

Prof. Dr. Viola Schmid, LL.M. (Harvard)

Informations- und Datenschutzrecht I

Modul 3

DATUM	MODUL	TITEL
15.11.2005	3	IT-Sicherheit – die Convention on Cybercrime

A. Grundlagen des Völkerrechts	3
I. Begriff des Völkerrechts	3
II. Rechtsquellen des Völkerrechts	3
1. Völkerrechtliche Verträge.....	4
2. Gewohnheitsrecht	4
3. Allgemeine Rechtsgrundsätze.....	4
III. Abgrenzung Völkerrecht – Europarecht	5
1. Grundsätzliche Erkenntnisse zum Völkerrecht	5
2. Grundsätzliche Erkenntnisse zum Europarecht.....	5
3. Besonderheiten im Recht der Europäischen Union (EU).....	6
IV. Grundgesetz und Völkerrecht.....	7
1. Übertragung von Hoheitsrechten (Art. 24 Abs. 1 GG)	7
2. Kollektives Sicherheitssystem (Art. 24 Abs. 2 GG)	7
3. Allgemeine Regeln des Völkerrechts (Art. 25 GG)	7
4. Völkerrechtliche Verträge (Art. 59 GG)	8
B. Der Europarat.....	9
I. Allgemeines	9
II. Struktur.....	10
C. Die EMRK.....	10
I. Allgemeines	10
II. Klageverfahren vor dem EGMR.....	11
III. Informationsfreiheit und Datenschutz in der EMRK.....	11
D. Rechtslage in Deutschland aus einer strafrechtlichen Perspektive (StGB).....	12
I. Vorbemerkung zum deutschen Strafrecht und einigen allgemeine Voraussetzungen der Strafbarkeit und Strafverfolgung.....	12
1. (Neben)Strafrecht – Rechtsquellen	12
2. Geltungsbereich des deutschen Strafrechts	13
3. Täterschaft und Teilnahme.....	15
4. Prüfungsschema	16
5. Eröffnung des Geltungsbereichs des deutschen Strafrechts bei Internet-Nutzung – ein ausgewähltes Beispiel aus der Rechtsprechung.....	16
II. Deutsches Strafgesetzbuch: Informationsspezifische Delikte	18
1. Integration elektronischer Dokumente in die Vorschriften des StGB	18
2. Informationsspezifische Delikte.....	20

3.	Anwendung des StGB auf neue Informationstechnologien	23
E.	<i>Convention on Cybercrime (CCC)</i>	27
I.	Grundlagen	27
1.	Fundstellen.....	27
2.	Auslegung von völkerrechtlichen Verträgen.....	28
3.	Grammatische Auslegung und authentische Sprachen.....	28
II.	Literatur	29
III.	Cybercrime - Konvention: Allgemeine Bestimmungen	29
1.	Geltungsbereich (jurisdiction).....	29
2.	Vorsatz und „Befugnis“	30
3.	Teilnahme, Versuch und Verantwortlichkeit juristischer Personen	31
4.	Bedingungen und Garantien (conditions and safeguards).....	32
IV.	Cybercrime – Konvention: Einzelne Tatbestände	34
1.	Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und –systemen 34	
2.	Computerstraftaten (computer - related offences).....	36
3.	Kinderpornographie	37
4.	Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte....	38
V.	Cybercrime – Konvention: Strafverfolgung	39
1.	Artikel 16 und 17 CCC, Rasche Sicherung und Weitergabe gespeicherter Daten (expedited preservation and partial disclosure of stored computer data)	39
2.	Artikel 18 CCC, Herausgabeordnung (production order)	40
3.	Artikel 19 CCC, Durchsuchung und Beschlagnahme gespeicherter Computerdaten (search and seizure of stored computer data).....	40
4.	Artikel 20 CCC, Echtzeit – Erhebung von Verbindungsdaten (real – time collection of traffic data)41	
5.	Artikel 21 CCC, Abfangen von Verbindungsdaten (interception of content data)	42
F.	<i>Rahmenbeschluss 2005/222/JI des Rates der Europäischen Union über Angriffe auf Informationssysteme</i>	43
I.	Zur rechtlichen Bedeutung von Rahmenbeschlüssen	43
II.	Inkrafttreten	43
III.	Sanktionen bei Angriffen auf Informationssysteme im einzelnen	44
G.	<i>Vorschlag für eine Richtlinie über die Vorratsspeicherung von Daten</i>	50
I.	Zur rechtlichen Bedeutung einer Richtlinie	50
II.	Definition der Vorratsdatenspeicherung	50
III.	Gegenwärtige Rechtslage bei der Speicherung dynamischer IP-Adressen	51
IV.	Zusammenfassung des Richtlinienvorschlags zur Vorratsdatenspeicherung	51

A. Grundlagen des Völkerrechts

I. Begriff des Völkerrechts

Das Völkerrecht regelt die Beziehungen der Völkerrechtssubjekte untereinander.

Völkerrechtssubjekte sind etwa:

- Staaten
- Internationale Organisationen (Vereinte Nationen (UN), Europarat)¹
- „Traditionelle Völkerrechtssubjekte“, etwa: „Heiliger Stuhl“, Internationales Komitee vom Roten Kreuz, Malteser Orden
- bisweilen: Nichtregierungsorganisationen (Non Governmental Organisations, NGO's)
- Individuen (soweit ihnen subjektiv-öffentliche Rechte und ein Verfahren zur Durchsetzung dieser Rechte eingeräumt werden; so z.B. in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK))

Anders als es die grammatische Auslegung nahe legt, sind die „Völker“ historisch gesehen keine Subjekte des Völkerrechts. Nur im Hinblick auf das in seinem Umfang und seinen Wirkungen unklare Selbstbestimmungsrecht der Völker kommt ihnen Völkerrechtssubjektivität zu. In einer historischen Auslegung handelt es sich beim Völkerrecht zunächst nur um „Staatenrecht“ (was ein völlig ungebräuchlicher Ausdruck ist). Dieses „Staatenrecht“ entwickelt sich zu einem Recht, das Völker (in ihrer Selbstbestimmung) und Einzelne schützt und verpflichtet. Dieser Prozess wird in anderen Rechtsordnungen durch eine andere Wortwahl als im deutschen Recht reflektiert. Statt von Völkerecht spricht man dort von internationalem (öffentlichem) Recht.

II. Rechtsquellen des Völkerrechts

Art. 38 des Statuts des Internationalen Gerichtshofs

1. Der Gerichtshof, dessen Aufgabe es ist, die ihm unterbreiteten Streitigkeiten nach dem Völkerrecht zu entscheiden, wendet an

- (a) internationale Übereinkünfte allgemeiner oder besonderer Natur, in denen von den streitenden Staaten ausdrücklich anerkannte Regeln festgelegt sind;
- (b) das internationale Gewohnheitsrecht als Ausdruck einer allgemeinen, als Recht anerkannten Übung;
- (c) die von den Kulturvölkern anerkannten allgemeinen Rechtsgrundsätze;
- (d) vorbehaltlich des Artikels 59 richterliche Entscheidungen und die Lehrmeinung der fähigsten Völkerrechtler der verschiedenen Nationen als Hilfsmittel zur Feststellung von Rechtsnormen.

¹ Im Cyberlaw gibt es von den UN etwa: Guidelines concerning computerized Personal Data Files adopted by the General Assembly on 14 December 1990 (englische und deutsche Fassung http://www.datenschutz-berlin.de/recht/int/uno/gl_pbden.htm)

2. Diese Bestimmung lässt die Befugnis des Gerichtshofs unberührt, mit Zustimmung der Parteien ex aequo et bono zu entscheiden

1. Völkerrechtliche Verträge

Völkerrechtliche Verträge entstehen wie privatrechtliche Verträge durch aufeinander bezogene, übereinstimmende Willenserklärungen (mit Rechtsbindungswillen) der Vertragsparteien. Beispiele sind multilaterale und bilaterale Verträge. Siehe später zu der Problematik der „Safe-Harbor-Vereinbarungen und Erklärungen“ zwischen der EG und den Vereinigten Staaten von Amerika (USA).

2. Gewohnheitsrecht

Bei Gewohnheitsrecht handelt sich um Recht, das nicht durch einen Gesetzgeber oder durch Vertrag geschaffen wird. Die Geltung von Gewohnheitsrecht beruht auf zwei Komponenten:

- Einheitliche Übung von gewisser Dauer und Verbreitung (Consuetudo, objektives Element)
- „Allgemeine“ Anerkennung als Recht (Opinio iuris, subjektives Element)

Die Nennung lateinischer Begriffe in dieser Vorlesung verdeutlicht, dass es sich bei Gewohnheitsrecht um eine ebenso bedeutende wie alte Rechtsquelle handelt. Beide Komponenten müssen aufeinander bezogen sein:

- Aus bloßer Übung eines bestimmten Verhaltens kann kein Recht entstehen (Angriffskrieg).
- Aus bloßer Rechtsüberzeugung kann kein Recht entstehen, weil es vorher nicht erkennbar ist (siehe allerdings die Problematik des „spontanen Gewohnheitsrechts“).

Zahlreiche Normen des Völkergewohnheitsrechts sind mittlerweile kodifiziert, so etwa in den Wiener Übereinkommen zum Recht der diplomatischen und konsularischen Beziehungen oder in der Wiener Vertragsrechtskonvention².

3. Allgemeine Rechtsgrundsätze

Es handelt sich um Grundsätze, Rechtsprinzipien, die den meisten innerstaatlichen Rechtsordnungen gemeinsam sind (z.B. Treu und Glauben, Verbot des widersprüchlichen Verhaltens).

² <http://www.jura.uni-sb.de/BGBI/TEIL2/1990/19901415.2.HTML>

III. Abgrenzung Völkerrecht – Europarecht

Das Europarecht stellt auch (regionales) Völkerrecht dar. Die ersten europarechtlichen Normen waren völkerrechtliche Verträge zwischen Staaten. Mittlerweile hat sich das Europarecht aber stark weiterentwickelt und ist zu einem Rechtsgebiet ganz eigener Art geworden. Das Europarecht wird daher hier als eigenständige Rechtsquelle begriffen, die sich in wesentlichen Grundsätzen vom (globalen) Völkerrecht unterscheidet.

