Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung

Felix C. Freiling

Technischer Bericht TR-2009-005
Universität Mannheim
Institut für Informatik

22. Juni 2009

Überarbeitete Fassung meiner Stellungnahme
im Rahmen der Verfassungsbeschwerden 1 BvR 256/08, 263/08, 586/08
für das Bundesverfassungsgericht

Inhaltsverzeichnis

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 Schichten erläutern. Abbildung 1 stellt die Schichten im Zusammenhang dar. In der folgenden Darstellung wird zur Verdeutlichung eine Analogie zur Briefpost hergestellt, die etwas konstruiert erscheinen mag aber die Ausführungen möglicherweise etwas plastischer macht.

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 gemeinsamen Medium verbunden sind.

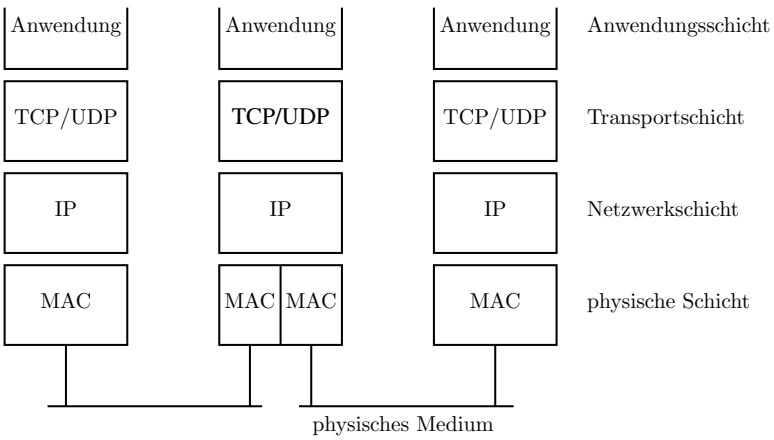

Abbildung 1: Schichtensttruktur IP-basierter Kommunikationssysteme

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 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. Die Bits werden zu Datenpaketen zusammengefasst. Vor dem Versand wird dem Datenpaket ein "Kopf" vorangestellt, der die MAC-Adressen von Sender und Empfänger enthält (*Protokollkopf*).

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-

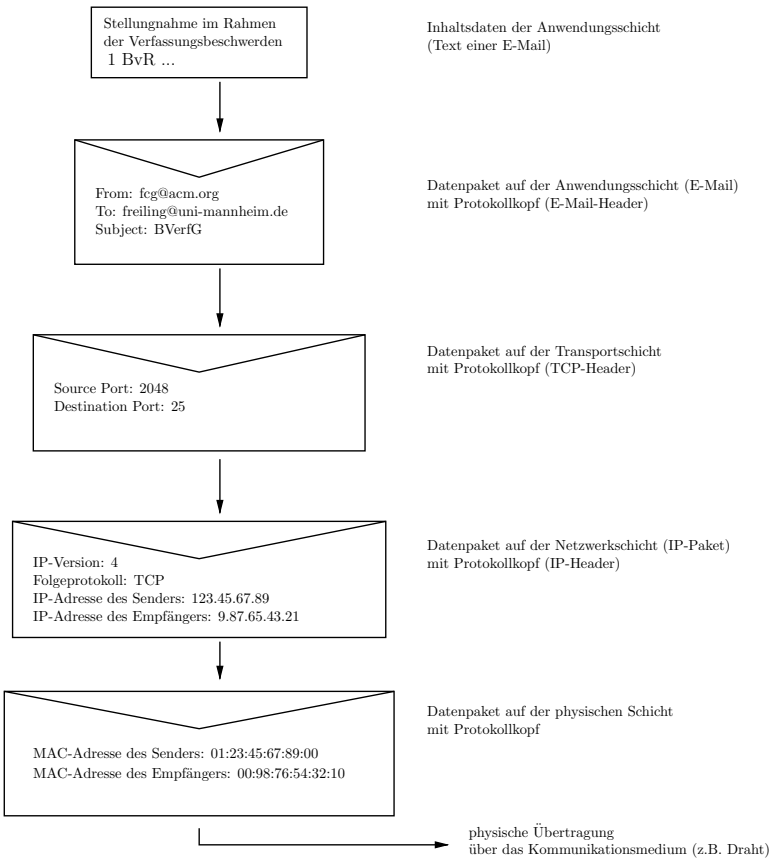

Abbildung 2: Darstellung der Schichtenstruktur mittels Analogie zur Briefpost.

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.

Die physische Schicht ist vergleichbar mit dem Hauspostdienst in einer größeren Organisation, der Briefumschläge zur Übermittlung beliebiger Dokumente zur Verfügung stellt. Auf die Umschläge dürfen nur Raumnummern geschrieben werden. Die Raumnummern entsprechen dabei den MAC-Adressen, denn sie haben in unterschiedlichen Organisationen eine unterschiedliche Bedeutung. Die Informationen auf dem Umschlag entsprechen dem Inhalt des Paketkopfes. Dies ist unten in Abbildung 2 dargestellt, auf die im folgenden noch mehrfach verwiesen wird.

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 fin-

den können (die so genannte *Wegewahl*, *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 Wegewahl 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 wieder ein Kopf vorangestellt, der unter anderem die IP-Adresse des Zielrechners sowie die IP-Adresse des Absenders enthält. Für die eigentliche Übertragung der Daten von Rechner zu Rechner wird jeweils auf die Dienstleistungen der physischen Schicht zurückgegriffen.

Das Beispiel aus Abbildung 2 kann hier fortgesetzt werden. Das IP-Paket kann man sich als Briefumschlag vorstellen. Die zu sendenden Daten werden in diesen Umschlag gesteckt und mit Informationen zur Wegewahl (IP-Adresse von Sender und Empfänger) versehen. Dieser komplette Umschlag (also Paketkopf inklusive Inhalt) wird in den Umschlag der physischen Schicht gesteckt. Die physische Schicht übernimmt die eigentliche Über-"Tragung" per Hauspost, wie in Abschnitt 2.1.1 dargestellt.

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. 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*).

Im Beispiel von Abbilding 2 ist ein Datenpaket auf der Transportschicht wieder vergleichbar einem Briefumschlag. In der Abbildung handelt es sich um ein Datenpaket des Protokolls TCP. Das Datenpaket hat wieder einen Protokollkopf bestehend aus der Aufschrift des Briefumschlages. Der Protokollkopf besteht hier nur aus den Anschlussnummern beim Sender und beim Empfänger. Die Anschlussnummer ist etwa analog zu unterschiedlichen Sachbearbeitern bei der Briefpost. Die zu versendenden Daten werden in den Umschlag gesteckt und an die Netzwerkschicht übergeben. Im Bild bedeutet das: Der gesamte Briefumschlag der Transportschicht wird in den Umschlag der Netzwerkschicht gesteckt.

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. In Abbildung 2 ist das Beispiel E-Mail dargestellt. Ein Text, der Inhalt einer E-Mail, wird in ein "E-Mail-Datenpaket" auf Anwendungsschicht gesteckt. Das Paket wird mit einer Aufschrift versehen: den Adressen von Sender und Empfänger, die Betreffzeile usw. Diese Informatio-

nen sind Teil des Protokollkopfes der Anwendungsschicht (hier des Anwendungsprotokolls SMTP). Das komplette Datenpaket (E-Mail-Inhalt mit E-Mail-Kopf) wird in den Umschlag der Transportschicht zum Weiterversand gesteckt.

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 lo-

kale IP-Adressen vergibt (zum Beispiel die in Deutschland sehr verbreitete “Fritz-Box” der Firma AVM).

In der Sprache des Beispiels aus Abbildung 2 besteht das Internet aus einer Sammlung von Organisationen, die für sich jeweils einen eigenen Hauspostdienst besitzen. Der Hauspostdienst operiert nach jeweils eigenen Regeln und mit eigenen physischen Adressen. Im folgenden gehen wir zur Vereinfachung von nur zwei benachbarten Organisationen aus, die durch Farben (rot und grün) bezeichnet werden sollen. Die Hauspost der roten Organisation hat also rote Briefumschläge, die grüne Organisation verwendet grüne Umschläge. Um im Bild zu bleiben: rote Umschläge können nicht im grünen Hauspostbereich benutzt werden (aufgrund verschiedener Netzwerktechnologien).

