jus novum **Band 19**

Dirk Lageveen

Telekommunikationsüberwachung im Internet

IP-Adressen in der strategischen Erfassung gemäß Artikel-10 Gesetz

§

Diplomica Verlag

Lageveen, Dirk: Telekommunikationsüberwachung im Internet: IP-Adressen in der strategischen Erfassung gemäß Artikel-10 Gesetz, Hamburg, Diplomica Verlag

ISBN: 978-3-8428-0468-5

Bibliographische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ARPA	Advanced Project Research Agency
AS	Autonomous System
ASN	Autonomous System Number
BND	Bundesnachrichtendienst
CIA	Central Intelligence Agency
DNS	Domain Name System
DPI	Deep Packet Inspection
TELEKOM	Deutsche Telekom AG
DVB	Digital Video Broadcasting
EGP	Exterior Gateway Protocol
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IGP	Interior Gateway Protocol
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPTO	Information Processing Techniques Office
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
LIR	Local Internet Registry
MCC	Mobile Country Code
MIT	Massachusetts Institute of Technology
NGN	Next Generation Networks
OCR	Optical Character Recognition
PDH	Plesiochrone Digitale Hirarchie
POP3	Post Office Protocol Version 3
POTS	Plain Old Telephone System
PSTN	Public Switched Telephone Network
RIR	Regional Internet Registry
RTP	Real Time Protocol
SAGE	Semi Automatic Ground Environment
SDH	Synchrone Digitale Hirarchie
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TLD	Top Level Domain
UCLA	University of California Los Angeles
UDP	User Datagram Protocol

VoIP	Voice over Internet Protocol
WWW	World Wide Web

Teil 1: Einleitung

Das Internet als weltumspannendes Kommunikationsnetz hat in den letzten Jahren stark an Bedeutung gewonnen. Eine ständig größer werdende Anzahl von Menschen hat Zugang zu diesem Medium und nutzt es in immer stärkerem Maße für private und geschäftliche Kommunikation. Auch Regierungen, Behörden und andere staatliche Organisationen haben die Vorteile des Netzes erkannt und bieten bereits heute unterschiedliche Dienste, wie z.B. die elektronische Steuererklärung (ELSTER[1]), über das Internet an. Politiker verwenden die Reichweite des Netzes, um eine große Anzahl von Bürgern und dabei vor allem junge Menschen erreichen zu können. Selbst die Bundeskanzlerin Fr. Dr. Merkel ist durch ihren regelmäßigen Podcast[2] „Die Kanzlerin – direkt“ im Internet präsent.

Durch die steigende Popularität des Netzes ist die Zahl der verfügbaren Kommunikationsdienste um ein Vielfaches angewachsen. Waren zu Beginn der neunziger Jahre noch die festnetzgebundene Telefonie für die Sprachkommunikation und das Telefax für die Übermittlung von gedruckten Zeichen und Bildern das Maß aller Dinge, existieren heute vielfältige Methoden, um Sprache oder Daten über das Internet rund um den Globus zu versenden.

Mit der Einführung des Mobiltelefons in den Massenmarkt Mitte der neunziger Jahre und der breiten Nutzung des Internet durch alle Bevölkerungsschichten ab Beginn des neuen Jahrtausends hat sich das Kommunikationsverhalten der Menschen in allen Nationen der Welt grundlegend verändert. Stetige Kommunikation ist nicht mehr nur exklusiv Unternehmen und Menschen vorbehalten, die sich entsprechende Endgeräte und Dienste leisten können, sondern sie ist massentauglich und zumindest in den Industrienationen beinahe für jeden erschwinglich.

Dieser Wandel auf dem Kommunikationsmarkt und die daraus resultierende Erreichbarkeit einer enormen Anzahl von Menschen weltweit, machte das Netz gleichfalls attraktiv für staatsfeindliche, kriminelle oder terroristische Organisationen. Das Internet ermöglicht es ihnen, verdeckt für die Öffentlichkeit ihre Interessen zu verfolgen und oft außerhalb der Zugriffsmöglichkeiten der Staatsgewalt rechtswidrige

---

1 siehe auch https://www.elster.de

2 Ein Mittel zur Massenkommunikation im Internet, dass sich in der Regel aus Audio- und Videodateien zusammensetzt und durch einen Nutzer abboniert werden kann.

Aktionen durchzuführen. Dabei ist es ihnen auf Grund der Struktur und der internationalen Ausrichtung des Netzes möglich, ihre Wege des Austausches von Nachrichten zu verschleiern und die Grauzone des Internet für ihre Zwecke zu missbrauchen. Als Beispiele seien hier nur die Verbreitung von rechtsextremistischem Gedankengut, kinderpornographischen Bildern oder terroristischen Hetzschriften genannt; im Bereich des organisierten Verbrechens sind Drogenschmuggel, Proliferation[3], Menschenhandel und Geldwäsche die Tatbestände mit internationaler Bedeutung.

Seit den Anschlägen auf das World Trade Center, am 11. September 2001 in New York steht eine weitere Gruppe im Fokus der Öffentlichkeit, die ebenfalls von dem oben genannten Fortschritt der Nachrichtenübertragung profitiert hat. Gruppierungen des internationalen Terrorismus, wie z.B. Al-Qaida oder Ansar al-Islam, nutzen moderne Kommunikationsmittel unter anderem zur Koordinierung ihrer Aktivitäten und Verbreitung ihrer Ideologie.

Diese Entwicklungen kann der Gesetzgeber nicht hinnehmen und muss ihnen wirkungsvoll entgegentreten. Dazu ist es notwendig, die Kommunikation der genannten Organisationen zu überwachen. Der Konflikt, in dem er sich dabei befindet, berührt grundlegende, in der Verfassung verankerte Schutzrechte, denn der Schutz der privaten Kommunikation ist als Grundrecht in Art. 10 Abs. 1 GG garantiert. Der Staat ist aber durch Art. 1 Abs. 1 GG ebenso verpflichtet, für die Sicherheit seiner Staatsbürger zu sorgen. Um dieser Verpflichtung nachzukommen, muss er auch solchen Bedrohungen entgegenstehen, die erst durch neue Technologien entstehen[4]. Um diesen Konflikt zu lösen, wurde durch den Gesetzgeber eine Ausnahmeregelung in Art. 10 GG verankert, die eine Beschränkung des grundrechtlichen Schutzes der Bürger zulässt. Die gesetzlichen Bestimmungen zu dieser Beschränkung finden sich im "Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses", auch als Artikel-10 Gesetz - G10 bezeichnet.

Im Rahmen dieser Studie wird die Eignung der Adressen des Internet-Protokolls als formaler Suchbegriff im Rahmen der Anordnung einer strategischen Erfassung des Bundesnachrichtendienstes im Sinne des § 1 Abs. 1 Nr. 2 G10 i.V.m. § 5 G10 untersucht.

---

[3] Verbreitung von Massenvernichtungswaffen
[4] Gysy, APuZ 44/2004, 14, 16

Dabei werden die in den folgenden Kapiteln verwendeten technischen Begriffe und Verfahren für den juristisch geschulten Leser aufbereitet, an praktischen Beispielen erläutert und im Anschluss die gesetzlichen Grundlagen wie der Art. 10 GG und das G10 in ihrer geschichtlichen Entwicklung dargestellt und auf ihren Wirkungsbereich und ihre Grenzen hin untersucht.

Um die Eignung einer IP-Adresse als formalen Suchbegriff zu beurteilen wird geprüft, in welcher Weise bereits eingeführte technische Verfahren und die darin verwendeten Zeichenfolgen zur Adressierung, wie z.B. die Rufnummer eines Telekommunikationsanschlusses im öffentlichen Telefonnetz, sich als formaler Suchbegriff i.S.d. G10 eignen.

Im Folgenden ist dann die Transformation der gewonnenen Erkenntnisse auf die Adressen des Internet-Protokolls notwendig und es wird untersucht, ob diese aus juristischer Sicht ähnlich oder gleich zu behandeln sind wie die bereits technisch bekannten Verfahren oder ob es notwendig scheint, die bestehenden Vorschriften für die neue Technologie zu erweitern.
Anschließend werden die Methoden zur Adressierung einzelner Teilnehmer für die Verfahren Voice over Internet Protocols (VoIP), d.h. Sprachkommunikation über die technische Infrastruktur des Internet und die elektronische Post mit der klassischen E-Mail und den neuen Diensten De-Mail und E-Postbrief auf Grundlage der gewonnen Erkenntnisse bewertet.

Teil 2: Grundlagen

A Begriffsdefinition

Um dem Leser zu ermöglichen, im Folgenden eine korrekte rechtliche Einordnung der technischen Vorgänge durchführen zu können, ist eine einheitliche Begriffsdefinition erforderlich. Auf Grund ihrer direkten Verknüpfung mit dem G10 wurden die folgenden Definitionen dem Telekommunikationsgesetz (TKG)[5] und der "Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung - TKÜV)"[6] entnommen.

I. Teilnehmer

Ein Teilnehmer ist gem. § 3 Nr. 20 TKG jede natürliche oder juristische Person, die mit einem Anbieter von Telekommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat.

II. Nutzer

Ein Nutzer ist gem. § 3 Nr. 14 TKG jede natürliche Person, die einen Telekommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne notwendigerweise Teilnehmer zu sein.

III. Teilnehmeranschluss

Der Teilnehmeranschluss ist gem. § 3 Nr. 21 TKG die physische Verbindung, mit dem der Netzabschlusspunkt in den Räumlichkeiten des Teilnehmers mit den Hauptverteilerknoten oder mit einer gleichwertigen Einrichtung in festen öffentlichen Telefonnetzen bezeichnet, verbunden wird.

---

5 Telekommunikationsgesetz vom 22. Juni 2004, BGBl. I 1190, das zuletzt durch Artikel 2 des Gesetzes vom 14. August 2009, BGBl. I 2821, geändert worden ist

6 Telekommunikations-Überwachungsverordnung vom 3. November 2005, BGBl. I S. 3136, die zuletzt durch Artikel 4 des Gesetzes vom 25. Dezember 2008, BGBl. I 3083, geändert worden ist

IV. Endgerät

Als Endgerät wird gem. § 2 Nr. 6 TKÜV die technische Einrichtung bezeichnet, mittels derer ein Nutzer einen Telekommunikationsanschluss zur Abwicklung seiner Telekommunikation nutzt.

V. Telekommunikationsnetz

Ein Telekommunikationsnetz ist gem. § 3 Nr. 27 TKG die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen und mobilen terrestrischen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information.

VI. Telekommunikationsdienst

Telekommunikationsdienste sind gem. § 3 Nr. 20 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen.

VII. Telekommunikationsanlage

Eine Telekommunikationsanlage ist gem. § 3 Nr. 23 TKG eine technische Einrichtung oder ein System, das als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren kann.

VIII. Telekommunikationsanschluss

Der Telekommunikationsanschluss ist gem. § 2 Nr. 10 TKÜV der durch eine Rufnummer oder andere Adressierungsangabe eindeutig bezeichnete Zugang zu einer Telekommunikationsanlage, der es einem Nutzer ermöglicht Telekommunikationsdienste mittels eines geeigneten Endgerätes zu nutzen.

IX. Kommunikationsvorgang

Als Kommunikationsvorgang wird die Übertragung von Informationen zwischen zwei Nutzern bezeichnet. Dieser Vorgang hat dabei einen zu definierenden Start- und Endzeitpunkt, der von der Art und Weise der Kommunikation abhängt und für die Beurteilung der zeitlichen Schutzwirkung des Art. 10 GG maßgeblich ist.

X. Bestandsdaten

Bestandsdaten sind gem. § 3 Nr. 3 TKG die Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Charakteristisch für Bestandsdaten ist, dass sie in keinem konkreten Bezug zu einem Telekommunikationsvorgang stehen[7]. § 111 Abs. 1 S. 1 TKG listet exemplarisch als Bestandsdaten die Rufnummern, den Namen und die Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns und evtl. des Vertragsendes, bei natürlichen Personen deren Geburtsdatum, sowie bei Festnetzanschlüssen auch die Anschrift des Anschlusses auf[8].

Als Bestandsdaten können alle das Vertragsverhältnis betreffenden Daten gesehen werden. Diese sind nicht nur auf den Zeitpunkt des Vertragsschlusses beschränkt, sondern umfassen sowohl die reibungslose Durchführung eines laufenden Vertragsverhältnisses als auch dessen Beendigung. Dazu zählen neben den bereits genannten Daten auch die technischen Merkmale eines Telekommunikationsanschlusses, wie z. B. der Information, dass es sich um einen Digital Subscriber Line (DSL)-Anschluss handelt. Für die Abwicklung des Vertragsverhältnisses benötigt der Diensteanbieter zusätzlich die rechnungsrelevanten Daten wie Rechnungsanschrift und Bankverbindung des Teilnehmers[9].

XI. Verkehrsdaten

Als Verkehrsdaten werden die näheren Umstände des Fernmeldeverhältnisses bezeichnet. Es sind gem. § 3 Nr. 30 TKG Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden und dem Anbieter einen näheren Aufschluss über die näheren Umstände eines Kommunikati-

---

7 Sankol, MMR 6/2006, 361, 363
8 Köcher/Kaufmann, DuD 30/2006, 360, 361
9 Geppert/Piepenbrock/Schütz/Schuster: Beck'scher TKG-Kommentar, 3.Auflage 2006, Rd.Nr. 13

onsvorgangs liefern sollen[10]. Gem. § 96 Abs. 1 TKG darf der Diensteanbieter als Verkehrsdaten speziell die Nummer oder Kennung der beteiligten Anschlüsse oder des Endgerätes, personenbezogene Berechtigungskennungen, den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und unter bestimmten Voraussetzungen auch die übermittelten Datenmengen der vom Nutzer in Anspruch genommenen Telekommunikationsdienste erheben und verwenden. Bei mobilen Anwendungen dürfen zusätzlich noch die Standortdaten hinzugefügt werden. Aber auch sonstige, zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten, können gem. § 96 Abs. 1 Nr. 5 TKG durch den Anbieter genutzt werden. Verkehrsdaten umfassen somit die Teilnehmer eines Kommunikationsvorgangs, die Tatsache der Kommunikation und zusätzlich o.g. technische Parameter[11].

XII. Standortdaten

Standortdaten sind gem. § 3 Nr. 19 TKG Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben.
Hier sei als Beispiel die Telekommunikation über den Satellitentelefondienst Thuraya[12] genannt. Jedes Endgerät, das in diesem Netz kommuniziert, verfügt über einen eingebauten Empfänger für das Global Positioning System[13] (GPS). Mit diesem kann der Nutzer jederzeit in Echtzeit seine aktuelle Position bestimmen, zusätzlich überträgt das System jedoch auch diese Standortdaten über das Signalisierungsprotokoll zum Telekommunikationsanbieter. So kann auch dieser jederzeit die aktuelle geographische Position des Nutzers feststellen. Aber auch immer mehr Mobiltelefone verfügen über ein solches Modul.

XIII. Inhaltsdaten

Die Inhaltsdaten repräsentieren den Kommunikationsinhalt, d.h. alles was die Kommunikation, also den Austausch von Informationen, zwischen den Nutzern

---

10 Köcher/Kaufmann, DuD 30/2006, 360, 362
11 Gusy in von Mangoldt/Klein/Stark *Kommentar zum Grundgesetz*, 5. Auflage, Art. 10 GG, S. 987, Rd.Nr. 45
12 http://www.thuraya.com
13 Ein satellitengestütztes System der USA zur Standortbestimmung. Die auf stationären Umlaufbahnen platzierten Satelliten senden Signale aus, die durch die Empfangsgeräte auf der Erde empfangen und mit mathematischen Verfahren korreliert werden. So ist eine metergenaue Standortbestimmung möglich.

ausmacht. Dabei handelt es sich in den modernen öffentlichen Telefonnetzen und im Internet immer um digitale Daten in binärer Form. Diese können sowohl menschliche Sprache als auch Texte oder jede andere Form multimedialer[14] Dokumente als Kommunikation zwischen natürlichen oder juristischen Personen enthalten.
Heute ist es üblich, dass auch Rundfunkdaten im Internet übertragen werden. Als Beispiel sei hier nur das Fernsehangebot der Deutschen Telekom AG (TELEKOM) über das Internet-Protokoll genannt. Die hier übertragenen Inhalte richten sich an die breite Öffentlichkeit und sind damit dem Rundfunk zuzuordnen[15]. Durch die Konvergenz der modernen Übertragungsnetze und dem Aufbau neuer Next Generation Networks (NGN)[16], paketvermittelte Netze die jegliche Art von Kommunikation und Daten, unabhängig vom Inhalt, transportieren, wird es immer schwieriger, ohne eine Bewertung die Inhaltsdaten einer Strecke in Individualkommunikation und Rundfunk zu trennen.

B Klassische Telefonie als Grundlage der Datenübertragung

Um die spätere Betrachtung der Übertragbarkeit von Vorschriften der klassischen Telefonie auf die Internettelefonie zu ermöglichen ist es notwendig, einen kurzen Überblick über die Geschichte und die Technologie herkömmlicher Telefonnetze zu geben.

I. Geschichte der Telefonie

Die klassische analoge Telefonie, auch *Plain Old Telephone Service* (POTS) genannt, begann ihren Siegeszug nach der Erfindung des Fernsprechapparates durch *Graham Bell* im Jahre 1876. Der große Bedarf der Menschen nach Kommunikation über weite Strecken führte nach dieser Innovation sehr schnell zum Aufbau eines weltumspannenden leitungsgebundenen Telefonnetzes.
Bereits 100 Jahre später, zu Beginn der 70er Jahre des letzten Jahrhunderts, wurden Strategien zur Digitalisierung des POTS entworfen die mit der Einführung des *Integrated Services Digital Network* (ISDN) im Jahre 1989 durch die Deutsche Bundespost erfolgreich umgesetzt wurden. Dieses digitale Netz wird heute auch als

---

[14] Gemäß Wikipedia bezeichnet der Begriff Multimedia Inhalte und Werke, die aus mehreren, meist digitalen Medien bestehen, z.B. Text, Fotografie, Grafik, Animation, Audio und Video.
[15] Gusy in von Mangoldt/Klein/Stark *Kommentar zum Grundgesetz*, 5. Auflage, Art. 10 GG, S. 986, Rd.Nr. 42
[16] Nachfolger der heutigen Sprach- und Datentransportnetze

Public Switched Telephone Network (PSTN) bezeichnet und entspricht dem öffentlichen Telefonnetz.

II. Technik

Die fortschreitende Industrialisierung und die Einführung der Digitaltechnik machten natürlich auch vor der Telefonie nicht halt. Wurde in den ursprünglichen analogen Netzen noch für jedes Gespräch eine separate Leitung benötigt, mussten mit der ständig steigenden Zahl von Telekommunikationsteilnehmern neue Verfahren gefunden werden, da die Menge an Verbindungen die Zahl der verfügbaren Wege deutlich überstiegen hat.

a) Bündelung über Multiplexverfahren

Im Zuge der Digitalisierung der Netze wurden daher technische Möglichkeiten geschaffen, die Gespräche mehrerer Teilnehmer über eine physikalische Leitung zu übertragen, sozusagen die Gespräche zu bündeln. Diese Bündelung wird technisch über ein sogenanntes Multiplexverfahren realisiert. Die gängigste Variante in den Weitverkehrsnetzen ist der Zeitmultiplex, in der englischen Bezeichnung *Time Division Multiple Access* (TDMA). Dabei werden verschiedene Übertragungen, egal ob Sprache oder Daten, in zeitlich begrenzte Abschnitte aufgeteilt und nach einem festgelegten Muster auf einer Leitung übertragen. Durch das vorgegebene Muster kann jederzeit einer der Kanäle aus dem Bündel extrahiert werden. Auch ist es möglich, mehrere Übertragungsbündel mit kleiner Kapazität zu einem größeren Bündel zusammenzufassen oder aber auch große Bündel wieder in mehrere kleinere aufzuteilen. Auf diesem Weg können Übertragungen aus mehreren Städten zusammengefasst und auf wenigen Datenautobahnen über weite Strecken transportiert werden. Am Zielort werden dann die Bündel nach und nach zerteilt bis nur noch der individuelle Kanal des Teilnehmers übrigbleibt. Zwei der gebräuchlichsten Verfahren sollen im Folgenden kurz erläutert werden.

(aa) Plesiochrone Digitale Hierarchie (PDH)

Das PDH Verfahren ist ein asynchrones Verfahren, d.h. die Daten werden ohne zentralen Zeitgeber übertragen. Es wird häufig auf den Zubringern von der Ortsvermittlung zu den großen Datenautobahnen verwendet.

Bis zur Ortsvermittlung wird jeder individuelle Teilnehmeranschluss über Kupferleitungen, der sogenannten „letzten Meile“, geführt. Diese Infrastruktur wurde nach dem Krieg durch die Bundespost aufgebaut und nach der Privatisierung der Post an die Telekom übergeben. Nur wenige Wettbewerber auf dem Telekommunikationsmarkt haben bisher in eine eigene Hausanschluss-Infrastruktur investiert und mieten daher diese Zugänge von der Telekom.
In der Ortsvermittlung sind die individuellen Leitungen mit einer Vermittlungsanlage verbunden. In dieser Anlage werden die einzelnen Verbindungen über das PDH Verfahren auf größere Telekommunikationsstrecken gebündelt, in der Fachsprache gemultiplext. Eine Leitung der untersten PDH Hierarchiestufe mit einer Bandbreite von 2 MBit/s, auch als E1 bezeichnet, kann dabei 30 Telefongespräche gleichzeitig führen. PDH wird üblicherweise bis zu einer Bandbreite von 34 MBit/s eingesetzt, mit einer solchen E3 genannten Leitung können immerhin schon 480 Nutzkanäle gleichzeitig übertragen werden. Ein E3 entspricht dabei einem Bündel aus 16 E1 Leitungen.

(bb) Synchrone Digitale Hierarchie (SDH)

Auf den Datenautobahnen zwischen den großen nationalen und internationalen Vermittlungsknoten wird das SDH Verfahren eingesetzt. Hauptsächlicher Unterschied zu PDH ist die synchrone Übertragung, d.h. alle Übertragungsstrecken sind im Idealfall synchron, d.h. sie laufen im gleichen Takt. Somit können einzelne Übertragungskanäle oder ganze Bündel an den Netzknoten ohne Aufwand einfach verteilt und in andere Bündel eingefügt werden. Durch die Zeitsynchronität ist es an jedem Knoten möglich ohne technischen Aufwand möglich, eine individuelle Verbindung zu identifizieren, auszugeben und aufzuzeichnen.
SDH Netze sind, wie der Name schon besagt, hierarchisch aufgeteilt. Die unterste Hierarchiestufe ist das *Synchronous Transport Module* - 0 (STM-0). Auf Grund der Kompatibilität zu PDH und der daraus resultierenden Weiterführung der Hierarchie hat sich in der Technik aber STM-1 mit einer Datenrate von 155 MBit/s als unterste Ebene durchgesetzt. Wie sich leicht erkennen lässt, können hier vier E3 Leitungen gebündelt und bereits 1920 Nutzkanäle parallel übertragen werden. Die weiteren in aktuellen Netzen genutzten Hierarchiestufen sind STM-4 (620 MBit/s), STM-16 (2,5 GBit/s), STM-64 (10 GBit/s) und STM-256 (40 GBit/s). Letztgenannte kann 491.520 Nutzkanäle für Sprache oder Daten gleichzeitig transportieren oder aber

einen Spielfilm von einer handelsüblichen DVD mit ca. 8 GByte Datenvolumen in 2 Sekunden übertragen.

b) Vermittlung

In den Anfängen der analogen Telefonnetze musste durch den Teilnehmer zuerst die Vermittlung angerufen werden. Hier wurde man durch eine freundliche Person mit dem gewünschten Gesprächspartner verbunden. Dies geschah durch die physische Herstellung der Verbindung auf großen Schalttafeln. In Deutschland wurden mit Fortschreiten der Technik in den 1960er Jahren die Damen und Herren vom Amt durch automatische analoge Vermittlungsanlagen abgelöst, die Verbindungen mit Hilfe elektrischer und mechanischer Einrichtungen automatisch herstellten konnten
Ab Mitte der 1990er Jahre wurde dann die analoge Vermittlungstechnik auf digitale Verfahren umgestellt. Hier wird die Rufnummer als digitale Information übertragen die in den Vermittlungsknoten elektronisch ausgewertet wird und die Anlage den Verbindungsweg schalten lässt.
In den heutigen Netzen erfolgt die Übertragung der für den Aufbau einer Übertragungsstrecke notwendigen Informationen in der Regel in einem separaten Signalisierungskanal. Dieser ist gesondert vom Übertragungskanal zu sehen, in dem die Inhaltsdaten übertragen werden. Technisch ist es durchaus möglich, dass Signalisierungsdaten und Inhaltsdaten unterschiedliche physikalische Leitungswege nehmen.
Für die Signalisierung in modernen Telekommunikationsnetzen wird häufig das Signalling Sytstem No. 7 (SS#7) [17] eingesetzt. Dieses Protokoll ermöglicht die gleichzeitige Übertragung von Signalisierungsinformationen für eine Vielzahl von Teilnehmern. Es ist außerdem in der Lage die Signalisierungsinformationen für mehrere Telekommunikationsbündel gleichzeitig zu übertragen.

Im Folgenden soll nun der Aufbau eines Gespräches zwischen Deutschland und Washington in den USA mit der Rufnummer 001412-123456 beispielhaft dargestellt werden.
Der Aufbau einer Verbindung beginnt mit dem Wählen der Rufnummer durch den Anrufenden. Die einzelnen Ziffern der Rufnummer werden z.B. bei ISDN über einen separaten Signalisierungskanal, den sogenannten D-Kanal, in die Ortsvermittlung übertragen. Hier wird die Rufnummer an das SS#7 Protokoll übergeben, das für den

[17] Signalling System No.7, entwickelt 1975 durch AT&T, standardisiert 1981 durch die ITU-T

weiteren Aufbau des Übertragungsweges auf der Weitverkehrsstrecke verantwortlich ist. In der Ortsvermittlung folgt die Einordnung als internationales Gespräch auf Grund der sogenannten Verkehrsausscheidungsziffern 00 zu Beginn der Rufnummer. Anschließend wird auf Grund der Landeskennziffer 1 ein Übertragungsweg zu dem internationalen Übergabepunkt mit der Verbindung zwischen Deutschland und den USA geschaltet. Diese wird in der Regel über ein internationales Weitverkehrskabel geführt. Im Vermittlungsknoten in den USA wird dann die 412 als Ortsvorwahl der Stadt Washington ausgewertet. Das System schaltet nun den Weg vom internationalen Vermittlungsknoten in den USA in die Hauptvermittlung der Stadt Washington. Dort wird nun die Rufnummer 123456 des Teilnehmers ausgewertet und eine Strecke zu der Ortsvermittlung geschaltet, an die der Angerufene angeschlossen ist. Diese Vermittlungsstelle verbindet nun den bisher geschalteten Weg mit dem Teilnehmeranschluss des Ziels und das Gespräch kann erfolgen.

In diesem Beispiel wird deutlich, dass für ein Telefongespräch sowohl ein Signalisierungsweg als auch einen Übertragungsweg notwendig ist. Der Signalisierungsweg transportiert Verkehrsdaten, also technische Informationen, die dem Aufbau und Betrieb der Verbindung dienen. Der Übertragungsweg transportiert den Inhalt des Gespräches, also die Inhaltsdaten. Eine Besonderheit heutiger Netze ist es, dass der Signalisierungsweg nicht zwangsläufig den gleichen Weg nutzen muss wie der Übertragungsweg.