1. Grundsätzliche Erkenntnisse zum Völkerrecht

- Gleichberechtigung: gleiche Rechte aller Rechtssubjekte bei Rechtsbildung und Rechtsdurchsetzung (Grund: Souveränität des Völkerrechtssubjekts Staat)
- Konsensprinzip: keine Mehrheitsentscheidungen (Grund: Souveränität des Völkerrechtssubjekts Staat)
- Souveränität (in externer Betrachtung): kein Rechtssubjekt wird dem fremden Willen eines anderen Staates oder eines übergeordneten Organs unterworfen
- Keine zwangsweise Rechtsdurchsetzung
- Keine obligatorische Gerichtsbarkeit: Es bedarf immer der einzelnen Unterwerfung unter die Gerichtsbarkeit des Internationalen Gerichtshofs in Den Haag (Art. 36 des Statuts des IGH „...alle ihm von den Parteien unterbreiteten Rechtssachen ...“)
- Erfordernis der Umwandlung (Transformation) eines völkerrechtlichen Vertrages in innerstaatliches Recht. Dies erfolgt entweder über eine generelle Regelung in der Verfassung (z.B. für die allgemeinen Regeln des Völkerrechts Art. 25 S. 1 GG) oder durch Ratifikation des völkerrechtlichen Vertrages.³

2. Grundsätzliche Erkenntnisse zum Europarecht

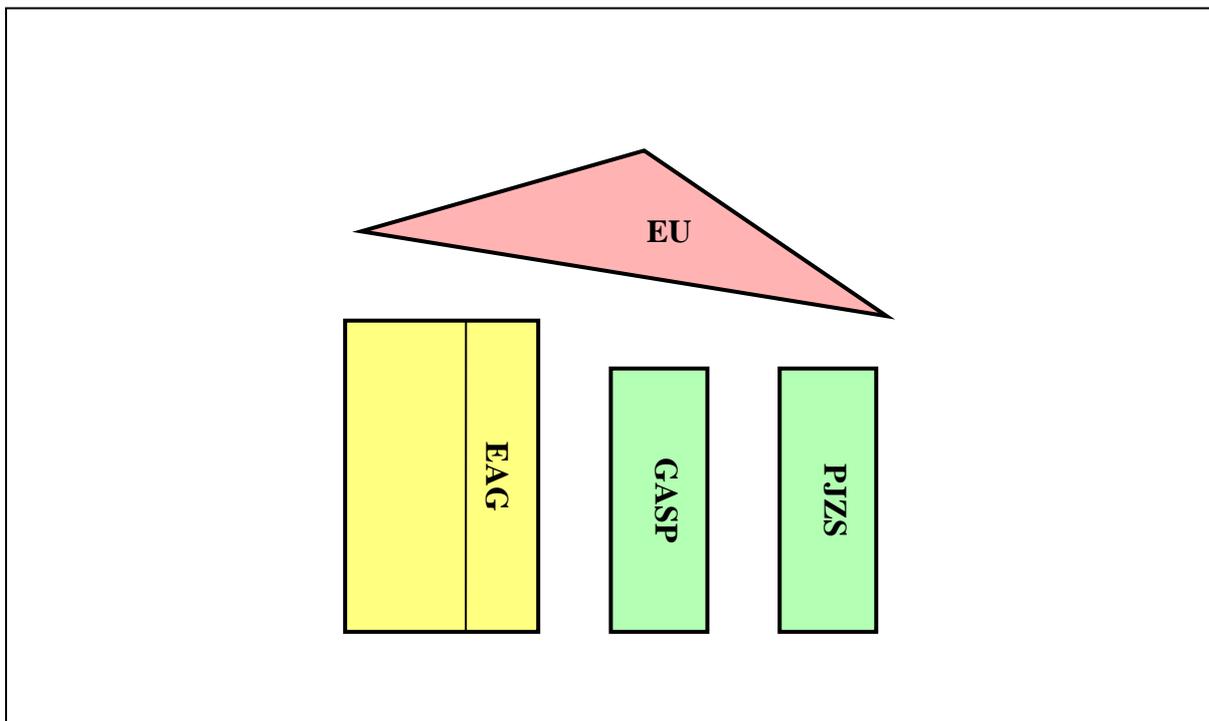
- Supranationalität: Schaffung einer eigenständigen Rechtsordnung, d.h. zwischen den Mitgliedsstaaten finden eigene Regeln Anwendung, welche zum einen die Regeln des allgemeinen, globalen Völkerrechts und zum anderen die innerstaatlichen Regeln der Mitgliedsstaaten ersetzen.
- Mehrheitsentscheidungen: Mitgliedstaaten können auch gegen ihren Willen gebunden werden.
- Anwendungsvorrang des Gemeinschaftsrechts vor dem mitgliedstaatlichen Recht

³ FEX: Nach deutschem Recht ist eine Ratifikation immer dann erforderlich, wenn es sich nicht um die von Art. 25 S. 1 GG erfassten allgemeinen Regeln des Völkerrechts handelt. Andere Staaten transformieren alle völkerrechtlichen Normen durch eine Generalklausel wie Art. 25 S. 1 GG in ihr jeweiliges innerstaatliches Recht.

- Schadenersatzpflicht der Mitgliedstaaten gegenüber dem Einzelnen bei Verletzung von Gemeinschaftsrecht (nicht normiert, vom Europäischen Gerichtshof (EuGH) entwickelt; zu unterscheiden von der Schadenersatzpflicht der EG für Schäden, die durch ihre Organe und Bediensteten verursacht wurden, Art. 288 EG)
- Obligatorische Gerichtsbarkeit durch den Europäischen Gerichtshof (EuGH)
- kein Transformationsakt erforderlich: Verordnung und Entscheidung gelten unmittelbar. Eine Richtlinie bedarf zwar grundsätzlich eines Umsetzungsaktes (Art. 249 EG), nicht jedoch, wenn der Mitgliedstaat untätig bleibt. Dann kann gemäß dem Grundsatz der effektiven Durchsetzung des Gemeinschaftsrechts (effet utile) die unmittelbare Geltung der Richtlinie eintreten.
- eigene Befugnis zum Abschluss völkerrechtlicher Verträge, die den Mitgliedstaaten die Vertragschlusskompetenz in diesen Bereichen nimmt. Beispiele: Art. 300-304, 310 EG⁴ sowie Kompetenzen kraft „implied powers“

3. Besonderheiten im Recht der Europäischen Union (EU)

Für die mit dem EU-Vertrag eingeführten gemeinsamen Politikbereiche GASP (Gemeinsame Außen- und Sicherheitspolitik) und PJZ (Polizeiliche und justizielle Zusammenarbeit in Strafsachen) gelten die genannten Prinzipien nicht, sie sind Formen völkerrechtlicher Zusammenarbeit, die insbesondere keine Mehrheitsentscheidungen kennt.



⁴ <http://europa.eu.int/eur-lex/de/treaties/selected/livre257.html>

IV. Grundgesetz und Völkerrecht

1. Übertragung von Hoheitsrechten (Art. 24 Abs. 1 GG)

Art. 24 Abs.1 GG

Der Bund kann durch Gesetz Hoheitsrechte auf zwischenstaatliche Einrichtungen übertragen.

Unter zwischenstaatlichen Einrichtungen im Sinne dieses Artikels versteht man in erster Linie internationale Organisationen. Diese Norm war ursprünglich Grundlage der Mitgliedschaft der Bundesrepublik in den Europäischen Gemeinschaften. Seit 1992 besteht für das „Europarecht“ in Art. 23 GG eine Sonderregelung.

2. Kollektives Sicherheitssystem (Art. 24 Abs. 2 GG)

Art. 24 Abs. 2 GG

Der Bund kann sich zur Wahrung des Friedens einem System gegenseitiger kollektiver Sicherheit einordnen; er wird hierbei in die Beschränkungen seiner Hoheitsrechte einwilligen, die einen friedliche und dauerhafte Ordnung in Europa und zwischen den Völkern der Welt herbeiführen und sichern.

Unter einem System gegenseitiger kollektiver Sicherheit versteht man Systeme, in denen sich die Mitglieder gegenseitig Hilfe für den Fall eines Angriffs durch einen Mitgliedstaat versprechen. Ein Beispiel hierfür sind die UN. Solche Bündnisse sollen der Friedenssicherung dienen. Strittig ist, ob auch Verteidigungsbündnisse gegen Angreifer von außen, also Nichtmitgliedern, von dieser Norm umfasst sind (Beispiel NATO).

3. Allgemeine Regeln des Völkerrechts (Art. 25 GG)

Art. 25 GG

Die allgemeinen Regeln des Völkerrechts sind Bestandteil des Bundesrechtes. Sie gehen den Gesetzen vor und erzeugen Rechte und Pflichten unmittelbar für die Bewohner des Bundesgebiets.

Zu den allgemeinen Regeln des Völkerrechts zählen etwa das Gewohnheitsrecht und die allgemeinen Rechtsgrundsätze. Durch Art. 25 GG werden alle deutschen Staatsorgane zur Einhaltung der allgemeinen Regeln des Völkerrechts verpflichtet, ohne dass es eines weiteren Transformationsaktes in innerstaatliches Recht bedürfte.

4. Völkerrechtliche Verträge (Art. 59 GG)

a. Vertretungsmacht (extern)

Art. 59 Abs. 1 GG

Der Bundespräsident vertritt den Bund völkerrechtlich. Er schließt im Namen des Bundes die Verträge mit auswärtigen Staaten.(...)