Die IP-Adressen sind global gültig. Möchte man Daten aus der roten in die grüne Organisation versenden, steckt man die Daten in einen Umschlag (IP-Paket), schreibt die IP-Adresse des Empfängers (aus der grünen Organisation) darauf und übergibt den Umschlag an die Hauspost. Auf den Umschlag der Hauspost (Paket auf der physischen Schicht) schreibt man als Ziel die Raumnummer der Postzentrale (Grenzrechner) der roten Organisation. Diese regelt den Übergang in den grünen Hauspostbereich.

Die Postzentrale hat zwei Türen (Netzwerkkarten), eine rote und eine grüne. Durch die rote Tür erreicht man alle Räume der roten Organisation, durch die grüne alle Räume der grünen Organisation. In der Postzentrale werden die aus dem roten Hauspostbereich eingehenden Briefumschläge entgegen genommen und ausgepackt. Wenn die IP-Adresse des darin liegenden Umschlags aus der grünen Organisation stammt (das aus der IP-Adresse ersichtlich), dann wird das IP-Paket in einen neuen grünen Briefumschlag gesteckt, mit der richtigen Raumnummer versehen und durch die grüne Tür ins Hauspostsystem der anliegenden Organisation gegeben. Hier wird deutlich, dass die Hauspostzentrale (Grenzrechner) die Zuordnung von IP-Adresse zu Raumnummer (MAC-Adresse) kennen muss, und zwar für jede angrenzende Organisation getrennt.

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 eine 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 Zugangspunkts 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.

2.4 Mobilfunktechnologie

Es folgt ein kursorischer 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 geführt[1].

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

[1] Walke S. 147.

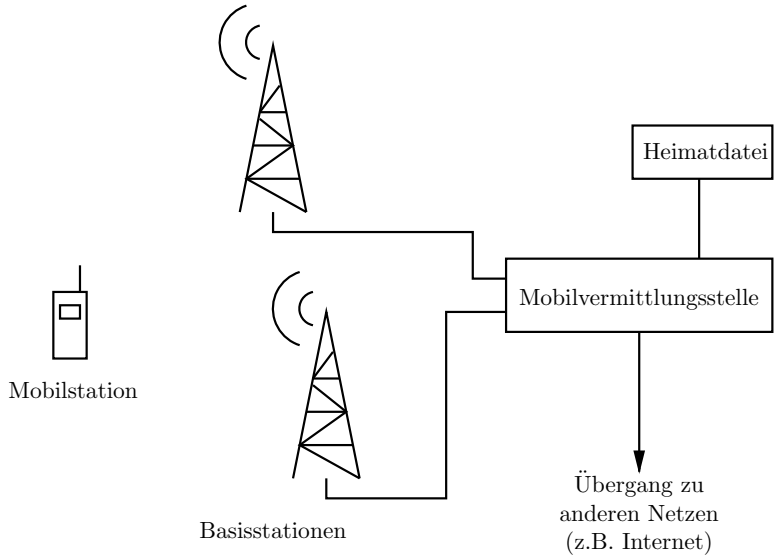

Abbildung 3: Vereinfachte Struktur des GSM-Systems.

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 den Funkruf über die für den Teilnehmer am Besten geeignete Basisstation wird die Telefonverbindung eröffnet[2].

Bei einem aussgehenden Ruf von der Mobilstation übergibt die Mobilstation die Rufnummer des gewünschten Teilnehmers an die Basisstation. Unter Rückgriff auf die Heimatdatei des Teilnehmers wird die aktuell zuständige Mobilvermittlungsstelle identifiziert und über diese das Gespräch aufgebaut.

2.4.2 Authentifizierung im GSM-Netz

In GSM benötigen Teilnehmer ein *subscriber identity module* (SIM). Das SIM wird heute meist als Chipkarte realisiert und gehört dem Betreiber des Mobilfunknetzes. Das SIM enthält Informationen, die den Teilnehmer identifizieren, insbesondere einen geheimen Schlüssel, der ansonsten nur dem Netzbetreiber bekannt ist, und die *international mobile station identity* (IMSI). Die IMSI enthält einen Eintrag für das Land des Teilnehmers, eine Identifizierung der Heimatdatei des Teilnehmers (hieraus ist auch der Netzbetreiber abzulesen), sowie eine eindeutige Kennung des Teilnehmers innerhalb der Heimatdatei.

Über die Informationen im SIM erfolgt die Authentifikation von Mobilstation gegenüber der Basisstation. Auf Wunsch der Basisstation kann dabei unter anderem auch die IMSI übertragen werden. Eine Authentifikation der Basisstation gegenüber der Mobilstation erfolgt *nicht*[3]. Die fehlende Authentifikation der Basisstation gegenüber der Mobilstation nutzt der so genannte *IMSI-Catcher*[4].

Alle teilnehmerbezogenen Daten werden auf der Funkschnittstelle verschlüsselt übertragen. Signalisierungsinformationen (etwa zur Aktualisierung des Standortes) werden aus

[2] Walke S. 263.
[3] Walke S. 326ff.
[4] Fox.

Effizienzgründen nicht verschlüsselt[5]. Zur Identifikation eines Teilnehmers wird dann eine temporäre Funkkennung verwendet (*temporary mobile subscriber identity*, TMSI)[6]. Die TMSI ist eine Zufallszahl, die die IMSI des Teilnehmers verschleiert. Die TMSI wird von der Mobilvermittlungsstelle vergeben und periodisch, bzw. bei Wechsel des durch die Mobilvermittlungsstelle kontrollierten Sendebereichs, gewechselt.

Auf Wunsch der Basisstation kann auch in einen unverschlüsselten Modus gewechselt werden. Dieser Modus wurde in den GSM-Standard aufgenommen, um ihn auch in Staaten etablieren zu können, in denen eine derartige Verschlüsselung verboten ist[7]. Aber auch der IMSI-Catcher verwendet diesen Modus, um Telefongespräche abzuhören.

Jedes Mobilgerät enthält ebenfalls eine eindeutige Kennung, die *international mobile equipment identity* (IMEI). Die IMEI spielt eine ähnliche Rolle wie die MAC-Adresse in lokalen Netzen, sie ist allerdings schwerer manipulierbar als eine MAC-Adresse. Auch die IMEI enthält Felder, die den Hersteller, das Modell und eine Seriennummer kodieren. Man kann beispielsweise anhand der IMEI herausfinden, ob es sich um ein Autotelefon handelt.

Wie die IMSI kann auch die IMEI auf Wunsch der Basisstation übermittelt werden. Über die IMEI realisieren die Mobilfunkbetreiber die Zugangskontrolle von Geräten (im Gegensatz zu Teilnehmern). Dazu führen die Betreiber drei Listen in einer Datenbank: eine *weiße* Liste mit gültigen Mobilstationen, eine *schwarze* Liste mit gestohlenen oder gesperrten Mobilstationen, und eine *graue* Liste von Geräten mit Funktionsstörungen, für die deshalb keine Dienste zur Verfügung gestellt werden[8].

2.4.3 SMS im GSM-Netz

Der populäre SMS-Dienst für Kurznachrichten mit maximal 160 Zeichen funktioniert ähnlich wie elektronische Post. Kurznachrichten für eine Mobilstation werden dabei in einem SMS-Betriebszentrum (*short messaging service center*, SMSC) zwischengespeichert und durch Kontaktaufnahme mit dem Mobilgerät ausgeliefert. SMS basiert auf der Nutzung des Signalisierungsprotokolls von GSM[9].

Das Absetzen einer SMS an ein Mobilgerät erfolgt zunächst ähnlich wie ein eingehender Ruf zur Mobilstation, indem eine Signalisierungsnachricht mit der TMSI des SMS-Empfängers an alle Mobilstationen im aktuellen Aufenthaltsbereich gesendet wird. Da eine SMS mehrere Empfänger haben kann, können in derselben Nachricht auch mehrere Empfänger mittels ihrer TMSI identifiziert werden. Die Empfänger antworten der Basisstation. Anschließend wird über eine verschlüsselte Verbindung der Inhalt der Nachricht übertragen[10].

Setzt man einen Protokollparameter auf einen bestimmten Wert, wird die SMS in der Regel beim Empfänger nicht angezeigt[11]. Dies wird häufig als “Ping”, “stille SMS” oder “stealth SMS” bezeichnet. Die Sonderbehandlung dieser Art von SMS resultiert allein aus dem Verhalten des Endgerätes. Eine stille SMS wird also beim Versenden und beim Transport im Netz genau so behandelt wie eine “nicht stille” SMS. Es werden also dieselben Verkehrsdaten erzeugt, die durch Strafverfolgungsbehörden abgefragt werden können. Eine technische Motivation zur Aufnahme der stillen SMS in den GSM-Standard (etwa zur Störungsbeseitigung) ist mir nicht bekannt.