C Die Geschichte des Internet

Der erfolgreiche Start des Satelliten *Sputnik* am 4. Oktober 1957 und die anschließend für die gesamte Welt hörbare Übertragung von rudimentären Signalen aus der Erdumlaufbahn, war für die Vereinigten Staaten von Amerika ein Schock. Die UdSSR[18] hatte den Wettlauf in das Weltall beweisbar gewonnen und nun befürchteten Politiker, Wissenschaftler und Militärs, dass die UdSSR einen uneinholbaren technologischen Vorsprung vor den USA erreichen könnte und in der Folge einen enormen Vorteil im kalten Krieg gewinnen würde.

[18] Union der Sozialistischen Sowjetrepubliken

Als Konsequenz aus dieser Erfahrung wurde die Advanced Project Research Agency (ARPA), als eine direkt dem Verteidigungsminister unterstellte Forschungseinrichtung, durch das amerikanische Department of Defense gegründet. Klares Ziel dieser Einrichtung war es, die amerikanische Führerschaft auf dem Gebiet der Hochtechnologie sicherzustellen und technologische Überraschungen, wie den Start des *Sputnik*, in Zukunft zu verhindern[19].

Eines der militärischen Projekte dieser Zeit war ein Frühwarnsystem gegen Bomberangriffe der Sowjetunion mit der Bezeichnung *Project LINCOLN*. Ziel des Projektes war es, ein System zu entwickeln, in dem Radardaten, Zielverfolgung und andere Parameter von Computern überwacht und gesteuert werden konnten. Dieses Konzept war für die damalige Zeit radikal und so noch nie verwirklicht worden. Als Weiterentwicklung sollten in einem Teilprojekt mit der Bezeichnung Semi Automatic Ground Environment (SAGE) 23 Überwachungszentren, in denen bis zu 50 Personen an Radarschirmen arbeiteten, mit je 2 Rechnern ausgerüstet werden, so dass sie mit Hilfe der Rechner in der Lage waren, 400 feindliche Flugzeuge gleichzeitig zu verfolgen. Ein völlig neuer Ansatz in diesem Entwurf sah vor, Informationen zwischen den Rechnern dieser Zentren über Telefonleitungen auszutauschen

Einer der Väter dieses Netzwerkes war *Joseph Carl Robnett Licklider*, beauftragt von der ARPA mit dem Aufbau des Information Processing Techniques Office (IPTO), einer Organisation, die sich mit dem Bereich "Command and Control" beschäftigen sollte. Licklider beschäftigte sich in seiner Funktion als Professor für experimentelle Psychologie am Massachusetts Institute of Technology (MIT) im Schwerpunkt mit der Interaktion von Mensch und Maschine. Seine Vision war es Echtzeitcomputer zu entwickeln, die mit dem Bediener interagieren, Bibliotheken für jedes nur erdenkliche Themengebiet enthalten und Text, Formeln, Grafiken oder jede andere Form von Informationen darstellen können. Der 1960 erschienene Artikel “Man-Computer Symbiosis[20]” legte den Grundstein für Forschungen, um diese Vision Realität werden zu lassen.

Es sollten noch weitere 7 Jahre vergehen, bis das erste Computernetzwerk zum Leben erwachen würde. Im Jahre 1967 beauftragte der 3. Direktor des IPTO, *Robert*

---

[19] Van Atta in DARPA: 50 Years of Bridging the Gap, 20, 20
[20] Licklider in IRE Transactions on Human Factors in Electronics

Taylor, den Wissenschaftler Larry Roberts mit dem Aufbau eines landesweiten Computernetzes zwischen einigen Standorten der ARPA. Dieser legte die folgenden 3 grundlegenden Eigenschaften der Architektur des Netzes fest, die auch heute noch die Basis des Internet bilden:

1. Ständige Verbindung aller Computer über feste Leitungen
2. Übertragung der Daten in Paketen anstatt als serieller Datenstrom
3. Das Netzwerk soll komplett dezentral entworfen werden, d.h. keine Steuerung und Kontrolle durch einen zentralen Rechner

Der erste Knoten des neuen ARPA-Netzes wurde am 2. September 1969 an der University of California, Los Angeles (UCLA) in Betrieb genommen.[21]
Dieser Tag gilt als die Geburtsstunde des Internet. 2 Monate später fand die erste Kommunikation mit einem Rechner im 500km entfernten Standfort statt. Die Zeit der bis dorthin nur autark arbeitenden Computer war damit vorüber. Das *Arpanet*, Mutter des heutigen Internet, war geboren.

D Transport von Informationen im Internet

Für die spätere Betrachtung der rechtlichen Zusammenhänge ist es notwendig, dem Leser die Grundlagen der vorgestellten Technologien an Hand von Beispielen verständlich zu erläutern.

I. Der Wandel von der Analog- zur Digitaltechnik

Das Internet ist ein Telekommunikationsnetz, das Informationen über Telekommunikationsanlagen mit Hilfe optischer oder elektrischer Signale überträgt. Die Informationen müssen dazu in ein maschinenlesbares Format gebracht werden. Das dafür verwendete Verfahren wird als Digitaltechnik bezeichnet. In der modernen Welt ist der Wandel von der Analog- hin zur Digitaltechnologie das bestimmende Thema. Als Beispiel sei hier nur der Wechsel der Fernsehlandschaft von der analogen Übertragung hin zu Digital Video Broadcasting (DVB), dem digitalen Standard für die Ausstrahlung eines Fernsehsignals, genannt. Im Folgenden soll kurz der Unterschied zwischen einem analogen und einem digitalen Signal dargestellt werden.

---

[21] Waldrop in DARPA: 50 Years of Bridging the Gap, 78, 83

Ein analoges Signal kann in einem definierten Bereich jeden beliebigen Zustand dieses Bereiches annehmen. Das ist vergleichbar mit einer klassischen Armbanduhr, die über einen Stunden- und einen Minutenzeiger verfügt. Beide Zeiger werden durch das Uhrwerk kontinuierlich über das Zifferblatt geführt. Der Minutenzeiger überquert dabei innerhalb einer Stunde den gesamten Bereich der Uhr. Zu jedem beliebig gemessenen Zeitpunkt innerhalb dieses Zeitraums befindet er sich an einem anderen Punkt auf dem Ziffernblatt, wobei die zurückgelegte Distanz bei kleineren Messzeiträumen ebenfalls immer kleiner wird.

Die moderne Digitaltechnik bedient sich elektronischer Schaltungen, die mit Hilfe elektrischer Energie Signale verarbeiten. Aber gerade der elektrische Strom kennt nur 2 Zustände. Strom fließt oder Strom fließt nicht. In der Digitaltechnik werden diese beiden Zustände mit 0 und 1 beschrieben. Eine beliebig hohe Anzahl von verschiedenen Zuständen, wie in der Analogtechnik, ist somit nicht darstellbar.
Jede Form eines analogen Signals muss daher mit verschiedenen Aneinanderreihungen von 0 und 1 beschrieben werden, um in einem digitalen System verarbeitet werden zu können. Diese Informationen werden nach dem Mathematiker *Claude Shannon* Binary Digits oder aber auch Bits genannt[22]. Das technische Verfahren zur Übersetzung des analogen Signals in eine digitale Version wird als Digitalisierung bezeichnet.

Damit bei der Telefonie die mit der Stimme moduliert Worte durch ein digitales System übertragen werden können, ist die Digitalisierung dieser Worte notwendig, denn die menschliche Stimme stellt ein analoges Signal dar. Dies ist leicht nachzuvollziehen, da ein Mensch innerhalb seines Fähigkeitsbereiches in der Lage ist, alle Tonlagen in feinster Abstufung hörbar zu machen. Nach der Umsetzung von Analog nach Digital besteht die gesprochene Nachricht aus einer Abfolge von Nullen und Einsen, die sich, je nach verwendeten technischen Verfahren, unterschiedlich darstellt und sich in dieser Form auf digitalen Speichermedien, wie z.B. einer Festplatte, speichern lässt.

Die einfachste Form der Übertragung dieser Daten ist, auf einer elektrischen Leitung mit einer vorgegebenen Taktfrequenz, den Strom entweder ein oder auszuschalten.

---

[22] Shannon, Bell System Technical Journal, Nr. 27, S. 379-423 und 623-656

"Strom an" bedeutet dabei 1, "Strom aus" bedeutet die Übertragung einer 0. Der Takt ist wichtig, da sonst auf der Gegenseite nicht klar wäre, welches Bit aus der Sequenz aktuell übertragen wird. Setzen wir einen Takt von 1 Information pro Sekunde voraus, dann wissen wir, dass nach 10 Sekunden die Information übertragen wird, die an der 11ten Stelle des digitalisierten Signals steht.

Auf der Empfangsseite existiert ebenfalls ein Übersetzer, der die empfangenen digitalen Daten wieder in eine Folge von analogen Tönen umwandelt. Diese können dann über einen Lautsprecher für das menschliche Ohr hörbar gemacht werden.

Mit dem gleichen Verfahren können Texte, Bilder und andere Ausdrucksformen menschlichen Schaffens in digitale Signale übersetzt und übertragen werden. Auf elektrischen Leitungen geschieht dies mit dem bereits beschriebenen Verfahren "Strom an" und "Strom aus". Auf optischen Leitungen wird, vereinfacht gesprochen, mit "Licht an" und "Licht aus" gearbeitet. Eine Umwandlung von einer elektrischen auf eine optische Übertragung und umgekehrt ist durch spezielle elektro-optische Wandler möglich.

II. Leitungs- und paketvermittelte Übertragung

Die Übertragung von Sprache oder Daten kann mit zwei unterschiedlichen technischen Methoden erfolgen. Seit der Erfindung der Telegraphie ist die leitungsvermittelte Übertragung das vorherrschende Verfahren. Erst mit dem Aufkommen des Internets wurde die paketvermittelte Übertragung eingeführt.
Der Unterschied zwischen leitungs- und paketvermittelter Übertragung soll anhand einer Postkarte dargestellt werden, die durch ein Rohrpostsystem geschickt wird. Dies entspricht weitestgehend einem Datenpaket im Internet, das auf Grund seiner problemlosen Lesbarkeit, ohne weitere Manipulationen, unverschlüsselt Postkartencharakter hat[23].

Bei der leitungsvermittelten Übertragung wird die Übertragungsstrecke zum Ziel vor dem Versenden der Nachricht festgelegt und exklusiv für diese Übertragung genutzt. Während die Kartusche mit der Karte im System ist, kann keine andere Nachricht

[23] Sievers, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, 80

diesen Weg nutzen. Wenn mehrere Nachrichten parallel übertragen werden sollen ist es notwendig, zusätzliche Übertragungswege zu schalten.

Im Gegensatz dazu wird die Postkarte bei der paketvermittelten Übertragung in mehrere Abschnitte unterteilt. Diese werden vom Absender nummeriert und anschließend mit separaten Kartuschen versendet. Jede Kartusche erhält dabei, nach außen hin sichtbar, die Adresse des Absenders und des Empfängers. Das Rohrpostsystem kann gleichzeitig von vielen Nutzern verwendet werden. Daher ist es möglich, dass Teile des Systems bereits durch Nachrichten belegt sind und einzelne Kartuschen nicht den kürzesten Weg zum Empfänger nehmen können, sondern über einen alternativen Weg umgeleitet werden müssen. Der alternative Weg wird automatisch durch das Rohrpostsystem bestimmt, dass an Knotenpunkten des Systems die Zieladresse der Kartusche ausliest und nach festgelegten Verfahren den neuen bestmöglichen Weg bestimmt. Der Empfänger erhält daher die einzelnen Kartuschen mit den Briefabschnitten nicht zwingend in der abgesendeten Reihenfolge. Auf Grund der vorherigen Nummerierung ist er aber in der Lage, den Text der Karte in der korrekten Abfolge wieder zusammenzusetzen.

Der Vorteil der leitungsgebundenen Übertragung ist die Exklusivität der Leitung und die Zusicherung ihrer vollen Übertragungskapazität. Der Nachteil ist, dass bei einem Defekt im System oder bei Blockade eines Teilstücks die Nachricht nicht übertragen werden kann. Bei diesem Verfahren kann der Betreiber der Rohrpost auf Grund der vorherigen Festlegung des Weges exakt sagen, welchen Weg die Nachricht durch sein System nehmen wird.

Bei der paketvermittelten Übertragung hingegen ist es möglich, dass viele Nutzer gleichzeitig eine Leitung benutzen. Bei Blockade, Defekt oder Überlastung wird automatisch durch das System ein alternativer Weg gewählt. Nachteil ist, dass auf Grund der verschiedenen Wege die gesamte Nachricht länger für die Übertragung benötigen kann und dass der Empfänger die einzelnen Nachrichtenteile wieder in die richtige Reihenfolge bringen muss. Der eindeutige Vorteil ist, dass eine Nachricht auch bei Störungen sicher übertragen werden kann. Auf Grund der automatischen Wegewahl ist es für den Betreiber des Rohrpostsystems nicht möglich vorherzusagen, welcher Teil der Nachricht zu welchem Zeitpunkt wo im System zu finden sein wird.

Als Beispiel für die leitungsgebundene Übertragung von Nachrichten soll hier das öffentliche Telefonnetz genannt sein. Durch das Wählen der Rufnummer leitet der Kommunikationsteilnehmer die Schaltung des Übertragungsweges ein. Dieser wird, noch vor dem Gespräch, bis hin zum Ziel geschaltet und exklusiv für beide Teilnehmer gehalten. Während eines Gespräches ändert sich der Übertragungsweg nicht. In den klassischen Telefonnetzen werden für einen bestimmten Zielpunkt in den meisten Fällen die gleichen Wege mit festen Übergabepunkten für die Kommunikation genutzt. Somit ist es zum Beispiel oft möglich den verwendeten Kommunikationsweg für eine Verbindung von Deutschland nach England gezielt vorherzusagen.

Das Internet hingegen überträgt Informationen in Form von kleinen Datenpaketen, die wie die oben beschriebene Rohrpostkartusche den Absender und die Adresse des Ziels enthalten. Das System entscheidet an Hand von verschiedenen Kriterien automatisch über den Übertragungsweg. Dieser Weg kann im Internet, anders als bei der leitungsvermittelten Kommunikation, nicht sicher vorhergesagt werden. Die Zusammensetzung der Pakete und der Transport sind in Protokollen geregelt. Diese Vorschriften sind die technischen Gesetze des Internet und sollen daher im nächsten Abschnitt erläutert werden.

E Die Kommunikationsprotokolle im Internet

Jedes Paket im Internet enthält verschiedene Informationen mit denen es identifiziert und weitergeleitet werden kann. Diese Informationen dienen allein dem Transport der Pakete und stehen in keinerlei Zusammenhang mit seinem Inhalt. Da diese Daten Informationen über Informationen entsprechen, werden sie gemäß dem Entwickler des World Wide Web (WWW), *Tim Berners-Lee*, als Metadaten bezeichnet. Ein grundlegendes Kriterium für Metadaten ist, dass sie maschinenlesbar und damit durch Automaten auswertbar sein müssen. Die Metadaten eines Paketes werden durch die verschiedenen Kommunikationsprotokolle generiert und den zu transportierenden Informationen vorangestellt. Sie enthalten die näheren Umstände eines Kommunikationsvorgangs und sind somit gem. § 3 Nr. 30 TKG als Verkehrsdaten einzuordnen.

Die Kommunikation zwischen zwei Endgeräten im Internet geschieht auf unterschiedlichen Ebenen innerhalb der Geräte. Eine durch den Nutzer generierte Information wird in transportierbare Stücke aufgeteilt und durchläuft diese Ebenen, in der

Technik auch als Schichten[24] bezeichnet. Zur besseren Einordnung der späteren Kommunikationsprotokolle sollen im Folgenden die wichtigsten Schichten erörtert werden.

I. Das Schichtenmodell

Im Jahre 1977 war es die Aufgabe der *International Organization for Standardization* (ISO), ein standardisiertes Modell zu entwickeln, das die Kommunikation zwischen den Rechnern eines Computernetzwerkes darstellt. Als Ergebnis dieses Prozesses entstand ein Schichtenmodell, das die unterschiedlichen Kommunikationsvorgänge zwischen den einzelnen Applikationen auf einem Rechner beschreibt. Dieses Schichtenmodell wurde standardisiert und ist heute bei der ITU-T[25] als Standard X.200[26] dokumentiert.
Es besteht aus 7 unterschiedlichen Ebenen, gemäß der anglophonen Prägung der Technik auch als Layer[27] bezeichnet. Für das Arpanet wurde dieses 7-stufige Modell auf Grund praktischer Erwägungen im Auftrag des US-Verteidigungsministeriums überarbeitet und bildet heute, in zusammengefasster Form, als TCP/IP-Referenzmodell mit 4 Schichten die Grundlage der Kommunikation im Internet[28]. Die 4 Schichten setzen sich wie folgt zusammen:

Die 4. Schicht, auch als Applikationsschicht bezeichnet, ist für den Nutzer am greifbarsten. Sie bildet die Schnittstelle von den Applikationen (z.B. E-Mail Programm, Software zur Internettelefonie, u.s.w.) zum Netzwerk. Diese Applikationen ermöglichen dem Nutzer die Interaktion mit seinem Endgerät und stellen die Werkzeuge für die elektronische Kommunikation dar. Bildlich gesehen sind die Applikation mit Briefpapier und Tinte vergleichbar, mit denen der Nutzer in der Lage ist einen Brief zu verfassen.

---

[24] engl. Layer
[25] International Telecommunication Union - Telecommunication Standardization Sector
[26] ITU-T Data Networks and Open System Communications
[27] Das OSI-Schichtenmodell teilt sich in 7 Layer auf: 1. Das Netzwerklayer. Diese Schicht beschreibt den Transport der einzelnen Datenbits auf den physikalischen Verbindungen. 2. Die Sicherung dient der Überprüfung der Übertragenen Daten auf Richtigkeit und Vollständigkeit. 3. Die Vermittlungsschicht ist für die Vermittlung der Datenpakete auf ihrem Weg durch das Netz verantwortlich. 4. Die Transportschicht dient der Verbindung zwischen den Schichten 1-3 und den Schichten 5-7. 5. In der Sitzungsschicht werden die Verbindungen zwischen den Endsystemen organisiert. 6. Die Darstellungsschicht wandelt den transportierten Inhalt in lokal darstellbare Daten um. Das kann zum Beispiel notwendig sein, wenn ein Nutzer in einem anderen Land unterschiedliche Schriftzeichen benötigt. 7. Die Anwendungsschicht stellt die Verbindung zwischen Netzwerk und den Applikationen dar.
[28] Doyle/Carroll: CCIE Professional Development Routing TCP/IP, Volume I

Die Transportschicht ist als 3. Schicht für den Transport der in der Applikationsschicht erzeugten Daten verantwortlich. Dazu baut diese Schicht eine Ende-zu-Ende Verbindung mit einem Kommunikationspartner auf. Dazu wird entweder das verbindungsorientierte *Transport Control Protocol* (TCP) oder das verbindungslose *User Datagram Protocol* (UDP) verwendet. Verbindungsorientiert bedeutet, dass beide Rechner sich den Erhalt der gesendeten Pakete bestätigen, bei der verbindungslosen Übertragung wird ein Paket ohne Empfangsbestätigung auf den Weg gegeben.
Um die Daten einer Applikationen versenden zu können, werden diese in der Transportschicht auf ein für das Transportnetz verständliches Maß und Format gebracht. Wird in dieser Schicht das TCP verwendet, werden die von einem Kommunikationspartner empfangenen Pakete geprüft und verlorengegangene oder beschädigte Daten automatisch erneut angefordert. Die Transportschicht ist auch dafür verantwortlich, dass empfangene Pakete wieder in die Reihenfolge gebracht werden, wie sie beim Absender abgeschickt wurden. Im bildlichen Vergleich kann diese Schicht als Postamt gesehen werden. Der geschriebene Brief wird in einen, für den Weitertransport genormten, Umschlag gesteckt, um unterschiedliche Papiergrößen auf ein Einheitsmaß zu bringen. Anschließend wird der Umschlag mit einer Absender- und einer Zieladresse versehen und frankiert. Bei TCP wird der Brief als Einschreiben mit Rückschein gesendet, bei UDP als normales Schreiben. Sind die Datenpakete entsprechend aufbereitet, werden sie an die 2. Schicht übergeben.

Diese, auch als Vermittlungs- oder Internetschicht bezeichnete Ebene, regelt den Transport der Datenpakete durch das Netzwerk. Die Zieladresse der Pakete wird in den Knotenpunkten des Netzes, sogenannten Routern, ausgewertet. In diesen Knoten gibt es Listen, auch Routing-Tabelle genannt, die jeden Zielbereich des Internet in zusammengefasster Form enthalten. Nach einem Abgleich der Zieladresse mit dieser internen Datenbank weiß der Router, an welchem seiner Ausgänge er das Paket auf die Reise schicken muss, damit es seinen Zielpunkt erreicht. Am Anfang des Transportes wird die Granularität des Zielpunktes sehr grob sein. Je näher das Paket jedoch seinem Ziel kommt, desto genauer kann der nächste Punkt bestimmt werden.
In dem verwendeten Beispiel wird in der Vermittlungsschicht der Transport eines Briefes durch die Post abgebildet. Nach Abgabe beim Postamt wird der Brief in ein Verteilzentrum weitergeleitet. Dort wird die Zieladresse ausgewertet um zu entscheiden, auf welchem Transportweg der Brief sein Ziel am Besten erreicht. Und auch hier

ist anfangs die Welt nur grob in weitere Ziele aufgeteilt. Wird z.B. ein Brief von Frankfurt nach Washington geschickt, wird im Briefzentrum der Brief auf den Weg in die USA gegeben. Eine weitere Festlegung des Weges findet in Deutschland nicht statt. Erst in den USA wird das empfangende Verteilzentrum den Bundesstaat näher bestimmen, das dann folgende die Stadt u.s.w., bis der Brief im Auslieferungszentrum für den Zielbereich landet.

Die Netzwerkschicht, ist als 1. Schicht dafür verantwortlich, den physikalischen Zugriff auf das Übertragungsmedium zu regeln. In dem bisherigen Beispiel des Transportes eines Briefs ist die Netzwerkschicht der Disponent, der den Transportweg organisiert. Eine strategische Erfassung wird in der Regel immer auf dieser Schicht erfolgen, da nur so die automatische Verarbeitung der Daten gewährleistet ist.

II. Das Transport Control Protokoll

Wie bereits in Punkt I beschrieben ist das TCP in der Transportschicht für die Steuerung und Kontrolle des Versands der Datenpakete verantwortlich. Zum besseren Verständnis der Vorgänge ist zuerst einmal der grundsätzliche Aufbau eines Datenpakets im Internet zu klären.

a) Der Aufbau eines IP-Pakets

Ein IP-Paket enthält als wichtigsten Baustein die vom Nutzer mit Hilfe einer Anwendung erzeugten Inhaltsdaten. Diese stellen technisch gesehen einen seriellen Bitstrom dar, der für den Transport in kleine Teile zerlegt und auf Pakete aufgeteilt wird. Für die weitere Verarbeitung im Netzwerk und auf dem Zielsystem stellt jede Anwendung den Datenpaketen notwendige Informationen, den sogenannten Header, vorweg. Gemäß der auf Seite 29 festgelegten Definition handelt es sich hierbei bereits um Metadaten bzw. rechtlich gesehen um Verkehrsdaten.

Die Daten werden als Nutzdaten der Transportschicht übergeben. Diese fügt wiederum weitere Metadaten hinzu, um die folgende Verarbeitung und den Transport zu ermöglichen. Bei diesen Metadaten handelt es sich z.B. um die Sequenznummer des Paketes, die für die Ermittlung der Reihenfolge am Zielort notwendig ist oder aber auch den Sende- und den Zielport.

Ein Port stellt sowohl einen Eingang als auch einen Ausgang für Datenpakete in der Transportschicht dar. Jeder Computer verfügt über 65.535 Ports, die gleichzeitig für die Kommunikation mit anderen Rechnern genutzt werden können. Dabei wird jeder Port ständig auf eingehende Pakete überwacht, damit eine verzuglose Weiterverarbeitung sichergestellt werden kann. Die Ports von 0 bis 1023 sind durch die *Internet Assigned Numbers Authority* (IANA)[29] wichtigen Applikationen bereits fest zugeordnet und werden als *well-known Ports* bezeichnet. Eine E-Mail wird z.B. von einem Quellrechner über das *Simple Mail Transport Protocol* (SMTP) laut Festlegung von Port 25 gesendet und auf dem Zielrechner mit *Post Office Protocol Version 3* (POP3) an Port 110 empfangen.
In dem bisherigen Beispiel des Briefzentrums stellen Ports unterschiedliche Laderampen dar, an denen Transporter ihre Ladung aufnehmen oder abgeben. Dabei können einzelne Rampen z.B. exklusiv für die Versendung oder Annahme von Luftpostbriefen bzw. Expressbriefen reserviert sein.

Die gesendeten Datenpakete verfügen zu diesem Zeitpunkt somit über 2 Header aus verschiedenen Schichten und werden von der Transportschicht im Gesamten als Nutzdaten an die Vermittlungsschicht und das dort verantwortliche Internet-Protokoll übergeben.

III. Das Internet-Protokoll

Das Internet-Protokoll ist in der Vermittlungsschicht für die Adressierung der einzelnen Pakete zuständig. Aktuell ist im Internet das IPv4[30] maßgeblich. Auf Grund einer Adressknappheit, besonders in den asiatischen Ballungsräumen, ist aber ein Wechsel auf die Version 6 in Planung oder teilweise auch bereits im praktischen Einsatz.

a) Adressierung im Internet

Die Adressierung der Pakete im Internet ist für die spätere rechtliche Einordnung von Interesse. Daher wird in diesem Abschnitt eingehend auf die verschiedenen Verfahren zur Adressierung und den Aufbau von Adressen eingegangen.

---

[29] *www.iana.org*
[30] Internet Protokoll Version 4

Eine Internetadresse in der Version 4 hat eine Größe von 32 Bit, gleichbedeutend mit 32 Stellen die entweder eine 0 oder eine 1 darstellen können. Somit ergibt sich nach der Umrechnung vom Binär- in das Dezimalsystem eine maximale Anzahl von ca. 4,3 Milliarden möglichen Adressen. Diese lassen sich über die sogenannte Netzmaske in verschiedene Bereiche, Klassen genannt, aufteilen.

Die Vergabe von Internetadressen wird über die IANA geregelt. Diese Organisation ist seit Einführung des Internet weltweit für diese Aufgabe zuständig. Seit dem Jahre 1998 wird die IANA durch die eigens gegründete *Internet Corporation for Assigned Names and Numbers* (ICANN) verwaltet. In den Anfangstagen des Netzes ahnte niemand, wie dramatisch das Internet eines Tages wachsen würde. Daher wurden große Bereiche an US-amerikanische Firmen, Universitäten und Behörden gegeben. So erhielt z.B. die Firma IBM 1992 den Adressbereich 009.000.000.000 bis 009.255.255.255, mit ca. 16,7 Millionen verfügbaren Adressen den 256sten Teil des gesamten IPv4 Adressbereiches.