Art. 59 Abs. 1 GG betrifft nur die Außenvertretung des Bundes, nicht die innerstaatliche Willensbildung, für die Regierung und Parlament zuständig sind. Entgegen dem Wortlaut, der die Vertretungskompetenz nur dem Bundespräsidenten zuschreibt, ist aber auch die Bundesregierung bzw. der jeweilige Bundesminister zum Abschluss völkerrechtlicher Verträge befugt.

b. Vertretungsmacht (intern)

Art. 59 Abs. 2 GG

Verträge, welche die politischen Beziehungen des Bundes regeln oder sich auf Gegenstände der Bundesgesetzgebung beziehen, bedürfen der Zustimmung oder der Mitwirkung der jeweils für die Bundesgesetzgebung zuständigen Körperschaften in der Form eines Bundesgesetzes. (...)

Art. 59 Abs. 2 GG stellt das innerstaatliche Erfordernis auf, dass das Parlament und ggf. der Bundesrat dem völkerrechtlichen Vertrag durch Bundesgesetz zustimmt. Dies gilt allerdings nur für so genannte hochpolitische Verträge, die von gewisser Bedeutung sind.

Das Zustimmungsgesetz hat zwei Wirkungen:

- die Exekutive wird zum Vertragsschluss ermächtigt.
- der völkerrechtliche Vertrag wird in innerstaatliches Recht transformiert.

c. Verfahren bei Abschluss eines völkerrechtlichen Vertrages

➤ Verhandlungen

Der Vertragstext wird durch die Delegierten der Staaten ausgehandelt.

➤ Paraphierung

Der Vertragstext wird durch die Delegierten vorläufig als Ergebnis der Verhandlungen angenommen. Dies geschieht durch Unterzeichnung mit einer Paraphe (Namenskürzel). Änderungen des Vertragstextes sind jetzt nur noch durch die erneute Aufnahme von Verhandlungen möglich.

➤ Unterzeichnung

Mit der Unterzeichnung durch ein abschlussbefugtes Organ wird der Vertragstext als endgültig festgelegt. Änderungen sind nicht mehr möglich. Sofern das Erfordernis der Ratifikation (siehe zugleich) nicht ausdrücklich in den Vertrag aufgenommen ist, tritt die völkerrechtliche Bindung bereits zu diesem Zeitpunkt ein.

➤ **Innerstaatliches Zustimmungsverfahren (innerstaatliche Ratifikation)**

Die innerstaatlichen Organe werden beteiligt. In der Bundesrepublik erfolgt dies gemäß Art. 59 Abs. 2 GG durch das Zustimmungsgesetz. Bei weniger bedeutsamen Verträgen entfällt dieses Erfordernis.

➤ **Ratifikation (völkerrechtliche Ratifikation)**

Die Ratifikation im völkerrechtlichen Sinne bedeutet die Abgabe der Erklärung des zuständigen Organs (in der Bundesrepublik gemäß Art. 59 Abs. 1 GG des Bundespräsidenten) gegenüber dem Vertragspartner, dass der Vertrag als völkerrechtlich bindend angesehen wird.

- Bsp.: Die Convention on Cybercrime (CCC) des Europarates ist bisher von 31 Staaten unterzeichnet worden, und von 11 Staaten ratifiziert⁵ worden. Nachdem 5 Staaten (und davon 3 Mitgliedstaaten des Europarats) die CCC unterzeichnet und ratifiziert hatten, ist die CCC am 1.07.2004 für diejenigen Staaten, die sie ratifiziert haben, in Kraft getreten. Deutschland hat die Convention on Cybercrime zwar unterzeichnet, bisher aber nicht ratifiziert, obwohl dies für die vergangene Legislaturperiode vorgesehen war.

Art. 36 CCC Signature and entry into force

- (1) This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
- (2) This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
- (3) This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.**
- (4) In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

B. Der Europarat

I. Allgemeines

Der Europarat ist eine 1949 gegründete Internationale Organisation, die sich die Förderung wirtschaftlicher, sozialer, kultureller und humanitärer Ziele zur Aufgabe gemacht hat. Mitglied können nur europäische Länder werden, welche die Grundsätze der Rechtsstaatlichkeit, der Demokratie, der Menschenrechte sowie der Grundfreiheiten anerkennen. Derzeit hat der

⁵ Die CCC wurde bisher von Albanien, Bulgarien, Dänemark, Mazedonien, Estland, Kroatien, Litauen, Rumänien, Slowenien, Ungarn und Zypern ratifiziert.

Europarat 46 Mitglieder. Er arbeitet eng mit der EU, den Vereinten Nationen und der OECD zusammen. Sitz des Europarats ist Straßburg.

Bis heute hat der Europarat 199 Konventionen verabschiedet. Die bekannteste ist die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) von 1950. Weitere wichtige Abkommen sind etwa die Anti-Folter-Konvention, die Europäische Sozialcharta und das Rahmenabkommen zum Schutz nationaler Minderheiten.

Beachte: Der Europarat ist eine Internationale Organisation. Er ist zu unterscheiden vom Rat der Europäischen Gemeinschaften, einem Organ der EG, und dem Europäischen Rat, dem Handlungsorgan der EU.

II. Struktur

Der Europarat besitzt zwei Organe, das Ministerkomitee und die Beratende Versammlung.

Das Ministerkomitee setzt sich aus den Außenministern der Mitgliedsstaaten zusammen. Es ist das Entscheidungs- und Exekutivorgan des Europarates, das allein befugt ist, im Namen des Europarates zu handeln.

Die Beratende Versammlung (oder Parlamentarische Versammlung) setzt sich aus Abgeordneten der Mitgliedsstaaten zusammen. Die Zahl der Abgeordneten, die jedes Mitgliedsland entsenden darf, richtet sich nach der Bevölkerungszahl. Derzeit hat die Versammlung 630 Mitglieder. Ihre Aufgabe besteht darin, für das Ministerkomitee Empfehlungen und Stellungnahmen auszuarbeiten. Unterstützt wird sie dabei durch das Generalsekretariat, das einen Verwaltungsapparat von ca. 1800 Beamten zur Verfügung stellt.

C. Die EMRK

I. Allgemeines

Die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) wurde 1950 im Rahmen des Europarates verabschiedet. Sie ist von 45 Mitgliedstaaten des Europarates ratifiziert worden.⁶ Ergänzt wird die EMRK von 11 Zusatzprotokollen, denen jedoch nicht alle Vertragsstaaten der EMRK beigetreten sind.

Die EMRK besteht im Wesentlichen aus zwei Abschnitten. In Abschnitt I befindet sich der Katalog der Menschenrechte und Grundfreiheiten, in Abschnitt II ist unter anderem das völkerrechtliche Durchsetzungsverfahren vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) geregelt.

⁶ Einziges Mitgliedsland des Europarates, das die Konvention nicht ratifiziert hat, ist Monaco.

II. Klageverfahren vor dem EGMR

Seit Inkrafttreten des 11. Zusatzprotokolls zur EMRK (1998) ist der Gerichtshof das einzige Judikativorgan der EMRK. Die Zahl der Richter entspricht derjenigen der Mitgliedstaaten.

Art. 34 EMRK [Individualbeschwerden]

Der Gerichtshof kann von jeder natürlichen Person, nichtstaatlichen Organisation oder Personengruppe, die behauptet, durch eine der Hohen Vertragsparteien in einem der in dieser Konvention oder den Protokollen dazu erkannten Rechte verletzt zu sein, mit einer Beschwerde befasst werden. Die Hohen Vertragsparteien verpflichten sich, die wirksame Ausübung dieses Rechts nicht zu behindern.

Art. 35 EMRK [Zulässigkeitsvoraussetzungen]

Der Gerichtshof kann sich mit einer Angelegenheit erst nach Erschöpfung aller innerstaatlichen Rechtsbehelfe in Übereinstimmung mit den allgemein anerkannten Grundsätzen des Völkerrechts und nur innerhalb einer Frist von sechs Monaten nach der endgültigen innerstaatlichen Entscheidung befassen.

(...)

Zulässigkeitsvoraussetzungen einer Individualbeschwerde vor dem EGMR

➤ Beschwerdeführer

Jede natürliche Person, nichtstaatliche Organisation oder Personengruppe, Art. 34 EMRK.

➤ Beschwerdegegner

Mitgliedstaat der EMRK

➤ Beschwerdebefugnis

Beschwerdeführer muss geltend machen, in den in der EMRK gewährten Menschenrechten und Grundfreiheiten verletzt zu sein.

➤ Rechtswegerschöpfung

Beschwerdeführer muss alle innerstaatlichen Rechtsmittel ausgeschöpft haben, Art. 35 EMRK.

➤ Frist

Die Beschwerde muss 6 Monate nach der letzten endgültigen innerstaatlichen Entscheidung eingereicht werden.

III. Informationsfreiheit und Datenschutz in der EMRK

Spezielle Regelung für den Datenschutz ist auf Ebene des Europarats die Europäische Datenschutzkonvention von 1980. Aber auch einige Artikel der EMRK enthalten Regelungen, aus denen sich informations- und datenschutzrechtliche Grundsätze herleiten lassen. Dabei handelt es sich um Art. 8 EMRK, der den Schutz des Privat- und Familienlebens zum Inhalt hat, sowie Art. 10 EMRK, der die Meinungs- und Informationsfreiheit garantiert.

Art. 8 EMRK [Recht auf Achtung des Privat- und Familienlebens]

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Art. 10 EMRK [Freiheit der Meinungsäußerung]

(1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.(...)

(2) Die Ausübung dieser Freiheiten ist mit Pflichten und Verantwortung verbunden; sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung.

D. Rechtslage in Deutschland aus einer strafrechtlichen Perspektive (StGB)⁷**I. Vorbemerkung zum deutschen Strafrecht und einigen allgemeine Voraussetzungen der Strafbarkeit und Strafverfolgung****1. (Neben)Strafrecht – Rechtsquellen**

Die Strafbarkeit eines Tuns oder Unterlassens bemisst sich

- zum einen nach dem Strafgesetzbuch (StGB)
- zum anderen nach dem sogenannten Nebenstrafrecht. Beispiele sind etwa

§ 44 Bundesdatenschutzgesetz (BDSG) [Strafvorschriften]

Wer eine in § 43Abs.2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 43 BDSG [Strafvorschriften]

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet (...).