2.4.4 GPRS im GSM-Netz

GPRS ist ein im GSM-Netz angebotener Datendienst, d.h. man kann GPRS sehr einfach als Trägermedium für IP-basierten Datenverkehr verwenden. Die Systemarchitektur von

[5] Walke S. 328.
[6] Walke S. 327.
[7] Fox.
[8] Walke S. 150.
[9] Walke S. 185ff.
[10] Enck et al.
[11] Engel Folie 17.

GPRS ordnet jeder Mobilvermittlungsstelle eine *GPRS-Unterstützungsknoten* (*GPRS Support Node*) zu. Der Unterstützungsknoten dient einerseits als Verbindung zu sonstigen Datennetzen (wie dem Internet). In dieser Eigenschaft setzt er externe Protokolladressen (wie eine IP-Adresse) in interne Protokolladdressen (wie einer IMSI) um. Andererseits dient der Unterstützungsknoten als Anfangs- und Endpunkt eines "Datentunnels" zur Mobilstation. Hier wird GSM quasi als physische Schicht zur Datenübetragung verwendet. Das bedeutet beispielsweise, dass dort Datenpakete der Mobilstation entkapselt werden und in Richtung des richtigen Paketdatennetzwerkes (wie dem Internet) weitergeleitet werden[12]. Über diesen Tunnel können beliebige Paketdatenprotokolle gesendet werden. Der Unterstützungsknoten (in Verbindung mit den Basisstationen) übernimmt also ähnliche Aufgaben wie der Zugangspunkt im WLAN.

Zur Aktivierung des Paketdatendienstes wird ein logischer Verbindungskontext zwischen Mobilstation und Unterstützungsknoten erstellt[13]. Hierfür erhält die Mobilstation eine eindeutige temporäre Verbindungskennung zugewiesen (*temporary logical link identity*, TLLI). Wenn GPRS aktiv ist, dann befindet sich die Mobilstation in einem von drei logischen Zuständen: Aktiv (*ready*), Stand-by, Leerlauf (*idle*). Im aktiven Zustand prüft die Mobilstation regelmäßig ihren Aufenthaltsbereich. Bei einer Änderung der Funkzelle wird dies im GPRS-Register aktualisiert. (Das GPRS-Register ist ein Teilbereich der Heimatdatei.)

Werden eine gewisse Zeit keine Datenpakete geschickt, geht die Mobilstation in den GPRS-Zustand Stand-by über. Im Stand-by-Zustand werden lediglich Änderungen des durch den Unterstützungsknoten abgedeckten Bereichs im GPRS-Register gespeichert (dieser Bereich entspricht in etwa dem durch eine Mobilvermittlungsstelle verantworteten Bereich, also einer Menge von Funkzellen).

Heute gibt es bereits viele mobile Geräte, die mit einem Festpreistarif für den mobilen Datenzugang ausgestattet sind (z.B. Apple iPhone oder das Mobiltelefon von Google). Diese bieten viele ortsabhängige Dienste an, beispielsweise einen Routenplaner oder Informationen über den Zugfahrplan am nächstgelegenen Bahnhof. Während der Interaktion stellen diese Geräte also notwendigerweise regelmäßig Datenverbindungen mit dem Internet her.

2.4.5 MMS im GSM-Netz

MMS (*multimedia messaging service*) ist eine Weiterentwicklung von SMS, die den Versand von multimedialen Nachrichten erlaubt (Bilder, Tonaufnahmen, Videos). MMS ist vollkommen IP-basiert und benutzt ähnlich wie GPRS das GSM-System als Tunnel zur Übertragung von Datenpaketen.

Technisch funktioniert der Empfang einer MMS-Nachricht wie folgt: Zunächst wird die Mobilstation mittels einer speziellen SMS-Nachricht über das Vorliegen einer für sie bestimmten MMS-Nachricht informiert. Anschließend kontaktiert die Mobilstation über GPRS eine zentrale Sammelstelle für MMS-Nachrichten und lädt die Nachricht auf die Mobilstation[14]. Ausgehende MMS-Nachrichten werden direkt über GPRS übertragen.

2.5 LKW-Mautsystem der Firma TollCollect

Mobilkommunikation kommt auch im LKW-Mautsystem der Firma TollCollect zum Einsatz. Die automatische Mauterhebung wird dabei durch so genannte *onboard units* (OBUs) ermöglicht. Eine OBU enthält neben einem Empfangsgerät des globalen satellitengestützten Positionierungssystems GPS ein GSM-Mobiltelefon mit SIM.

Während der Fahrt prüft die OBU regelmäßig den Standort des LKW und vergleicht diesen mit intern gespeicherten Verzeichnissen mautpflichtiger Straßen. Wird erkannt, dass

[12] Walke S. 304.
[13] Walke S. 304f.
[14] Mulliner/Vigna.

der LKW eine mautpflichtige Strecke befährt, generiert die OBU eine Erhebungsnachricht und speichert sie in einem internen Puffer ab. Wenn der Puffer voll ist, wird sein Inhalt mittels SMS an TollCollect verschickt. TollCollect verwendet anschließend diese Daten zur Abrechnung der Maut. Die an Autobahnen angebrachten Kontrollbrücken haben mit der eigentliche Abrechnung nichts zu tun. Sie fotografieren passierende LKW von verschiedenen Seiten, um stichprobenartig die mautrelevanten Angaben (Größe des LKW, Anzahl der Achsen, etc.) zu überprüfen.

Die im Rahmen des LKW-Mautsystems übertragenen SMS-Nachrichten unterscheiden sich von ihrer Struktur her nicht von regulären SMS-Nachrichten anderer Benutzer. Es fallen also alle Verkehrsdaten an, die auch bei eine privaten Nutzung von SMS entstehen.

3 Zur Begriffsbildung

Die in der Telekommunikation anfallenden Daten werden rechtlich in Inhalts-, Verkehrs- und Bestandsdaten klassifiziert. Dieser Abschnitt versucht, diese Definitionen aus einer technischen Perspektive zu beleuchten.

3.1 Inhaltsdaten

Unter *Inhaltsdaten* versteht man alle bei einem Kommunikationsvorgang anfallenden Daten. Diese umfassen bei der Telefonie etwa die konkreten Gesprächsinhalte eines Telefonates und in der Datenkommunikation *alle* übertragenen Informationen[15].

3.1.1 Legaldefinition und Beispiele

Der Begriff der Inhaltsdaten ist nirgends legal definiert[16]. In der Literatur taucht zum Teil eine leicht einschränkende, engere Definition auf, die unter Inhaltsdaten *ausschließlich* den Inhalt von Gesprächen oder die Inhalte von E-Mails versteht[17]. Wie die Ausführungen in Abschnitt 3.2 zeigen werden, ist diese Unterscheidung aus technischer Sicht schwer fassbar. Problematisch ist zusätzlich, dass die engere Definition von Inhaltsdaten implizit von einem menschlichen Urheber der Nachrichten auszugehen scheint. Kommunikationsvorgänge, die komplett zwischen Maschinen geschehen, laufen Gefahr, nicht durch den Begriff abgedeckt zu werden. Ein Beispiel für rein maschinell generierte Kommunikationsvorgänge sind die Erhebungsnachrichten der Autobahnmaut (siehe Abschnitt 2.5).

3.1.2 Technische Betrachtung der Definition

Der Begriff der Inhaltsdaten ist als Maximalbegriff aus technischer Sicht unproblematisch. Er umfasst dann die Gesamtheit der Daten, die im Rahmen eines Kommunikationsvorgangs ausgetauscht werden. Das schließt sowohl die Daten ein, die zum Aufbau einer (auch vertraglichen) Kommunikationsbeziehung anfallen, als auch alle über das Kommunikationsmedium übertragenen Bits.

Wenn man Inhaltsdaten als das Maximum derjenigen Daten definiert, die im Rahmen eines Kommunikationsvorgangs anfallen, dann wird deutlich, dass die Gesamtheit der Inhaltsdaten den Kommunikationsvorgang vollständig beschreibt. Umfassende Kenntnis der Inhaltsdaten impliziert somit auch umfassende Kenntnis des Kommunikationsvorgangs.

[15] Bär RN. 42.
[16] Bär RN. 41.
[17] Seitz S. 71.

3.2 Verkehrsdaten

Verkehrsdaten sind allgemein alle Daten, die über die näheren Umstände eines Kommunikationsvorgangs Auskunft geben. Konkret bedeutet das im Bereich der Telefonie etwa, wer mit wem wann und wie lange kommuniziert hat[18].