Heute werden IP Adressbereiche durch die IANA an *Regional Internet Registries* (RIR) vergeben, die sich um die weitere Verteilung kümmern. Seit 2005 existieren 5 dieser Registries, die sich die Welt wie folgt aufteilen:

- AfriNIC[31] Afrika
- APNIC[32] Asien/Pazifik
- ARIN[33] Nord Amerika
- LACNIC[34] Lateinamerika und Karibik
- RIPE[35] Europa, Mittlerer Osten, Zentralasien

Von diesen Organisationen werden die zu verwaltenden Adressbereiche weiter aufgeteilt und *Local Internet Registries* (LIR) zugewiesen. Bei diesen handelt es sich entweder um einzelne Kunden, meistens Großunternehmen oder Organisationen, oder *Internet Service Providern* (ISP). Letztere stellen ihren Kunden die Infrastruktur für einen Internetzugang zur Verfügung und kümmern sich auch um dessen Adres-

31 African Network Information Centre
32 Asia Pacific Network Information Centre
33 American Registry for Internet Numbers
34 Regional Latin-American and Caribbean IP Address Registry
35 Réseaux IP Européens Network Coordination Centre

sierung. Der größte Internet Service Provider Deutschlands ist die TELEKOM mit ca. 13 Millionen DSL Anschlüssen.

Damit ein Telekommunikationsanschluss für andere Teilnehmer in einem Telekommunikationsnetz erreichbar ist, benötigt er eine Adresse. Die einfachste Variante der Zuweisung einer Adresse zu einem Telekommunikationsanschluss ist die feste Vergabe. Im Internet werden bei diesem Verfahren einem Anschluss eine oder mehrere IP-Adressen fest zugewiesen. Mit den zugehörigen Einträgen in den öffentlich zugänglichen Namensdatenbanken ist der Anschluss somit für jeden Nutzer aus dem Internet erreichbar. Auch kann über die RIR und LIR der für den Adressbereich verantwortliche ISP gefunden werden. Anschließend ist nur noch eine Abfrage des ISP über seine Datenbank mit den Bestandsdaten der Kunden notwendig und der zugehörige Teilnehmer zu einer IP-Adresse, sei es eine natürliche oder juristische Person, kann zweifelsfrei den bei dem Datenverkehr entstandenen Verkehrsdaten zugeordnet werden[36]. Ein Rückschluss auf den Nutzer der Verbindung ist aber auf Grund der Möglichkeit mehrere Endgeräte an einem Anschluss zu betreiben nicht ohne weiteres möglich.

Wegen des enormen Wachstums des Internet in den letzten Jahren und der freizügigen Vergabe in den Anfangsjahren, ist es heute nicht mehr möglich, jedem Endgerät eine feste Adresse zuzuweisen. Daher wurde die Technik der dynamischen Adressvergabe entwickelt, um diesem Umstand Rechnung zu tragen.

b) Die dynamische Vergabe von Adressen im Internet

Bei der dynamischen Vergabe von IP-Adressen wird mit einem sogenannten Adresspool gearbeitet. Dabei teilen sich mehrere Teilnehmer einen Adressbereich mit einer deutlich kleineren Anzahl von Adressen. Da davon auszugehen ist, dass nie alle Teilnehmer gleichzeitig Zugang zum Internet benötigen, werden die Adressen aus dem Pool jeweils zum Zeitpunkt der Nutzung temporär einem Anschluss zugeordnet. Beendet ein Teilnehmer seine Sitzung, wird die Adresse im Pool wieder freigegeben und kann für andere Telekommunikationsanschlüsse erneut vergeben werden[37].

---

[36] Schmitz in Hoeren/Sieber*, Handbuch Multimedia-Recht,* 7.6 Rdnr. 53
[37] Schmitz in Hoeren/Sieber*, Handbuch Multimedia-Recht,* 7.6 Rdnr. 52

Somit ist es möglich, dass eine Adresse innerhalb eines definierten Zeitraums von mehreren Nutzern verwendet wird. Eine eindeutige Zuordnung ist somit ohne zusätzliche Informationen nicht mehr möglich. Zum Zweck der Abrechnung speichert der ISP die Daten der zeitlichen Zuordnung einer Adresse zu einem definierten Anschluss. Nur in Verbindung mit diesen Verkehrsdaten kann dann eine dynamische Adresse zweifelsfrei einem Teilnehmer zugeordnet werden[38].

Ein Beispiel, dass den Unterschied zwischen der Vergabe von statischen und dynamischen IP-Adressen sehr gut darstellt, ist die Verwendung von Kennzeichen im öffentlichen Straßenverkehr. Jedes auf Deutschlands Strassen betriebene KFZ verfügt über ein amtliches Kennzeichen, zu dem bei der Vergabe durch die Behörden Name, Anschrift und sonstige Daten des Halters gespeichert werden. Auf Grund ihrer Beschaffenheit sind diese Daten vergleichbar mit den Bestandsdaten, die ein Telekommunikationsdienstleister gem. TKG von seinen Kunden erhebt.
Das Kennzeichen ist einem KFZ fest zugeordnet. Wird es erfasst, ist es den Behörden mit Hilfe der gespeicherten Daten jederzeit möglich, den Halter zu ermitteln. Dies gilt auch für Fahrzeuge aus dem Ausland, wenn die Unterstützung von ausländischen Behörden in Anspruch genommen wird. Der Halter entspricht hier analog dem Teilnehmer eines Telekommunikationsanschlusses.

Ist der Halter nun ein Unternehmen das Fahrzeuge vermietet, nutzt dieses in der Regel einen Fuhrpark, in dem jedes der Fahrzeuge angemeldet ist und über ein amtliches Kennzeichen verfügt. Im laufenden Geschäftsbetrieb werden die KFZ temporär an unterschiedliche Nutzer vermietet und die in Zusammenhang mit diesem Vertragsverhältnis entstehenden Daten wie Name und Adresse des Nutzers, Führerschein, Beginn und Ende der Nutzung und andere Informationen durch den Vermieter gespeichert.
Wird nun eines dieser Fahrzeuge während der Fahrt durch die Behörden erfasst und das amtl. Kennzeichen registriert, können diese über die ihnen zur Verfügung stehenden Daten den Halter ermitteln. Der Versuch den Nutzer zu ermitteln, wird regelmäßig an der Grenze zu dem Unternehmen scheitern, das als Halter der Fahrzeuge registriert ist. Nur wenn, mit Hilfe des Unternehmens, die Daten der Behörden über Kennzeichen und Zeitraum der Erfassung mit den Daten über die

[38] Braun, jurisPR-ITR 4/2006, Anm.6

Mietverträge korreliert werden, kann einem Kennzeichen für einen festgelegten Zeitraum ein Nutzer zugeordnet werden.
Bei der Erfassung eines Telekommunikationsvorgangs mit dynamischer IP-Adresse muss dieser Vorgang mit anderen Daten vergleichbar durchgeführt werden.
Es ist aber auch der Fall denkbar, dass ein Fahrzeug mehreren Nutzern zur Verfügung steht, ohne dass der Halter ein Fahrtenbuch oder einen sonstigen zeitlichen Nachweis führt. Hier kann über das amtl. Kennzeichen zwar der Halter des Fahrzeuges ermittelt werden, der Nutzer zu einem definierten Zeitpunkt bleibt aber ab einer bestimmten Größe der Gruppe unbekannt.
Ähnlich verhält es sich für statische und dynamische IP-Adressen. In öffentlichen Bereichen mit freien drahtlosen Internetzugängen oder in Einrichtungen in denen eine Authentifizierung[39] der Nutzer fehlt, kann der Teilnehmer, z.B. der Betreiber des Zugangs in einem Café, den jeweiligen Nutzer nicht eindeutig identifizieren und eine Anfrage der Ermittlungsbehörden würde keinen Erfolg bringen[40].

c) Namensauflösung im Internet

Auf Grund der Komplexität der Zahlenkolonnen einer IP-Adresse sind diese für einen menschlichen Nutzer nur schwer zu merken, Eigennamen sind deutlich eingängiger. Aus diesem Grund wurde die Namensauflösung über das *Domain Name System* (DNS) im Internet eingeführt. Bei diesem Verfahren wird einem Domainnamen über eine Datenbank eine IP-Adresse zugewiesen. Bei einer Domain handelt es sich um einen Teilbereich des Internet, hinter dem sich ein oder mehrere vernetzte Endgeräte verbergen. In der Regel stellt eine Domain Inhalte im Internet für den Abruf zur Verfügung[41].
Das DNS ist von seiner Struktur her wie ein Baum aufgebaut, einzelnen Zweige werden dabei durch Punkte voneinander getrennt. Die Zeichenfolge am rechten Ende des Zweiges ist die Wurzel und wird als *Top-Level Domain* (TLD) bezeichnet. Die Adressen sind daher bei der Wurzel beginnend von rechts nach links zu lesen
Bei der TLD handelt es sich um durch die ICANN vergebene Buchstabenkombinationen, die in der Regel Länder, Organisationen oder bestimmte Gruppen repräsentieren. Verantwortlich für die Verwaltung der deutschen TLD ".de" ist die DENIC eG[42] mit Sitz in Frankfurt am Main. Aktuell existieren weltweit ca. 2500 TLDs, deren

---

39 Schmitz in Hoeren/Sieber*, Handbuch Multimedia-Recht,* 7.6 Rdnr. 53
40 Dix/Petri, DuD 9/2009, 531, 532
41 z.B. www.dejure.org
42 DE Network Information Center - www.denic.de

zuständige DNS Server auf 13 sogenannten Root-Servern gespeichert sind. Hat ein DNS Server in einer unteren Hierarchieebene keinen Eintrag für eine bestimmte TLD in seinen Datenbanken, stellt er eine Anfrage an einen der Root-Server. Er erhält dann die Adresse des für die Anfrage zuständigen DNS Servers. Die Root-Server zählen zur kritischen Infrastruktur des Internet. Denn würden diese Server ausfallen, wäre das System der Namensauflösung innerhalb weniger Tage nicht mehr nutzbar und das Internet würde zusammenbrechen. Politisch interessant ist die Tatsache, dass die Verwaltung und Vergabe der Top-Level Domains seit 1998 der ICANN, einer privaten Gesellschaft die indirekt dem US-amerikanischen Wirtschaftsministerium unterstellt ist, unterliegt. Dies lässt erkennen, wie groß der Einfluss der US-Regierung auf das Internet auch heute noch ist.
Als Beispiel für eine Namensauflösung im Internet sei der Internetauftritt der Bundesregierung genannt. Die Domain "bundesregierung.de" ist gemäß einer Abfrage bei der DENIC eG im Besitz der Regierung der Bundesrepublik Deutschland; die Abfrage eines DNS Servers liefert die IPv4-Adresse 217.79.215.248. Nachteil des Systems ist, dass eine TLD von jedem Teilnehmer des Internet beantragt werden kann und die Server auf denen das Angebot bereitgehalten wird sich nicht in dem Landesbereich befinden müssen, der durch die TLD bezeichnet wird. Als Beispiel sei hier der Inselstaat Tuvalu genannt, dem durch die ICANN die TLD ".tv" zugeteilt wurde. Diese Endung findet auf Grund ihrer Bedeutung als Abkürzung für Television große Nachfrage bei Fernsehstationen auf der ganzen Welt. Eine Domain mit der Endung ".tv" ist rechtlich zwar dem Inselstaat Tuvalu zuzuordnen, die Nutzungsrechte werden aber in der Regel bei einer natürlichen oder juristischen Person in einem anderen Staat liegen. Die Domain "rtl.tv" führt z.B. auf die Internetpräsenz eines Senders der Bertelsmann-Gruppe mit Hauptsitz in Köln.

d) Autonome Systeme

Die technische Infrastruktur des Internet steht unter keiner zentralen Verwaltung. Vielmehr ist es ein Zusammenschluss einzelner, eigenständiger Netzbereiche, die im Eigentum und unter der Verwaltung verschiedenster Unternehmen und Organisationen stehen[43]. Diese einzelnen Netze werden als *Autonome Systeme* (AS) bezeichnet. Will ein Unternehmen ein solches AS betreiben, muss es eine Adresse, die sogenannte *Autonomous System Number* (ASN), bei der zuständigen RIR beantra-

[43] Doyle/Carroll, *CCIE Professional Development Routing TCP/IP, Volume I*

gen. Auf Grund technischer Rahmenbedingungen ist eine maximale Anzahl von 65.535 AS möglich. Als Beispiel sei hier das AS der Deutsche Telekom AG genannt, die ihr weltweites Netz unter der ASN 3320 betreibt.

In diesem Zusammenhang ist der grenzüberschreitende Entwurf des Internet noch einmal deutlich darzustellen. Die TELEKOM betreibt Router in verschiedenen Ländern der Erde. Ein Router in New York im Netz der Deutschen Telekom befindet sich geografisch gesehen eindeutig außerhalb der Landesgrenzen Deutschlands, aus Sicht des Netzwerkes hat man die Grenzen des AS3320 jedoch nicht verlassen. Sollte es zu Störungen oder Überlastungen innerhalb des Netzes der TELEKOM kommen ist es durchaus möglich, dass Verkehr mit dem Startpunkt München und dem Zielort Hamburg über New York transportiert wird, ohne dass dieser das Netz des Providers verlässt.

Die Übergabepunkte zwischen den Grenzen zweier AS werden als sogenannten Peering Points bezeichnet. Hier geht der Verkehr aus dem AS des einen ISP in das AS des anderen ISP über. In der Praxis hat man sich hier zwei unscheinbare technische Geräte vorzustellen, die über eine oder mehrere Glasfaserleitungen verbunden sind. An diesen Peering Points finden sich die realen Grenzen des heutigen Internet[44]. Die TELEKOM verfügt in ihrem Netz über mehr als 420 Peering Points in verschiedenen Ländern.

Der größte Grenzübergang Europas befindet sich in Deutschland am *German Internet Exchange*[45] (DE-CIX) in Frankfurt am Main. Hier sind über 300 ISP an den Grenzen ihrer AS miteinander verbunden. Tagtäglich wird ein Datenvolumen von ca. 500 GBit/s ausgetauscht, das entspricht sekündlich ca. 11.000 Exemplaren der Schönfelder Gesetzessammlung in digitaler Form. Ausgehend von einer Breite von ca. 20cm pro Ausgabe würde sich damit in jeder Sekunde eine Reihe mit reellen Büchern von München bis Stuttgart aufstellen lassen.

Die deutsche Telekom ist interessanterweise nicht am DE-CIX vertreten. Auf Grund ihrer Marktmacht kann sie bestimmen, wer sich mit ihrem Netz verbinden darf. Für diese Verbindungen betreibt die TELEKOM eigene Übergabepunkte in Deutschland.

e) Routing im Internet

Unter dem Begriff Routing versteht man in der Terminologie des Internet die Wegewahl für ein Datenpaket an den Netzknoten. Wie bereits eingehend beschrieben,

---

44 Gusy, APuZ 18-19/2009, 26, 29

45 www.de-cix.net

enthält jedes Paket sowohl eine Start- und eine Zieladresse als auch den Quell- und den Zielport. Mit diesen Informationen lässt sich ein Paket sowohl identifizieren als auch inhaltlich qualifizieren. In der Fachterminologie werden diese Metadaten als Quadrupel bezeichnet.

Jedes AS verfügt über 2 verschiedene Tabellen zur Wegeführung, sogenannte Routing-Tabellen. Diese Tabellen stellen die Sicht des Routers auf das interne Netz des Providers und auf die externen Verbindungen dar. Die interne Tabelle wird über ein *Interior Gateway Protocol* (IGP) erzeugt, die externe Sicht über ein *Exterior Gateway Protocol* (EGP).

Jeder Router innerhalb des Netzes kennt durch diese Informationen seine direkten Nachbarn und weiß, wohin er ein Datenpaket weiterleiten muss, damit es seinen vorgeschriebenen Zielpunkt erreicht. Um die Tabellen der Router überschaubar zu halten sind aber nicht alle Adressen des Internet innerhalb des Netzes bekannt, sondern nur zusammengefasste Bereiche. Sollte ein Datenpaket für eine Adresse außerhalb des eigenen Netzes bestimmt sein, kennen die Router innerhalb eines Netzes nur den entsprechenden Grenzrouter für diese Adresse. Die Erzeugung der Routing-Tabellen erfolgt dabei dynamisch über die oben genannten Protokolle. Ziel der dort enthaltenen mathematischen Algorithmen ist es, immer den wirtschaftlich günstigsten Weg durch das Netz zu wählen. Sollte dabei ein Defekt oder die Überbelegung einer Leitung auftreten gelingt es dem System, dynamisch diese Engstelle zu umgehen. Die Grenzrouter eines AS führen in ihren Tabellen sowohl die innere Sicht des eigenen Netzes als auch die Sicht in das Internet hinaus. Herauszustellen ist dabei die Unvorhersehbarkeit der Wegewahl im Internet. Da Router ihre Tabellen regelmäßig über elektronische Verfahren untereinander aktualisieren, kann sich der Weg eines Paketes von A nach B je nach Zustand des Netzes schnell ändern.

Gerade auf internationalen Strecken wird hier die Wegeführung wirtschaftlich optimiert. Tagesgenau bieten auf dem sogenannten Spot-Market[46] Netzbetreiber Leitungskapazitäten an. Einige Provider mieten hier die günstigsten Strecken für einen definierten Zeitraum an und leiten ihren gesamten Verkehr über diese Datentrasse[47]. Sollte ein anderer Anbieter eine Leitung günstiger anbieten, wird der Verkehr auf diese Leitung umgeschaltet. Dieses Verfahren wurde automatisiert und kann ohne

---

[46] Unter einem Spot-Market versteht man einen Markt, auf dem vorwiegend Warengeschäfte verzugslos abgewickelt werden. Die Preise auf einem Spot-Market werden von Angebot und Nachfrage bestimmt und können sich schnell ändern. Kommunikationsleitungen werden auf einem Spot-Market in London mit tagesaktuellen Preisen gehandelt.

[47] Keromytis/Prevelakis/Turner, 1, 1

den Eingriff eines Technikers geschehen. So ist der Provider sicher, immer die günstigste Leitung zu verwenden. Eine Vorhersage des Weges der Daten von A nach B wird auf Grund dieser Verfahren für einen Dritten sehr schwierig.

IV. Anwendungen zur Kommunikation

Für die rechtliche Bewertung der Vorgänge im Internet ist nicht nur der Transportweg relevant. Auch die Anwendungen, die ein Nutzer zur Kommunikation im Netz verwendet spielen eine Rolle. Im Nachfolgenden sollen zwei der bekanntesten und meistgenutzten Anwendungen vorgestellt werden. Dabei handelt es sich zum einen um die elektronische Post, auch als E-Mail bezeichnet und zum anderen um *Voice over Internet Protocol* (VoIP), eine Technologie die Telefonie über das Internet ermöglicht.

a) E-Mail

Das Verfahren elektronische Post über ein Netzwerk von Rechnern zu senden, fand bereits zwei Jahre nach der Inbetriebnahme des *Arpanet* Verwendung. Im Jahre 1971 entwickelte der Ingenieur *Ray Tomlinson* eine Software mit der die Adressierung eines Nutzers innerhalb eines Rechnernetzwerkes deutlich vereinfacht wurde. Dazu verknüpfte er den Nutzernamen des Adressaten mit dem Hostnamen des Zielrechners und führte als Bindeglied zwischen beiden Teilen das @-Zeichen ein. Diese Applikation wurde, auf Grund der hohen Akzeptanz durch die Nutzer, schnell eine der wichtigsten Anwendungen im *Arpanet* und ist mittlerweile das Hauptwerkzeug der geschäftlichen und privaten Kommunikation im Internet[48]. Eine E-Mail Adresse besteht noch heute aus zwei Teilen. Der Abschnitt vor dem @-Zeichen wird in der Technik als lokaler Teil, der nachfolgende Teil als Domain Teil bezeichnet. Eine E-Mail Adresse kann sich jeder Teilnehmer nach seinen Wünschen ohne weiteres erstellen. Dies ist nicht nur auf Diensteanbieter in Deutschland begrenzt, sondern international möglich. Deutsche Kommunikationsteilnehmer können sich somit hinter jeder TLD verbergen. Umgekehrt können aber auch Ausländer problemlos E-Mail Adressen mit der TLD ".de" erhalten. Auch ist es nicht zwingend notwendig, dass ein E-Mail Server der Postfächer mit der Endung ".de" verwaltet auf dem Gebiet der Bundesrepublik Deutschland verortet ist. Der Server kann physikalisch an einem beliebigen Ort der Welt betrieben werden und über eine dedizierte Telekom-

[48] Waldrop, DARPA: 50 Years of Bridging the Gap, 78, 83

munikationsverbindung direkt mit einem Zugangsknoten in Deutschland verbunden sein. Dieses Verfahren wird oft von deutschen Firmen angewendet, die in infrastrukturschwachen Regionen Internetservices für ausländische Unternehmen oder Organisationen über Satellit zur Verfügung stellen.
Bleibt noch die Eignung des *local-part* für eine eindeutige Zuordnung zu prüfen. Hier werden oft Vor- und Nachname einer Person verwendet, um für den Adressaten den Absender transparenter zu machen. Das ein solches E-Mail Konto von der beinhalteten Person verwendet wird ist aber nicht zwingend, da sich jeder Teilnehmer frei eine E-Mail Adresse erstellen kann, wenn sie auf dem jeweiligen Server noch verfügbar ist. Somit ist es beispielsweise möglich, die Adresse mit dem lokalen Teil Helmut.Kohl auf einem Mailserver seiner Wahl zu registrieren, ohne dass die genannte Person hinter der Adresse steht. Zudem bietet die Absenderadresse innerhalb einer E-Mail das Potential zur Fälschung da der Absender weder durch die Anwendung noch durch den Server verifiziert wird. Daher ist es mit geringem technischen Sachverstand möglich, z.B. eine E-Mail mit dem Absender angela.merkel@bund.de zu versenden. Eine eindeutige Zuordnung ist somit durch die E-Mail Adresse nicht machbar.

In der heutigen juristischen Literatur wird der Übertragungsvorgang einer E-Mail in vier Phasen unterteilt[49]:

Für die Vorbereitung der Übertragung erstellt der Absender auf einem Endgerät mit Hilfe eines Texteditors seine Nachricht. Diese wird über eine E-Mail Software für den weiteren Transport über das SMTP verarbeitet. Dieses Protokoll stellt die Vorschrift für den digitalen Transport von elektronischen Nachrichten dar. Schickt der Nutzer die Nachricht ab, wird diese mit einem SMTP Header versehen, der sowohl Absender- als auch Zieladresse enthält. Hierbei handelt es sich um eine E-Mail Adresse, nicht zu verwechseln mit der IP-Adresse, die erst in einer tieferen Schicht hinzugefügt wird.

In der ersten Übertragungsphase wird die Nachricht in Datenpakete unterteilt, an einen Postausgangsserver gesendet und hier auf einem Datenspeicher abgelegt. Dieser Server kann im Hoheitsbereich des Nutzers liegen, z.B. der Postausgangs-

[49] Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, Rd-Nr. 102

server eines großen Unternehmens. In diesem Falle wäre dieser vergleichbar mit einer internen Poststelle. Der Nutzer hat eine Nachricht bereits auf den Weg gebracht, sie befindet sich aber noch im Einflussbereich des Teilnehmers. Bei Privatpersonen ist es in der Regel üblich, dass der Postausgangsserver durch einen externen Dienstleister betrieben wird. In diesem Fall ist das Absenden der elektronischen Post mit dem Einwerfen einer Postkarte, aufgeteilt in verschiedene Abschnitte, vergleichbar. Die Nachricht verlässt mit dem Senden den Einflussbereich des Absenders und befindet sich auf dem Transport und in der Verantwortung des Anbieters.

Der folgende Übertragungsvorgang ist in der Literatur der 2. Phase zugeordnet. Diese Phase spielt für die strategische Erfassung eine bedeutende Rolle, da sie die Übertragung einer E-Mail vom Postausgangs- zum Posteingangsserver umfasst. Dabei handelt es sich in der Regel um ISP übergreifenden Verkehr, der oft in gebündelten Weitverkehrsstrecken zu finden ist. Bei diesem Übertragungsvorgang ermittelt der Postausgangsserver über die Namensauflösung die Ziel IP-Adresse des Empfängers, ergänzt die Datenpakete der Nachricht entsprechend und schickt sie auf ihren Weg durch das Internet an den Posteingangsserver des Ziels. Die Pakete werden durch das Netz bis zu ihrem Zielserver geroutet. Dort werden alle zu der Nachricht gehörenden Datenpakete gesammelt, zusammengefügt und als elektronische Nachricht im Postfach des Adressaten, ein Datenspeicher auf dem Posteingangsserver, zum Abruf bereitgehalten.

In der Literatur stellt der Abruf einer Mail durch den Nutzer die 3. Phase der Übertragung dar. Dazu gibt es zwei unterschiedliche Protokolle, die in ihrer Handhabung deutlich voneinander abweichen. Bei dem meistgebrauchten Verfahren mit der Bezeichnung POP3 ruft der Nutzer seine neuen Nachrichten vom Posteingangsserver ab und speichert diese lokal auf seinem Endgerät, in der Regel einem handelsüblichen PC. Die Nachricht auf dem Server wird im Anschluss gelöscht und es existiert nur noch die lokale Version der E-Mail. Vergleichbar ist dies mit dem Leeren eines privaten Briefkastens. Ein Posteingangsserver eines externen Betreibers kann in diesem Zusammenhang wie ein Postfach betrachtet werden, dass in einer Filiale der Post aufgestellt ist. Nach Leerung des Postfachs ist keine Nachricht mehr in diesem vorhanden.

Das zweite gängige Verfahren wird als *Internet Message Access Protocol* (IMAP) bezeichnet. Hier synchronisiert der Nutzer nur sein Postfach auf dem Server mit dem auf seinem lokalen Endgerät befindlichen Posteingang der E-Mail Anwendung. Das Original der Nachricht verbleibt weiterhin auf dem Posteingangsserver, lokal wird nur eine Kopie gespeichert. Vorteil dieses Verfahrens ist, dass der Nutzer von allen Punkten auf der Welt und unabhängig von einem Endgerät immer vollen Zugriff auf sein E-Mail Postfach hat.

Der 4. Phase ist nicht mehr die Übertragung der Nachricht zuzuordnen, sondern das bereits beschriebene Erstellen der Nachricht und die im Anschluss an die Übertragung stattfindende lokale Speicherung beim Empfänger. Dabei ist strittig, wann der Schutzbereich des Art. 10 GG verlassen wird. Bei POP3 dürfte die Übertragung regelmäßig mit der lokalen Speicherung auf dem Rechner des Nutzers beendet sein. Gemäß Urteil des BVerfG[50] vom 16.06.2009 unterliegt aber auch eine E-Mail auf einem IMAP Server noch dem Schutz des Art. 10 GG.

(aa) Webmail

Häufig greifen Nutzer für die Erstellung und den Versand elektronischer Nachrichten auf Webmailer zurück. Das sind Dienste, wo im Unterschied zu den klassischen E-Mail Programmen, bei denen ein E-Mail Client wie z.B. Microsoft Outlook oder Mozilla Thunderbird auf dem Rechner des Nutzers installiert ist, für die Nutzung lediglich ein Internetbrowser[51] benötigt wird. Der Anbieter des Dienstes stellt sowohl den E-Mail Server als auch die Benutzeroberfläche zur Verfügung. Der große Vorteil für den Nutzer ist die Unabhängigkeit von seinem lokalen Rechner. Er kann immer und überall auf seine Nachrichten zugreifen, da diese zentral gespeichert werden und über jedes internetfähige Endgerät abgerufen werden können. Bekannte Dienste sind zum Beispiel Google Mail, GMX, Web.de und Windows Live, um nur einige zu nennen. Dabei spielt es keine Rolle, wo der Diensteanbieter seine Server geografisch betreibt. Nutzer aus Deutschland können ohne Schwierigkeiten Mailkonten in den USA eröffnen.
Mit dem Zugang zu seinem Webmail Konto erhält der Nutzer immer öfter auch Funktionen einer sog. Groupware, d.h. erweiterte Funktionen die das Zusammenarbeiten in einer Arbeitsgruppe erleichtern. Darunter fallen Kalenderfunktionen, Online-

[50] 2 BvR 902/6
[51] Programm zum Aufruf und Darstellung von Internetinhalten

Besprechungen, Adressbücher. Diese Funktionen können ebenfalls über den Webbrowser gesteuert und aufgerufen werden. Eine Trennung zwischen Mailverkehr und Groupware Funktionalitäten ist kaum noch möglich.