⁷ „A-Phase“ der Vorlesung: Mit weiteren Bestimmungen des „Nebenstrafrechts“ (etwa den Vorschriften des Bundesdatenschutzgesetzes §§ 43 f) befasst sich die Vorlesung zu einem späteren Zeitpunkt ausführlicher. Des Weiteren verzichtet die Vorlesung vorläufig auf die Behandlung von Ordnungswidrigkeiten.

§ 148 Telekommunikationsgesetz (TKG) [Strafvorschriften]

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer
1. entgegen § 89 Satz 1 oder 2 eine Nachricht abhört oder den Inhalt einer Nachricht oder die Tatsache ihres Empfangs einem anderen mitteilt (...).

Dieses so genannte Nebenstrafrecht ist den Strafgesetzen des StGB gleichgestellt, insbesondere finden die Regelungen des Allgemeinen Teils des StGB auch auf das Nebenstrafrecht Anwendung.

2. Geltungsbereich des deutschen Strafrechts

Mit dem Geltungsbereich wird festgelegt, wann deutsches Strafrecht von den deutschen Strafverfolgungsbehörden anzuwenden ist. Es gibt unterschiedliche Sachverhalte, etwa wenn die Straftat von einem Deutschen im Ausland begangen worden ist oder ein Ausländer eine Tat in Deutschland begangen hat.

a. Regel: Territorialprinzip**§ 3 StGB [Territorialprinzip]**

Das deutsche Strafrecht gilt für die Taten, die im Inland begangen werden.

Anknüpfungspunkt ist der Tatort. Unabhängig von der Nationalität des Täters findet demzufolge deutsches Strafrecht Anwendung. In § 9 Abs. 1 StGB wird der Begriff des Tatortes legal definiert.

§ 9 Abs. 1 StGB Ort der Tat

Eine Tat ist an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist (...).

Der Täter muss also nicht in Deutschland gehandelt haben, damit der Geltungsbereich des deutschen Strafrechts eröffnet ist. Es genügt, wenn der „Erfolg“ im Inland eintritt.

Das Flaggenprinzip in § 4 StGB ergänzt das Territorialprinzip hinsichtlich des Inlandbegriffes.

§ 4 StGB [Geltung für Taten auf deutschen Schiffen und Luftfahrzeugen]

Das deutsche Strafrecht gilt, unabhängig von dem Recht des Tatortes, für Taten, die auf einem Schiff oder Luftfahrzeug begangen werden, das berechtigt ist, die Bundesflagge oder das Staatszugehörigkeitszeichen der Bundesrepublik Deutschland zu führen.

b. Ausnahme 1: Personalitätsprinzip

Straftaten eines Deutschen können auch dann deutschem Strafrecht unterliegen, wenn sie im Ausland begangen wurden. Begründet wird dies mit der Bindung des Einzelnen an die deut-

sche Rechtsordnung. Niedergeschlagen hat sich dieses Prinzip in § 5 Nr. 8 und 9 StGB sowie § 7 Abs. 2 Nr. 1 StGB.

§ 5 Nr. 8 und 9 StGB [Auslandstaten gegen inländische Rechtsgüter]

Das deutsche Strafrecht gilt, unabhängig vom Recht des Tatorts, für folgende Taten, die im Ausland begangen werden: (...)

8. Straftaten gegen die sexuelle Selbstbestimmung

in den Fällen (...), wenn der Täter und der, gegen den die Tat begangen wird, zur Zeit der Tat Deutsche sind und ihre Lebensgrundlage im Inland haben, und

in den Fällen (...), wenn der Täter Deutscher ist;

9. Abbruch der Schwangerschaft (§ 218), wenn der Täter zur Zeit der Tat Deutscher ist und seine Lebensgrundlage im räumlichen Bereich des Gesetzes hat; (...)

§ 7 Abs. 2 Nr. 1 StGB [Geltung für Auslandstaten in anderen Fällen]

Für andere Taten, die im Ausland begangen werden, gilt das deutsche Strafrecht, wenn die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt und wenn der Täter

1. zur Zeit der Tat Deutscher war oder es nach der Tat geworden ist (...)

c. Ausnahme 2: Schutzprinzip

Das deutsche Strafrecht ist unabhängig vom Recht des Tatorts anwendbar, wenn es sich um Straftaten handelt, die sich gegen bestimmte inländische Rechtsgüter richten.

§ 5 Nr. 7 StGB [Auslandstaten gegen inländische Rechtsgüter]

Das deutsche Strafrecht gilt, unabhängig vom Recht des Tatorts, für folgende Taten, die im Ausland begangen werden: (...)

7. Verletzung von Betriebs- oder Geschäftsgeheimnissen eines im räumlichen Geltungsbereich dieses Gesetzes liegenden Betriebes, eines Unternehmens, das dort seinen Sitz hat, oder eines Unternehmen mit Sitz im Ausland, das von einem Unternehmen mit Sitz im räumlichen Geltungsbereich dieses Gesetzes abhängig ist und mit diesem einen Konzern bildet;

§ 7 Abs. 1 StGB [Auslandstaten gegen inländische Rechtsgüter]

Das deutsche Strafrecht gilt für Taten, die im Ausland gegen einen Deutschen begangen werden, wenn die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt.

Das deutsche Strafrecht gilt also auch für Taten im Ausland, die bestimmte inländische Rechtsgüter gefährden oder verletzen.

d. Ausnahme 3: Weltrechtsprinzip

Auslandstaten unterliegen dem deutschen Strafrecht, wenn sie sich gegen international geschützte Rechtsgüter wenden.

§ 6 Nr. 6 und 9 StGB [Auslandstaten gegen international geschützte Rechtsgüter]

Das deutsche Strafrecht gilt weiter, unabhängig vom Recht des Tatortes, für folgende Taten, die im Ausland begangen werden;

(...)

6. Verbreitung pornographischer Schriften in den Fällen der §§ 184a und 184b Abs. 1 bis 3, auch in Verbindung mit § 184c Satz 1;

(..)

9. Taten, die auf Grund eines für die Bundesrepublik Deutschland verbindlichen zwischenstaatlichen Abkommens auch dann zu verfolgen sind, wenn sie im Ausland begangen werden.

3. Täterschaft und Teilnahme

Das deutsche Strafrecht unterscheidet zwischen Täter, Anstifter und Gehilfen.

§ 25 Abs. 1 StGB [Täterschaft]

Als Täter wird bestraft, wer die Straftat selbst oder durch einen anderen begeht.

Eine Teilnahme an einer Tat ist durch Anstiftung oder Beihilfe möglich:

§ 26 StGB [Anstiftung]

Als Anstifter wird gleich einem Täter bestraft, wer vorsätzlich oder fahrlässig einen anderen zu dessen vorsätzlich begangener rechtswidriger Tat bestimmt hat.

§ 27 Abs. 1 StGB [Beihilfe]

Als Gehilfe wird bestraft, wer vorsätzlich oder fahrlässig einen anderen zu dessen vorsätzlich begangener rechtswidriger Tat Hilfe geleistet hat.

Der Strafbarkeit unterliegen nur natürliche Personen. Ein Unternehmen kann sich nur durch seine vertretungsberechtigten Personen, z.B. Geschäftsführer oder Vorstandsmitglieder „strafbar machen“. So ist z.B. im Fall CompuServe⁸ nicht die CompuServe Information Services GmbH zur strafrechtlichen Verantwortung gezogen worden, sondern der Geschäftsführer.

⁸ In diesem Fall ging es um die strafrechtliche Verantwortung von Internet Service Providern. CompuServe – bzw. der Geschäftsführer - sollte als Access-Provider für fremde pornographische Inhalte verantwortlich gemacht werden. Die Verurteilung in erster Instanz durch das AG München ist in der Berufung vom LG München I wieder aufgehoben worden. Urteil des LG München: MMR 2000, 171ff.

4. Prüfungsschema

- Geltungsbereich des deutschen Strafrechts eröffnet?
- Tatbestand
 - Objektiver Tatbestand (Äußere Merkmale): Täter, Tathandlung, Tatobjekt, Erfolg (bei Erfolgsdelikten), Kausalität und objektive Zurechenbarkeit
 - Subjektiver Tatbestand (Innere Merkmale): Vorsatz, Absichten, Motive
- Rechtswidrigkeit

Diese ist grundsätzlich indiziert. Rechtfertigungsgründe lassen die Strafbarkeit entfallen.

- Schuld
 - Schuldfähigkeit
 - Unrechtsbewusstsein
 - Spezielle strafsärfende oder –mildernde Schuldmerkmale
 - Fehlen von Schuldausschließungsgründen
- Strafaufhebungs- und -ausschließungsgründe (Absehen von Strafe)
 - Rücktritt vom Versuch
 - Tätige Reue

5. Eröffnung des Geltungsbereichs des deutschen Strafrechts bei Internet-Nutzung – ein ausgewähltes Beispiel aus der Rechtsprechung

Fundstelle: [BGHSt 46, 212](#), Rdn.45, 62 und 63

a. Fall 1:

Ein deutscher Staatsbürger stellt eine nach § 130 Abs. 1 Nr. 1, Nr. 2 und Abs. 3 StGB „strafbare“, sogenannte „Auschwitzlüge“, ins Internet.

Strafbarkeit nach § 130 StGB

§ 130 StGB [Volksverhetzung]

- (1) Wer in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören,
1. zum Haß gegen Teile der Bevölkerung aufstachelt oder zu Gewalt- oder Willkürmaßnahmen gegen sie auffordert oder
 2. die Menschenwürde anderer dadurch angreift, daß er Teile der Bevölkerung beschimpft, böswillig verächtlich macht oder verleumdet, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft.
- (2) (...)
- (3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer eine unter der Herrschaft des Nationalsozialismus begangene Handlung der in § 6 Abs. 1 des Völkerstrafge-

setzbuches bezeichneten Art in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören, öffentlich oder in einer Versammlung billigt, leugnet oder verharmlost. (...)