3.2.1 Legaldefinition und Beispiele

Der Begriff der Verkehrsdaten ist in § 3 Nr. 30 TKG legal definiert. Als Verkehrsdaten sind dort alle Daten zu verstehen, "die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden." Als englische Übersetzung hat sich der Begriff *traffic data* eingebürgert[19].

Konkret zählt § 96 TKG eine Reihe von Verkehrsdaten auf, beispielsweise

- die Kennungen (z.B. Rufnummern) von Sender und Empfänger,
- Datum und Uhrzeit des Beginns und des Endes der Verbindung und
- Standort beim Mobilfunk.

3.2.2 Technische Betrachtung der Definition

Eine naheliegende technische Interpretation des Begriffs Verkehrsdaten im Rahmen der paketvermittelten Datenkommunikation liegt in der Unterscheidung zwischen Kopf und Inhalt eines Datenpaketes (siehe Abschnitt 2.1.1). Verkehrsdaten könnten interpretiert werden als die Inhalte des Protokollkopfes von Datenpaketen, die über das Medium transportiert werden.

Ein Problem bei dieser Definition entsteht aus der Schichtenstruktur modernen Kommunikationssysteme (siehe Abschnitt 2.1). Datenpakete höhere Schichten liegen vollständig im Inhaltsbereich von niedrigeren Schichten. Folglich sind Protokollköpfe auf höheren Schichten Inhalte auf niedrigeren Schichten. Beispielsweise werden die kompletten Protokollinformationen der Transportschicht (inklusive der Nummer des adressierten Anschlusses) im Inhaltsteil der Transportschicht transportiert (vergleiche Abbildung 2).

Für eine exakte Unterscheidung müsste man eine Schicht festlegen, an der der Wechsel von Verkehrs- zu Nicht-Verkehrsdaten (also Inhaltsdaten im engeren Sinne) vollzogen wird. Hierfür bieten sich entweder die Netzwerkschicht, die Transportschicht oder eine darüber liegende Schicht an.

Nähme man die Netzwerkschicht mit dem IP-Protokoll als Grenze, wären also alle Daten, die im Protokollkopf eines IP-Paketes stehen, Verkehrsdaten. Alles, was im Inhaltsfeld des IP-Paketes steht, wäre kein Verkehrsdatum sondern ein Inhaltsdatum im engeren Sinn. Um diese technische Interpretation zu prüfen, betrachten wir die relevanten Einträge im IP-Protokollkopf etwas näher. Diese umfassen im Wesentlichen (vergleiche auch Abbildung 2)

- die IP-Adresse des Absenders und Empfängers, sowie
- ein Code für das im IP-Paket transportierte Protokoll (das so genannte *Folgeprotokoll*, beispielsweise TCP oder UDP, siehe die vollständige Liste der IANA[20]).

Zusammen mit dem Zeitpunkt der Datenübertragung kann man diese Informationen als eine minimale Charakteristik eines einzelnen Datenpaketes auffassen.

Je weiter man in der Schichtenstruktur hinaufklettert, desto mehr Protokollköpfe fallen in den Definitionsbereich der Verkehrsdaten. E-Mail-Adressen etwa gehören in den Protokollkopf des Anwendungsprotokolls SMTP. Technisch sind E-Mail-Adressen auf derselben

[18] Seitz S. 71.
[19] Bär RN. 19.
[20] IANA.

Stufe anzusiedeln wie die Kennungen von besuchten Webseiten im WWW (die URL ist Teil des Protokollkopfes des Anwendungsprotokolls HTTP). Wenn man E-Mail-Adressen als Verkehrsdaten klassifiziert, dann müsste man auch besuchte URLs als Verkehrsdaten ansehen. Eine andersartige Klassifikation ist technisch schwer nachzuvollziehen.

Theoretisch können beliebige Inhaltsdaten in den Protokollkopf eines Datenpaketes hineincodiert werden. Beispielsweise kann man die Antwort auf eine Ja/Nein-Frage (also einen Teil des Inhaltes eines Datenpaketes) an die Verwendung eines bestimmten Protokolls auf der Transportschicht binden (falls die Antwort "Ja" lautet, verwende etwa TCP, falls "Nein", verwende UDP). Diese Information ist jedoch Teil des Protokollkopfes der Netzwerkschicht (vergleiche Abbildung 2, Eintrag "Folgeprotokoll" auf dem "Umschlag" der Netzwerkschicht). Inhaltsdaten werden dann zu Verkehrsdaten.

Umgekehrt können auch beliebige Einträge des Protokollkopfes auf einer Schicht im Inhaltsfeld eines Datenpaketes wiederholt werden. Man könnte beispielsweise die IP-Adresse des Empfängers in den Inhalt einer E-Mail hineinschreiben. Verkehrsdaten werden dadurch zu Inhaltsdaten.

Egal wo man die Grenze also auch ansetzt, es besteht immer die Möglichkeit, dass diese Grenze bei der Konstruktion und Definition zukünftiger Protokolle in Datennetzen nach "oben" oder nach "unten" verschoben wird. Inhaltsdaten werden dann plötzlich zu Verkehrsdaten und umgekehrt.

3.2.3 Bildung von Bewegungsprofilen

Die Preisgabe von Verkehrsdaten in Form von IP-Adressen oder Standorten ermöglicht aufgrund der Tendenz zu immer kürzeren Kommunikationsvorgängen (wie etwa bei SMS) eine nahezu lückenlose räumliche Überwachung. Dies wird in Zukunft im Fall von mobilen Internetzugängen (beispielsweise mittels iPhone) auch auf Basis einer dynamisch vergebenen IP-Adresse möglich sein.

Ein Experiment mit einem mobilen Internetzugang über GPRS des Anbieters Vodafone Anfang Juni 2009 ergab auf einer Bahnreise von Mannheim nach Frankfurt, dass meinem Rechner 6 verschiedene IP-Adressen zugeteilt wurden. Diese IP-Adressen waren eindeutig identifizierbar als Adressen, die durch Vodafone vergeben wurden. Sie stammten aus einem zentralisiert verwalteten Kontingent, das auf eine Adresse des Anbieters im Berliner Raum zugelassen war. Es ist zu erwarten, dass TK-Anbieter den Zugangsdienst regional verteilen werden und wie im Festnetzbereich bereits praktiziert abhängig vom Ort des Teilnehmers IP-Adressen aus unterschiedlichen Adressbereichen zuweisen werden. Wenn der Teilnehmer eine *roaming*-Option für sein mobiles Gerät gewählt hat, dann deutet bereits heute ein Wechsel der IP-Adresse in den Bereich eines anderen Anbieters auf einen Wechsel des Standortes des Teilnehmers hin.

3.3 Bestandsdaten

Bestandsdaten sind im Rahmen einer Telekommunikation alle Daten, die keinen Bezug zu einem konkreten Telekommunikationsvorgang besitzen.

Nach § 3 Nr. 3 TKG sind sie legal definiert als alle Daten eines Teilnehmers, "die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden." Beispiele für Bestandsdaten sind

- die Rufnummer des Teilnehmers,
- Name und Anschrift des Teilnehmers,
- Anschrift des Anschlusses bei Festnetzanschlüssen und
- Datum des Vertragsbeginns und des Vertragsendes.

Technisch gesehen gehören auch die MAC-Adresse einer Netzwerkkarte zu den Bestandsdaten, auch wenn Sie aktuell durch TK-Anbieter nicht flächendeckend erhoben werden und relativ leicht fälschbar sind.

Technisch gesehen ist die IMSI im Mobilfunk eine Art Telefonnummer und kann demnach auch zu den Bestandsdaten gerechnet werden. Die IMEI wird in der Literatur eher als Verkehrsdatum angesehen[21]. Technisch ist sie aber vergleichbar mit einer MAC-Adresse und wäre darum auch zu den Bestandsdaten zu rechnen, da sie keinen Rückschluss auf einen konkreten Kommunikationsvorgang zulässt. Im Vergleich zur MAC-Adresse ist die IMEI auch schwerer fälschbar. Eine statisch zugewiesene IP-Adresse gehört auch klar zu den Bestandsdaten eines Nutzers.