Die im Abschnitt E-Mail bereits dargestellten 4 Phasen für die Übertragung der elektronischen Post finden auf den ersten Blick auch für einen Webmailer Anwendung.
Ein deutlicher Unterschied ist jedoch die Vorbereitung und der Empfang einer Nachricht. Statt eines lokalen Texteditors auf dem Rechner des Nutzers wird für die Nachrichtenerstellung ein vom Diensteanbieter über den Webbrowser zur Verfügung gestellter Editor benutzt. Im Anschluss kann die Mail dann entweder versendet oder aber auch als Entwurf auf den Servern des Anbieters gespeichert werden. Dabei ist der letzte Fall besonders interessant, denn es wurde zwar die komplette Nachricht über die Datenleitungen des Internet übertragen, aber nicht wie in Phase 1 beschrieben versendet.
Auch der Empfang einer Nachricht unterscheidet sich von den klassischen vier Phasen. Der Nutzer öffnet zur Betrachtung empfangener elektronischer Post wiederum nur die Benutzeroberfläche des Dienstanbieters und liest seine Nachrichten online, d.h. ohne eine lokale Kopie auf seinem Endgerät zu speichern. Auch das Betrachten von Anhängen kann mit dieser Oberfläche durchgeführt werden. Die Mail bleibt weiterhin auf den Servern des Anbieters gespeichert und befindet sich, ähnlich wie bei IMAP, nicht im Herrschaftsbereich des Nutzers.

(bb) De-Mail

Wie bereits beschrieben besteht das Problem der klassischen E-Mail darin, dass fehlende Vertraulichkeit und mangelnde Möglichkeiten zur Identifikation des Absenders keine rechtsverbindlichen Handlungen zulassen.
Diese Lücke soll nun unter dem Dach des von der Bundesregierung initiierten Programms E-Government 2.0 geschlossen werden. Eine der vier Säulen dieser Maßnahme ist das Projekt „Bürgerportal“, mittlerweile umbenannt in „De-Mail“. Das Projekt wird federführend durchgeführt vom *Bundesministerium des Inneren* (BMI). Dieses wird dabei von einer Reihe öffentlicher und privater Institutionen unterstützt. Die technische Umsetzung des Projektes wird durch das *Bundesamt für Sicherheit in*

der Informationstechnik (BSI) begleitet. Dabei ist sie zuständig für das Sicherheits- und Zertifizierungskonzept, eine der Kernkompetenzen dieser Behörde[52].

Grundlage für das Projekt ist die EU-Dienstleistungsrichtlinie[53] aus dem Jahre 2006 die das Ziel hat einen Rechtsrahmens zu schaffen, der die Niederlassungsfreiheit und den freien Dienstleistungsverkehr zwischen den Mitgliedstaaten garantiert. In Art. 8 Abs. 1 der Richtlinie wird die elektronische Verfahrensabwicklung behandelt. Dort ist geregelt, dass es möglich sein muss, alle Formalitäten, welche die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch über den betreffenden einheitlichen Ansprechpartner oder bei der betreffenden zuständigen Behörde abzuwickeln.

De-Mail ist nun der Versuch des Gesetzgebers, diese Richtlinie in nationales Recht umzusetzen. Der „Entwurf eines Gesetzes zur Regelung von De-Mail Diensten und zur Änderung weiterer Vorschriften“ vom 13. Oktober 2010 dient der Absteckung eines Rechtsrahmens zur Einführung vertrauenswürdiger De-Mail-Dienste und zur Schaffung von Rechtssicherheit für *De-Mail Diensteanbieter* (DMDA). Dabei sollen vertrauenswürdige Lösungen für die elektronische Kommunikation im Geschäftsverkehr entstehen bei denen die Sicherheit der Dienste, Vertraulichkeit der Nachrichten, die zuverlässige Identität der Kommunikationspartner und die Nachvollziehbarkeit des Kommunikationsvorgangs gewährleistet sind.

Die Stärkung der Rechtssicherheit im elektronischen Geschäftsverkehr soll durch verbesserte Beweismöglichkeiten und Schaffung der Möglichkeiten für eine rechtssichere Zustellung elektronischer Dokumente erreicht werden. Dabei sollen durch das Gesetz Rahmenbedingungen vorgeschrieben werden, die eine vergleichbare Vertrauenswürdigkeit gewährleisten wie die auf Papier beruhende Kommunikation. Eine Eigenschaft von der die aktuelle E-Mail Kommunikation auf Grund der bereits beschriebenen Unsicherheiten weit entfernt ist.

Um die diesen Standard zu erreichen und die geforderte Sicherheit auch über DMDA Grenzen hinweg zu gewährleisten, haben sich die Anbieter zu einem Verbund zusammengeschlossen und stellen eine geschlossene Benutzergruppe im Internet dar. Dabei werden folgende Dienste über den De-Mail Dienst angeboten[54]:

---

52 Bürgerportale (De-Mail) und die EU-Dienstleistungsrichtlinie, Broschüre 10/2008
53 Europäische Dienstleistungsrichtlinie (RL 2006/123/EG)
54 BSI, De-Mail, TR 01201, S.10

(1) Postfachdienst

Der elektronische Briefkasten des Dienstes, der über eine dem Nutzer eindeutig zugeordnete De-Mail-Adresse erreichbar ist. Diese Adresse soll in dem De-Mail Verbund eine ähnliche Funktionen wie die postalische Adresse erfüllen und eine gleichgestellten rechtlichen Status bekommen.
Über den Postfachdienst können Nachrichten empfangen, gespeichert und verwaltet werden.

(2) Versanddienst

Der Versanddienst ermöglicht den Versand von Nachrichten mit der Möglichkeit der Information über die erfolgreiche Zustellung. Dabei sollen die Nachrichten über den gesamten Weg, auch über die Grenzen der DMDA, verschlüsselt werden.

(3) De-Safe

Mit diesem Service kann der Benutzer seine elektronischen Dokumente sichern und verwalten, ohne einen Datenverlust fürchten zu müssen. Rechtlich interessant wird dabei die Funktion, qualifiziert signierte Dokumente so zu speichern, dass ihre Beweiskraft langfristig erhalten bleibt.

(4) De-Ident

Im Rahmen der Registrierung für De-Mail ist eine eindeutige Identifizierung des Nutzers erforderlich. Diese verifizierten Daten sollen im Rahmen von De-Ident anderen Diensten zur Identifizierung des Benutzers zur Verfügung gestellt werden können.

De-Mail ist ein umfassendes Konzept zur Verbesserung der elektronischen Post und steht kurz vor der technischen Einführung. Voraussetzung dafür ist die Verabschiedung des oben genannten Gesetzentwurfes. Geplant ist dies im ersten Quartal 2011, De-Mail soll dann schnellstmöglich im Frühjahr 2011 umgesetzt werden.

(cc) E-Postbrief

Der E-Postbrief ist ein von der Deutschen Post geschaffenes Produkt um die schwindenden Umsätze im Briefgeschäft zu kompensieren und den Kunden eine elektronische Alternative zum klassischen Brief zu bieten.
Dabei setzt die Post auf den Hybridbrief, eine Mischung aus elektronischer Post und auf Papier gedrucktem Brief. Sind Absender und Empfänger beide bei der Post als Nutzer des E-Postbriefes registriert, verlässt eine Nachricht die elektronische Welt nicht. Ist der Empfänger jedoch nicht registriert, wird die Nachricht von der Post ausgedruckt und konventionell zugestellt.
Der E-Postbrief bietet viele Funktionen, die auch im De-Mail Dienst enthalten sind. Darunter fallen z.B. die Möglichkeit Einschreiben mit Empfangsbestätigung zu versenden, die klare Identifikation der Kommunikationsteilnehmer, durchgehende Verschlüsselung der Nachrichten und sichere Speicherung von Dokumenten. Wobei gerade der Punkt durchgehende Verschlüsselung nur für außenstehende Dritte zutrifft. Für einen Hybridbrief muss die Post das Dokument ausdrucken und spätestens hier wird die Verschlüsselung natürlicherweise unterbrochen.
Die Post möchte nach der Verabschiedung des „ Gesetzes zur Regelung von De-Mail Diensten und zur Änderung weiterer Vorschriften“ eine Zulassung des E-Postbriefs als De-Mail Dienst beantragen. Dabei ist der E-Postbrief nicht Teil des De-Mail Verbunds sondern basiert wie bereits geschildert auf einem eigenständigen Konzept. Die Post sieht den E-Postbrief sogar in Konkurrenz zu den De-Mail Angeboten. Aus diesem Grunde hat sie den Unternehmen United Internet (z.B. 1&1, Web.de und GMX) und der Telekom als Anbietern für De-Mail Dienste die Nutzung des Dienstes Postident verweigert und bestehende Verträge zum 01.01.2011 gekündigt. Da dieses zur zweifelsfreien Identifikation eines Nutzers verwendete Verfahren in der heutigen Geschäftswelt als Standard gesehen wird und für reines Internetunternehmen wie United Internet keine Alternativen vorhanden sind, hat die «1&1» Internet AG gegen die Post Klage vor dem Landgericht Köln eingereicht. Das Verfahren beginnt am 23.12.2010 und dürfte interessant für die Zukunft von De-Mail sein.[55]

b) Telefonie über das Internet-Protokoll

Die ersten Übertragungen von Sprache über ein Datennetzwerk fanden bereits im Jahre 1973 im *Arpanet* statt. Auf Grund der fehlenden Übertragungskapazitäten und

[55] Beck-aktuell, becklink 1008080

den daraus resultierenden Störungen, Mängeln in der Übertragungsqualität und Verzögerungen konnte sich diese Technologie jedoch nicht von Beginn an durchsetzen. Bei der Internettelefonie ist, ebenso wie im PSTN, ein Signalisierungs- und ein Übertragungspfad notwendig. Großer Unterschied ist dabei die im Internet übliche paketvermittelte Übertragung der Datenpakete.

Das am häufigsten verwendete Protokoll für die Internettelefonie ist heute das *Session Initiation Protocol* (SIP). Es ähnelt im Aufbau seiner Adressen stark dem Verfahren der elektronischen Post[56]. Einziger Unterschied ist der vorangestellte Kenner "sip:". Der lokale Teil einer SIP-Adresse kann dabei aus einer beliebigen Zeichenfolge bestehen. Um aber den Übergang in das PSTN zu erleichtern und auf Grund der besseren Handhabbarkeit besteht dieser aber in der Regel aus einer Ziffernfolge, die von ihrem Aufbau einer Rufnummer im PSTN entspricht.

Wie bereits bei der elektronischen Post beschrieben, kann auch bei einer SIP Adresse die TLD ".de" nicht als eindeutige Identifikation für einen Teilnehmer aus Deutschland verwendet werden. Selbst eine Rufnummer mit dem vermeintlichen Landeskenner 49 im lokalen Teil der Adresse kann einen Anschluss im Ausland repräsentieren[57].

Der Aufbau einer VoIP Verbindung über SIP findet wie folgt statt. Nach Eingabe der Zieladresse durch den Anrufenden wird diese in Datenpakete verpackt und an einen SIP Gateway Server gesendet. Dieser Server kann an Hand der SIP Adresse über das DNS die IP-Adresse des Ziels ermitteln.

Im Anschluss baut der Gateway Server eine paketvermittelte Verbindung mit der SIP Anwendung des Angerufenen auf und teilt anschließend beiden Teilnehmern die IP-Adresse des Gegenübers mit. Die technischen Parameter der Gespräches, wie z.B. Bandbreite und verwendetes Sprachkompressionsverfahren, auch als Codec[58] bezeichnet, werden nach erfolgreichem Verbindungsaufbau durch das SIP mit Hilfe

---

[56] sip:zieladresse@gateway.de oder sip:00494012345667@hamburg.de

[57] Mozek/Zendt in Hoeren/Sieber, *Handbuch Multimedia-Recht,*Multimediarecht, Teil 23, Rd.Nr. 51

[58] **Codec** ist zusammengesetzt aus Coder und Decoder. Ein Codec dient dazu, die Größe digitaler Daten zu reduzieren. Ein bekanntes Beispiel ist das Verfahren MP3. Dieser Codec ermöglicht es, digitale Musikdateien auf einen Bruchteil der ursprünglichen Datenmenge zu reduzieren, ohne dass der Hörer einen Unterschied zum Original spürt. Eine CD mit normalen Musikdateien hat eine Laufzeit von 74min, eine CD mit MP3 Dateien kann, je nach Verfahren, eine Laufzeit von mehreren Stunden haben.
Auf die Übertragung von Sprache optimierte Codecs werden heute in modernen Kommunikationsnetzen eingesetzt. Bei ISDN ist es z.B. der Codec G.711 nach ITU-Standard mit einer Datenrate von 64.000 Bit/s. In modernen Mobilfunknetzen kommt der GSM Codec zum Einsatz. Dieser benötigt für die Übertragung von Sprache nur noch 13.000 Bit/s. In einem ISDN Kanal können somit 4 GSM Kanäle übertragen werden. Auch bei VoIP kommen viele verschieden Codecs zum Einsatz. Ohne die Verwendung eines passenden Decoders kann die digital übertragene Sprache nicht hörbar gemacht werden.

des eingebetteten *Session Description Protocol* (SDP) ausgehandelt. Sind sich beide Endgeräte über das technische Verfahren einig, werden die Inhaltsdaten des Gespräches über das *Real Time Protocol* (RTP) bezeichnetes Protokoll zwischen beiden ausgetauscht. Das SIP-Gateway spielt für diesen Vorgang keine Rolle mehr. Hier wird besonders deutlich, dass bei VoIP die Signalisierungs- und die Inhaltsdaten völlig unterschiedliche Wege nehmen können[59].

Bei VoIP ist es durch die Verwendung eines Gateway möglich, mit einem VoIP Endgerät sowohl Verbindungen zu anderen Teilnehmern mit einem VoIP Endgerät als auch in das öffentliche Telefonnetz und umgekehrt zu schalten. Bei dem Endgerät kann es sich dabei sowohl um einen PC mit VoIP fähiger Software als auch um ein herkömmliches Telefon mit VoIP Schnittstelle handeln. Entsprechende Geräte, die sich gleichzeitig mit dem PSTN und dem Internet verbinden lassen, sind bereits vielfach auf dem Markt verfügbar. Die Wahl des jeweiligen Netzes geschieht bei einem Anruf automatisch durch das Endgerät, abhängig von der gewählten (Ruf-) Nummer.

Die Schwierigkeit einer gesetzlichen Regelung liegt dabei in dem Umstand, dass eine Unterscheidung zwischen VoIP und öffentlicher Telefonie für den Nutzer teilweise nicht mehr möglich ist. Mittlerweile bieten viele Telekommunikationsunternehmen reine Internetanschlüsse an, bei denen ein herkömmliches Endgerät über VoIP an das öffentliche Telefonnetz angeschlossen ist. In Aussehen, Benutzung und Qualität unterscheidet sich ein solcher Anschluss nicht von einem herkömmlichen Telefon. Es ist daher unverständlich, warum das Gesetz hier eine Unterscheidung trifft. Dies wäre so, als ob der Gesetzgeber die analoge Telefonie und das ISDN in der Gesetzgebung unterschiedlich handhaben würde. Auch hier sind die Endgeräte gleich, die zugrunde liegende Technologie aber ist grundverschieden.

Die Vermischung der Netze und die Ähnlichkeit der Technologien PSTN und VoIP lässt sich an einem Beispiel zeigen. Bei großen Telefonanbietern ist es heute durchaus üblich, die Verbindungsstrecken zwischen großen Knotenpunkten über interne VoIP Verbindungen durch das Internet zu transportieren. Als Beispiel soll hier ein klassisches Telefonat von München nach Hamburg im Netz der TELEKOM gezeigt werden. Dabei wählt sich der Nutzer in München über seinen klassischen Telefonanschluss bei der Vermittlungsstelle ein und wird über das Telefonnetz weiter verbunden. In einem großen Knotenpunkt in München wird das Gespräch für den Transport

[59] Bär, MMR 4/2008, 215, 219

nach Hamburg auf eine Verbindungsstrecke geschaltet, die rein auf der VoIP Technologie basiert und durch das Internet führt. In dem Knotenpunkt in Hamburg werden die Daten wieder in das klassische Telefonnetz transferiert und über die Ortsvermittlung zum Telefonanschluss des Angerufenen geschaltet. Der Definition des TKG folgend würde es sich bei der Ziffernfolge für die Signalisierung in dem klassischen Telefonnetz um eine Rufnummer gem. § 3 Nr. 18 TKG handeln. Während des Transportes über die providerinterne VoIP Strecke wäre es aber temporär eine Nummer gem. §3 Nr. 13 TKG, da die Daten sich nicht mehr im öffentlichen Telefonnetz, sondern im Internet befinden. Diese Technologie soll im Rahmen der Einführung von NGN im Netz der TELEKOM bis 2012 das PSTN vollständig ablösen.

Zusammenfassend kann gesagt werden, dass sich die Verfahren zum Aufbau einer Kommunikationsverbindung im öffentlichen Telefonnetz und im Internet vom technischen Aufbau ähnlich sind, sich in der Wegewahl aber deutlich voneinander unterscheiden. Ist der Weg von Signalisierungs- und Nutzdaten im PSTN klar vorhersehbar, so können diese im Internet völlig unterschiedliche und dynamisch gewählte Wege gehen. Des Weiteren ist die Zuordnung einer Vorwahl zu einer Stadt oder einem Land im PSTN eindeutig, da es eine feste Zuordnung dieser Nummern zu physikalischen Anschlüssen gibt. Eine solche Zuordnung für Nummern existiert bei VoIP nicht. Daher kann die Identifikation eines Teilnehmers oder Nutzers erst in Verbindung mit einer IP-Adresse möglicherweise zum Erfolg führen.

Teil 3: Der Artikel 10 Grundgesetz

A Die Entstehung des Artikel 10 Grundgesetz

Der Schutz der Menschenwürde ist eine der zentralen Aufgaben des Grundgesetzes[60]. Um die sachgerechte Erfüllung dieser Aufgabe zu gewährleisten, haben die Väter des Grundgesetzes Vorschriften entwickelt, die eine freie Entfaltung des mündigen Bürgers innerhalb des demokratischen Staates ermöglichen. Die ist aber nur möglich, wenn das einzelne Individuum in der Lage ist, außerhalb des Zugriffs des Staates in seiner eigenen Privatsphäre zu denken, zu handeln und bei Bedarf mit anderen Individuen zu kommunizieren[61]. Gerade die Erfahrung aus der Zeit des 3. Reiches hat die Schöpfer des Grundgesetzes gelehrt, dass private Kommunikation eine der Säulen der persönlichen Meinungsentfaltung in einer Gesellschaft darstellt.
Dabei ist mit privat nicht nur der einzelne Bürger gemeint, sondern im Kontext der Kommunikation mehr ein geschlossener Kreis von Personen, die den Umfang und den Zugang zu dieser Gruppe selbst bestimmen können. Die innerhalb dieser Gruppe stattfindende Kommunikation ist in der Regel nicht für Dritte bestimmt. Im Gegensatz zur öffentlichen Kommunikation, deren Zielgruppe die breite Öffentlichkeit ist, bedarf die private Kommunikation eines differenzierteren Schutzes. Bei öffentlicher Kommunikation ist der Schwerpunkt eher bei der Freiheit der Meinungsäußerung zu setzen, die durch Art. 5 Abs. 1 GG gewährt wird.
Bei privater Kommunikation ist grundsätzlich von der Freiheit der Meinungsäußerung auszugehen, da jedes Individuum in seinem privaten Umfeld die Kommunikationspartner selbst bestimmen kann und somit nicht mit einer Unterdrückung seiner Meinung rechnen muss. In diesem Zusammenhang ist der notwendige Schutzzweck eines Gesetzes vielmehr die Zusicherung der Privatheit der Kommunikation. Der sich Äußernde muss sichergehen können, dass seine Kommunikation nur den von ihm ausgewählten Kommunikationspartnern bekannt wird und dem Zugriff von unberechtigten Dritten entzogen bleibt. Dieser Dritte können sowohl andere Individuen als auch juristische Personen, Organisationen oder aber auch der Staat mit seinen ausführenden Organen sein[62].

---

60 Art. 1 Abs.1 GG: "Die Würde des Menschen ist unantastbar"
61 Kindt, MMR 10/2009, 661, 666
62 Gusy in Mangoldt/Klein/Stark, Kommentar zum Grundgesetz, Bd. 1, 5. Aufl. 2005, 973, Rd.Nr. 14-17

War in früherer Zeit private Kommunikation auf Grund fehlender Möglichkeiten in der Regel auf einen Ort beschränkt, so änderte sich dieses grundsätzlich mit der Einführung des Postsystems im Heiligen Römischen Reich Deutscher Nation Mitte des 16. Jahrhunderts. Mit dem Kommunikationsmedium Brief war es den Menschen möglich, einem von ihnen ausgewählten Kommunikationspartner über die Distanz eine private Nachricht zukommen zu lassen und auch eine entsprechende Antwort zu erhalten. Auf Grund der Umstände fand diese Kommunikation nicht in Echtzeit statt, an dem Merkmal der Privatheit ändert dies aber nichts.
Zum Schutz dieser Privatsphäre wurden bereits in den Anfangsjahren gesetzliche Regelungen erlassen. Ein wichtiger Grundstein für das heute geltende Briefgeheimnis findet sich im § 142 in der Frankfurter Paulskirchenverfassung[63] von 1849. Dort heißt es bereits:

> *"Das Briefgeheimniß ist gewährleistet..."*[64].

Diese Vorschrift wurde im Laufe der Zeit auch als Postgeheimnis bezeichnet und sollte die Geheimhaltung von Sendungen durch die Post sicherstellen unabhängig davon, ob es sich um Briefe oder sonstige Sendungen handelt[65]. Neben dem Postgeheimnis wurde in den geänderten Vorschriften des Briefgeheimnisses zusätzlich der Schutz der Sendungen vor dem Zugriff durch Dritte, insbesondere durch die Staatsgewalt, geregelt.
Mit der Einführung der Telegraphie im 19. Jahrhundert war es erstmals möglich, Nachrichten über elektrische Leitungen nahezu in Echtzeit zu übertragen. Durch die Umwandlung der schriftlichen Nachricht in elektrische Signale wurde hier den Kommunikationsteilnehmern vollends die Kontrolle über die Verschwiegenheit der Nachricht entzogen. Konnte ein Brief noch verschlossen und gesiegelt werden, so war ein Schutz der Nachricht bei der Telegraphie für den Nutzer unmöglich geworden. Er musste diesen Schutz vollkommen in die Hände des betreibenden Unternehmens abgeben.
Um den Nutzer in seiner Privatsphäre trotzdem zu schützen, wurden die Vorschriften des Telegraphengeheimnisses geschaffen. Das Gesetz über das Telegraphenwesen vom 6. April 1892 enthält im § 8 folgende Formulierung:

---

63 Die Paulskirchenverfassung trat nie in Kraft, diente aber als Grundlage für spätere Verfassungen
64 Sievers, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, 1.Auflage 2003, 103
65 Gusy in Mangoldt/Klein/Stark, Kommentar zum Grundgesetz, Bd. 1, 5. Aufl. 2005, 973, Rd.Nr. 14-17

"Das Telegraphengeheimnis ist unverletzlich,..."[64]

Die Vorschriften des Post-, Brief- und Telegraphengeheimnisses wurden in der Weimarer Reichsverfassung im Jahre 1919 erstmals nebeneinander in einer Vorschrift geregelt. Ein Auszug aus § 117 WRV lautet:

"Das Briefgeheimnis sowie das Post- Telegraphen- und Fernsprechgeheimnis sind unverletzlich."

Diese Formulierung wurde durch die Väter des Grundgesetzes im Jahre 1949 nahezu unverändert übernommen. Art. 10 Abs. 1 GG lautet heute:

"Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich".

Diese knappe Vorschrift des Art. 10 G Abs. 1 GG ist eines der zentralen Schutzrechte des Grundgesetzes und dient als Freiheitsrecht, wie beschrieben, dem Schutz der Privatsphäre von Kommunikationsteilnehmern vor dem Zugriff des Staates.
Der zwangsweise Kontrollverlust durch die Übergabe der Verantwortung für die Privatheit der Kommunikation während der Übertragungsphase an den Kommunikationsdienstleister soll durch einen erhöhten gesetzlichen Schutz ausgeglichen werden[66]. Der hohe Rang des Grundrechts als Schutzrecht für die Garantie der Privatsphäre ist erkennbar an der engen Verknüpfung des Art. 10 GG mit den Art. 1,2 GG durch das BVerfG[67].

B Die Adressaten des Artikel 10 Grundgesetz

Für die spätere rechtliche Einordnung ist es notwendig zu prüfen, in wie weit staatliche Stellen durch das Grundgesetz gebunden sind und wem gegenüber der Schutzbereich des Art. 10 GG gilt. Die Adressaten des Art. 10 GG unterscheiden sich in Grundrechtsträger und Grundrechtsverpflichtete.

I. Grundrechtsverpflichtete

Als die Grundrechtsverpflichteten, d.h. solche gegenüber denen die Grundrechte als unmittelbar geltendes Recht wirken, werden in Art. 1 Abs. 3 GG die drei Säulen des

---

66 Gusy in Mangoldt/Klein/Stark, Kommentar zum Grundgesetz, Bd. 1, 5. Aufl. 2005, 980, Rd.Nr. 19
67 BVerfGE 27, 1ff., 344 ff.; 34, 205f.; 36, 41ff.

Staates, Legislative (Gesetzgebung), Judikative (Rechtsprechung) und Exekutive (vollziehende Gewalt) genannt. Natürliche oder juristische Personen sind nicht direkt Grundrechtsverpflichtete i.S.d. GG. Gegenüber diesen Gruppen gelten abgeleitete Gesetze, welche die Gedanken der Grundrechte in Rechtsvorschriften umsetzen.

II. Grundrechtsträger

Grundrechtsträger sind alle natürlichen Personen unabhängig von ihrem Alter, Mündigkeit oder ihrer Staatsangehörigkeit, wobei einige Grundrechte aber Deutschen vorbehalten sind[68]. Gem. Art. 19 Abs. 2 GG gilt der Grundrechtsschutz auch für inländische juristische Personen. Grundrechtsträger i.S.d. Art. 10 GG sind alle natürlichen Personen, da diese Vorschrift nicht, wie. z.B. Art. 8,9 GG Deutschen vorbehalten ist.

C Der Schutzbereich des Artikel 10 Grundgesetz

Wie bereits beschrieben, schaffen die modernen Mittel der Telekommunikation eine technische Möglichkeit des Austausches von Informationen unter Abwesenden. Damit einhergehend ist der zwangsweise Verlust der Privatheit, die bei der direkten Kommunikation von zwei oder mehreren Individuen unter deren Kontrolle liegt. Um die Zulässigkeit von Maßnahmen der strategischen Überwachung bewerten zu können ist es notwendig, den Schutzbereich des Art. 10 GG zu definieren.