§ 6 VStGB [Völkermord]

Wer in der Absicht, eine nationale, rassische, religiöse oder ethnische Gruppe als solche ganz oder teilweise zu zerstören,

1. ein Mitglied der Gruppe tötet,
 2. einem Mitglied der Gruppe schwere körperliche oder seelische Schäden, insbesondere der in § 226 des Strafgesetzbuches bezeichneten Art, zufügt,
 3. die Gruppe unter Lebensbedingungen stellt, die geeignet sind, ihre körperliche Zerstörung ganz oder teilweise herbeizuführen,
 4. Maßregeln verhängt, die Geburten innerhalb der Gruppe verhindern sollen,
 5. ein Kind der Gruppe gewaltsam in eine andere Gruppe überführt,
- wird mit lebenslanger Freiheitsstrafe bestraft.

Prüfung

➤ Tatbestand

- Objektiver Tatbestand (Äußere Merkmale): Täter: Jeder, Tathandlung: leugnen, Tatobjekt: Äußerung im Zusammenhang mit Handlungen des Nationalsozialismus nach § 220a Abs. 1 StGB, Erfolg: konkrete Eignung zur Friedensstörung in der BRD
- Subjektiver Tatbestand (Innere Merkmale): Vorsatz

➤ Rechtswidrigkeit

Diese ist grundsätzlich indiziert.

➤ Schuld

➤ Strafaufhebungs- und -ausschließungsgründe

b. Fall 2:

Ein australischer Staatsbürger stellt die gleiche Behauptung ins Internet (über einen australischen Server). Das Landgericht kann nicht feststellen, dass außer den ermittelnden Polizeibeamten Internetnutzer aus Deutschland die Homepage des australischen Staatsbürgers anwählen.

Eröffnung des Geltungsbereichs des deutschen Strafrechts

§ 9 Abs. 1 StGB [Ort der Tat]

Eine Tat ist an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist (...).

Prüfung

➤ Geltungsbereich des deutschen Strafrechts eröffnet?

- § 9 Abs. 1 3. Alt. StGB – „Erfolg“ – BGH meint, dass der „Erfolg“ in Deutschland eingetreten ist („konkrete Eignung der Friedensstörung“ siehe Rn. 45, 57):

„Nach dem Grundgedanken der Vorschrift soll deutsches Strafrecht - auch bei Vornahme der Tathandlung im Ausland - Anwendung finden, sofern es im Inland zu der Schädigung von Rechtsgütern oder zu Gefährdungen kommt, deren Vermeidung Zweck der jeweiligen Strafvorschrift ist“.

- § 9 Abs. 1 1. Alt. StGB – „Handlung“ – BGH zweifelt, weil nicht nachgewiesen werden konnte, dass

„...inländische Internet-Nutzer die (erg. englischsprachigen) Seiten auf dem australischen Server aufgerufen und damit die Dateien nach Deutschland „heruntergeladen“ hätten. (Rn. 62)

➤ Tatbestand

- Objektiver Tatbestand (Äußere Merkmale): Täter, Tathandlung, Tatobjekt, Erfolg (bei Erfolgsdelikten, Kausalität und objektive Zurechenbarkeit) wie bei der Fallvariante 1
- Subjektiver Tatbestand (Innere Merkmale): Vorsatz

➤ Rechtswidrigkeit

Diese ist grundsätzlich indiziert.

➤ Schuld

- Schuldfähigkeit
- Unrechtsbewusstsein

➤ Strafaufhebungs- und -ausschließungsgründe (Absehen von Strafe)

II. Deutsches Strafgesetzbuch: Informationsspezifische Delikte

1. Integration elektronischer Dokumente in die Vorschriften des StGB

Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen stehen „Schriften“ im Sinne des StGB gleich, wenn eine Vorschrift des StGB auf § 11 Abs. 3 StGB verweist.

§ 11 Abs. 3 StGB [Personen- und Sachbegriffe]
Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen.

Deshalb ist etwa das Verbreiten pornographischer Inhalte über das Internet über § 11 Abs. 3 StGB dem Verbreiten pornographischer Schriften nach § 184 StGB gleichgestellt.

§ 184 StGB [Verbreitung pornographischer Schriften]

(1) Wer pornographische Schriften (§ 11 Abs. 3)

1. einer Person unter achtzehn Jahren anbietet, überläßt oder zugänglich macht,
2. an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, ausstellt, anschlügt, vorführt oder sonst zugänglich macht,
3. im Einzelhandel außerhalb von Geschäftsräumen, in Kiosken oder anderen Verkaufsstellen, die der Kunde nicht zu betreten pflegt, im Versandhandel oder in gewerblichen Leihbüchereien oder Lesezirkeln einem anderen anbietet oder überläßt,
- 3a. im Wege gewerblicher Vermietung oder vergleichbarer gewerblicher Gewährung des Gebrauchs, ausgenommen in Ladengeschäften, die Personen unter achtzehn Jahren nicht zugänglich sind und von ihnen nicht eingesehen werden können, einem anderen anbietet oder überläßt,
4. im Wege des Versandhandels einzuführen unternimmt,
5. öffentlich an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, oder durch Verbreiten von Schriften außerhalb des Geschäftsverkehrs mit dem einschlägigen Handel anbietet, ankündigt oder anpreist,
6. an einen anderen gelangen läßt, ohne von diesem hierzu aufgefordert zu sein,
7. in einer öffentlichen Filmvorführung gegen ein Entgelt zeigt, das ganz oder überwiegend für diese Vorführung verlangt wird,
8. herstellt, bezieht, liefert, vorrätig hält oder einzuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummern 1 bis 7 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, oder
9. auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Ausland unter Verstoß gegen die dort geltenden Strafvorschriften zu verbreiten oder öffentlich zugänglich zu machen oder eine solche Verwendung zu ermöglichen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) (...)

§ 184a StGB [Verbreitung gewalt- oder tierpornographischer Schriften]

Wer pornographische Schriften (§ 11 Abs. 3), die Gewalttätigkeiten, den sexuellen Mißbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben,

1. verbreitet,
2. öffentlich ausstellt, anschlügt, vorführt oder sonst zugänglich macht oder
3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummern 1 oder 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 184b StGB [Verbreitung, Erwerb und Besitz kinderpornographischer Schriften]

(1) Wer pornographische Schriften (§ 11 Abs. 3), die den sexuellen Missbrauch von Kindern (§§ 176 bis 176b) zum Gegenstand haben (kinderpornographische Schriften),

1. verbreitet,
2. öffentlich ausstellt, anschlügt, vorführt oder sonst zugänglich macht oder
3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummer 1 oder Nummer 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft.

(2) (...)

§ 6 Nr. 6 StGB [Auslandstaten gegen international geschützte Rechtsgüter]

Das deutsche Strafrecht gilt weiter, unabhängig vom Recht des Tatortes, für folgende Taten, die im Ausland begangen werden;

(..)

6. Verbreitung pornographischer Schriften in den Fällen der §§ 184a und 184b Abs. 1 bis 3, auch in Verbindung mit § 184c Satz 1;

2. Informationsspezifische Delikte

1.	Personal-aktiv	<p>“Berufsgruppen” (etwa Arzt in § 203 StGB, Amtsträger in § 353b StGB und in Steuersachen § 355 StGB), die in einer inhaltlichen Betrachtung “Geheimnisnähe” haben</p> <p>“Berufsgruppen”, die in einer prozeduralen Betrachtung für den Informationstransfer von Bedeutung sind (§ 206 StGB – Verletzung des Postgeheimnisses)</p>
2 a)	Personal – passiv Datenschutz allgemein	<p>§ 201 StGB Verletzung der Vertraulichkeit des Wortes</p> <p>§ 202a StGB Ausspähen von Daten</p> <p>§ 263a StGB Computerbetrug</p> <p>§ 269, 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung</p> <p>§ 95 ff StGB Offenbarung von Staatsgeheimnissen</p>
2b)	Personal – passiv Datenschutz professionell	<p>§ 203 StGB Verletzung von Privatgeheimnissen</p> <p>§ 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses</p> <p>§ 303b StGB Computersabotage</p> <p>§ 353b StGB Verletzung von Dienstgeheimnissen</p> <p>§ 355 StGB Verletzung des Steuergeheimnisses</p>
3.	Objekt	<p>Staatsgeheimnis, 93 StGB</p> <p>Vertraulichkeit des Wortes, § 201 StGB</p> <p>Briefgeheimnis, § 202 StGB</p> <p>Privatgeheimnis, § 203 StGB</p> <p>Post- oder Fernmeldegeheimnis § 206 StGB</p> <p>Datenverarbeitungsvorgang, §§ 263a, 270</p>

		Datenverarbeitungsanlage und –träger, § 303b StGB Telekommunikationsanlage, § 317 StGB Dienstgeheimnis, § 353b StGB Steuergeheimnis, § 355 StGB
4.	Kausal/Zweck	Interesse an und Schutz von Geheimnissen, Informationen und Daten
5.	Qualität der Information(stechnik)	Offenbaren, Auskundschaften, Preisgabe Aufnahme und Zugänglichmachen Öffnen von Briefen und Kenntnisverschaffung vom Inhalt Zugriffverschaffen Verfälschung von Daten Datenveränderung, -unterdrückung und -unbrauchbarmachung
6.	Verfahren	Die Straftaten werden nach der Strafprozessordnung (StPO) verfolgt.
7.	Rechtfertigung/ Verhältnismäßigkeit	Siehe Vorlesung und Modul 1, in dem der verfassungsrechtliche Schutz von Daten vorgestellt wurde

➤ **Personal-aktiv**

§ 206 StGB [Verletzung des Post- oder Fernmeldegeheimnisses]

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,

2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigen Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 303a StGB [Datenveränderung]

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

➤ Personal-passiv (Datenschutz allgemein)

§ 202a StGB [Ausspähen von Daten]

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 263a StGB [Computerbetrug]

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 7 gilt entsprechend.