4 Entstehung und Speicherung von Verkehrsdaten

4.1 Durch § 113a TKG erfasste Daten

§ 96 TKG regelte bisher genau, welche Daten von einem Telekommunikationsanbieter gespeichert werden durften und wann diese zu löschen waren. Im wesentlichen erstreckte sich dies auf Daten, die zu Abrechnungszwecken anfielen. § 113a TKG schreibt nun vor, dass bestimmte Daten unabhängig von der Entgeltermittlung für eine Dauer von 6 Monaten zu speichern sind. Es folgt ein Auszug aus der Liste der zu speichernden Daten:

- Für Telefondienste:
  - Rufnummern des anrufenden und des angerufenen Anschlusses
  - Beginn und Ende der Verbindung (mit Angabe der Zeitzone)
  - Angabe zu den genutzten Diensten
- Für mobile Telefondienste zusätzlich (Mobiltelefonie, SMS, MMS, etc.):
  - IMSI von anrufendem und angerufenen Teilnehmer
  - IMEI von anrufendem und angerufenen Endgerät
  - Bezeichnung der vom anrufenden und angerufenen Teilnehmer zu Beginn der Verbindung genutzten Funkzellen
- Für Internettelefondienste zusätzlich:
  - Die IP-Adressen des anrufenden und angerufenen Anschlusses
- Für elektronische Post:
  - IP-Adressen und E-Mail-Adresse des Senders einer Nachricht sowie E-Mail-Adressen aller Empfänger der Nachricht beim deren Versand
  - Beim Empfang einer Nachricht die E-Mail-Adesse und die IP-Adresse des Absenders
  - IP-Adresse eines Rechners, der auf ein elektronisches Postfach zugreift
  - Die Zeitpunkte der genannten Aktivitäten
- Für den Internetzugang:
  - Beginn und Ende der Internetnutzung eines Teilnehmers mit Angabe der verwendeten IP-Adresse

Zusätzlich müssen in Mobilfunknetzen noch Informationen über die geographische Lage der Funkantennen und ihrer Hauptabstrahlrichtung vorgehalten werden.

[21] Bär RN. 20.

4.2 In der Praxis anfallende Daten ohne Bezug zu § 113a TKG

Generell fallen im Rahmen der Telekommunikation fast alle in § 113a TKG genannten Daten an. Einzige Ausnahme ist meines Wissens die Zeitzone innerhalb einer Mobilvermittlungsstelle, die explizit generiert werden muss.

Im Rahmen der Mobilkommunikation fallen zusätzlich die TMSI an sowie die Funkzellen, durch die sich ein Teilnehmer während des Gespräches bewegt. Wie in Abschnitt 2.4 beschrieben, werden im GSM-System auch die Standortdaten einer Mobilstation verarbeitet, wenn sie empfangsbereit ist (Stand-by-Betrieb). Bei der Mobiltelefonie ist das die geographische Region (mehrere Funkzellen), in der sich ein Teilnehmer befindet.

Bei einer aktiven mobilen Datenkommunikation (über GPRS oder UMTS etwa) fallen, ähnlich wie bei der Telefonie, Daten über die jeweils benutzten Funkzellen an. Von § 113a TKG werden zwar die diesen Geräten zugeteilten IP-Adessen erfasst, jedoch nicht die Funkzellen die beim mobilen Internetzugang durchschritten werden. Die bei der Verwendung von GPRS verwendete TLLI ist auch ein Verkehrsdatum, das nicht durch § 113a TKG erfasst wird.

Im Rahmen der IP-basierten Datenkommunikation fallen viele Daten an, die durch § 113a TKG nicht erfasst werden, da die Norm nur auf Kommunikationsverbindungen bzw. den Internetzugang abhebt und nicht auf die aus vielen Datenpaketen bestehenden Ströme, die im Rahmen der Kommunikation verarbeitet werden. Von den Informationen in den Protokollköpfen werden nur die IP-Adresse und die Zeitpunkte des Versendens und Empfangens des ersten bzw. letzten Datenpaketes erfasst. Alle anderen Informationen der Netzwerkschicht und der physischen Schicht liegen außerhalb von § 113a TKG, etwa die MAC-Adressen der Teilnehmer oder die SSID beim Zugriff über WLAN.

4.3 Probleme bei extern angebotenen Datendiensten

Die in Abschnitt 3.1 beschriebene Problematik bei der Unterscheidung von Inhalts- und Verkehrsdaten kommt erneut zum Vorschein, wenn man diejenigen Verkehrsdaten betrachtet, die für Internettelefondienste gespeichert werden sollen (etwa die IP-Adressen der beteiligten Teilnehmer). Da Internettelefonie auf der Anwendungsebene abgewickelt wird, erfordert ihre Erkennung eine detaillierte Analyse aller Daten auf der Anwendungsebene. Telekommunikationsanbieter, die einen reinen Internetzugang anbieten, haben darum gar keine effektive Möglichkeit, die von § 113a geforderten Daten zu erheben (auch wenn sie sie verarbeiten).

Dieser Umstand ist vor allem aus Sicht der Ermittlungsbehörden bedenklich, da Anbieter von Internetzugängen ausschließlich die Verkehrsdaten von denjenigen Internettelefondiensten erheben können, die sie selbst anbieten. Nicht jeder Anbieter von Internettelefonie muss aber seinen Sitz in Deutschland haben, wie das prominente Beispiel der Firma Skype zeigt. Auch besteht die Möglichkeit, dass zwei Personen mit existierender Software direkt über das Internet telefonieren, sozusagen ohne einen Anbieter in Anspruch zu nehmen.

Ähnliche Überlegungen sind auch auf jede andere Form von Datendiensten (auch elektronische Post) übertragbar. Eine mögliche Intention des § 113a TKG, nämlich die möglichst vollständige Erfassung der wesentlichen Verkehrsdaten heutiger Internetkommunikation, wird in Zukunft in Bezug auf Applikationsdaten zunehmend leer laufen.

4.4 Extern initiierte Datenkommunikation

Datenkommunikation ist zumeist von Teilnehmer selbst initiiert, indem er beispielsweise einen Anruf tätigt oder eine Internetverbindung aufbaut. Kommunikationsverbindungen werden aber auch häufig extern initiiert, etwa durch einen eingehenden Anruf. Am Internet angeschlossene Rechner initiieren heute eine Vielzahl von Kommunikationsvorgängen vollkommen autonom. Beispiele sind die vielen Aktualisierungsvorgänge von Betriebssystemen und gutartigen Applikationen wie Browsern und Antivirenprodukten. Aber auch

bösartige Anwendungen (Trojaner, Würmer, etc.) entfalten Kommunikationsaktivität, etwa bei der Suche nach weiteren infizierbaren Rechnern. Relevant für § 113a TKG wird diese Kommunikation, wenn etwa durch eine solche Datenkommunikation eine Internetverbindung aufgebaut wird oder ein Keylogger die durch ihn gesammelten Passwörter per E-Mail verschickt[22].

Bis auf den E-Mail-Versand sind derartige extern initiierte Verbindungen im privaten Umfeld weniger relevant, da dort der Trend zu langfristig bestehenden Internetverbindungen anhält, die durch Festpreise (*flatrate*) bezahlt werden.

Im Falle von Mobilkommunikation entstehen extern initiierte Verbindungen beispielsweise durch SMS-Mitteilungen des Betreibers beim *roaming* (etwa beim Grenzübertritt). Auch die "stille SMS" (siehe Abschnitt 2.4.3) erzeugt Verkehrsdaten gemäß § 113a TKG.

Insgesamt wird die Kontrolle des Benutzers über den Zeitpunkt und die Menge der durch ihn verursachten Verkehrsdaten in Zukunft abnehmen.

4.5 Entstehungsorte der Verkehrsdaten und alternative Zugriffsmöglichkeiten

Die meisten durch § 113a TKG erfassten Daten fallen direkt beim Telekommunikationsanbieter an. So werden die Informationen über verschickte und empfangene E-Mails meist direkt aus den Protokolldateien der Server ausgelesen. Ein anderes Beispiel sind die Zuordnungen von dynamischen IP-Adressen, die direkt bei der Zugangskontrolle erfasst werden und anschliessend in eigenen Datenbanken gespeichert werden. Theoretisch könnten die Verkehrsdaten also auch über eine Beschlagnahme gewonnen werden.