I. Der räumliche Schutzbereich des Art. 10 GG

Für die räumliche Gültigkeit des Schutzbereiches des Fernmeldegeheimnisses ist es nicht von Bedeutung, ob die Kommunikation innerhalb des deutschen Staatsgebietes stattfindet. Vielmehr ist zu beurteilen, in wie weit staatliches Handeln im Inland mit einem Vorgang verknüpft ist[69]. Der Grundrechtsschutz erstreckt sich für die Grundrechtsträger auch über Staatsgrenzen hinweg. Bezogen auf das Handeln des *Bundesnachrichtendienstes* (BND) als deutsches Staatsorgan im Ausland vertritt das BVerfG dabei folgende Auffassung:

---

[68] Epping, Grundrechte, 63 Rd.Nr. 149
[69] Gysy/Hueck, NJ 1995, 461, 464

"Der räumliche Schutzumfang des Fernmeldegeheimnisses ist nicht auf das Inland beschränkt. Art. 10 GG kann vielmehr auch dann eingreifen, wenn eine im Ausland stattfindende Telekommunikation durch Erfassung und Auswertung im Inland hinreichend mit inländischem staatlichem Handeln verknüpft ist" [70]

Das Gericht hat mit seiner Argumentation den internationalen Wirkungsbereich des Fernmeldegeheimnisses als Schutzrecht betont[71], wenn eine hinreichende Verknüpfung mit dem Handeln deutscher Staatsgewalt, z.B. durch Erfassung und Auswertung ausländischer Telekommunikationsverkehre im Inland, gegeben ist. Die Aufhebung der Privatsphäre einer Kommunikation und des daraus resultierenden Schutzes ist nur dann möglich, wenn alle an ihr Beteiligten dem zustimmen[72]. Strittig ist in der Literatur die Frage, in wie weit der Schutzbereich des Art. 10 GG auch für Ausländer im Ausland gilt, wenn kein deutscher Staatsbürger an einem Kommunikationsvorgang beteiligt ist. Diese Entscheidung wurde durch das BVerfG bewusst offen gelassen[73].

II. Der zeitliche Schutzbereich des Art. 10 GG

Maßgeblich für die Eröffnung des Schutzbereiches gem. Art. 10 GG ist der Zeitpunkt des Kommunikation. Denn nur während der Übertragung stehen die Telekommunikationsdaten unter dem Schutz des Fernmeldegeheimnisses. Das BVerfG traf in einer Entscheidung vom 2.3.2006 folgende Festlegung für den Wirkungsbereich des Fernmeldegeheimnisses und machte diesen an den beiden Merkmalen "Abschluss des Übertragungsvorgangs" und "fehlende Beherrschbarkeit des Kommunikationsteilnehmers" fest[74]. Die Ausführungen über den Abschluss des Kommunikationsvorgangs lauten wie folgt:

> *" Wird der laufende Kommunikationsvorgang überwacht, liegt ein Eingriff in das Fernmeldegeheimnis auch dann vor, wenn die Erfassung des Nachrichteninhalts am Endgerät erfolgt. Die Einheitlichkeit des Übermittlungsvorgangs steht hier einer rein technisch definierten Abgrenzung entgegen (vgl. BVerfGE 106, 28 <38>). Ist die Nachrichtenübermittlung abgeschlossen, bestehen jedoch für die nunmehr bei den Teilnehmern gespeicherten Kommunikationsinhalte und -*

---

70 BVerfGE 100, 313, (313)
71 Krieger, Reichweite der Grundrechtsbindung, 10/2007
72 Gusy in Mangoldt/Klein/Stark, Kommentar zum Grundgesetz, Bd. 1, 5. Aufl. 2005, 990, Rd.Nr. 45
73 BVerfGE 100, 313, (364)
74 BVerfGE 115, 166-204

umstände nicht mehr dieselben spezifischen Risiken, wie sie sich aus der Nutzung einer Fernmeldeeinrichtung als Kommunikationsmedium ergeben."

Das Merkmal der "fehlenden Beherrschbarkeit" durch den Teilnehmer wird durch das Gericht wie folgt beschrieben:

"Art. 10 Abs. 1 GG soll einen Ausgleich für die technisch bedingte Einbuße an Privatheit schaffen und will den Gefahren begegnen, die sich aus dem Übermittlungsvorgang einschließlich der Einschaltung eines Dritten ergeben (vgl. BVerfGE 85, 386 <396>; 106, 28 <36>; 107, 299 <313>). Das Fernmeldegeheimnis knüpft an das Kommunikationsmedium an (vgl. BVerfGE 100, 313 <363>; Gusy, in: v. Mangoldt/Klein/Starck, Grundgesetz, 5. Aufl. <2005>, Art. 10 Rn. 32 und 40; Hermes, in: Dreier, Grundgesetz, 2. Aufl. <2004>, Art. 10 Rn. 25)."

Damit gilt, dass wenn sich die Kommunikationsdaten noch im Einflussbereich des Absenders, z.B. der Entwurf einer E-Mail auf einem lokalen Computer, oder bereits im Herrschaftsbereich des Empfängers, z.B. die von einem Server abgerufene und lokal gespeicherte E-Mail, unterliegen die Daten nicht dem Schutz des Fernmeldegeheimnisses, sondern gleichwohl dem besonderen Schutz durch das Recht auf informelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[75]. Fraglich ist in diesem Zusammenhang, in wie weit eine auf einem Mailserver gespeicherte E-Mail bereits dem Herrschaftsbereich des Empfängers zuzuordnen ist. Dabei ist entscheidend, ob diese Kommunikation bereits abgeschlossen ist und damit nicht mehr dem Schutz des Fernmeldgeheimnisses unterliegt oder aber, ob der Kommunikationsvorgang auf unbestimmte Zeit andauert, bis der Nutzer die Mail auf seinen Rechner kopiert und das Original löscht. Besonders bei den bereits beschriebenen IMAP Servern ist diese Frage in der Zukunft zu beantworten. Für Interessierte wird auf den Beschluss des BVerfG vom 16.06.2009, Az 2 BvR 902/06, verwiesen.

III. Der sachliche Schutzbereich des Art. 10 GG

Zu den durch Art. 10 GG geschützten Daten zählen sowohl die Inhalts- als auch die Verkehrsdaten[76]. Die nicht direkt mit der Kommunikation in Zusammenhand stehenden Bestandsdaten fallen nicht unter den Schutz.
Ob Standortdaten unter die Verkehrsdaten fallen ist unklar. In dem bereits genannten Beispiel der Übertragung im Signalisierungsprotokoll einer Thuraya Verbindung

[75] Eckhardt, DuD 30/2006, 365, 365
[76] Eckhardt, DuD 30/2006, 365, 366

dürfte diese Frage zu bejahen sein. Die anfallenden Standortdaten werden parallel zur Kommunikation übertragen und verarbeitet und stehen damit in unmittelbarem Zusammenhang mit dem Kommunikationsvorgang. Denn ohne die Standortdaten lässt das Netzwerk eine Kommunikationsverbindung nicht zu.

Anders ist es wiederum bei der mobilen Telefonie über das Global System for Mobile Communication (GSM) zu sehen. Hier werden im Signalisierungsprotokoll lediglich die Identifizierungsnummern der Basisstation übertragen, in dessen Sende- und Empfangsbereich sich das Mobiltelefon zum Zeitpunkt der Kommunikation befindet. Der Standort des Nutzers kann mit diesen Informationen nicht direkt festgestellt werden. Erst durch die Verknüpfung der Daten mit den Plänen der Provider, in denen die Standorte aller Basisstationen des Netzes verzeichnet sind, kann der Aufenthaltsort eines Nutzers bestimmt werden. In diesem Fall ist die Einordnung der Standortdaten als Verbindungsdaten eher zu verneinen. Allgemein existiert bei den Sicherheitsbehörden ein gesteigertes Interesse an den Standortdaten, da mit Hilfe dieser Informationen Bewegungsprofile von Zielpersonen erstellt werden können[77].

Der Schutz des Fernmeldegeheimnisses knüpft an die Art einer Übertragung und das dazu verwendete Medium an. Dabei ist es notwendig, dass die Kommunikation nicht direkt zwischen den Beteiligten, sondern in Abwesenheit über technischen Anlagen stattfindet und den Vorgaben für die Individualkommunikation entspricht. Als Transportmedien kommen dabei die Luft (z.B. GSM Telefonie, Satellitentelefon, Richtfunkverbindungen), aber auch elektrische und optische Leitungen in Frage[78].

Auf Grund der Konvergenz der Netze, d.h. Sprach- Daten- und öffentliche Massenkommunikation werden auf demselben Medium befördert, kann der Schutz des Fernmeldegeheimnisses nicht mehr für das gesamte Medium gelten. Vielmehr ist für eine Beurteilung zu prüfen, um welche Art der Kommunikation es sich im Einzelnen handelt. Dazu ist die Auswertung der Inhaltsdaten notwendig. Technisch wäre dies z.B. durch die Analyse der einzelnen IP-Pakete möglich, der sogenannten Deep Packet Inspection (DPI). Bei dieser Technik werden die Datenpakete bis auf Schicht 4 des bereits vorgestellten TCP-Referenzmodells analysiert, was technisch einer automatisierten Bewertung des Inhalts entspricht.

Rechtlich stellt sich hier sofort die Frage der Zulässigkeit[79]. Denn eine Auswertung des Inhaltes zur Prüfung des Schutzes gem. Art. 10 Abs. 1 GG würde die Kenntnis-

---

77 Garstka, NJ 10/2002, 524, 524

78 Gusy in Mangoldt/Klein/Stark, Kommentar zum Grundgesetz, Bd. 1, 5. Aufl. 2005, 985, Rd.Nr. 40

79 Bedner, 3

nahme und damit einen potentiellen Eingriff bereits voraussetzen und damit dem Zweck des Grundrechts entgegenlaufen[80]. Demnach gilt:

> *" Sofern ... wegen der technischen Gegebenheiten keine Abgrenzung möglich ist, ... muss für den Grundrechtsschutz des Art. 10 Abs. 1 die Möglichkeit genügen, dass mit einem solchen elektronischen Medium auch Individualkommunikation vermittelt wird."*[81]

Die Klassifizierung des Inhaltes einzelner Pakete durch die DPI im Rahmen einer Telekommunikationsüberwachung hätte somit bereits Eingriffscharakter und würde dem Schutzgedanken des Art. 10 GG widersprechen.

D Die Entstehung des Artikel-10 Gesetzes (G10)

In den 60er Jahren des letzten Jahrhunderts befindet sich die damals noch junge Bundesrepublik Deutschland in einer besonderen Bedrohungslage. Von außen droht die Gefahr des Einmarsches der Staaten des Warschauer Paktes, geführt durch die UdSSR und auch im Inneren ist die politische und gesellschaftliche Situation mehr als kritisch. Durch Studentenproteste und Demonstrationen, mit teilweise bürgerkriegsähnlichen Zuständen, sieht sich die Regierung gezwungen, im Jahre 1968 eine Notstandsgesetzgebung zu beschließen. Diese enthält unter anderem eine Neufassung des Art. 10 GG. Im neu geschaffenen Art. 10 Abs. 2 GG wird der Vorbehalt des förmlichen Gesetzes in die drei Schutzbereiche des Brief-, Post- und Fernmeldegeheimnisses geregelt[82].
Art. 10 Abs. 2 S. 2 GG wird als Ablösung für die alliierten Vorbehaltsrechte[83] in diesem Bereich ebenfalls im Rahmen der Notstandsgesetzgebung eingeführt[84]. Er enthält Regelungen über den Eingriff in das Grundrecht ohne Benachrichtigung der betroffenen Personen.

Mit dem am 13. August 1968 verabschiedeten Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses[85] werden die Verfassungsschutzbehörden des

---

80 Gusy in Mangoldt/Klein/Stark, Kommentar zum Grundgesetz, Bd. 1, 5. Aufl. 2005, 987, Rd.Nr. 42
81 Gusy in Mangoldt/Klein/Stark, Kommentar zum Grundgesetz, Bd. 1, 5. Aufl. 2005, 987, Rd.Nr. 44
82 Gusy in Mangoldt/Klein/Stark, Kommentar zum Grundgesetz, Bd. 1, 5. Aufl. 2005, 997, Rd.Nr. 65
83 Vorschriften zur Regelung der Beziehungen zwischen den 3 Besatzungsmächten der Westzone und der BRD nach dem 2. Weltkrieg
84 Arndt, NJW 3/1985, 107, 107
85 BGBl. 1968 I S. 949

Bundes und der Länder, das Amt für Sicherheit der Bundeswehr und der Bundesnachrichtendienst ermächtigt, das Brief-, Post- und Fernmeldegeheimnis zu verletzen, wenn dies "zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen" der Nato-Verbündeten erforderlich sein sollte.[86] Damit ist die in Art. 10 Abs. 1 S. 1 GG geforderte gesetzliche Regelung für einen zulässigen Eingriff in die Schutzrechte des Art. 10 GG geschaffen.

E Die Novellierungen des Artikel-10 Gesetzes

Die sich ändernden Herausforderungen im Bereich der Verbrechens- und Terrorismusbekämpfung machen eine regelmäßige Anpassung des G10 notwendig. Die wichtigsten Änderungen werden in den folgenden Abschnitten erläutert.

I. Das Verbrechensbekämpfungsgesetz

Im Rahmen des Verbrechensbekämpfungsgesetzes erfolgt die Erste grundlegende Anpassung des $G10_{1968}$ mit einer deutlichen Erweiterung der Ermächtigungen des Bundesnachrichtendienstes[87]. Der neu gestaltete § 3 Abs. 2 $G10_{1994}$ gestattet dem BND Einschränkungen für internationale nicht leitungsgebundene Fernmeldeverkehrsbeziehungen zu beantragen, wenn die Gefahr

1. eines bewaffneten Angriffs auf die Bundesrepublik Deutschland
2. der Begehung internationaler terroristischer Anschläge in der Bundesrepublik Deutschland
3. der internationalen Verbreitung von Kriegswaffen
4. der unbefugten Verbringung von Betäubungsmitteln in nicht geringer Menge aus dem Ausland in das Gebiet der Bundesrepublik Deutschland
5. im Ausland begangener Geldfälschungen
6. der Geldwäsche im Zusammenhang mit den in den Nummern 3 bis 5 genannten Handlungen

---

[86] Borowsky, Informationen zur politischen Bildung, Heft 258
[87] BGBl. 1994 I S. 3194

besteht und die Sammlung von Erkenntnissen notwendig ist, um diese Gefahren rechtzeitig zu erkennen und ihnen zu begegnen. Neu ist ebenfalls, dass für unter Punkt 1 subsumierbare Sachverhalte Beschränkungen auch für leitungsgebundene Fernmeldeverkehrsbeziehungen angeordnet werden dürfen. Die Anordnungen waren bis zu diesem Zeitpunkt auf nicht leitungsgebundene Verbindungen beschränkt.
In der Novellierung von 1994 ändern sich die Beschränkungen im Sinne des § 3 Abs.1 $G10_{1994}$ in der Hinsicht, dass die Möglichkeit der Verwendung von Suchbegriffen eingefügt wird. Diese Begriffe darf der Bundesnachrichtendienst zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich beantragen und dann für die strategische Erfassung verwenden. Voraussetzung ist, dass die Begriffe bestimmt und geeignet sind, Erkenntnisse über den angeordneten Sachverhalt zu gewinnen. Sie dürfen keine Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Fernmeldeanschlüsse führen[88]. Dies gilt nicht für Fernmeldeanschlüsse im Ausland, sofern ausgeschlossen werden kann, dass Anschlüsse deutscher Staatsangehöriger erfasst werden[89].
Die Suchbegriffe i.S.d. G10 lassen sich in zwei Kategorien unterscheiden.

a) Der formale Suchbegriff i.S.d. G10

Unter einem formalen Suchbegriff wird die Kennung eines Teilnehmeranschlusses verstanden. Dabei kann es sich z.B. um die Rufnummer eines Telefonanschlusses, aber auch um die Nummer eines sonstigen Telekommunikationsanschlusses handeln. Diese Informationen finden sich in der Regel innerhalb der Verkehrsdaten eines Kommunikationsvorgangs. Bei den formalen Suchbegriffen gibt es zwei mögliche Arten der Selektion:

(aa) Die positive Selektion

Bei der positiven Selektion werden die erfassten Signalisierungsdaten von Kommunikationsvorgängen mit einer Datenbank verglichen, in der die angeordneten formalen Suchbegriffe gespeichert sind. Erkennt die Maschine einen positiven Treffer, d.h. eine erfasste Nummer stimmt mit einem Eintrag in der Datenbank überein, wird der entsprechende Telekommunikationsvorgang aufgezeichnet und der weiteren Verarbeitung zugeführt.

---

[88] Arndt, NJW 3/1995, 169, 170
[89] § 3 G10 1994

(bb) Die negative Selektion

Die negative Selektion schließt Vorgänge von der Erfassung aus. Dabei werden ebenfalls alle erfassten Nummern automatisch mit einer Datenbank abgeglichen. Im Gegensatz zur positiven Selektion werden hier Treffer aber nicht aufgezeichnet sondern der gesamte Vorgang sofort verworfen. Somit kann z.B. sichergestellt werden, dass kein Telekommunikationsvorgang mit dem Landeskenner 49 für Deutschland aufgezeichnet wird.

b) Der inhaltliche Suchbegriff i.S.d. G10

Unter einem inhaltlichen Suchbegriff versteht man eine Zeichenfolge, die mit den Inhaltsdaten von Telekommunikationsvorgängen verglichen wird. Daher ist für die Suche mit inhaltlichen Suchbegriffen immer der gesamte Kommunikationsvorgang aufzuzeichnen und les- bzw. hörbar zu machen, um anschließend einen manuellen oder automatischen Abgleich mit den angeordneten Suchbegriffen durchführen zu können.
In der Sprachkommunikation ist die automatisierte Suche nach den gesprochenen Zeichenfolgen auf Grund der heute verfügbaren Technologie nur sehr eingeschränkt möglich. Für klar gesprochene Worte, die ohne Kompressionsverfahren übertragen werden, ist dieses für gängige Sprachen wie Deutsch oder Englisch durchaus in Teilen durchaus machbar. Sobald aber ein Sprachkompressionsverfahren eingesetzt wird oder es sich um eine komplexe Fremdsprache wie z.B. Arabisch oder Chinesisch handelt, ist eine automatisierte Erkennung von gesprochenen Zeichenfolgen nahezu unmöglich.
Auch die manuelle Suche durch einen Bearbeiter ist bei Verwendung eines Codec erst nach der Decodierung möglich, da die digitale Sprache ansonsten nicht hörbar gemacht werden kann. Für die Decodierung ist es technisch notwendig, einen großen Teil der Übertragenen Informationen aufzuzeichnen.
Bei Verfahren wie z.B. der Telefax-Übertragung kann eine automatischer Abgleich erst nach der vollständigen Erfassung erfolgen, da ein Telefax als Bild und nicht als Text übertragen wird. Die Umwandlung des Bildes in Text mit einer sogenannten Optical Character Recognition (OCR) Software ermöglicht dann eine automatisierte Suche nach Zeichenfolgen in einer Übertragung.
Die automatisierte Suche in einer E-Mail stellt sich deutlich einfacher dar, da eine solche Nachricht bereits als Text übertragen wird. Für diese Suche ist trotzdem eine

nahezu vollständige Aufzeichnung notwendig, da auf Grund der paketvermittelten Übertragung zuerst einmal alle Pakte in der korrekten Reihenfolge zusammengesetzt werden müssen, um die Nachricht lesbar zu machen.

Bei der Verwendung sowohl von formalen als auch von inhaltlichen Suchbegriffen kann technisch mit sogenannten Wildcards[90] gearbeitet werden. Dabei werden ein oder mehrere Zeichen in den Suchbegriffen durch sogenannten Platzhalter repräsentiert. Bei der Verwendung der Ziffernfolge mit den Ziffern 004940 und dem angehängten Platzhalter *, der eine beliebige weitere Anzahl an Ziffern darstellt, als formalen Suchbegriff, könnten z.B. alle Telefonnummern der Hansestadt Hamburg erfasst werden.
Gleiches gilt bei inhaltlichen Suchbegriffen. Der Platzhalter kann dabei ebenfalls ein oder mehrere beliebige Zeichen repräsentieren. Wird z.B. das Zeichen * als Wildcard in der Form Bundes*gericht als inhaltlicher Suchbegriff verwendet, werden als Ergebnisse unter anderem die Begriffe Bundes*verfassungs*gericht, Bundes*verwaltungs*gericht, Bundes*arbeits*gericht, Bundes*sozial*gericht und Bundes*patent*gericht angezeigt.

II. Das Urteil des BVerfG zur Telekommunikationsüberwachung

Im Jahre 1999 sorgt ein Urteil des BVerfG für eine Neuausrichtung der zulässigen Einschränkungen des Fernmeldegeheimnisses. Nach der Klage deutscher und ausländischer Staatsbürger gegen die Befugnisse des Bundesnachrichtendienstes gem. § 3 Abs. 1 S. 2 G10 stellt das BVerfG fest, dass § 3 Abs. 1 S. 1, S. 2 Nr. 5, Abs. 3, Abs. 4, Abs. 5 S. 1, Abs. 7 S. 1, Abs. 8 S. 2 G10 sowie § 9 Abs. 2 S. 3 G10 in der Fassung des $G10_{1994}$ mit Art. 10 GG unvereinbar sind[91]. Das Gericht gibt dem Gesetzgeber auf, das Gesetz bis zum 30.06.2001 in einer verfassungsgemäßen Version zu verabschieden.

Mit Art. 1 des Gesetzes zur Neuregelung von Beschränkungen des Brief-, Post und Fernmeldegeheimnisses vom 26. Juni 2001[92] ist die vorgegebene Frist eingehalten und das G10 grundlegend geändert. Die Änderungen, die vor allem die Pflichten der

---

90 Ein Begriff aus der Informatik, der einen Platzhalter in einer beliebigen Zeichenfolge bezeichnet. Der Platzhalter kann dabei ein oder mehrere beliebige Zeichen repräsentieren.
91 BVerfGE 100, 313 - Telekommunikationsüberwachung I
92 BGBl. I, 1254, 2298

beteiligten Behörden beim Umgang mit personenbezogenen Daten[93] umfassen gehen so weit, dass das bisher gültige $G10_{1994}$ aufgehoben und durch eine neue Version ersetzt wird.

Eine weitere wichtige Änderung im Bereich der strategischen Erfassung durch den BND ist die Erweiterung der Möglichkeiten im Bereich des Übertragungsmediums, da im $G10_{1994}$ die strategische Erfassung rein auf nicht leitungsgebundene Übertragungsstrecken beschränkt ist. Begründet durch die grundlegende Änderung der Telekommunikationsnetze, ausgelöst durch die Digitalisierung und der damit verbundenen Verlegung von digitalen Glasfaserleitungen rund um den Globus, waren plötzlich die Kosten für die Übertragungsmedien Richtfunk und Satellit deutlich höher, als bei der leitungsgebundenen Kommunikation. Auch der Anstieg der Kommunikationsmenge, durch das Aufkommen der paketvermittelten Übertragung von Daten, kann durch die alleinige Verwendung nicht leitungsgebundener Netze nicht bewältigt werden. Um dem BND die in die digitalen Glasfasernetze abgewanderten Strecken trotzdem zu erhalten und in der Folge noch sinnvolle Ergebnisse aus der strategischen Erfassung zu bekommen, ist, gemäß Begründung, eine Neufassung der die Einschränkung auf internationale nicht leitungsgebundene Fernmeldeverkehrsbeziehungen aus § 3 Abs. 1 S.1 $G10_{1994}$ im § 5 Abs. 1 S.1 $G10_{2001}$ notwendig und auf internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, auszudehnen[94].

III. Erstes Gesetz zur Änderung des G10

Die Erfahrungen aus der Novellierung des G10 Gesetzes müssen, gemäß eines Beschlusses des Bundestages vom 11.05.2001, dem Plenum zwei Jahre nach der Verabschiedung des Gesetzes durch die Bundesregierung vorgelegt werden. Diese Vorgabe erfüllt der am 12.11.2003 vorgelegte "Bericht der Bundesregierung über die Erfahrungen mit dem Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses"[95].

Innerhalb dieses Berichtes kommt die Regierung zu der Auffassung, dass die Anpassungen des G10 nicht in allen Bereichen ausreichend sind und die Befugnisse des BND vor allem in den Bereichen Proliferation und organisierten Schleusung Lücken aufweisen. Vor allem die fehlende Möglichkeit der Erfassung von Telekom-

---

93 BT-Drucks 14/5655, 1
94 BT-Drucks 14/5655, 17
95 siehe BT-Drucks 15/2042

munikationsanlagen auf deutschen Handelsschiffen steht dabei in der Kritik, denn diese sind häufig an der Ausfuhr und dem Transport von "Dual-Use"[96] Gütern beteiligt. Die Möglichkeit der Erfassung ist aber weder im Katalog des § 3 Abs. 1 S. 1 $G10_{2001}$ vorhanden noch auf Grundlage des § 5 $G10_{2001}$ zulässig[97].

Nach den Erfahrungen aus der Geiselnahme der deutschen Familie Wallert auf den Philippinen im Jahre 2000 und weiteren Entführungen deutscher Staatsbürger, z.B. im Irak oder Jemen, stellt die Bundesregierung weiterhin fest, dass dem BND im Falle einer Entführung deutscher Staatsbürger die rechtlichen Rahmenbedingungen fehlen, um eine strategische Erfassung im Umfeld der Geiseln durchzuführen[98]. Auch wenn diese über ein eigenes Mobiltelefon verfügen, ist die Aufnahme der Rufnummer in die strategische Erfassung aufgrund des Verbotes der Verwendung inländischer Rufnummern als formalen Suchbegriff gem. § 5 Abs. 2 S. 2 $G10_{2001}$ unzulässig. Es wird die Empfehlung ausgesprochen, das G10 um entsprechende Vorschriften zu erweitern, die ein Handeln des BND im Falle einer Entführung und bei Gefahr für Leib und Leben der Betroffenen ermöglichen[99].

Auch die Möglichkeiten der Überwachung von Mobilfunkendgeräten sind gemäß Bericht unzureichend. Dies liegt vor allem daran, dass angeordnete Rufnummern der Individualüberwachung auf Grund des regelmäßigen Austausches der SIM[100]-Karte nur für kurze Zeit durch die Zielperson genutzt und dann sehr schnell unbrauchbar werden. Daher scheint die Erweiterung des G10 um die Möglichkeit zur Erfassung der gerätespezifischen Merkmale notwendig[101].

Um die Empfehlungen dieses Berichtes umzusetzen, wird am 02.02.2006 der Entwurf eines ersten Gesetzes zur Änderung des Artikel-10 Gesetzes vorgelegt[102]. Ziel des Entwurfes ist es, dem BND erweiterte Befugnisse im Rahmen der strategischen Telekommunikationsüberwachung einzuräumen[103]. Der Vorschlag lautet, die Aufklärungsfähigkeiten des Dienstes durch eine Anpassung des § 3 Abs. 1 G10 in den Bereichen Proliferation und internationaler Waffenhandel dadurch zu erweitern, dass der BND auch die Befugnis zur Beantragung einer Individualüberwachung der

---

96 Güter mit doppeltem Verwendungszweck gem. Kap. 1 Art. 2 Nr. 1 Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009

97 BT-Drucks 15/2042, 10, B II Nr. 1

98 BT-Drucks 15/2042, 12, B II Nr. 4

99 Schafranek, DöV 20/2002, 846, 849

100 Subscriber Identity Module - herausnehmbare Chipkarte in Mobiltelefonen, die Informationen zur Nutzeridentifikation in Mobilfunknetzen enthält

101 BT-Drucks 15/2042, S. 13, B II Nr. 5

102 BT-Drucks 16/509

103 BT-Drucks 16/509, S. 1, B

Telekommunikationseinrichtungen an Bord deutscher Hochseeschiffe erhält. Dabei dürfte es sich in der Regel um die Erfassung von Satellitentelefonen wie z.B. Inmarsat[104] oder Thuraya handeln.