§ 269 StGB [Fälschung beweiserheblicher Daten]

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(...)

§ 270 StGB [Täuschung im Rechtsverkehr bei Datenverarbeitung]

Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich.

➤ **Personal-passiv (Datenschutz professionell)**

§ 303b StGB [Computersabotage]

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er

1. eine Tat nach § 303a Abs. 1 begeht oder
2. eine Datenverarbeitungsanlage oder einen

Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

➤ **Objekt**

§ 317 StGB [Störung von Telekommunikationsanlagen]

(1) Wer den Betrieb einer öffentlichen Zwecken dienenden Telekommunikationsanlage dadurch verhindert oder gefährdet, daß er eine dem Betrieb dienende Sache zerstört, beschädigt, beseitigt, verändert oder unbrauchbar macht oder die für den Betrieb bestimmte elektrische Kraft entzieht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) (...)

➤ **Personal – passiv Datenschutz allgemein**

§ 303a StGB [Datenveränderung]

(1) Wer rechtswidrig Daten (§ 202a Abs. 2)

löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(..)

3. Anwendung des StGB auf neue Informationstechnologien

a. Sachverhalt

Der Sachverhalt ist an die Entscheidung des OLG Karlsruhe vom 10.01.2005⁹ angelehnt.

Die Hochschule H bietet ihren Mitarbeitern an, Kommunikationseinrichtungen wie insbesondere Internet und E-Mail zu privaten und zu geschäftlichen Zwecken zu nutzen. Auch der externe Mitarbeiter M nutzt diese Möglichkeit. Der Leiter des Hochschulrechenzentrums U setzt, ohne seine Mitarbeiter zu informieren, ein E-Mail-Filtersystem ein, das M als nicht vertrauenswürdigen Absender ansieht. Dies hat zur Folge, dass die E-Mails des M zwar zunächst vom Mail-Server der H angenommen, dann aber intern ausgefiltert und nicht an die vorgesehenen Empfänger ausgeliefert werden. M erhält kurze Zeit später eine Fehlermeldung. Die vorgesehenen Empfänger der Mails erhalten keine Benachrichtigung.

⁹ Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04; MMR 2005, 178

b. Strafbarkeit des U

U könnte sich durch die Verwendung der Filter-Software wegen Verletzung des Fernmeldegeheimnisses, insbesondere durch Unterdrückung der Sendung (§ 206 Abs. 2 Nr. 2 Strafgesetzbuch), strafbar gemacht haben.

§ 206 StGB [Verletzung des Post- oder Fernmeldegeheimnisses]

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(...)

i. Tatbestandsmäßigkeit (Objektiver Tatbestand)

➤ Unternehmen, das geschäftsmäßig Telekommunikationsdienste erbringt

Die Hochschule H muss ein Unternehmen sein, das geschäftsmäßig Telekommunikationsdienste erbringt, damit U Täter des Delikts sein kann.

- „geschäftsmäßiges Erbringen von Telekommunikationsdiensten“

Eine Legaldefinition bietet § 3 Nr. 30 Telekommunikationsgesetz (TKG).

§ 3 TKG [Begriffsbestimmungen]

Im Sinne dieses Gesetzes ist oder sind

(...)

10. „geschäftsmäßiges Erbringen von Telekommunikationsdiensten“ das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht;

(...)

Die Hochschule bietet Telekommunikationsdienste an. Dies geschieht auch nachhaltig, denn das Angebot ist auf Dauer angelegt. Auf eine Gewinnerzielungsabsicht kommt es gerade nicht an. Die Mitarbeiter sind schließlich auch Dritte in diesem Sinne. Dieses Merkmal liegt nur dann nicht vor, wenn die Telekommunikationsdienste ausschließlich für den betrieblichen Eigenbedarf bestimmt sind. Sobald auch eine private Nutzung durch die Mitarbeiter erfolgt, ist dies nicht mehr der Fall. Die Arbeitnehmer sind als Dritte anzusehen.

- Unternehmen

H muss auch ein Unternehmen darstellen. Dies könnte im Hinblick auf die hoheitliche Tätigkeit der H zweifelhaft sein. Ausgehend vom Zweck der Norm, sowohl das subjektive Recht auf Geheimhaltung wie den Anspruch auf Übermittlung einer Sendung zu schützen, könnte der Unternehmensbegriff aber weit auszulegen sein. Davon ausgehend wäre jede Betätigung im geschäftlichen Verkehr, die nicht ausschließlich hoheitlich erfolgt oder auf eine rein private Tätigkeit beschränkt ist, als Unternehmen anzusehen. Durch das Angebot der H an ihre Mitarbeiter, die Telekommunikationsdienste auch privat zu nutzen, liegt keine ausschließlich hoheitliche Tätigkeit mehr vor. H ist daher nach hier vertretener Auffassung Unternehmen.

U als Leiter des Rechenzentrums der H kann sich also aus § 206 Abs. 2 StGB strafbar machen.

➤ **zur Übermittlung anvertraute Sendung**

- Sendung

Es muss zunächst eine Sendung vorliegen. Fraglich ist, ob dies zwingend ein körperlicher Gegenstand wie etwa ein Brief sein muss oder ob auch nichtkörperliche Sendungen wie hier die E-Mails des M von der Vorschrift erfasst sind.

Gegen eine Geltung der Norm auch für E-Mails könnte der Wortlaut von § 206 Abs. 2 Nr. 1 StGB sprechen, der verschlossene Sendungen nennt. Eine E-Mail kann aber nicht wie ein Brief verschlossen werden. Dem entspräche bei der E-Mail noch am ehesten eine Verschlüsselung. Verschlossenheit und Verschlüsselung können aber nicht gleichgesetzt werden. Ein Brief kann nämlich sowohl verschlossen als auch verschlüsselt im Sinne von chiffriert werden. Dies zeigt, dass beides wesentlich verschieden ist. Bei der E-Mail gibt es eben nur die Möglichkeit der Verschlüsselung und nicht die des Verschließens.

Für eine Geltung des § 206 Abs. 2 Nr. 2 StGB auch für E-Mails spricht hingegen, dass § 206 Abs. 2 Nr. 2 StGB im Gegensatz zu Nr. 1 gerade nicht von verschlossenen, sondern nur von zur Übermittlung anvertrauten Sendungen spricht. Außerdem verbliebe § 206 Abs. 2 Nr. 2 im Telekommunikationssektor kaum ein Anwendungsbereich, wenn dieser sich nur auf körperliche Sendungen bezöge. Schließlich ist auch die herkömmliche Telekommunikation nichtkörperlich.

Danach könnte in einer E-Mail eine Sendung in diesem Sinne gesehen werden.

- „zur Übermittlung“

Diese Sendung sollte auch durch U als Leiter des Rechenzentrums der H an den jeweiligen Adressaten übermittelt, also weitergeleitet, werden.

- „anvertraut“

Schließlich war die Sendung dem U auch anvertraut. Anvertraut ist eine Sendung immer dann, wenn sie auf vorschriftsmäßige Weise in den Verkehr gelangt ist und sich im Gewahrsam des Unternehmens befindet. Da die E-Mails des M zunächst vom Mail-Server des Hochschulrechenzentrums angenommen werden, ist dies der Fall.

➤ **“Unterdrücken“**

Die Sendung des M muss unterdrückt worden sein. Voraussetzung hierfür ist, dass die Sendung dem ordnungsgemäßen Post- oder Telekommunikationsverkehr entzogen wird. Dies ist hier geschehen. Die E-Mails des M werden von der Filter-Software ausgefiltert und nicht an die bestimmungsgemäßen Empfänger weitergeleitet. Gleichgültig ist dabei, ob U die E-Mails des M letztlich löscht oder ob er sie archiviert etc. Nicht nur die Vernichtung einer Sendung stellt ein Unterdrücken dar, sondern bereits das längere Zurückhalten einer Sendung, wenn dies zu einer Verzögerung der Zustellung führt. Diese Schwelle wurde hier eindeutig überschritten.

➤ **Unbefugt**

U muss dabei auch unbefugt gehandelt haben. Das Merkmal unbefugt könnte etwa nicht vorliegen, wenn der Betroffene in die Verwendung der Filter-Software eingewilligt hat. Dies hat M aber nicht getan.

ii. *Tatbestandsmäßigkeit (subjektiver Tatbestand)*

Schließlich muss der U auch vorsätzlich gehandelt haben. Dies kann bei der willentlichen Installation einer Filter-Software angenommen werden.

iii. *Rechtswidrigkeit*

Die Handlung des U muss auch rechtswidrig sein. Die Rechtswidrigkeit könnte entfallen, wenn eine andere gesetzliche Vorschrift das Verhalten des U erlaubt.

Eine solche die Maßnahmen des U rechtfertigende Vorschrift könnte § 109 Abs. 1 Nr. 2 TKG sein.

§ 109 TKG [Technische Schutzmaßnahmen]

(1) Jeder Diensteanbieter hat angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

1. des Fernmeldegeheimnisses und personenbezogener Daten und
2. der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen.

Von M muss ein unerlaubter Zugriff auf das E-Mail-System der H erfolgt sein oder befürchtet worden sein. Ein solcher unerlaubter Zugriff könnte im Zusammenhang mit E-Mails vor allem in der E-Mail angehängten schädlichen Programmen, etwa ein „Trojanisches Pferd“, gesehen werden. Die E-Mails des M enthielten aber keine derartigen Programme.

Die Maßnahme des U könnte dann trotzdem als gerechtfertigt erscheinen, wenn es irgendwelche Anhaltspunkte dafür gab, dass die E-Mails des M solche Programme oder Viren etc. enthielten. Auch dies war aber nicht der Fall. Die rein subjektive Einschätzung von U, der M sei nicht (mehr) vertrauenswürdig, kann ohne einen entsprechenden Tatsachenhintergrund die Unterdrückungshandlung nicht rechtfertigen.