Andere Verkehrsdaten wie etwa die MAC-Adressen der Endgeräte fallen häufig nur in den lokalen Netzen der Endnutzer an. Im Heimbereich protokollieren die Zugangspunkte in der Regel auch jede Herstellung einer Internetverbindung (mit zugewiesener IP-Adresse) und die Zuweisung von lokalen IP-Adressen an die Rechner im lokalen Netz. Die Protokollierung reicht oft nur wenige Tage in die Vergangenheit und ist durch ein vom Benutzer vergebenes Passwort geschützt. Eine Beschlagnahme der Verkehrsdaten ist hier also wenig erfolgversprechend. Manche Zugangspunkte (beispielsweise die "Fritz-Box" des Herstelles AVM) bieten so genannte "Push-Dienste" an, die das Zugangsprotokoll (verwendete dyamische IP-Adresse, MAC-Adressen der lokalen Rechner) regelmäßig per E-Mail an eine definierte Adresse schickt. Falls die Hardware so konfiguriert ist, könnte man die Verkehrsdaten auch durch Beschlagnahme von E-Mail gewinnen.

4.6 Sorgfaltspflichten des Speichernden

§ 113a Abs. 10 Satz 1 TKG verpflichtet die Telekommunikationsanbieter, die gespeicherten Verkehrsdaten mit der "im Bereich der Telekommunikation erforderlichen Sorgfalt" zu schützen. In der Praxis werden für die durch § 113a erfassten Daten meist eigene Datenbanken verwendet, die durch besondere Vorkehrungen geschützt sind. Wesentlich sind hier eine strikte Befolgung des Vier-Augen-Prinzips sowie ausführliche Protokollierungen sowohl von Zugriffen als auch von Änderungen der Zugriffsberechtigungen. Sinnvoll ist auch eine regelmäßige Überprüfung der Infrastruktur durch unabhängige Abteilungen im eigenen Unternehmen oder durch externe Dienstleister (Penetrationstests).

Wesentlich sind aber nicht nur der Schutz der Daten, sondern auch ihre unverzügliche Verfügbarkeit für den Fall einer Verkehrsdatenabfrage. Durch wiederholte interne Tests muss deshalb regelmäßig geprüft werden, ob die Daten auch bei fehlerhafter Hardware oder einem internen Sicherheitsvorfall wiederhergestellt werden können. Diese Anforderungen sind ähnlich zu denen, die auch betriebswirtschaftliche Kodizes und Gesetzesregelungen erfordern, wie etwa *Sarbanes-Oxley* oder *Basel II*.

[22] Holz/Engelberth/Freiling.

Die umfassende Sammlung von Verkehrsdaten ist natürlich auch für Dienstleister interessant (beispielsweise die Werbeindustrie) oder für Unternehmen, die interne Korruption bekämpfen oder Kontrolle über ihre Mitarbeiter ausüben wollen. Schutzvorkehrungen vor einem Missbrauch der Verkehrsdaten können in der Praxis immer durch die Kooperation mehrerer Innentäter ausgehebelt werden. Diese Gefahren können praktisch kontrolliert werden, jedoch nur mit hohem Aufwand. Die Datenskandale der Vergangenheit haben ihren Ursprung einerseits in einem Missbrauch von *Abrechnungsdaten*, auf die organisatorisch bedingt deutlich mehr Personen Zugriff haben, und andererseits in zu Unrecht erhobenen Verkehrsdaten direkt im Unternehmen.

Der beste Schutz gegen die missbräuchliche Nutzung von Daten bleibt, Daten frühzeitig zu löschen oder am besten gar nicht zu speichern (Gebot der Datensparsamkeit).

4.7 Kosten der Speicherung

Die gesetzlich geforderte Sorgfalt bei der Speicherung von Verkehrsdaten hat ihren Preis. Die Kosten setzen sich zusammen aus einmaligen Infrastrukturkosten und regelmäßigen Kosten für die Aufrechterhaltung der Infrastruktur sowie der Bedienung von Auskunftsersuchen durch die Ermittlungsbehörden.

Bei den Infrastrukturkosten sind diejenigen Telekommunikationsanbieter im Vorteil, die bereits eine bestehende organisatorische Infrastruktur zur Bedienung von Auskunfsersuchen besitzen. Diese müssen die technische Infrastruktur mit zusätzlichen Schnittstellen versehen, um die Verkehrsdaten aus dem Produktivsystem auszulesen. Kosten entstehen auch durch den Aufbau einer geschützten Datenbankinfrastruktur zur Speicherung der Daten. Die Deutsche Telekom AG schätzt die Kosten für die zusätzliche Infrastruktur allein für Festnetztelefonie auf etwa 1 Million Euro.

Kleine Telekommunikationsanbieter, die bisher auch keine Auskunftsersuchen nach § 100g StPO beantworten müssen, werden aufgrund des Fehlens einer entsprechenden technischen Infrastruktur im Verhältnis stärker belastet, da sie auf externe Dienstleister und die durch diese angebotenen Geräte zum Abhören von Telefonverbindungen angewiesen sind. Wäre die Universität Mannheim eine Telekommunikationsanbieter, würden schätzungeweise 200.000 Euro zum Aufbau der Infrastruktur anfallen.

Die Datenmengen, die im Rahmen der Datenspeicherung von Verkehrsdaten anfallen, sind schwer abzuschätzen. Die Deutsche Telekom AG schätzt die Datenmenge allein für die Festnetztelefonie auf 12 Terabyte pro Speicherungszeitraum (6 Monate). Die Speicherung der Verkehrsdaten aus dem Mobilfunk erfordert schätzungsweise weitere 8 Terabyte. Diese Mengen schließen diejenigen Verkehrsdaten nicht mit ein, die aus dem E-Mail-Verkehr entstehen.

Der dauerhaft anfallende Aufwand hängt von der Größe der Infrastruktur und damit der Anzahl der erwarteten Auskunftsersuchen ab. Die Deutsche Telekom AG schätzt die Kosten des Betriebs der Infrastruktur auf 100.000 Euro pro Monat. Die Anzahl der eingehenden Auskunftsersuchen pro Jahr erfordert dort den Personalaufwand von schätzungsweise 10 Vollzeitmitarbeitern.

Wäre die Universität Mannheim ein Telekommunikationsanbieter, der zur Speicherung von Verkehrsdaten verpflichtet wäre, müsste eine zusätzliche Vollzeitkraft zur Pflege der Infrastruktur und Bearbeitung der Auskunftsersuchen eingestellt werden, was jährlichen Mehrausgaben von etwa 50.000 Euro entspricht.

5 Notwendigkeit der Speicherung von Verkehrsdaten

Das TKG erlaubt die Speicherung von Verkehrsdaten im Wesentlichen aus zwei Gründen: zu Abrechnungszwecken (§ 96 TKG) und zur Verfolgung von Straftaten (§ 113b TKG). Für beide Fälle wird im folgenden der notwendige Umfang an Verkehrsdaten untersucht.

5.1 Zu Abrechnungszwecken

Abrechnungszwecke erfordern die Speicherung einer fest umrissenen Menge von Verkehrsdaten, die wesentlich von der Tarifgestaltung abhängt. Für Tarife, die abhängig von der Anzahl und der Dauer getätigter Telefongespräche sind, sind die gewählten Rufnummern und die Legitimation für die entstandenen Kosten zu speichern (in der Regel Anfangszeitpunkt und Dauer des Gespräches). In der Praxis wurden zudem Kundenwünsche bei der Speicherung berücksichtigt, etwa eine Kürzung der gewählten Rufnummern um die letzten drei Ziffern. Im Bereich der Datenkommunikation gibt es analog so genannte Volumentarife. Dabei ist nicht die Dauer einer Kommunikationsverbindung relevant, sondern die Menge der übertragenen Daten, die dann ebenfalls gespeichert werden muss. Die Daten dürfen bis zur Rechnungsstellung und für einen kurzen Zeitraum darüber hinaus gespeichert werden.

Sowohl bei der Telefonie als auch verstärkt beim Internetzugang haben sich Festpreise (*flatrates*) etabliert, die vollkommen unabhängig von den getätigten Gesprächsminuten oder dem Übertragungsvolumen sind. Bei derartigen Tarifen entfällt die Notwendigkeit zur Speicherung von Verkehrsdaten komplett.

5.2 Zur Verfolgung von Straftaten

§ 113b erlaubt den Zugriff auf die durch § 113a gespeichert Daten

- "zur Verfolgung von Straftaten,
- zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder
- zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes."

Außerdem sind Zugriffe auf Verkehrsdaten nach § 100g Abs. 1 Nr. 2 StPO erlaubt, wenn eine Straftat "mittels Telekommunikation begangen" wurde.