Auch sollen die Befugnisse zur strategischen Telekommunikationsüberwachung durch die Einführung eines neuen Gefahren- und Beobachtungsbereiches "illegale Schleusung" erweitert werden.

Die Verfasser des Berichtes schlagen ebenfalls vor, eine umfassende Erweiterung der gesetzliche Grundlage für die Weitergabe der aus der strategischen Erfassung des BND gewonnenen Kenntnisse an ausländische Stellen die mit nachrichtendienstlichen Aufgaben betraut sind, durchzuführen. Zu diesem Zweck soll ein neu geschaffener § 7a G10 in den Gesetzentwurf eingebracht werden. Die Erweiterung beschränkt sich auf die Bereiche "internationaler Terrorismus", "Proliferation" und den neu eingeführten Gefahrenbereich "illegale Schleusung"[105]. Dabei ist zu beachten, dass laut Bericht im Ausland die Trennung von Polizei und Nachrichtendiensten nicht üblich ist. Diese existiert in Deutschland seit Ende des 2. Weltkriegs. Mit dem „Polizeibrief" der Alliierten wurde die so genannte Funktionentrennung eingeführt, die sich später in Art. 87 Abs. 1 S.2 GG fortsetzt[106].

Die vorgeschlagene Erweiterung des G10 ermöglicht die Weitergabe der Ergebnisse an Stellen im Ausland, die sowohl polizeiliche als auch nachrichtendienstliche Tätigkeiten wahrnehmen. Fraglich ist nun, in wie weit das in Deutschland gültige Trennungsgebot durch diese Regelung aufgeweicht wird, wenn der BND befugt ist, Informationen aus seiner strategischen Erfassung an entsprechende ausländische Regierungsstellen weiterzugeben.

Der Entwurf des § 7a Abs. 1 Nr. 2 G10 sieht zwar vor, dass die Übermittlung der Daten den überwiegend schutzwürdigen Interessen des Betroffenen nicht entgegenstehen darf, eine Prüfung in wie weit diese Vorgaben im Ausland eingehalten werden stellt sich gerade im nachrichtendienstlichen, durch strikte Geheimhaltung geprägten, Bereich zwischen den Staaten als äußerst schwierig dar. Fraglich ist dies auch vor dem Hintergrund, da die Weitergabe von personenbezogene Daten an mit polizeilichen Aufgaben betrauten Behörden in Deutschland gem. § 7 Abs. 4 $G10_{2001}$ bereits umstritten ist[107].

---

[104] Diensteanbieter für Sprach- und Datenübertragung mit mobilen Endgeräten über Satellit. www.inmarsat.com

[105] BT-Drucks 16/509, S. 10, B zu Nummer 7

[106] Roggan, Bergemann: NJW 2007, 876, 876

[107] Schafranek, DöV 20/2002, 846, 851

Als Beispiel für mögliche Konsequenzen sei hier nur die fiktive Möglichkeit der gezielten Tötung von Verdächtigen durch die *Central Intelligence Agency* (CIA) auf Grund von Informationen aus der strategischen Erfassung des BND in Deutschland genannt. Dieses Szenario dürfte den BND Untersuchungsausschuss zum Irak-Krieg in seiner politischen Wirkung deutlich übertreffen. Ob die Auswirkungen dieser Vorschriften vom Gesetzgeber bis ins Detail durchdacht wurden ist daher mehr als fraglich.

Auch der Entwurf zur Zulassung der gerätenummernbezogenen Überwachung für die Individualüberwachung der Telekommunikation für alle Nachrichtendienste stellt eine grundlegende Erweiterung dar[108]. Er sieht vor den Nachrichtendiensten zu gestatten, zu den bisherigen formalen Suchbegriffen wie der Rufnummer eines Telekommunikationsanschlusses auch die *International Mobile Equipment Identifier (*IMEI)[109] als Gerätekennung eines Mobiltelefons oder die auf dem *Subscriber Identifier Module* (SIM-Karte) gespeicherte *International Mobile Subscriber Identifier* (IMSI)[110] hinzuzufügen.

Begründet wurde diese Ergänzung mit den Schwierigkeiten bei der Erfassung eines Mobilfunknutzers, wenn dieser regelmäßig die SIM-Karte seines Mobiltelefons und damit auch die Rufnummer wechselt. Eine in Kreisen des internationalen Terrorismus oder der organisierten Kriminalität durchaus beliebte Vorgehensweise zur Verschleierung der eigenen Kommunikation. Dabei werden vor allem sogenannten Pre-Paid[111] Karten verwendet, die auf dem Schwarzmarkt ohne Verknüpfung zu einem Teilnehmer erworben werden können. Der einzige technische Parameter der bei einem Wechsel der SIM-Karte konstant bleibt, ist die IMEI des Endgerätes. Diese wird bei der Anmeldung eines Endgerätes GSM im Netz innerhalb des Signalisierungskanals übertragen und kann somit als formaler Suchbegriff zur strategischen Überwachung verwendet werden.

Wird nur das Endgerät ausgetauscht, kann der Teilnehmer über die Auswertung der IMSI weiter eindeutig identifiziert werden. Erst bei einem Wechsel von Endgerät und SIM-Karte ist eine Identifizierung anhand technischer Daten nicht mehr machbar.

---

[108] BT-Drucks 16/509, S. 11, B zu Nummer 8

[109] Eindeutige 15-stellige Seriennummer mit der ein Endgerät im GSM Netz eindeutig identifiziert werden kann.

[110] 15-stelliger Code der zur eindeutigen Identifikation eines Nutzers im GSM Netz verwendet wird. Die IMSI setzt sich zusammen aus dem 3-stelligen Mobile Country Code (z.B. 262 für Deutschland), dem Mobile Network Code (z.B. 01 für T-Mobile) und der zehnstelligen Mobile Subscriber Identification Number, mit der ein Nutzer eindeutig im Netz identifiziert werden kann.

[111] Karten die zur Nutzung eines GSM-Netzwerkes berechtigen und über ein im Voraus bezahltes Guthaben verfügen

Der Gesetzentwurf des "Ersten Gesetzes zur Änderung des Artikel 10-Gesetzes" vom 02.02.2006 wird am 25.03.2009 vom Bundestag mit den Stimmen der CDU und der SPD in geänderter Fassung angenommen und tritt mit der Veröffentlichung im Bundesgesetzblatt[112] am 31.07.2009 in Kraft[113].
Bis heute sind keine weiteren Änderungen an dem Gesetz beschlossen worden.

F Strategische Erfassung des BND im Sinne des G10

Die Maßnahmen des Artikel 10-Gesetzes unterscheiden sich grundsätzlich in zwei verschiedene Arten der Erfassung. Der erste Teil sind Individualmaßnahmen gem. §3 G10, d.h. es wird die Überwachung einzelner festgelegter Individuen von den Sicherheitsbehörden beantragt und über eine Einzel- oder Individualbeschränkung durch das Bundesministerium des Inneren genehmigt. Diese Überwachungsmaßnahmen dienen der Erkundung im strafrechtlichen Vorfeld, d.h. sie unterstützen Ermittlungen der in §3 G10 abschließend aufgeführten Katalogstraftaten.
Die strategische Erfassung zielt gerade nicht auf die Überwachung einzelner Individuen sondern verfolgt vielmehr den Zweck der Prävention hinsichtlich im Gesetz vorgeschriebener Sachverhalte. Darf die Überwachung mit Einzelmaßnahmen noch durch verschiedene Sicherheitsbehörden beantragt werden, ist die strategische Überwachung rein dem Bundesnachrichtendienst vorbehalten.
Im Zuge einer strategischen Überwachung darf gem. §5 Abs. 1 G10 die Überwachung internationaler Telekommunikationsleitungen angeordnet werden, soweit diese im Bündel übertragen werden. Da in den modernen Telekommunikationsnetzen auf Grund der digitalen Übertragung über die SDH in der Regel eine Bündelung vorliegt, dürfte diese Voraussetzung immer vorliegen und bedeutet keine wirkliche Einschränkung mehr. Hier kann man sehen, dass der aktuelle Text des Gesetzes nicht mehr der technischen Wirklichkeit entspricht.
Die zu überwachenden Telekommunikationsbündel dürfen nach einer Anordnung durch das BMI und der Freigabe durch das Parlamentarische Kontrollgremium erfasst werden. Eine solche Anordnung hat in der Regel eine Gültigkeit von 3 Monaten und bezieht sich auf festgelegte physikalische Leitungen. Auch diese Regelung stammt noch aus Zeiten der Analogtechnik, wo es immer festgelegte Leitungen in eine Region der Welt gab. Durch die gewonnene Flexibilität im Rahmen der Digital-

[112] BGBl I 2009, S. 2499
[113] Huber, NVwZ 21/2009, 1321, 1323

technik ist diese Vorgehensweise mittlerweile ihrer Wirkung enthoben, da moderne Verfahren Netze dynamisch konfigurieren und keine Rücksicht mehr auf Leitungswege oder sogar Netzgrenzen nehmen.
Eine solche Anordnung müsste daher fast stündlich erfolgen um dem Zweck des Gesetzes dienen zu können und nur vorgegebene Verkehre zu erfassen.
Zweckmäßiger wäre es hier, Adressräume anzuordnen, die einer zu überwachenden Region zugeordnet werden können. Dabei könnte es sich um Vorwahlen, IP Adressbereiche, Domain Teilen von Mailadressen oder Rufnummernbereiche von VoIP handeln. Eine Anpassung des Gesetzes an die aktuellen Entwicklungen scheint hier mehr als notwendig.
Die angeordneten Kommunikationsbündel darf der Bundesnachrichtendienst erfassen und mit Hilfe von vorher angeordneten Suchbegriffen relevante Verkehre herausfiltern. Dabei darf der BND gem. § 5 Abs. 2 G10 nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Er darf keine Suchbegriffe verwenden werden, die Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen oder den Kernbereich der privaten Lebensgestaltung betreffen. Fraglich bleibt nun, in wie weit z.B. Telefonnummern oder Adressen des Internet Protokolls für die Verwendung als formaler Suchbegriff im Rahmen der strategischen Erfassung des BND gem. § 5 G10 geeignet sind.

Teil 4: Prüfung der Eignung

In diesem Kapitel soll nun die Eignung der Suchbegriffe geprüft werden. Für diese Bewertung ist es zunächst notwendig, bereits verwendete formale Suchbegriffe, wie die Rufnummer eines Telekommunikationsanschlusses im öffentlichen Telefonnetz, auf ihre Eignung hin zu untersuchen und die praktische Umsetzung zu betrachten. Anschließend sollen in einem nächsten Schritt die in der Neuregelung des G10 aus dem Jahre 2009 hinzugefügten eindeutigen technischen Merkmale eines Endgerätes zur Mobilkommunikation beurteilt werden. In einer anschließenden Betrachtung muss dann eine allgemeine Bewertung der Eignung der Adressen des Internet-Protokolls als formaler Suchbegriff stattfinden. Dabei ist besonders auf die möglichen Unterschiede bei statischen und dynamischen IP-Adressen einzugehen. Abschließend folgt die Übertragung der gewonnenen Erkenntnisse auf zwei Kommunikationsanwendungen, die Informationen auf Basis des Internet-Protokolls austauschen. Dabei handelt es sich um die Telefonie über das Internet Protokoll und die elektronische Post. Bei letzterer wird noch einmal explizit auf die neu geschaffenen Angebote De-Mail und E-Postbrief und die daraus resultierenden Besonderheiten eingegangen.

A Generelle Eignung eines Suchbegriffs

Bei der automatischen Auswertung von Telekommunikationsbündeln kommen viele verschiedene Identifizierungsmerkmale in Frage. Hauptsächlich lassen sich diese Merkmale in zwei Gruppen unterscheiden. Die erste Gruppe sind Suchbegriffe aus den Metadaten einer Kommunikationsbeziehung, d.h. Verkehrsdaten oder Standortdaten. Diese Daten lassen sich sehr leicht automatisch mit Datenbanken bestehend aus verschiedenen Suchbegriffen abgleichen, da sie alle digital übertragen werden und somit maschinenlesbar sind.
Die Gefahr, dass Suchbegriffe aus dieser Gruppe zur Identifizierung eines einzelnen Teilnehmers verwendet werden können ist groß. Denn Verkehrsdaten dienen oft dem Verbindungsaufbau oder der Abrechnung von Telekommunikationsdienstleistungen und müssen daher ohne großen Aufwand durch den Telekommunikationsanbieter mit den Bestandsdaten verknüpft werden können. Ob ein Datum die Voraussetzungen für die Identifikation eines Individuellen Teilnehmers grundsätzlich erfüllt und damit gem. §5 Abs. 2 Nr. 1 G10 für die Verwendung als Suchbegriff unzulässig ist, muss für jeden Typ von Verkehrsdaten gesondert geprüft werden.

Die zweite Gruppe der Suchbegriffe kommt aus dem Bereich der Inhaltsdaten, d.h. die Inhalte einer Kommunikationsbeziehung werden mit Suchbegriffen aus einer Datenbank verglichen. Dabei kann es sich im einfachen Bereich um den Abgleich von Zeichenfolgen handeln, z.B. bei E-Mail oder SMS Verkehren. Hier werden die Inhaltsdaten, analog zur Übertragung der Verkehrsdaten digital übertragen und sind somit ebenfalls maschinenlesbar.
Komplizierter wird es bei der Erkennung von Landessprachen und Sprachmustern. Die Zahl der möglichen Betonungen eines gesprochenen Wortes und die Varianz in der Stimmmelodie verschiedener Sprecher ist so unendlich groß, dass ein einfacher digitaler Abgleich kein brauchbares Ergebnis liefert. Wie weit die Technik bei den Nachrichtendiensten hier fortgeschritten ist lässt sich jedoch an Hand der frei verfügbaren Literatur nur schwer beurteilen.
Die Suchbegriffe für den Bereich der Inhaltsdaten können mit hoher Wahrscheinlichkeit nicht für die Identifikation eines individuellen Teilnehmers genutzt werden. Hier ist es wahrscheinlicher, dass sie den Kernbereich der privaten Lebensgestaltung betreffen können und damit gem. §5 Abs. 2 Nr. 2 G10 unzulässig sind.
Diese Studie beschäftigt sich mit der Verwendung von Suchbegriffen die der ersten Gruppe der Verkehrsdaten entstammen. Auf die zweite Gruppe soll innerhalb dieses Buches nicht eingegangen werden, da die private Lebensgestaltung oft Freiraum für eine Auslegung des Sachverhalts eröffnet.

B Rufnummern im PSTN

Ein Teilnehmeranschluss im öffentlichen Telefonnetz ist auf Grund der festen Zuordnung einer Rufnummer ein bestimmter Telekommunikationsanschluss i.S.d. §5 Abs. 2 G10. Nach dieser Vorschrift dürfen die für die strategische Erfassung des BND eingesetzten Suchbegriffe keine Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung solcher bestimmter Telekommunikationsanschlüsse im Inland führen[114]. Die Relevanz der Vorschrift wurde in einem Urteil durch das BVerwG wie folgt dargestellt[115]:

"Besonders wichtig sei das gesetzliche Verbot der gezielten Überwachung bestimmter individueller Telefonanschlüsse. Der der strategischen Telefonüberwachung zu

[114] Soiné, DöV 5/2006, 204, 209
[115] BVerwG, *Urteil* vom 23. 1. 2008 - 6 A 1/07, Rd.Nr. 35

Grunde liegende besondere Zweck der Auslandsaufklärung, die nicht auf Maßnahmen gegenüber bestimmten Personen abziele, sondern internationale Gefahrenlagen betreffe, über die die Bundesregierung unterrichtet werden solle, rechtfertige es, die Eingriffsvoraussetzungen niedriger anzusetzen als im Polizei- und Strafprozessrecht."

Die Verwendung von Rufnummern ausländischer Anschlüsse ist jedoch gem. § 5 Abs. 2 G10 zulässig, wenn diese nicht deutschen Staatsangehörigen gehören oder von Gesellschaften mit Sitz im Ausland betrieben werden, die überwiegend in deutschem Besitz sind, sich unter tatsächlicher Kontrolle deutscher natürlicher oder juristischer Personen befinden oder wenn die Vertretungsberechtigten mehrheitlich deutsche Staatsangehörige sind. Durch den Landeskenner 49 ist in der Regel eine eindeutige Zuordnung einer Rufnummer zum Staatsgebiet der Bundesrepublik Deutschland möglich und somit zweifelsfrei der Schutzbereich des Art. 10 GG eröffnet. Ausreichend für den Schutz ist dabei, dass entweder Quell- oder Zielrufnummer mit dem Landeskenner versehen ist.
Fraglich ist, ob bei der alleinigen Verwendung des Landeskenners 49 in einem formalen Suchbegriff bereits eine gezielte Überwachung eines bestimmten Telekommunikationsanschlusses in der strategischen Erfassung gem. § 5 Abs. 2 Nr. 1 G10 gegeben ist. Die Nutzung von Wildcards würde in diesem Fall die Erfassung aller deutschen Verkehre (z.B. 0049*) oder aber aller Verkehre einer Region (z.B. 004940* für Hamburg) ermöglichen. Durch die hierdurch entstehende Unschärfe würde eine Vielzahl von Anschlüssen überwacht und es läge keine Erfassung eines bestimmten Telekommunikationsanschlusses vor.
Diese Vorgehensweise würde aber dem Sinn des Gesetzes widersprechen. Ziel der Vorschrift ist es, den individuellen Nutzer vor einer gezielten Überwachung durch den BND zu schützen. Könnten die Sicherheitsbehörden die Regelungen des G10 und den Schutz des Art. 10 GG mit Einbringen einer gewissen Unschärfe, z.B. durch die Nutzung von Wildcards, erreichen, wären die o.g. Vorschriften wirkungslos und ihr Zweck verfehlt. Somit kann auf Grund der hohen Bedeutung des Art. 10 GG als Freiheitsrecht die Verwendung einer Rufnummer mit der Landeskennzahl 49 als formaler Suchbegriff nicht zulässig sein.

I. Schlussfolgerung

Im Ergebnis kann gesagt werden, dass die Verwendung von Rufnummern mit dem Landeskenner 49 als formaler Suchbegriff im Rahmen einer strategischen Erfassung des BND generell unzulässig ist. Rufnummern mit ausländischen Landeskennern dagegen sind zulässig, wenn diese die Kriterien des § 5 Abs. 2 G10 erfüllen.
Diese Vorgabe kann durch eine rein technische Prüfung nur sehr bedingt umgesetzt werden. Denn der verwendete Landeskenner für diese Gespräche ist immer eindeutig dem Ausland zuzuordnen. Auch die Erkennung der Art und Bedeutung von Sprache durch Automaten ist mit dem heutigen Stand der Technik auf Grund der Vielfalt und Unterschiedlichkeit der menschlichen Ausdrucksweise nicht realistisch[116]. Zusätzlich scheint dieses Kriterium zu oberflächlich, da nicht sichergestellt ist, dass nur weil die deutsche Sprache verwendet wird, auch deutsche Staatsangehörige beteiligt sind. Ein Gespräch zwischen zwei österreichischen Staatsbürgern, das im Ausland erfasst wird, erfüllt dieses Kriterium ebenfalls vollständig, ist aber nicht durch Art. 10 GG geschützt[117].
Demnach scheint im Falle einer Rufnummer aus dem Ausland nur die manuelle Auswertung durch einen Bearbeiter des BND praktikabel, der nach eingehender Prüfung eine Erfassung nach ihrer Zugehörigkeit bewertet und im Zweifel rückstandsfrei löscht[118]. Eine weitere Möglichkeit zur Verhinderung von unzulässigen Erfassungen wäre das Erstellen einer sogenannten Blacklist[119], d.h. einer Datenbank, in der alle ausländischen Rufnummern registriert werden, die auf Grund ihrer Verwendung durch deutsche Staatsbürger nicht als formale Suchbegriffe verwendet werden dürfen. Somit kann sichergestellt werden, dass Telekommunikationsvorgänge mit den beschriebenen Merkmalen noch nicht einmal in die erste Stufe der generellen Erfassung[120], der sogenannten Zwischenspeicherung, gelangen. Dieses Verfahren ist aber auf Grund seiner hohen Fehleranfälligkeit abzulehnen.
Bei einem positiven Treffer auf eine ausländische Rufnummer ist auf Grund der gesetzlichen Regelung in einer zweiten Stufe automatisiert durch eine Negativselektion zu prüfen, ob die zweite beteiligte Rufnummer des Kommunikationsvorgangs

---

[116] Kleinschmidt, Robust speech recognition based on spectro-temporal processing, 1
[117] BVerfGE 100, 313 (319)
[118] vgl. §6 Abs.1 G10
[119] Negativliste, alle Inhalte dieser Liste werden nicht verwendet (siehe auch negative Selektion). Dagegen steht die sogenannten Whitelist, eine Positivliste, deren Begriffe für einen bestimmten Zweck verwendet werden.
[120] BVerfGE 100, 313 (326)

den Landeskenner 49 trägt. Sollte dies der Fall sein, muss die Aufzeichnung umgehend rückstandsfrei durch das System gelöscht werden.

C IMSI und IMEI von mobilen Endgeräten in GSM Netzen

Bei der Erfassung der Kommunikation aus GSM-Netzen ist technisch grundsätzlich die Verwendung der IMSI, der IMEI und der Rufnummer als formaler Suchbegriff möglich. Daher sind diese drei Parameter auf ihre Eignung hin zu Beurteilen.
Die Rufnummer eines Mobilfunkanschlusses unterscheidet sich nur durch die Vorwahlbereiche von einer Rufnummer im öffentlichen Telefonnetz. Bei den verwendeten Vorwahlen ist auf Grund der mobilen Nutzung der Ortsnetzbezug nicht gegeben. Keine Unterscheidung gibt es beim Landeskenner. Die 49 steht hier weiterhin für einen Anschluss in einem deutschen Mobilfunknetz.
Die auf der SIM-Karte gespeicherte IMSI erlaubt es einem Teilnehmer, sich mittels eines Mobiltelefons in einem Mobilfunknetz anzumelden und über dieses Netz Telekommunikationsdienste zu nutzen. Für die Adressierung innerhalb des Netzes wird die der IMSI fest zugeordnete Rufnummer genutzt. Die IMSI ermöglicht somit einem Nutzer in Verbindung mit der Rufnummer den Zugang zu einer Telekommunikationsanlage, unabhängig vom Endgerät. Damit handelt es sich bei einem Mobiltelefon mit eingelegter SIM-Karte um einen Telekommunikationsanschluss i.S.d. § 2 Nr. 10 TKÜV und somit auch um einen bestimmten Telekommunikationsanschluss i.S.d. § 5 Abs. 2 G10.
Bleibt zu prüfen, in wie weit die IMEI als eindeutiges Identifizierungsmerkmal eines Endgerätes einen Telekommunikationsanschluss darstellt.
Die IMEI ermöglicht für sich betrachtet einem Endgerät keinen Zugang zu einer Telekommunikationsanlage. Das lässt sich schon daran sehen, dass ein Mobiltelefon ohne SIM-Karte nicht für die Kommunikation im Netz zugelassen wird. Auch wird eine IMEI nicht über die Rufnummer adressiert, da diese nur der IMSI zugeordnet ist. Somit handelt es sich bei einem Endgerät mit einer IMEI nicht um einen Telekommunikationsanschluss i.S.d. §2 Nr. 10 TKÜV und auch nicht um einen bestimmten Telekommunikationsanschluss i.S.d. §5 G10. Die IMEI ist vergleichbar mit einer Seriennummer und stellt eine reine Gerätekennung zur Identifikation eines Endgerätes dar.
Zu prüfen bleibt, in wie weit die IMEI ein Identifizierungsmerkmal darstellt, dass zur Erfassung eines bestimmten Telekommunikationsanschlusses verwendet werden

kann. Wechselt der Nutzer eines Mobiltelefons seine SIM-Karte nicht, kann, nach einer ersten Zuordnung, im Folgenden der durch die IMSI definierte Telekommunikationsanschluss auch durch Verwendung der IMEI als formaler Suchbegriff gezielt erfasst werden. Und auch wenn der Nutzer die SIM-Karte und damit IMSI und Rufnummer wechselt, ist eine gezielte Erfassung dieses Nutzers über die IMEI des Endgerätes weiterhin möglich.

I. Schlussfolgerung

Die Verwendung einer IMSI als formaler Suchbegriff im Rahmen einer strategischen Erfassung gem. § 5 G10 ist generell nicht zulässig.
Eine Ausnahme muss hier, analog zu den Rufnummern im öffentlichen Telefonnetz, für IMSI gelten, die eindeutig einem Teilnehmer im Ausland zugeordnet werden können. Bei der IMSI lässt sich der Landesbezug an Hand bestimmter Kriterien eindeutig feststellen. Die ersten drei Ziffern der IMSI bilden den *Mobile Country Code* (MCC), der das Ursprungsland der SIM-Karte beschreibt. Der MCC für Deutschland ist gemäß Definition die 262. Somit ist die Verwendung einer IMSI als formaler Suchbegriff nur unter der Voraussetzung zulässig, dass Anschlüsse mit dem Mobile Country Code 262 wirksam von der Aufzeichnung ausgeschlossen werden, um die Erfassung bestimmter individueller Telekommunikationsanschlüsse aus Deutschland im Rahmen der strategischen Erfassung zu verhindern.
Eine IMEI ist auf Grund ihrer Eigenschaft als Identifizierungsmerkmal zur gezielten Erfassung eines bestimmten Nutzers nicht als formaler Suchbegriff i.S.d. G10 geeignet.
Da die IMEI nicht über die Möglichkeit der Zuordnung zu einem Land verfügt, kann die Ausnahme des § 5 Abs. 2 G10 für ausländische Rufnummern analog nur in Verbindung mit einer Prüfung der verwendeten IMSI zulässig sein. Um diesen Abgleich durchführen zu können, ist bei einer Erfassung mit Hilfe der IMEI eine Zwischenspeicherung des Kommunikationsvorgangs notwendig, um die automatisierte Prüfung der IMSI über eine Negativselektion vorzunehmen.
Sowohl bei der Erfassung nach der IMSI als auch nach der IMEI ist zusätzlich eine automatische Prüfung der Quell- und Zielrufnummern nach der Landesvorwahl zwingend, um sicherstellen zu können, dass keine Rufnummern mit dem Landeskenner 49 erfasst werden.

D Adressen des Internet-Protokolls

I. Internetzugang als bestimmter Telekommunikationsanschluss

Um die Eignung der Adressen des Internet-Protokolls als formaler Suchbegriff i.S.d. § 5 Abs. 2 G10 zu bewerten ist zuerst einmal zu prüfen, in wie weit es sich bei einem Internetzugang um einen bestimmten Telekommunikationsanschluss i.S.d. § 5 G10 handelt.

Das Internet ist physikalisch gesehen eine Zusammenschaltung von Übertragungssystemen und Vermittlungseinrichtungen, sogenannten Router und Switches, welche die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, unabhängig von der Art der übertragenen Information. Damit handelt es sich beim Internet um ein Telekommunikationsnetz i.S.d. § 3 Nr. 27 TKG.

