bei Walke.

2.4.1 Telefonie im GSM-Netz

Das GSM-Netz besteht aus den *Mobilstationen* (z.B. Mobiltelefone), *Basisstationen* (den meist auf Sendemasten angebrachten Antennen) sowie dem *Vermittlungsteilsystem*. Nur die Kommunikation zwischen Mobilstation und Basisstation ist drahtlos, alles sonstige ist drahtgebunden und liegt im Herrschaftsbereich eines oder mehrerer Betreiber.

Basisstationen decken mit ihren Antennen eine Funkzelle ab. Funkzellen haben einen Durchmesser von wenigen 100 Metern (in Ballungsgebieten) bis zu wenigen Kilometern (in ländlichen Regionen). Eine oder mehrere Funkzellen sind in geographische Bereiche zusammengefasst, die durch eine *Mobilvermittlungsstelle* verwaltet werden. An die Vermittlungsstellen sind regional verteilt so genannte Heimatdateien angegliedert. Eine Heimatdatei ist eine Datenbank, die Teile der Kundendaten (Name, Telefonnummer, etc.) sowie den Betriebszustand und ggf. auch den aktuellen Aufenthaltsort eines Teilnehmers speichert. Jeder Teilnehmer wird dabei in genau einer Heimatdatei geführt¹.

Im eingeschalteten Zustand prüft die Mobilstation regelmäßig die Signalstärken der Basisstationen in ihrem Empfangsbereich. Wenn die Mobilstation den geographischen Bereich verläßt, der durch ein und dieselbe Mobilvermittlungsstelle verwaltet wird, meldet sie eine Aktualisierung des Aufenthaltsortes an die Basisstation. Dies führt zu einer Aktualisierung des entsprechenden Eintrages in der Heimatdatei.

Bei einem eingehenden Ruf zur Mobilstation wird über die Rufnummer die Heimatdatei des Mobilteilnehmers identifiziert. Durch Abfrage der Heimatdatei wird die für den aktuellen Aufenthaltsort zuständige Mobilvermittlungsstelle abgefragt, die daraufhin einen Funkruf an allen ihr zugeordneten Funkzellen startet. Nach Antwort der Mobilstation auf

¹Walke S. 147.