5.2.1 Ablauf einer Verkehrsdatenabfrage

Der Zugriff auf die Verkehrsdaten erfolgt im Rahmen eines Auskunftsersuchens. In der Praxis läuft dies häufig wie folgt ab: Die Strafverfolgungsbehörden senden dem Telekommunikationsanbieter meistens per Fax eine Beschreibung der ersuchten Verkehrsdaten in Verbindung mit der nötigen richterlichen Genehmigung. Anschliessend prüft der Telekommunikationsanbieter die formelle Richtigkeit der Anfrage, recherchiert die angefragten Daten und sendet eine entsprechende Antwort zurück. Die Notwendigkeit einer manuellen Prüfung impliziert, dass derartige Anfragen nur zu den normalen Dienstzeiten des Telekommunikationsanbieters beantwortet werden können. Die Beantwortung erfolgt dann jedoch relativ schnell (in der Größenordnung von einer Stunde Bearbeitungszeit).

Es ist absehbar, dass in Zukunft der Kommunikationsweg per Fax abgelöst wird von einem IT-gestützten System zur elektronischen Abwicklung derartiger Anfragen. Da die Strafverfolgung in den Zuständigkeitsbereich der Bundesländer fällt, bestimmen diese die Form der Auskunftsersuchen. Bundesländer mit einem erhöhten Bedarf an Verkehrsdatenabfragen (beispielsweise Bayern und Nordrhein-Westfalen) werden voraussichtlich eher den elektronischen Weg bevorzugen. Trotz elektronischer Abwicklung entfällt die manuelle Prüfung der Anfrage durch einen Mitarbeiter der Telekommunikationsanbieter aber nicht. Der manuelle Arbeitsaufwand pro Anfrage bleibt.

5.2.2 Nutzen von Verkehrsdatenabfragen in der Praxis

Einen guten Überblick über die in der Praxis abgefragten Verkehrsdaten gibt ein Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht[23]. 70% der

[23] Albrecht/Grafe/Kilchling.

durch die Studie erfassten Beschlüsse entfielen auf Katalogstraftaten gemäß § 100g StPO vor allem Betäubungsmittel-, Raub- und Tötungsdelikte[24]. Dabei fällt auf, dass Verkehrsdatenabfragen oft in der überwiegenden Menge sehr schnell (innerhalb von 14 Tagen nach Beginn der Ermittlungen) erwirkt werden, meist als Vorstufe zur Telekommunikationsüberwachung, um erste Erkenntnisse über das Kommunikationsverhalten der an der Tat beteiligten Personen zu gewinnen. Die Ergebnisse der Verkehrsdatenabfrage sind zudem eher in den Ermittlungen relevant als später vor Gericht (Geständnis nach Konfrontation mit Verkehrsdaten sowie Ergebnissen von Durchsuchungen, die aufgrund von Verkehrsdatenabfragen initiiert wurden)[25]. Die Verkehrsdatenabfrage erscheint demnach als ein universelles, sehr breit eingesetztes Ermittlungsinstrument und wird von Praktikern im Vergleich zu konventionellen und anderen verdeckten Ermittlungsmaßnahmen als weniger belastend eingestuft[26]. Die Zahl der Verkehrsdatenabfragen liegt überall deutlich über der Zahl der Inhaltsdatenabfragen.

5.2.3 Mittels Telekommunikation begangene Straftaten

Von besonderem Interesse sind Straftaten, die ohne Zugriff auf Verkehrsdaten nicht oder nur sehr schwer verfolgt werden können.

Im Bereich der Telefonie zählen hierzu Formen des Betruges (Enkeltrick), der Beleidigung und Bedrohung. Insbesondere einmalige oder sehr seltene Anrufe sind ohne eine Verkehrsdatenabfrage nicht wirksam zu untersuchen.

Im Bereich der Datennetze sind vor allem Delikte im Kontext des “Hackings” relevant, insbesondere das Ausspähen von Daten durch bösartige Software (*keylogger*) oder gefälschte Webseiten (*phishing*).

Wesentlich bei der Verfolgung dieser Straftaten ist die Zuordnung einer IP-Adresse zu einem Anschlussinhaber. Eine entsprechende Verkehrsdatenabfrage ist zur Verfolgung solcher Straftaten erforderlich und geeignet.

Langwierige und größere Ermittlungen, etwa im Bereich der organisierten Kriminalität, des internationalen Terrorismus oder der Wirtschaftskriminalität, die eine längerfristige Speicherung von Verkehrsdaten motivieren könnten, machen nicht so viele Fälle der Rechtswirklichkeit aus[27]. Bei diesen Verfahren gibt es jedoch auch vielfältige weitere Ermittlungsansätze, wie etwa die Verfolgung von Geldflüssen oder das Abhören von Telefongesprächen, die genutzt werden können.

Im Bereich der Wirtschaftskriminalität existiert eine Tendenz, Einbrüche in Datennetze von Firmen nicht oder erst verspätet zur Anzeige zu bringen. Unternehmen ermitteln zunächst intern und versuchen den verursachten Schaden einzuschätzen und zu begrenzen. Sie verzichten auf eine sofortige Anzeige, um nicht die Kontrolle über das Ermittlungsverfahren zu verlieren, insbesondere aus Rücksicht auf den Ansehensverlust, den ein solcher Vorgang in der Öffentlichkeit verursachen könnte. Eine Anzeige wird häufig nur als letztes Mittel gesehen, wenn etwa Schäden sich als schwerwiegend herausstellen oder interne Ermittlungen an Grenzen stoßen. In diesen Fällen ist eine längerfristige Speicherung von Verkehrsdaten von Nutzen.

Die Verfolgung des Austauschs urheberrechtlich geschützter Dateien (Softwarepiraterie) hat sich in der Vergangenheit in den Bereich des Zivilrechts verlagert. Auch der Handel mit illegalen Inhalten (etwa Kinderpornographie) spielt in der Rechtswirklichkeit eine untergeordnete Rolle.

[24] Albrecht/Grafe/Kilchling S. 406.
[25] Albrecht/Grafe/Kilchling S. 412.
[26] Albrecht/Grafe/Kilchling S.407f.
[27] Albrecht/Grafe/Kilchling S. 409.

6 Zusammenfassende Diskussion des § 113a TKG

6.1 Verkehrsdaten vs. Inhaltsdaten

Die Unterscheidung zwischen Inhaltsdaten und Verkehrsdaten ist, wie in den Abschnitten 3.1 und 3.2 beschrieben, nicht nur rechtlich sondern auch technisch mit Schwierigkeiten verbunden.

Es ist zudem absehbar, dass über Verkehrsdaten in Zukunft sehr viel stärker auf Kommunikationsinhalte geschlossen werden kann als heute, insbesondere durch die Erstellung von Bewegungsprofilen in der Mobilkommunikation. Kritisch ist vor allem die dynamische IP-Adresse zu sehen. Eine dynamische IP-Adresse verrät nicht nur die Tatsache, *dass* kommuniziert wurde[28]. Sie läßt in Zukunft verstärkt auch Rückschlüsse über den aktuellen Aufenthaltsort zu. Eine dynamisch vergebenen IP-Adresse hat somit klare Bezüge zu einem konkreten Telekommunikationsvorgang. Eine Zuordnung von dynamischer IP-Adresse zum Anschlussinhaber sollte also mindestens dieselben Eingriffsschranken besitzen wie eine reine Verkehrsdatenabfrage.

6.2 Nutzen von Verkehrsdaten für die Praxis

Die Verkehrsdatenabfrage ist ein universelles, sehr breit eingesetztes Ermittlungsinstrument. In der Vergangenheit sind Verkehrsdatenabfragen jedoch zu einem überwiegenden Teil in Verfahren angewendet worden, die der mittleren Kriminalität zugerechnet werden (Geringfügigkeitseinstellungen, Geldstrafen, Bewährungsstrafen, etc.)[29].

Aus den oben ausgeführten Gründen erscheint es mir sinnvoll, Verkehrsdaten generell stärker als Inhaltsdaten zu bewerten. Eine Behandlung von Verkehrsdaten im Sinne von Inhaltsdaten würde zudem die Ermittlungsbehörden auch darin unterstützen, sich auf die Verfolgung von für die Gesellschaft wesentlich schädlicheren und schwereren Deliktsarten zu konzentrieren. Ansonsten folgt eher ein Verzetteln bei Ermittlungen in kleiner oder mittlerer Kriminalität mit dem Resultat einer Ablenkung und Verschwendung von Ressourcen.

Sinnvoll ist zusätzlich eine Stärkung der Ressourcen und der Expertise der Ermittlungsberhörden, um etwa weltweit operierende IT-Kriminelle zu verfolgen[30].