Um Informationen in diesem Netz auszutauschen, muss ein Nutzer ein technisches Gerät an den Schnittstellen zu diesem Telekommunikationsnetz betreiben. Damit ist er in der Lage, im Netz vorgehaltene Informationen abzurufen und für sich sichtbar oder hörbar zu machen. Gleichfalls kann er Informationen mit anderen Nutzern über das Netz austauschen. Gem. § 2 Nr. 6 TKÜV handelt es sich um ein Endgerät, da ein Nutzer mit diesem technischen Gerät einen Telekommunikationsanschluss zur Abwicklung seiner Telekommunikation nutzt. Dieses Endgerät wird in der Regel ein PC sein, es kann sich aber auch um ein Mobiltelefon mit entsprechender Schnittstelle oder ähnliche technische Geräte handeln.

Die Verteilung und Speicherung von im Netz bereitgehaltenen Informationen, die Speicherung und Weiterleitung von E-Mails und die Vermittlung von VoIP wird mit Hilfe von technischen Geräten durchgeführt, die auch als Server bezeichnet werden. Diese Systeme sind in der Lage, als Nachrichten identifizierbare elektromagnetische oder optische Signale zu senden, übertragen, vermitteln, empfangen, steuern oder zu kontrollieren. Damit handelt es sich bei diesen Geräten um Telekommunikationsanlagen i.S.d. § 3 Nr. 23 TKG, wenn sie der Übermittlung oder Speicherung von Nachrichten dienen. Bei den Anwendungen E-Mail und VoIP dürfte dies in der Regel gegeben sein.

Sowohl Endgeräte als auch Server müssen über einen Internetanschluss mit dem Internet verbunden werden. Sie dienen dem technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen. Dieser Prozess ist gem. § 3 Nr. 22 TKG als Telekommunikation definiert.

Fraglich bleibt, ob das Internet ein öffentliches Telefonnetz i.S.d. § 3 Nr. 21 TKG ist.
Das öffentliche Telefonnetz besteht aus einer klaren Struktur und ist unterteilt in verschiedene Ortsnetzbereiche, denen feste Rufnummern zugeordnet sind. Es zeichnet sich dadurch aus, dass es auf einer rein leitungsvermittelten Technologie beruht. Es ist zwar möglich in diesem Netz sowohl Sprache als auch Daten zu transportieren, der Grundzweck des Netzes ist aber die Sprachtelefonie. Das Internet nutzt für den Zugang zu den Räumlichkeiten der Teilnehmer und auch auf den Verbindungsstrecken der Vermittlungsknoten häufig die physikalische Infrastruktur des öffentlichen Telefonnetzes[121], wird aber durchgängig in getrennten logischen Kanälen geführt. Es beruht in seiner Gesamtheit auf der Technologie der paketvermittelten Übertragung und ist von seiner Auslegung unabhängig von der Art der zu transportierenden Information. Es ist daher eindeutig vom öffentlichen Telefonnetz zu trennen. Das Internet ist somit nicht Teil des öffentlichen Telefonnetzes und ein Internetanschluss ist kein Teilnehmeranschluss i.S.d. § 3 Nr. 21 TKG.
Zu prüfen bleibt, ob es sich bei einem Internetanschluss um einen Telekommunikationsanschluss i.S.d. § 2 Nr. 10 TKÜV handelt.
Ein Internetanschluss ermöglicht es einem Nutzer, Telekommunikationsdienste mittels eines geeigneten Endgerätes zu nutzen. Wie bereits festgestellt beschränkt sich der Begriff der Telekommunikation nicht wie der Teilnehmeranschluss auf das PSTN, sondern berücksichtigt ebenso neue Technologien der Telekommunikation. Ein Telekommunikationsanschluss stellt daher die physikalische Schnittstelle zum Anschluss eines Endgerätes an ein Telekommunikationsnetz dar. Technisch gesehen kann ein Teilnehmeranschluss mehrere Telekommunikationsanschlüsse beinhalten[122].
Ein bestimmter Telekommunikationsanschluss muss weiterhin durch eine Rufnummer oder andere Adressierungsangabe eindeutig bezeichnet sein und den Zugang zu einer Telekommunikationsanlage darstellen. Daher stellt sich die Frage, ob sich ein Internetzugang durch eine IP-Adresse eindeutig bezeichnen lässt und somit die Zuordnung als bestimmter Telekommunikationsanschluss gegeben wäre. Dies wäre dann der Fall, wenn eine IP-Adresse fest einem solchen Anschluss zugeordnet wäre. Bei dieser Betrachtung ist zu prüfen, ob von der Bewertung zwischen statischen und

---

[121] z.B. für DSL Anschlüsse
[122] Als Beispiel kann hier ein Anschluss der Deutschen Telekom genannt werden. Dieser enthält neben einem Teilnehmeranschluss für das PSTN oft zusätzlich einen Telekommunikationsanschluss für das Internet. An diesen können Endgeräte wie PC oder VoIP Telefone angeschlossen werden, die mit einer entsprechenden Software eine Telekommunikationsanlage i.S.d. TKG für z.B. E-Mail oder VoIP darstellen.

dynamischen Adressen unterschieden werden muss. Im Anschluss kann dann entschieden werden, ob so eine Unterscheidung technisch überhaupt realisierbar scheint.

a) Statische IP Adresse

Um eine Internetwebseite, einen E-Mail Server oder andere Dienste im Internet anbieten zu können, ist die Erreichbarkeit dieser Telekommunikationsanlagen über eine feste IP-Adresse notwendig. Denn nur wenn die Adresse nicht ständig wechselt kann das DNS über die Namensauflösung einer Domain einem Internetnutzer die Adresse seines gesuchten Ziels übermitteln[123]. Diese fixen Adressen werden als statische IP Adressen bezeichnet und durch einen Provider fest einem physikalischen Internetzugang zugeordnet.
Diese Zuordnung ist mit dem Verfahren bei der Vergabe einer Rufnummer im öffentlichen Telefonnetz vergleichbar. Über eine öffentlich zugängliche Datenbank des Regional Internet Registry für Europa, Réseaux IP Européens (RIPE), kann eine statische IP-Adresse einer natürlichen oder juristischen Person eindeutig zugeordnet werden. In dieser Datenbank sind sowohl der Provider als auch Name und Anschrift des Teilnehmers verzeichnet. Andere RIR gehen hier ähnlich vor.
Ein Internetzugang mit einer statischen IP-Adresse ist somit ein Telekommunikationsanschluss i.S.d. § 2 Nr. TKÜV und somit auch ein bestimmter Telekommunikationsanschluss i.S.d. § 5 Abs. 2 G10.

b) Dynamische IP Adresse

Dynamische IP-Adressen werden, wie bereits beschrieben, in der Regel in einem Pool zusammengefasst und dienen hauptsächlich der Adressierung von Internetzugängen für private Nutzer, die nur einige Stunden am Tag einen Zugang zum Netz benötigen. Aufgrund der Dynamik und der begrenzten Gültigkeit wird dieses Verfahren für Server oder geschäftlich genutzte Zugänge nur selten verwendet.
Eine dynamische IP-Adresse kann nicht ohne weiteres eindeutig einem Internetzugang zugeordnet werden, da sie über einen festgelegten Zeitraum wahrscheinlich von mehreren Nutzern genutzt wurde. Erst mit den Angaben Beginn und Dauer der Nutzung wird eine dynamische Adresse eindeutig. Aber auch wenn diese Informationen vorliegen, kann der Anschlussinhaber nicht ohne den Bezug auf die Bestandsda-

[123] Technische existiert auch noch das Verfahren über dynamisches DNS. Dieses wird hier aber nicht näher betrachtet.

ten des Providers identifiziert werden[124], da eine Auskunft über die RIPE-Datenbank nur auf diesen verweisen würde, tiefer gehende Informationen aber nicht bereitstellt.
Sind diesen Informationen bei einem Provider verfügbar, handelt es sich um personenbezogenen Daten i.S.d. § 15 TMG, § 3 Abs. 1 BDSG[125]. Dieser kann also mit Hilfe der Informationen Beginn der Nutzung und Nutzungszeitraum in Verbindung mit der dynamischen IP-Adresse den Kommunikationsvorgang eindeutig einem Internetzugang zuweisen.
Ein Internetzugang mit dynamischer IP-Adresse ist somit ein Telekommunikationsanschluss i.S.d. § 2 Nr. TKÜV und somit auch ein bestimmter Telekommunikationsanschluss i.S.d. § 5 Abs. 2 G10.

Offen bleibt, ob dies auch gilt, wenn kein direkter Zugriff auf die Providerdaten möglich ist. Diese Frage kann über die Betrachtung eines ähnlichen Sachverhaltes gelöst werden. In einem Verfahren vor dem Amtsgericht Berlin Mitte wurde die Betreiberin einer Webseite auf Unterlassung der Speicherung personenbezogener Daten, die im Zusammenhang mit der Nutzung der Seite entstehen, verklagt. In seinem Urteil vom 27.03.2007 begründete das Amtsgericht die Entscheidung wie folgt:

> *"Dynamische IP-Adressen stellen in Verbindung mit den weiteren von der Beklagten ursprünglich gespeicherten Daten personenbezogene Daten i.S.d. § 15 TMG dar, da es sich um Einzelangaben über bestimmbare natürliche Personen im Sinne des § 3 Abs. 1 BDSG handelt."*

Dabei stellte das Amtsgericht auf den Aufwand ab, den es für eine dritte Person macht, den Nutzer einer dynamischen IP Adresse herauszufinden, wenn er über Zeit und Dauer der Nutzung verfügt. Dieser Aufwand wurde als gering bewertet[126]. Dieses Urteil wurde in dem oben genannten Punkt am 06.09.2007 durch das LG Berlin bestätigt[127] und die Berufung zurückgewiesen.
In der Literatur wird dieser Rechtsauffassung teilweise widersprochen[128], einige Gerichte haben sich in ihrer Rechtsprechung dieser Auffassung aber bereits angeschlossen[129].

---

[124] Braun, jurisPR-ITR 4/2006 S.1
[125] Meyerdirks, MMR 1/2009, 8, 9
[126] AG Berlin Mitte, 5 C 314/06
[127] LG Berlin 23 S 3/07
[128] Meyerdirks, MMR 1/2009, 8, 13
[129] VG Wiesbaden, *Beschluss* vom 27.2.2009 - 6 K 1045/08.WI, Nr. 37

Anbieter von Telekommunikationsdiensten haben gem. § 111 TKG die Pflicht zur Speicherung bestimmter Daten, die sie bei Vertragsabschluß von einem Kunden zu erheben haben. Über diese Bestandsdaten besteht eine Auskunftspflicht gegenüber dem BND gem. §§ 112 Abs. 2 Nr. 4, 113 Abs. 1 TKG. Somit stellt es für diesen kein Problem dar, die Informationen zu erhalten die notwendig sind, um eine dynamischen IP Adresse einem definierten Internetzugang zuzuordnen[130].

Die Auffassung der Bundesregierung ist dabei, dass es sich bei dem Auskunftsersuchen rein um eine Abfrage von Bestandsdaten handelt, da dem BND die Verkehrsdaten bereits auf Grund einer Erfassung gem. § 5 G10 bekannt sind. Auch wenn der Provider auf gespeicherte Verkehrsdaten zurückgreifen muss um den entsprechenden Nutzer zu ermitteln, liegt gem. dieser Auffassung kein Eingriff in das Fernmeldegeheimnis vor[131]. Diese Auffassung wurde in der Rechtsprechung durch verschiedene Gerichte bestätigt[132].

Diese Meinung steht interessanter Weise im Gegensatz zum Gesetzentwurf der Bundesregierung "zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums"[133]. Hier lautet die Formulierung:

> *"Dieser Fall ist bei Rechtsverletzungen im Internet denkbar wenn Daten mit Hilfe von dynamischen IP (Internet Protocol) - Adressen, vor allem über so genannte FTP (file transfer protocol) - Server, im Netz ausgetauscht werden. Potenzielle Rechtsverletzer können in solchen Fällen meist nicht unmittelbar über Bestandsdaten ermittelt werden, sondern nur mit Hilfe von Verkehrsdaten[134]"*

Die Verkehrsdaten wiederum unterliegen, wie bereits besprochen, dem Schutz des Fernmeldgeheimnisses aus Art. 10 GG.

Der Argumentation, dass es sich bei einem Auskunftsersuchen über den Nutzer einer dynamischen IP-Adresse nur um Bestandsdaten handelt, kann nicht gefolgt werden. Denn nur durch die angefragten Daten kann eine für sich gesehen nutzlose Information, wie eine dynamische IP-Adresse, erst zu einem für den Anfragenden relevanten Datum werden. Die Abfrage an sich stellt keinen Eingriff in das Fernmeldegeheimnis dar. Das Zusammenfügen der beiden Datenpakete aus der Erfassung und der Auskunft des Providers hat hingegen die Qualität eines erneuten Eingriffs in

---

130 Köcher, DuD 1/2009, 20, 20
131 BR-Drs. 275/07, S.53
132 Schramm, DuD 30/2006, 785, 785
133 Bizer, DuD 31/2007, 8
134 BR-Drs. 64/07, S.93

das Fernmeldegeheimnis des Art. 10 GG. Denn die nun vorhandenen Daten geben Information über einen Kommunikationsvorgang und dessen nähere Umstände. Zusätzlich können diese Informationen jetzt einem Kommunikationsteilnehmer individuell zugeordnet werden, dessen Grundrechte erst durch das Zusammenfügen der Daten wirksam beeinträchtigt werden[135].

Zusammenfassend kann gesagt werden, dass es sich bei einem Internetzugang der über eine dynamische IP-Adresse den Zugang zum Internet hat, um einen bestimmten Telekommunikationsanschluss i.S.d. § 5 Abs. 2 G10 handelt. Da es für den BND auf Grund der Möglichkeiten des Auskunftsersuchens gem. §§ 112, 113 TKG auf die gem. § 111 TKG durch den Provider gespeicherten Bestandsdaten keine Hürde darstellt zu einer dynamischen IP-Adresse den jeweiligen Nutzer zu erfragen, müssen hier die gleichen Hürden gelten wie bei einer statischen IP-Adresse.

II. Schlussfolgerung

Da es sich sowohl bei Internetanschlüssen mit statischen als auch bei denen mit dynamischen IP-Adressen um bestimmte Telekommunikationsanschlüsse i.S.d. § 5 Abs. 2 G10 handelt, ist eine Verwendung von IP-Adressen als formaler Suchbegriff im Rahmen einer strategischen Erfassung nicht zulässig. Da auch hier die Verwendung von Wildcards möglich ist (z.B. 192.168.*), ist sicherzustellen, dass eine Unschärfe in der Technologie nicht den Zweck des Gesetzes in Frage stellen darf.

Nur für eindeutig dem Ausland zuzurechnende IP-Adressen muss ebenfalls die Ausnahmeregelung des § 5 Abs. 2 G10 gelten. Die Verwendung solcher Adressen als formaler Suchbegriff im Rahmen einer strategischen Erfassung ist zulässig, wenn diese die entsprechenden gesetzlichen Voraussetzungen des § 5 Abs. 2 G10 für ausländische Rufnummern erfüllen. Somit kann diese Ausnahme nur für solche IP-Adressen gelten, die der BND eindeutig einem Ziel im Ausland zuordnen kann.

Eine automatisierte Prüfung der IP-Adressen auf ihre lokale Zuordnung könnte z.B. durch eine automatisierte Abfrage der einschlägigen RIR Datenbanken erfolgen. Diese Datenbanken werden mittlerweile auf Grund wirtschaftlicher Interessen und zum Zwecke der Lokalisierung von Internetangeboten sehr gut gepflegt und sind äußerst zuverlässig.

Auch die weiteren an einer Kommunikation beteiligten Adressen sind nach den oben genannten Maßgaben zu prüfen. Im Zweifel muss die manuelle Bearbeitung durch

---

[135] Schramm, DuD 30/2006, 785, 787

einen Mitarbeiter des Bundesnachrichtendienstes erfolgen, der eine Bewertung der Zulässigkeit der Erfassung des Verkehrs vornehmen muss.
Die Gefahr bei diesem Verfahren unbeteiligte Personen zu erfassen ist als gering anzusehen, da nur qualifizierte Adressen als formale Suchbegriffe verwendet werden dürfen und somit die Erfassungsbreite möglichst schmal gehalten wird.

E Adressen der elektronischen Post

I. Klassische E-Mail

Um die Zulässigkeit der Adressen der elektronischen Post (E-Mail Adressen) als formaler Suchbegriff im Rahmen einer strategischen Erfassung festzustellen, ist ihre Eignung als eindeutiges Identifizierungsmerkmal für einen bestimmten Telekommunikationsanschluss zu prüfen. Da E-Mail und Webmail zur Adressierung die gleichen Adressen verwenden, wird zwischen diesen Verfahren nicht unterschieden.
Eine E-Mail Adresse dient im Internet der Adressierung der elektronischen Post. Da dieses nicht dem öffentlichen Telefonnetz zuzurechnen ist, handelt es sich bei einer E-Mail Adresse um einer Nummer i.S.d. § 3 Nr. 13 TKG.
Über diese Nummer ist es möglich, Nachrichten einem bestimmten Nutzer zuzuordnen und über eine DNS Abfrage die IP-Adresse des zugehörigen Mailservers zu ermitteln.
Für die Erfassung einer E-Mail sind zwei der vier beschriebenen Phasen maßgeblich. Zum einen die Übertragung der Nachricht vom Endgerät des Nutzers auf den Postausgangsserver, zum anderen der Transport vom Postausgangsserver auf den Posteingangsserver des Empfängers. Daher ist zu prüfen, ob es sich bei beiden Vorgängen um die Erfassung eines bestimmten Telekommunikationsanschlusses handelt, wenn eine E-Mail Adresse als formaler Suchbegriff verwendet wird.
Für die Übertragung einer E-Mail an den Postausgangsserver muss das Endgerät eines Nutzers mit einem Internetanschluss verbunden sein. Wie bereits festgestellt, handelt es sich bei einem solchen Anschluss um einen bestimmten Telekommunikationsanschluss i.S.d. §5 Abs. 2 Nr. 1 G10.
Fraglich bleibt, ob die Verwendung der E-Mailadresse als formaler Suchbegriff zur spezifischen Überwachung dieses Anschlusses ausreichend ist. Ein Internetanschluss verfügt über das Potential, Nachrichten über mehr als 60.000 Ports gleichzeitig zu versenden und zu empfangen. Die Anwendung E-Mail nutzt weniger als 5

Ports. Somit ist die Erfassung des gesamten Verkehrs eines Internetanschlusses über eine E-Mail Adresse nicht möglich. Dies kann erst über den Umweg und die Verwendung der zugehörigen IP-Adresse erfolgen.
Zusätzlich wird auf Grund der Möglichkeiten der nomadischen Nutzung einer E-Mail Software auf verschiedenen Endgeräten und an unterschiedlichen Zugängen durch die Erfassung mit der E-Mail Adresse als formaler Suchbegriff in der Phase der Übertragung vom Endgerät auf den Server gerade nicht immer der bestimmte Telekommunikationsanschluss erfasst, sondern nur das E-Mail Konto. Somit scheint es, dass eine E-Mail Adresse nicht als Identifizierungsmerkmal eines bestimmten Telefonanschlusses geeignet ist und somit als formaler Suchbegriff im Rahmen einer strategischen Erfassung zulässig wäre.
Diese Lösung kann nicht zufriedenstellen, da das Gesetz ja gerade verhindern will, dass ein bestimmter individueller Nutzer mit Hilfe der strategischen Erfassung gezielt überwacht wird[136]. Daher muss die Lösung mit einer teleologischen Auslegung der Vorschrift gefunden werden. Eine E-Mail Adresse ist in der Regel fest einem Nutzer zugeordnet, der seine elektronische Post über diese Adresse sendet und empfängt. Wird eine E-Mail Adresse als formaler Suchbegriff verwendet, kann ein solcher Nutzer gezielt überwacht werden. Somit ist eine E-Mail Adresse eben nicht als formaler Suchbegriff geeignet.
Fraglich bleibt, ob es sich bei dem Zugang eines E-Mail Servers ebenfalls um einen bestimmten Telekommunikationsanschluss i.S.d. § 5 Abs. 2 Nr. 1 G10 handelt. Ein E-Mail Server kann als technisches System Nachrichten senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren und ist damit gem. Definition des § 3 Nr. 23 TKG als Telekommunikationsanlage zu sehen. Über eine E-Mail Adresse, die einem Postfach auf dem Server zugeordnet ist, lässt sich diese Telekommunikationsanlage gezielt überwachen. Diese Anlage verfügt über in der Regel über eine statische IP-Adresse und ist zur Kommunikation mit dem Netz mit einem Internetzugang verbunden. Somit handelt es sich bei diesem um einen bestimmten Telekommunikationsanschluss. Das ein E-Mail Server über eine Vielzahl von Postfächern mit verschiedenen Adressen verfügt, spielt für die Beurteilung keine Rolle, da das Gesetz für einen Telekommunikationsanschluss keine Begrenzung der möglichen Nutzer vorsieht.

[136] BVerwG, *Urteil* vom 23. 1. 2008 - 6 A 1/07, Rd.Nr. 35

II. De-Mail und E-Postbrief

Die auf Basis der Dienste De-Mail und E-Postbrief verwendeten Adressen sind auf Grund der von diesen Diensten verfolgten Ziele der eindeutigen Identifikation der Nutzer und der Nachvollziehbarkeit der Kommunikation zweifelsfrei zur eindeutigen Identifikation eines Teilnehmers geeignet.
Denn bereits die Zusammensetzung des lokalen Teils der E-Mail Adressen beider Dienste, der aus Vorname und Name des Benutzers gebildet wird, ermöglicht die Identifikation des Teilnehmers oder zumindest eine enge Einschränkung bei mehrfach vorhandenen Namenskombinationen. Als Beispiel sei hier die Adresse „Max.Mustermann@epost.de“ für den E-Postbrief genannt. Hier kann über den Domain Teil der Adresse die E-Mail eindeutig dem Dienst E-Postbrief zugeordnet werden.
Gleiches gilt De-Mail. Auch hier ist die Zeichenfolge „de-mail“ bei jedem Dienstleister im Domain Teil der Adresse enthalten und kann somit eindeutig diesem Dienst zugeordnet werden.

III. Schlussfolgerung

Mit der Verwendung einer E-Mail Adresse als formaler Suchbegriff im Rahmen einer strategischen Überwachung des BND kann ein Nutzer oder aber ein bestimmter Telekommunikationsanschluss gezielt überwacht werden. Daher ist Eignung einer E-Mail Adresse als formaler Suchbegriff im Rahmen einer strategischen Erfassung auf Grund der Vorschriften des § 5 Abs. 2 G10 grundsätzlich zu verneinen.
Eine Ausnahme kann hier nur für solche E-Mail Adressen gelten, die der BND eindeutig einem Ziel im Ausland zuordnen kann. Eine automatisierte Differenzierung zwischen deutschen und ausländischen Teilnehmern ist, wie bereits festgestellt, über die TLD technisch so gut wie unmöglich. Die Endung ".de", analog zum Landeskenner 49, als Ausschlusskriterium für die Verwendung einer E-Mailadresse als formalen Suchbegriff zu verwenden, würde aber einem möglichen Missbrauch durch den internationalen Terrorismus und der organisierten Kriminalität Tür und Tor öffnen, da mit der Verwendung solcher Adressen durch diese Organisationen eine strategische Überwachung nahezu nutzlos würde. Somit muss eine Zuordnung von Adressen durch die manuelle Erstellung einer Positivliste erfolgen. Diese kann dann z.B. die Adressen von Rüstungsfirmen im Ausland oder anderweitig gewonnenen Adressen enthalten. Ist eine Domain eindeutig dem Ausland zugeordnet, ist dann auch die

Verwendung von Wildcards zulässig (z.B. *. ukrspetsexport.com für alle E-Mail Adressen einer Rüstungsfirma aus der Ukraine die verdächtigt wird, Waffen illegal an den Iran geliefert zu haben). Auf Grund der oben genannten Gründe müssen in dieser Liste aber auch Adressen mit der TLD ".de" zulässig sein, wenn sie auf Grund anderer Erkenntnisse einem ausländischen Teilnehmer eindeutig zugeordnet werden können.

Da eine automatisierte Prüfung der zweiten beteiligten Adresse auf Grund der oben beschriebenen Gegebenheiten nicht zweifelsfrei möglich ist, muss diese Prüfung bei einem positiven Treffer durch einen Bearbeiter des Bundesnachrichtendienstes erfolgen. Die Gefahr unbeteiligte Personen zu erfassen ist bei dieser Vorgehensweise als gering anzusehen, da nur Adressen als formale Suchbegriffe verwendet werden dürfen, die eindeutig dem Ausland zuzuordnen sind und eine mehr oder weniger geartete Beteiligung eines Adressnutzers an den Sachverhalten des Katalog gem. §5 Abs. 1 G10 wahrscheinlich ist.

Die Adressen der Dienste E-Postbrief und De-Mail dürfen eindeutig nicht als Suchbegriff im Rahmen einer strategischen Erfassung verwendet werden, da sie eindeutig für die nationale Verwendung bestimmt sind. In ihrer Art entsprechen sie damit Rufnummern mit der Landesvorwahl 0049. Im Rahmen einer strategischen Erfassung müssen diese Adressen daher über eine Negativselektion von der Aufzeichnung ausgeschlossen werden.

F Nummern der Telefonie über das SIP-Protokoll

Um die Zulässigkeit der Adressen des SIP-Protokolls als formaler Suchbegriff im Rahmen einer strategischen Erfassung festzustellen, ist auch ihre Eignung als eindeutiges Identifizierungsmerkmal für einen bestimmten Telekommunikationsanschluss zu prüfen.

Wie bereits in den Grundlagen beschrieben, entsprechen die von SIP zur Adressierung verwendeten Zeichenfolgen in ihrem Aufbau einer E-Mail Adresse. Die vollständige Adresse wird aber in der Regel nur zwischen Endgeräten und Gateways verwendet, der Nutzer wählt üblicherweise eine Ziffernfolge, die in ihrem Aufbau einer Rufnummer im öffentlichen Telefonnetz gleicht. Daher ist fraglich, ob die zur Anwahl eines VoIP Gespräches verwendete Ziffernfolge als Rufnummer i.S.d. TKG einzuordnen ist. Gem. §3 Nr. 18 TKG ist eine Rufnummer eine Nummer, durch deren Wahl im öffentlichen Telefondienst eine Verbindung zu einem bestimmten Ziel

aufgebaut werden kann. Da es sich bei der Kommunikation über VoIP nicht um Verbindungen im öffentlichen Telefonnetz sondern im Internet handelt, kann es sich bei der zur Adressierung benutzten Ziffernfolge nur um eine Nummer i.S.d. § 3 Nr. 13 TKG und nicht um eine Rufnummer handeln[137].

Die Eignung dieser Nummer als Identifizierungsmerkmal für einen bestimmten Telekommunikationsanschluss bleibt zu prüfen. Eine Applikation zur Telefonie über das SIP Protokoll kann, ebenso wie ein E-Mail Programm, an jedem beliebigen Internetzugang auf der Welt genutzt werden. Somit ist, analog zur E-Mail, die Eignung einer Adresse des SIP als Identifizierungsmerkmal für einen bestimmten Telekommunikationsanschluss nicht gegeben. Eine VoIP Nummer ermöglicht aber gleichfalls die eindeutige Zuordnung von Kommunikationsvorgängen zu einem Nutzer, unabhängig vom verwendeten Anschluss. Daher ist auch hier eine teleologische Auslegung des G10 notwendig, um die gezielte Erfassung eines individuellen Nutzers wirksam zu verhindern.

Die rechtliche Bewertung eines Gateway-Servers entspricht auf Grund gleicher Betriebsweisen der eines E-Mail Servers.