Das Verhalten des U war daher rechtswidrig.

iv. *Schuld*

U hat auch schuldhaft gehandelt. Ihm war zwar möglicherweise nicht klar, dass die Verwendung von Filter-Software strafbar sein kann, diese Unkenntnis allein reicht aber nicht, sein Verhalten zu entschuldigen. U hätte sich besser informieren müssen.

v. *Ergebnis*

U hat sich wegen Verletzung des Fernmeldegeheimnisses strafbar gemacht (§ 206 Abs. 2 Nr. 2 StGB).

E. Convention on Cybercrime (CCC)

I. Grundlagen

1. Fundstellen

a. CCC

Englisch:

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>

Französisch:

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=08/12/02&CL=FRE>

Arbeitsfassung auf Deutsch:

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=11/10/04&CL=GER>

b. Zusatzprotokolle

Am 7. November 2002 wurde das Zusatzprotokoll gegen Rassismus (Additional Protocol to the Convention on Cybercrime concerning the Criminalisation of Acts of a Racist or Xenophobic Nature committed through Computer Systems)¹⁰ vom Europarat verabschiedet. Es stellt die Verbreitung rassistischer Propaganda, die missbräuchliche Speicherung von Hassbotschaften und die Benutzung des Internet zum Menschenhandel unter Verbot. Dieses Protokoll muss nun von den Staaten ratifiziert werden.

2. Auslegung von völkerrechtlichen Verträgen

Art. 31 Wiener Vertragsrechtskonvention [Allgemeine Auslegungsregel]¹¹

(1) Ein Vertrag ist nach Treu und Glauben in Übereinstimmung mit der gewöhnlichen, seinen Bestimmungen in ihrem Zusammenhang zukommenden Bedeutung und im Lichte seines Zieles und Zweckes auszulegen. (...)

Art. 31 des Wiener Übereinkommens über das Recht der Verträge zwischen Staaten und internationalen Organisationen oder zwischen internationalen Organisationen vom 23. Mai 1969 (BGBl. II 1990 S. 1415-1457)¹² enthält eine allgemeine Regel zur Auslegung von völkerrechtlichen Verträgen.

3. Grammatische Auslegung und authentische Sprachen

a. Wiener Übereinkommen über das Recht der Verträge

Artikel 33 Wiener Vertragsrechtskonvention [Auslegung von Verträgen mit zwei oder mehr authentischen Sprachen]¹³

(1) Ist ein Vertrag in zwei oder mehr Sprachen als authentisch festgelegt worden, so ist der Text in jeder Sprache in gleicher Weise maßgebend, sofern nicht der Vertrag vorsieht oder die Vertragsparteien vereinbaren, daß bei Abweichungen ein bestimmter Text vorgehen soll.

(2) Eine Vertragsfassung in einer anderen Sprache als einer der Sprachen, deren Text als authentisch festgelegt wurde, gilt nur dann als authentischer Wortlaut, wenn der Vertrag dies vorsieht oder die Vertragsparteien dies vereinbaren.

(3) Es wird vermutet, daß die Ausdrücke des Vertrags in jedem authentischen Text dieselbe Bedeutung haben.

(4) Außer in Fällen, in denen ein bestimmter Text nach Absatz 1 vorgeht, wird, wenn ein Vergleich der authentischen Texte einen Bedeutungsunterschied aufdeckt, der durch die Anwendung der Artikel 31 und 32 nicht ausgeräumt werden kann, diejenige Bedeutung zugrunde gelegt, die unter Berücksichtigung von Ziel und Zweck des Vertrags die Wortlaute am besten miteinander in Einklang bringt.

¹⁰ <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=12/9/04&CL=ENG>

¹¹ <http://www.jura.uni-sb.de/BGBl/TEIL2/1990/19901431.2.HTML>

¹² im Volltext unter <http://www.jura.uni-sb.de/BGBl/TEIL2/1990/19901415.A20.HTML>

¹³ <http://www.jura.uni-sb.de/BGBl/TEIL2/1990/19901432.2.HTML>

b. Art. 48 CCC – „Notification“

Im Falle der CCC bestimmt Art. 48 CCC, dass die englische und die französische Fassung authentisch sind.

Art. 48 CCC

(...) Done at Budapest, this day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. (...)

c. Bedeutung der CCC und der Zusatzprotokolle in der Zukunft

§ 6 Nr. 9 StGB [Auslandstaten gegen international geschützte Rechtsgüter]

Das deutsche Strafrecht gilt weiter, unabhängig vom Recht des Tatortes, für folgende Taten, die im Ausland begangen werden;

(..)

9. Taten, die auf Grund eines für die Bundesrepublik Deutschland verbindlichen zwischenstaatlichen Abkommens auch dann zu verfolgen sind, wenn sie im Ausland begangen werden.

Die völkerrechtliche Verpflichtung zur Verfolgung rechtfertigt die Eröffnung des Geltungsbereichs des deutschen Strafrechts (soweit es im verbindlichen zwischenstaatlichen Abkommen verlangt wird).

II. Literatur

M. Gercke, Die Cybercrime Konvention des Europarates, CR 2004, 782.

D. Kugelman, Völkerrechtliche Mindeststandards für die Strafverfolgung im Cyberspace – Die Cyber-Crime Konvention des Europarats - , TKMR 2002, 14.

B. Valerius, Der Weg zu einem sicheren Internet - Zum In-Kraft-Treten der Convention on Cybercrime, KMR 2004, 513.

III. Cybercrime - Konvention: Allgemeine Bestimmungen

1. Geltungsbereich (jurisdiction)

Article 22 CCC – Jurisdiction

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

(a) in its territory; or

(b) on board a ship flying the flag of that Party; or

(c) on board an aircraft registered under the laws of that Party; or

(d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

- (2) Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- (3) Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
- (4) This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
- (5) When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Der Geltungsbereich der Cybercrime – Konvention ist in Art. 22 CCC geregelt.

Es besteht eine weitgehende Übereinstimmung zu den diesbezüglichen Normen des StGB.

Die Strafbarkeit nach der CCC ist danach begründet, wenn die Straftat begangen wird:

Auf dem Hoheitsgebiet einer Vertragspartei, Art. 22 Abs. 1 a) CCC. Dies entspricht dem Territorialprinzip des § 3 StGB.

An Bord eines Schiffes, das die Flagge eines Vertragsstaats führt, Art. 22 Abs. 1 b) bzw. an Bord eines Flugzeugs eines Vertragsstaats, Art. 22 Abs. 1 c). Dies entspricht der Regelung des Art. 4 StGB.

Von einem Staatsangehörigen eines Vertragsstaats, wenn die Tat am Tatort strafbar ist oder der Ort keiner Strafgewalt unterliegt, Art. 22 Abs. 1 d) CCC. Entsprechende Regelung ist § 7 Abs. 1 StGB

Für den Fall, dass die Gerichtsbarkeiten verschiedener Vertragsstaaten begründet sind, fordert Art. 22 Abs. 5 CCC eine gegenseitige Konsultation und Abstimmung der Vertragsstaaten untereinander.

2. Vorsatz und „Befugnis“

a. Vorsatz

Die Tatbestände der CCC setzen sämtlich eine vorsätzliche Begehungsweise voraus (committed intentionally). Ein „bloß“ fahrlässiges Handeln ist damit nicht strafbar.

b. „Befugnis“

Zudem fordern alle Tatbestände der Konvention ein „unbefugtes“ Verhalten (without right). Wer „befugt“ ist, das im Tatbestand der Strafvorschriften umschriebene Verhalten auszuführen, macht sich also nicht strafbar. Eine solche Befugnis kann auf verschiedenen Gründen beruhen:

- Einwilligung des Betroffenen (bspw. bei Zugriff auf ein Computersystem zur Fernwartung)
- Vertrag, der zum Zugriff auf Computersystem berechtigt (bspw. bei Tätigwerden als Systemadministrator)
- Handeln staatlicher Stellen zur Strafverfolgung oder Gefahrenabwehr

Da dieses Merkmal („unbefugt“) auf Tatbestandsebene angesiedelt ist, könnte man argumentieren, dass bei „befugtem“ Handeln schon der Tatbestand der Strafnorm nicht erfüllt ist (vergleiche die Prüfungsreihenfolge unter D III 3 b i.). Es ließe sich aber auch vertreten, das Merkmal „unbefugt“ der Rechtswidrigkeit zuzuordnen und damit die „Befugnis“ als Rechtfertigungsgrund anzusehen.

3. Teilnahme, Versuch und Verantwortlichkeit juristischer Personen

a. Teilnahme (aiding or abetting)

Article 11 CCC – Attempt and aiding or abetting

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

Gemäß Art. 11 Abs. 1 CCC sind die Vertragsstaaten verpflichtet, auch die Teilnahme (aiding or abetting – sinngemäß: Beihilfe und Anstiftung – vergleiche unter D I 3 – der Begehung der Straftaten unter Strafe zu stellen. Eine nähere Ausgestaltung der Beteiligtenstrafbarkeit und insbesondere eine Definition der verschiedenen Beteiligungsformen (Mittäterschaft, Anstiftung, Beihilfe) enthält die Konvention nicht.

b. Versuch (attempt)

Article 11 CCC – Attempt and aiding or abetting

(2) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, and attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

(3) Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Art. 11 Abs. 2 CCC bestimmt die Strafbarkeit des Versuchs.

c. Verantwortlichkeit juristischer Personen (corporate liability)

Article 12 CCC – Corporate liability

(1) Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

- (a) a power of representation of the legal person;
- (b) an authority to take decisions on behalf of the legal person;
- (c) an authority to exercise control within the legal person.