6.3 Offener Zugriff auf Verkehrsdaten

Insbesondere die Zuordnung von einer IP-Adresse zu einem Anschluss ist in vielen Bereichen für eine erfolgreiche Ermittlung geeignet und erforderlich. Der Zugriff durch die Ermittlungsbehörden ist angemessen, insbesondere, wenn eine Durchsuchung (beim Telekommunikationsbetreiber oder in einer Privatwohnung) vermieden werden kann.

Gerade weil sie eine Durchsuchung ersparen, erscheint es sinnvoll, Zugriffe auf Verkehrsdaten wie bei einer Durchsuchung prinzipiell auch offen zu gestalten. Bei verdecktem Zugriff sollten Benachrichtigungspflichten vorgesehen und umgesetzt werden. Die Umsetzung der Benachrichtigung ist offenbar ein erheblicher Mangel in der aktuellen Rechtswirklichkeit[31].

Besonders problematisch ist in diesem Zusammenhang die Verwendung der so genannten stillen SMS. Das Versenden derartiger SMS durch die Polizei mit anschliessender Abfrage der Standortdaten ist eine gebräuchliche Methode zur Ortung von Straftätern. Die Ermächtigungsgrundlage für dieses Vorgehen ist vollkommen unklar.

[28] Seitz S. 100.
[29] Albrecht/Grafe/Kilchling S. 407.
[30] Holz/Engelberth/Freiling; Franklin et al.
[31] Albrecht/Grafe/Kilchling S. 411.

6.4 Kostenersatz bei Vorratsdatenspeicherung

Es erscheint sinnvoll, Datenspeicherung auf Vorrat mit einer Regelung zum Kostenersatz für Telekommunikationsanbieter zu flankieren. Wie die Ausführungen in Abschnitt 4.7 zeigen, sind die Kosten gerade für kleinere Telekommunikationsanbieter eklatant hoch. Sinnvoll wäre ein Kostenersatz auf Basis einer einzelnen Anfrage.

Danksagungen

Für hilfreiche Kommentare zu diesem Text bedanke ich mich bei Markus Engelberth, Thomas Fetzer, Jan Göbel, Dennis Heinson, Thorsten Holz und Philipp Trinius.

Literatur

Albrecht, Hans-Jörg/Grafe, Adina/Kilchling, Michael: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Freiburg i.Br., Februar 2008 – Forschungsbericht im Auftrag des Bundesministeriums der Justiz

Bär, Wolfgang: Handbuch zur EDV-Beweissicherung im Strafverfahren. Richard Boorberg Verlag, 2007

Enck, William et al.: Exploiting open functionality in SMS-capable cellular networks. In **Atluri, Vijay/Meadows, Catherine/Juels, Ari (Hrsg.):** Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005, Alexandria, VA, USA, November 7-11, 2005. ACM, 2005, 393–404

Engel, Tobias: SMS & all its features. Vortrag auf dem CCCongress, Dezember 2001, `http://berlin.ccc.de/ tobias/smsfeatures/`

Fox, Dirk: Der IMSI-Catcher. Datenschutz und Datensicherheit, 26 2002 Nr. 4, 212–215

Franklin, Jason et al.: An Inquiry Into the Nature and Causes of the Wealth of Internet Miscreants. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07). Alexandria, Virginia, USA, 2007, 375–388

Holz, Thorsten/Engelberth, Markus/Freiling, Felix C.: Learning more about the Underground Economy: A Case-Study of Keyloggers and Dropzones. Mannheim, 2008 (TR-2008-006). – Technischer Bericht

IANA: Protocol Numbers. `http://www.iana.org/assignments/protocol-numbers/`

Mulliner, Collin/Vigna, Giovanni: Vulnerability Analysis of MMS User Agents. In 22nd Annual Computer Security Applications Conference (ACSAC). IEEE Computer Society, 2006, 77–88

Seitz, Nicolai: Strafverfolgungsmaßnahmen im Internet. Carl Heymanns Verlag, 2004

Walke, Bernhard: Mobilfunknetze und ihre Protokolle 1. Grundlagen, GSM, UMTS und andere zellulare Mobilfunknetze. 3. Auflage. Teubner, 2001

A Bezüge des Artikels zu den Fragen aus dem Fragenkatalog

Es folgen Verweise von den Fragen aus dem Fragenkatalog zu relevanten Abschnitten im Text. Es sind nur diejenigen Fragen aufgeführt, für die ich mich sachkundig fühlte.

1. Welche Verkehrsdaten fallen im Rahmen der Telekommunikation an, werden durch § 113a TKG nicht erfasst?

   Siehe Abschnitt 4, insbesondere Abschnitt 4.2.

3. Auf welche Weise wird die Trennung der allein nach § 113a TKG gespeicherten Verkehrsdaten von anderen Verkehrsdaten gewährleistet?

   Siehe Abschnitt 4.6.

4. § 113a Abs. 2 S. 1 Nr. 4c TKG schreibt für mobile Telefondienste die Speicherung der Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen vor.

   – Lassen sich auch aus anderen nach § 113a TKG zu speichernden Daten Rückschlüsse auf das Bewegungsverhalten der Nutzer mobiler Telekommunikationsdienste ziehen?

     Ja. Siehe Abschnitt 3.2.3.

   – Werden im Rahmen des LKW-Maut-Systems durch den Datenaustausch zwischen der im LKW installierten Onboard-Unit und TollCollect Verkehrsdaten erzeugt, die nach § 113a TKG zu speichern sind? Um welche Daten handelt es sich?

     Siehe Abschnitt 2.5.

   – Müssen in der Praxis, etwa aus technischen Gründen, die Standortdaten von Mobiltelefonen auch im Stand-by-Betrieb gespeichert werden?

     Ja. Siehe Abschnitt 2.4.1.

   – Lassen sich durch den Einsatz stiller SMS oder Stealth-SMS gezielt speicherungspflichtige Verkehrsdaten erzeugen? Wird von dieser Möglichkeit in der Praxis der Strafverfolgungs- und Gefahrabwehrbehörden sowie der Nachrichtendienste Gebrauch gemacht? Auf welcher Grundlage?

     Siehe Abschnitte 2.4.3, 4.4 und 6.3.

6. Welche nach § 113a TKG zu speichernden Verkehrsdaten fallen bei einem Internetzugang über so genannte Hot Spots an? Inwiefern erfassen sie zuordenbare Daten einzelner Nutzer, die über den Hot Spot Zugang zu Internet nehmen? Ist dies unterschiedlich zu beantworten je nachdem, ob der Internetzugang über einen offenen WLAN-Anschluss oder kommerzielle WLAN-Dienste erfolgte?

   Siehe Abschnitt 2.3.

9. Welche mittels Telekommunikation zu verwirklichenden Straftatbestände oder typische Fallgruppen solcher Straftatbestände laufen ohne Rückgriff auf die nach § 113a TKG zu speichernden Daten im Wesentlichen leer?

   Siehe Abschnitt 5.2.3.

11. Welche Maßstäbe werden in der Praxis an die “im Bereich der Telekommunikation erforderliche sorgfalt” im Sinne von § 113a Abs. 10 Satz 1 TKG angelegt? Welche möglichen Anforderungen werden darüber hinaus diskutiert?

    Siehe Abschnitt 4.6.

12. Nach § 113a Abs. 10 Satz 2 TKG hat der zur Speicherung Verpflichtete im Rahmen der im Bereich der Telekommunikation zu beachtenden erforderlichen Sorgfalt durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den nach § 113a TKG gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.

    – Welche technischen und organisatorischen Maßnahmen kommen insoweit in Betracht? Inwieweit sind diese Maßnahmen auf eine regelmäßige Überprüfung verwiesen und welche Vorkehrungen werden diesbezüglich getroffen? Welche Konzepte werden insoweit diskutiert, worin liegen ihre Vor- und Nachteile?

      Siehe Abschnitte 4.6 und 4.7.

    – Wie sicher lässt sich mit solchen Maßnahmen ein missbräuchlicher oder unbefugter Zugriff verhindern?

      Siehe Abschnitt 4.6.

13. Welche Instrumente (z.B. Kennzeichnungs-, Löschungs- und Auskunftspflichten, Richtervorbehalte, Benachrichtigungspflichten, die eine ergänzende nachträgliche Gerichtskontrolle gewährleisten, oder — eventuell auch immaterielle — Schadensersatzansprüche bei rechtswidrigem Datenzugriff) werden zur Einhegung und rechtsstaatlichen Kontrolle der Nutzung der nach § 113a TKG zu speichernden Daten diskutiert? Worin liegen ihre Vor- und Nachteile?

    Siehe Abschnitt 6.