I. Schlussfolgerung

Nach teleologischer Auslegung des §5 G10 ist die Nummer eines VoIP Anschlusses nicht als formaler Suchbegriff im Rahmen einer strategischen Erfassung i.S.d. § 5 G10 geeignet, da sie die gezielte Erfassung eines individuellen Nutzers ermöglicht.

Eine Ausnahme kann auch hier nur für solche VoIP Nummern gelten, die eindeutig einem Ziel im Ausland zugeordnet werden können. Bei der Vergabe von Nummern für VoIP ist durch die Bundesnetzagentur zwar eine Ortsnetzbindung wie im PSTN vorgeschrieben, eine Kontrolle ist auf Grund der nomadischen Nutzungsmöglichkeiten[138] aber nahezu unmöglich. Auf Grund der Liberalisierung der Vorschriften der Rufnummernvergabe im Zusammenhang mit der Verbreitung von VoIP kann ein Teilnehmer heute eine Nummer zugeteilt bekommen, die von einer Rufnummer des öffentlichen Telefonnetzes mit deutschem Landeskenner nicht zu unterscheiden ist. Es ist ohne Probleme möglich, dass sich der Nutzer eines VoIP Anschlusses unter einer Rufnummer mit dem deutschen Landeskenner 49 im Ausland befindet, nicht deutscher Staatsangehöriger ist und dass sich der Server des Diensteanbieters außerhalb des Staatsgebietes der Bundesrepublik Deutschland befindet. Somit ist

[137] Mozek/Zendt in Hoeren/Sieber, Handbuch Multimedia-Recht Teil 23, Rd.Nr. 48
[138] Mozek/Zendt in Hoeren/Sieber, Handbuch Multimedia-Recht Teil 23, Rd.Nr. 49

ein wirksamer Ortsnetzbezug einer VoIP Nummer, analog zur Rufnummer des öffentlichen Telefonnetzes, faktisch nicht gegeben. Daher kann ein deutscher Teilnehmer weder über die TLD ".de" noch über den Landeskenner 49 im lokalen Teil der Adresse eindeutig identifiziert werden.

Somit muss die Handhabung dieser Ausnahmen muss im Rahmen einer strategischen Erfassung analog zu der Vorgehensweise bei Adressen der elektronischen Post erfolgen. Daher müssen auch SIP Nummern mit der TLD ".de" und dem Landeskenner 49 als formaler Suchbegriff zulässig sein, wenn diese durch den BND eindeutig einem nicht deutschen Nutzer im Ausland zugeordnet werden können.

Teil 5: Schlussbetrachtung

Das Zusammenwachsen moderner Kommunikationsnetze zu Next Generation Networks und die stetig größer werdende Anzahl von Applikationen zur Kommunikation zwischen Menschen wird auch die juristische Welt vor immer neue Herausforderungen stellen. Gerade Rechtsvorschriften, die der Regelung von Anwendungen und Verhaltensweisen im Internet dienen, sind in der Zukunft in deutlich kürzeren Abständen auf ihre Gültigkeit hin zu überprüfen. Der immer schneller werdende technische Wandel macht es schwierig, bei der Formulierung der Rechtsvorschriften die richtige Balance zwischen universeller Anwendung und Spezialisierung eines Gesetzes zu finden.

Das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist eines dieser Gesetze. Sein Anspruch ist es, den Schutzumfang des Art. 10 GG so einzuschränken, dass deutschen Sicherheitsbehörden über das Mittel der Telekommunikationsüberwachung in die Lage versetzt werden, Straftaten und staatsgefährdende Verhaltensweisen frühzeitig zu erkennen und abwehren zu können. Aber gerade terroristische Vereinigungen und die organisierte Kriminalität sind auf Grund ihrer Professionalität und ihrer finanziellen Möglichkeiten in der Lage, neueste Kommunikationstechnologien umgehend zu adaptieren und für ihre Zwecke zu nutzen.

Änderungen des Gesetzes hingegen nehmen im parlamentarischen Verfahren eine gewisse Zeit in Anspruch, wie die letzte Änderung des G10 im Jahre 2009 zeigt. Die Vorbereitung für diese Änderung dauerte ungefähr 5 Jahre. Dies ist in einem sensiblen Bereich wie der Einschränkung von Grundrechten auch durchaus angebracht, die Realität zeigt aber leider ein anderes Bild und beschränkt damit die Sicherheitsbehörden in ihren Möglichkeiten.

Die vorliegende Studie zeigt, dass moderne Kommunikationsverfahren trotz Auslegung des Gesetzes in ihrer Handhabung bei der strategischen Telekommunikationsüberwachung nur teilweise erfasst werden. Denn gerade dem Zusammenwachsen der Netze und der damit verbundenen Vermischung von Netzen und Kommunikationsanwendungen ist das G10 in seiner heutigen Form für die nachrichtendienstliche Arbeit der Zukunft nicht gewachsen. Vor allem die strategische Überwachung, die aus einer großen Menge von Daten relevante Ziele finden soll, benötigt effizientere Methoden der Suche, gerade auch um die Erfassung unschuldiger Bürger zu vermeiden. Hier sollte in Zukunft die Möglichkeit bestehen, bestimmte Gruppierungen

gezielter in die Erfassung aufzunehmen, um die materiellen und personellen Ressourcen der Sicherheitsdienste effizient zu nutzen.
Der breite Erfassungsansatz der Vergangenheit hat in vielen Beispielen gezeigt, dass relevante Daten einfach in der Masse der Erfassungen verschwinden und nicht rechtzeitig entdeckt werden. Nach terroristischen Anschlägen waren amerikanische Sicherheitsdienste immer in der Lage, aus der Masse der von ihnen erfassten Daten die beteiligten Personen und Netzwerke ausfindig zu machen. Leider ist ihnen dieses nur in wenigen Fällen bereits vor dem Ereignis gelungen.
Daher ist es wichtig, dass bei der Erarbeitung der Gesetzgebung das Fachwissen von Juristen und Ingenieuren stärker als bisher verbunden wird, um zum einen den Schutz der Grundrechte für alle Bürger gewährleisten zu können, zum anderen aber die Sicherheitsdienste in die Lage versetzt werden, dem modernen Technologiewandel schnell und effizient folgen zu können. Nur so kann der BND drohende Gefahren erkennen und dem Staat ermöglichen, diesen effektiv entgegentreten.
Das die aktuelle Gesetzeslage und deren Umsetzung den modernen Technologien nicht gewachsen ist, zeigt der aktuelle Bericht des parlamentarischen Kontrollgremiums vom 17.12.2010 für den Zeitraum vom 01. Januar – 31.Dezember 2009. In diesem Zeitraum haben sich zu den Gefahrenbereichen „Internationaler Terrorismus“, „Proliferation und konventionelle Rüstung“ und „unbefugten Verbringens von Betäubungsmitteln in Fällen von erheblicher Bedeutung“ insgesamt ca. 7 Millionen Verkehre qualifiziert, von denen sich am Ende 278 Verkehre als nachrichtendienstlich relevant herausstellten. Im Bereich „Internationaler Terrorismus“ war es eine (!) E-Mail in 12 Monaten, im Bereich der Betäubungsmittel sogar keine nachrichtendienstlich relevante Übertragung. Kommt man nun zurück auf die Kapazität einer STM-256 Leitung mit ca. 500.000 parallelen Übertragungen muss die Frage erlaubt sein, ob der aktuelle Ansatz wirklich zielführend ist und dem Nachrichtendienst wirksame Mittel an die Hand gegeben werden[139]. Denn einen Anschlag wirksam verhindern wird man mit einer E-Mail wohl nicht können.
Wie diese Untersuchung deutlich zeigt, ist die Verwendung von IP-Adressen und Adressierungen von paketbasierten Kommunikationsanwendungen als formaler Suchbegriff für die strategische Erfassung auf Grund der aktuellen Gesetzeslage stark eingeschränkt. Natürliche und juristische Personen, die an Sachverhalten des Katalogs gem. § 5 Abs. 1 G10 beteiligt sind, ist es daher ohne Schwierigkeiten

[139] BTDrucks 17/4278

möglich, sich gegenüber der strategischen Erfassung hinter vermeintlich deutschen E-Mail Adressen, VoIP Nummern oder Internetadressen zu verbergen, da diese nicht als formaler Suchbegriff zulässig sind. Hier muss der Gesetzgeber die Besonderheiten der neuen Technologien erkennen und die Möglichkeiten der nomadischen Nutzung stärker berücksichtigen.

Denn für die strategische Erfassung bedeutet die Suche mit inhaltlichen Suchbegriffen auf Grund der paketvermittelten Übertragung einen deutlich tieferen Eingriff in die Grundrechte als die Suche mit formalen Suchbegriffen. Um einen inhaltlichen Suchbegriff zu finden, müssen zuerst einmal alle Pakete eines Telekommunikationsvorgangs erfasst und zusammengesetzt und dekodiert werden, um dann die Inhaltsdaten durchsuchen zu können. Bei der Erfassung mit formalen Suchbegriffen hingegen ist ein Abgleich mit den Verkehrsdaten in der Regel ausreichend. Hier sollte das Gesetz ein mehrstufiges Selektionssystem, beginnend bei der Filterung mit formalen Suchbegriffen wie der IP-Adresse, ermöglichen. In einer zweiten Stufe kann dann die Adressierung der Anwendungen als formaler Suchbegriff verwendet werden, bis in einer dritten Stufe eine die Suche mit inhaltlichen Suchbegriffen stattfinden kann. Mit diesem Verfahren wäre sichergestellt, dass der Inhalt, als das zu schützende Gut einer Kommunikation, erst nach der Qualifikation des Vorgangs, in zwei vorgeschalteten automatisierten Stufen, ausgewertet wird.

Wegweisend in diese Richtung ist auch das Urteil[140] des Bundesverfassungsgerichtes zur Vorratsdatenspeicherung. Das Gericht kommt in seinem Urteil zu dem Entschluss, dass

> *„ es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. Auch wenn sich die Speicherung nicht auf die Kommunikationsinhalte erstreckt, lassen sich aus diesen Daten bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten, Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen. Je nach Nutzung der Telekommunikation kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits und Bewegungsprofile praktisch jeden Bürgers ermöglichen.“*

[140] 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –

Das Gericht ist der Auffassung, dass bei dem aktuellen Ansatz der Vorratsdatenspeicherung die Verhältnismäßigkeit nicht gewahrt ist. Es bleibt daher abzuwarten, wie der Gesetzgeber das Verfahren an die Vorgaben des Gerichts anpassen wird.
Fraglich ist, ob der Ansatz über die Speicherung von Verbindungsdaten ausreichend ist, um Bedrohungen wirksam im Vorfeld zu bekämpfen. Denn die Herausforderung der strategischen Erfassung besteht darin, mögliche Ereignisse der Zukunft zu erkennen und Schlimmeres zu verhindern. Das wird mit einer uferlosen Datensammelwut nicht zu lösen sein, denn am Ende der Auswertung steht immer noch der Mensch. Dieser ist mit der großen Menge an Verkehrsdaten aus heutigen Kommunikationsnetzen bei einer Erfassung von 100% überfordert, wie viele Beispiele zeigen. Somit ist die Gefahr des Missbrauchs der gesammelten Daten deutlich höher als die Möglichkeit, mit ihnen effektiv die gewünschten Ziele zu erreichen.
Die strategische Erfassung der Zukunft braucht intelligente Methoden, die den Fokus auf bestimmte Ziele setzen. Der breite Erfassungsansatz der heutigen strategischen Erfassung hat auf Grund der Fülle der Daten keine Zukunft.
Daher sollte das Ziel einer modernen Gesetzgebung sein, die Früherkennung von Gefahren durch flexible Ansätze der strategischen Erfassung zu ermöglichen und dabei den größtmöglichen Schutz der Grundrechte sicherstellen.
Auf keinen Fall aber dürfen sich terroristische Organisationen in den mühevoll erkämpften Schutzbereichen unseres Grundgesetzes verbergen können und somit den Zweck dieser Vorschriften ad absurdum führen.

Literaturverzeichnis

Ackermann, Rolf/Clages, Horst/Roll, Holger: *Handbuch der Kriminalistik - Kriminaltaktik für Praxis und Ausbildung*, 3., aktualisierte und geänderte Auflage, 2007, Richard Boorberg Verlag

Arndt, Claus: *Die "strategische Kontrolle" von Post- und Fernmeldeverkehrsbeziehungen*, NJW 3/1985, 107-111

Arndt, Claus: *Die Fernmeldekontrolle im Verbrechensbekämpfungsgesetz,* NJW 3/1995, 169-172

Bär, Wolfgang: *Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen*, MMR 4/2008, 215-222

Bär, Wolfgang: *Handbuch zur EDV-Beweissicherung im Strafverfahren,* 1. Auflage 2007, Richard Boorberg Verlag

Bedner, Mark: *Rechtmäßigkeit der „Deep Packet Inspection",* Projektgruppe verfassungsverträgliche Technikgestaltung, Universität Kassel 2009

Bizer, Johann: *IP-Adressen sind Verkehrsdaten,* DuD 31/2007, 602

Borowsky, Peter: *Große Koalition und Außerparlamentarische Opposition,* Informationen zur politischen Bildung, 258/1998, Bundeszentrale für politische Bildung

Braun, Frank: Herausgabe von persönlichen Daten bei dynamischen IP-Adressen, jurisPR-ITR 4/2006 Anm. 6

Bundesamt für Sicherheit in der Informationstechnik, *De-Mail - Technische Richtlinie BSI TR 01201,* Version 0.99.1, 26.08.2010

Bundesministerium des Inneren, Bürgerportale (De-Mail) und die EU-Dienstleistungsrichtlinie, Broschüre 10/2008

Dix, Alexander/Petri, Thomas B.: Das Fernmeldegeheimnis und die deutsche Verfassungsidentität, DuD 9/2009, 531-535

Doyle, Jeff/Carroll, Jennifer: *CCIE Professional Development Routing TCP/IP, Volume I,* Macmillan Technical Publishing; 2. Auflage 2008

Eckhardt, Jens: Wie weit reicht der Schutz des Fernmeldegeheimnisses (Art. 10 GG), DuD 30/2006, 365-368

Epping, Volker/Lenz, Sebastian/ Leydecker, Philipp: *Grundrechte*, 3. Ausgabe 2007, Verlag Springer Berlin Heidelberg

Garstka, Hansjürgen: Terrorismusbekämpfung und Datenschutz - Zwei Themen im Konflikt, NJ 10/2002, 524-525

Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz, Raimund/Schuster, Fabian: *Beck'scher TKG-Kommentar,* 3.Auflage 2006, Verlag C.H. Beck

Gusy, Christoph und Hueck, Ingo J. (1995): *Fernmeldegeheimnis für Auslandsgespräche?,* NJ 9/1995, 461-465

Gusy, Christoph/Worms, Christoph: *Grundgesetz und Internet,* Aus Politik und Zeitgeschichte 18-19/2009, 26-33

Gusy, Christoph: Geheimdienstliche Aufklärung und Grundrechtsschutz, APuZ 44/2004, 14-20

Information Technology - Open Systems Interconnection - Basic Reference Model : The Basic Model, Data Networks and Open System Communications, ITU-T 2004

Huber, Bertold: Die Reform der parlamentarischen Kontrolle der Nachrichtendienste und des Gesetzes nach Art. 10 GG, NVwZ 21/2009, 1321-1328

Hoeren, Thomas/Sieber, Ulrich: Handbuch Multimedia - Recht Rechtsfragen des elektronischen Geschäftsverkehrs, Stand März 2008, C. H. Beck München

Keromytis, Angelos D./Prevelakis, Vassilis/Turner, David Michael: *The Bandwidth Exchange Architecture,* Papier 10. IEEE Symposium on Computers and Communications (ISCC 2005), 27.-30-06.2005, La Manga del Mar Menor, Cartagena, Spanien

Kindt, Anne: Die grundrechtliche Überprüfung der Vorratsdatenspeicherung: EuGH oder BerfG - wer traut sich?, MMR 10/2009, 661-666

Kleinschmidt, Michael: *Robust speech recognition based on spectro-temporal processing,* Dissertation Universität Oldenburg, 2002

Köcher, Jan K.: Vorratsdatenspreicherung - Die Zweitel, DuD 1/2009, 20-24

Köcher, Jan K./Kaufmann, Noogie C.: Speicherung von Verkehrsdaten bei Internet-Access-Providern, DuD 30/2006, 360-364

Krieger, Heike: *Die Reichweite der Grundrechtsbindung bei nachrichtendienstlichem Handeln,* Veranstaltungsbeitrag Fachkonferenz zum Thema Parlamentarische Kontrolle der Nachrichtendienste im demokratischen Rechtsstaat, 10/2007

Krüger, Hartmut: *Anmerkung zu BVerfG: Beschlagnahme von E-Mails auf Server des Mailproviders, 2 BvR 902/06*, MMR 10/2009, 680-683

Ladeur, Karl-Heinz: Das Recht auf informelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2/2009, 45-55

Licklider, Joseph: *Man-Computer Symbiosis*, IRE Transactions on Human Factors in Electronics 03/1960, 4-11

Mangoldt von, Hermann/Klein, Friederich/Starck, Christian: *Kommentar zum Grundgesetz: GG,* Kommentar in 3 Bänden, Band 1: Präambel, Art. 1-19, 5. Auflage 2005, Vahlen

Meyerdirks, Per: *Sind IP-Adressen personenbezogene Daten?,* MMR 1/2009, 8-13

Roggan, Fredrik/Bergemann, Nils: *Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz* NJW 13/2007, 876-881

Sankol, Barry: *Die Qual der Wahl: 113 TKG oder §§ 100g, 100h StPO?,* MMR 6/2006, 361-365

Schafranek, Frank P.: *Die strategische Aufklärung durch den BND nach dem neuen G10*, DöV 20/2002, 846-851

Schramm, Marc: Staatsanwaltliche Auskunft über dynamische IP-Adressen, DuD 30/2006, 785-788

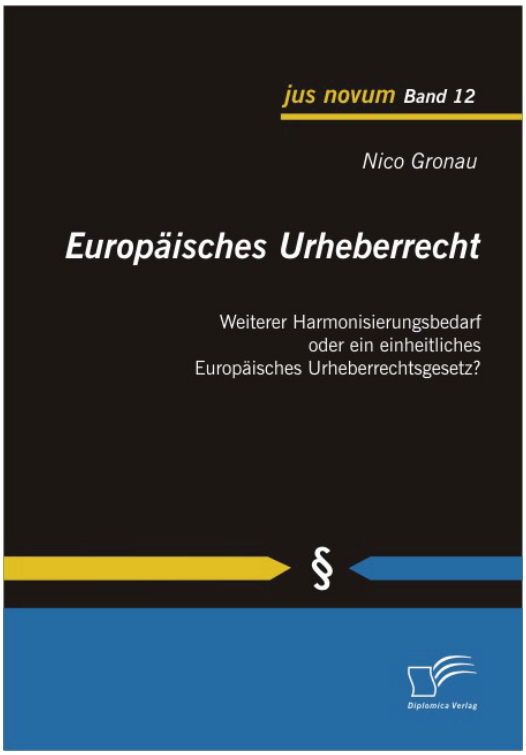
Shannon, C. E.: *A mathematical theory of communication,* Bell System Technical Journal 27/1948, 379-423 und 623-656

Sievers, Malte: *Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes,* Kieler Rechtswissenschaftliche Abhandlungen (NF) - Band 39, 1. Auflage 2003, Nomos Verlagsgesellschaft

Soiné, Michael: *Die Aufklärung der Organisierten Kriminalität durch den Bundesnachrichtendienst,* DöV 5/2006, 204-213

Van Atta, Dr., Richard: *Fifty years of innovation and Discovery*, DARPA: 50 Years of Bridging the Gap, 20-29, 2008

Waldrop, Mitch: *DARPA and the Internet Revolution,* DARPA: 50 Years of Bridging the Gap, 78-85, 2008



Nico Gronau

Europäisches Urheberrecht

Weiterer Harmonisierungsbedarf oder ein einheitliches Europäisches Urheberrechtsgesetz?

Diplomica 2010 / 184 Seiten / 49,50 Euro

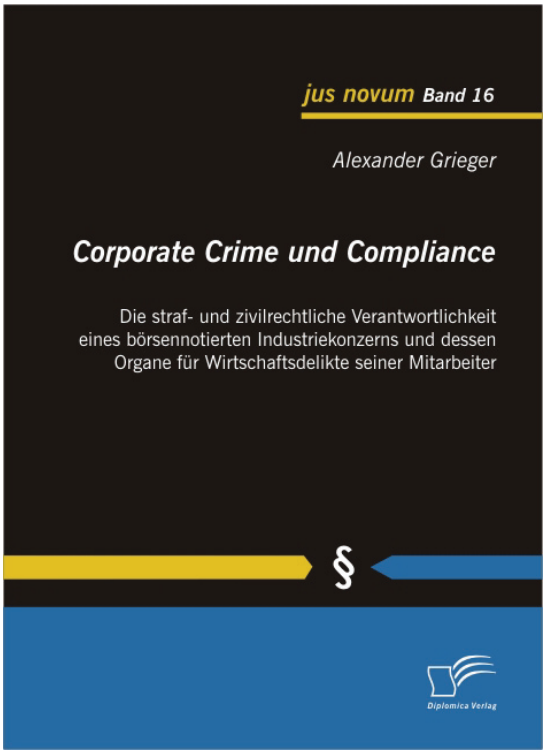
ISBN 978-3-8366-8985-4

EAN 9783836689854

Das Buch widmet sich der Frage, ob und inwieweit im Bereich des Urheberrechts zusätzlicher europarechtlicher Regelungsbedarf besteht. Der Autor zeigt auf, ob dieser Handlungsbedarf des Gemeinschaftsgesetzgebers besser durch Harmonisierungsmaßnahmen erfüllt werden kann oder ob ein einheitliches Europäisches Urheberrechtsgesetz eine vorteilhaftere Lösung darstellen würde.

Beginnend mit allgemeinen Erläuterungen zum Charakter und den Quellen des Europarechts sowie ergänzenden Betrachtungen zu internationalen Urheberrechtsabkommen, die Einfluss auf das Gemeinschaftsrecht haben, erläutert der Autor die europarechtlichen Zuständigkeiten des Gemeinschaftsgesetzgebers für den Bereich des Urheberrechts. Anschließend werden die materiell-rechtlichen Sachfragen des Urheberrechts aus dem acquis communautaire herausgearbeitet. Nach denselben Kriterien werden die nationalen Regelungen von Deutschland, Polen, Ungarn, Estland und Großbritannien untersucht.

Die hieraus resultierenden Ergebnisse nutzt der Autor zu einem grafisch unterstützten Vergleich des europäischen Schutzniveaus mit dem der nationalen Urheberrechtsordnungen. Ergänzend werden Sachverhalte zusammengetragen, die als regelungsbedürftig erachtet werden. Die Multimediaprodukte stehen hierbei im Fokus.



Alexander Grieger
Corporate Crime und Compliance
Die straf- und zivilrechtliche Verantwortlichkeit eines börsennotierten Industriekonzerns und dessen Organe
für Wirtschaftsdelikte seiner Mitarbeiter

Diplomica 2010 / 220 Seiten / 49,50 Euro

ISBN 978-3-8428-5316-4

EAN 9783842853164

Dieses Fachbuch, das durch die „Causa Siemens“ inspiriert wurde, stellt einzelne Wirtschaftsdelikte vor, mit welchen auf Grund der besonderen Strukturen eines börsennotierten Industriekonzerns vermehrt gerechnet werden muss. Ausgehend von diesem Fundament wird zuerst die strafrechtliche, dann die zivilrechtliche Verantwortlichkeit von Unternehmensorganen sowie des Unternehmens an sich beleuchtet. Zuletzt werden kurz einzelne Instrumente vorgestellt und bewertet, welche zur Begrenzung von Verantwortlichkeiten häufiger diskutiert werden.

Die Besonderheit dieses Buches besteht darin, dass die Themen nicht nur aus Richtung eines Rechtsgebietes, d.h. Strafrecht oder Zivilrecht, sondern aus Sicht beider Denkweisen umfassend dargestellt werden. Daneben fließen auch Ansatzpunkte aus der betriebswirtschaftlichen Praxis mit ein, die dieses Fachbuch sowohl für Einsteiger als auch Fortgeschrittene gleichermaßen interessant machen dürften.

Dieses Fachbuch basiert auf einer im Jahr 2008 im Studiengang Internationales Wirtschaftsrecht an der Friedrich-Alexander-Universität Erlangen-Nürnberg eingereichten Abschlussarbeit, welche im Jahr 2010 mit dem Luise Prell-Stiftungspreis für hervorragende wissenschaftliche Abschlussarbeiten ausgezeichnet wurde.

Ulrike Liss

Arbeitnehmerdatenschutz in IT-Entwicklungsprojekten

Datenschutzrechtliche Vorgaben bei der Entwicklung und Einführung von Personalinformationssystemen

Diplomica 2011 / 112 Seiten / 49,50 Euro

ISBN 978-3-8428-5407-9

EAN 9783842854079

Personalabteilungen in Unternehmen nutzen heute leistungsfähige IT-Systeme in nahezu jedem Tätigkeitsgebiet des Personalmanagements. Solche Personalinformationssysteme befassen sich überwiegend mit Daten, die unmittelbar oder mittelbar mit dem Beschäftigten in Beziehung stehen. Zum Schutz der Arbeitnehmerdaten dienen die Datenschutzgesetze.

Diese Studie ist ein Leitfaden, der den für die Entwicklung und Einführung von Personalinformationssystemen Verantwortlichen im Unternehmen das erforderliche datenschutzrechtliche Wissen vermittelt, spezifische Hinweise gibt und das Augenmerk für datenschutzrelevante Sicherheitslücken und Bedrohungen durch den Einsatz des Systems schult.

Anhand eines Phasenmodells werden die für jede Phase typischen Fragestellungen, die bei der Entwicklung und Einführung eines Personalinformationssystems auftreten, untersucht und beispielhaft Lösungen aufgezeigt.

Sarah C. Strauss

Neukundengewinnung und Kundenbindung im Internethandel unter Berücksichtigung rechtlicher Aspekte

Neukundengewinnung und Kundenbindung im Internethandel unter Berücksichtigung rechtlicher Aspekte

Diplomica 2011 / 164 Seiten / 49,50 Euro

ISBN 978-3-8428-5613-4

EAN 9783842856134

Heute ist das Internet als Kommunikationsmedium sowie als Transaktionsplattform selbstverständlich. Seit im Jahr 1995 auch die kommerzielle Benutzung des interaktiven Mediums zugelassen wurde, ist ein Ende des Wachstums, besonders für den Onlinehandel, nicht abzusehen. Der Onlinehandel ist der umsatzstärkste Versandhandelszweig in Deutschland. Durch das schnelle Voranschreiten der "digitalen Welt" haben sich die Marktbedingungen grundsätzlich geändert. Für Onlinehändler ist es aufgrund der steigenden Markttransparenz und des höheren Informationsgrades der Kunden schwieriger geworden eine Beziehung zu den Kunden aufzubauen. Auf der anderen Seite bietet das Internet vielfältige Möglichkeiten, die Konsumenten anzusprechen und persönliche Daten zu generieren. Die virtuelle Neukundengewinnung und Kundenbindung stellen daher eine Herausforderung für jedes im Internet vertretene Unternehmen dar.

Diese Untersuchung setzt sich mit Instrumenten und Maßnahmen der Neukundengewinnung sowie Kundenbindung im Internethandel auseinander. Ziel ist die Beantwortung der Fragestellung, ob die ausgewählten kundenpolitischen Aspekte mit dem deutschen Rechtsrahmen, insbesondere des UWG, zu vereinbaren sind und darüber hinaus eine nachhaltige Wirkung entfalten.