(2) In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

(3) Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

(4) Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Art. 12 CCC regelt die Verantwortlichkeit juristischer Personen, wenn natürliche Personen für sie handeln. Voraussetzung der Verantwortlichkeit der juristischen Person ist, dass die natürliche Person, die für sie handelt, eine Führungsposition innehat (die ihr eine Vertretungs-, Entscheidungs- oder Kontrollbefugnis verleiht). Gemäß Art. 12 Abs. 3 CCC kann die Verantwortlichkeit der juristischen Person straf-, zivil- oder verwaltungsrechtlicher Art sein. Zu beachten ist also, dass eine „Verantwortlichkeit“ im Sinne der CCC nicht unbedingt eine Strafbarkeit der juristischen Person bedeutet. **In Deutschland etwa können sich nur natürliche Personen strafbar machen, juristische Personen jedoch nicht.** Hier würde es für die Verantwortlichkeit im Sinne der CCC vielleicht ausreichen, wenn das durch betrügerisches Verhalten erlangte Vermögen der juristischen Person eingezogen werden kann.

Die Verantwortlichkeit der juristischen Person tritt neben die strafrechtliche Verantwortlichkeit der natürlichen Person (vgl. Art. 12 Abs. 4 CCC).

4. Bedingungen und Garantien (conditions and safeguards)

Article 15 CCC – Conditions and safeguards

(1) Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

(2) Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

(3) To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

a. Spielraum

Die Cybercrime – Konvention überlässt den Mitgliedsstaaten bei der Umsetzung der in der Konvention vorgesehen Straftatbestände und bei der Strafverfolgung einen sehr weiten Spielraum. Das ist angesichts der unterschiedlichen Rechtssysteme und Rechtstraditionen in den Unterzeichnerstaaten und der Offenheit der Konvention für grundsätzlich alle Staaten dieser Welt auch notwendig.

b. Mindeststandards

Jedoch sieht die Konvention einige Mindeststandards und Garantien vor, die von den Vertragsstaaten erfüllt werden müssen.

Gemäß Art. 15 Abs. 1 CCC müssen die Vertragsstaaten einen angemessenen Schutz der Menschenrechte garantieren, der sich insbesondere aus den Verpflichtungen nach der EMRK, dem Internationalen Pakt über bürgerliche und politische Rechte¹⁴ und sonstigen völkerrechtlichen Übereinkünften ergibt. Mit dieser Bestimmung können sowohl Informations- als auch Datenschutzrechte bei der Umsetzung der CCC berücksichtigt werden. Im Übrigen ist festzustellen, dass die CCC den Datenschutz nicht erwähnt.

Daneben spricht Art. 15 Abs. 2 CCC im Hinblick auf bestimmte Strafverfolgungsmaßnahmen rechtsstaatliche Voraussetzungen an, die in vielen „westlichen“ Staaten obligatorisch sind, etwa die gerichtliche Kontrolle und die Begrenzung einer Maßnahme nach Umfang und Dauer. Man hat sich allerdings dagegen entschieden, hier Details festzusetzen.

c. „Verhältnismäßigkeit im weiteren Sinne“

Des Weiteren wird der Grundsatz der Verhältnismäßigkeit (principle of proportionality) hervorgehoben.

¹⁴ <http://www.auswaertiges-amt.de/www/de/infoservice/download/pdf/mr/zivilpakt.pdf>

IV. Cybercrime – Konvention: Einzelne Tatbestände

Die CCC regelt insgesamt neun Delikte, die vier verschiedenen Titeln zugeordnet werden.

1. Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und –systemen

a. Artikel 2 CCC, Rechtswidriger Zugriff (illegal access)

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Der Straftatbestand des Art. 2 CCC stellt den rechtswidrigen Zugriff auf ein Computersystem unter Strafe. Nach Art. 2 S. 2 CCC wird den Vertragsstaaten die Möglichkeit gelassen, als Voraussetzung für die Strafbarkeit zu fordern, dass neben dem einfachen Zugriffsvorsatz noch zusätzlich die Absicht vorliegen muss, Computerdaten zu erlangen oder eine sonstige unredliche Absicht. Zudem kann die Verletzung von Sicherheitsmaßnahmen als Tatbestandvoraussetzung bestimmt werden.

Dem Artikel 2 CCC entspricht in der deutschen Rechtsordnung am ehesten § 202a StGB (Ausspähen von Daten). Bei diesem genügt aber als „Taterfolg“ nicht der Zugriff auf ein Computersystem, vielmehr muss der Täter sich auch tatsächlich Daten verschaffen.¹⁵

b. Artikel 3 CCC, Rechtswidriges Abfangen (illegal interception)

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Nach Art. 3 CCC ist das unbefugte Abfangen von nichtöffentlichen Daten strafbar. Durch das Abfangen von Daten erlangt der Täter tatsächlich Daten. Insofern würde dieses Verhalten zugleich ein „Verschaffen“ von Daten im Sinne des § 202a StGB darstellen. Allerdings setzt

¹⁵ Wenn dem Täter dies nicht gelingt, obwohl er es beabsichtigt hatte, ist sein Verhalten auch nicht als Versuch strafbar, da bei § 202a StGB der Versuch nicht unter Strafe gestellt ist.

§ 202a StGB zusätzlich voraus, dass die Daten gegen unberechtigten Zugriff besonders gesichert sind. Diese Voraussetzung lässt Art. 2 CCC ausdrücklich zu, Art. 3 CCC jedoch nicht.

c. Artikel 4 CCC, Eingriffe in Daten (data interference)

Article 4 – Data interference

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Art. 4 CCC stellt das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten (Definition in Art. 1 b) CCC) unter Strafe. Hier stellt § 303a StGB, Datenveränderung, eine kongruente Umsetzung im deutschen Recht dar.

d. Artikel 5 CCC, Eingriffe in das System (system interference)

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Art. 5 CCC betrifft die Behinderung der Funktionsweise eines Computersystems (Definition in Art. 1 a) CCC). Das StGB stellt dieses Verhalten bereits in § 303b StGB, Computersabotage, unter Strafe.

e. Artikel 6 CCC, Missbrauch von Vorrichtungen (misuse of devices)

Article 6 – Misuse of devices

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(a) the production, sale, procurement for use, import, distribution or otherwise making available of:

(i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

(ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

(b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

(2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession

referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

(3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Artikel 6 CCC verbietet die Herstellung, den Verkauf, das Beschaffen und das sonstige Zugänglichmachen von Vorrichtungen, einschließlich Computerprogrammen, die zur Begehung der in Art. 2 – 5 CCC genannten Straftaten benutzt werden können. Gemeint sind sogenannte „Hackertools“. Auch das Generieren von Zugangspasswörtern soll strafrechtlich geahndet und verfolgt werden.

2. Computerstraftaten (computer - related offences)

Unter dem Titel „Computerstraftaten“ fasst die Konvention Delikte zusammen, die seit jeher zum Kernbestand des Strafrechts zählen, die aber an die Begehungsweise mittels Computer angepasst werden müssen.

a. Artikel 7 CCC, „Computerfälschung“ (computer- related forgery)

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Als „Computerfälschung“ verbietet Art. 7 CCC das Herstellen „unechter“ (inauthentic) Daten durch unbefugtes Eingeben, Löschen oder Unterdrücken von Computerdaten mit der Absicht, dass diese Daten im Rechtsverkehr als „echt“ angesehen werden. „Unecht“ im Sinne der Urkundendelikte sind Daten dann, wenn sie nicht von dem Aussteller stammen, der aus den Daten ersichtlich ist.

Unmittelbar einsichtig ist, dass ein Täter, der den Tatbestand des Art. 7 CCC erfüllt, sich zugleich auch nach Art. 4 und Art. 5 CCC strafbar machen kann.

Das Pendant im deutschen Recht zu Art. 7 CCC ist § 269 StGB (Fälschung beweisbarer Daten) und § 270 StGB (Täuschung im Rechtsverkehr bei Datenverarbeitung).

b. Artikel 8 CCC, Computerbetrug (computer – related fraud)

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- (a) any input, alteration, deletion or suppression of computer data;
 - (b) any interference with the functioning of a computer system,
- with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Art. 8 CCC betrifft den Betrug, der mittels Eingeben, Verändern oder Unterdrücken von Computerdaten oder durch Eingriff in die Funktionsweise eines Computersystems begangen wird. Der sicherlich allen Strafrechtsordnungen bekannte „normale“ Betrug greift hier nicht ein, da er eine Täuschung und einen dadurch veranlassten Irrtum voraussetzt. Im Gegensatz zu Menschen kann man aber Computer durch Vorspiegelung von falschen Tatsachen nicht „täuschen“ (und „irren“ können sie sich schon gar nicht), sondern nur durch Datenmanipulation einen anderen Programmablauf erzeugen.

Im deutschen Recht ist der Computerbetrug in § 263a StGB geregelt.

3. Kinderpornographie

Artikel 9 CCC, Straftaten in Bezug auf Kinderpornographie

Article 9 – Offences related to child pornography

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

- (a) producing child pornography for the purpose of its distribution through a computer system;
- (b) offering or making available child pornography through a computer system;
- (c) distributing or transmitting child pornography through a computer system;
- (d) procuring child pornography through a computer system for oneself or for another person;
- (e) possessing child pornography in a computer system or on a computer-data storage medium.

(2) For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:

- (a) a minor engaged in sexually explicit conduct;
- (b) a person appearing to be a minor engaged in sexually explicit conduct;
- (c) realistic images representing a minor engaged in sexually explicit conduct.

(3) For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

(4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Art. 9 CCC stellt in einer Norm ganz verschiedene Verhaltensweisen im Zusammenhang mit Kinderpornographie unter Strafe. Strafbar sind das Herstellen, das Anbieten oder Zugänglichmachen, das Beschaffen und der Besitz von Kinderpornographie. Gemäß der Definition in Art. 9 Abs. 2 CCC wird als Kinderpornographie die Darstellung einer minderjährigen Person erfasst, die gemäß Abs. 3 noch nicht 18 Jahre alt ist. Eine niedrigere Altersgrenze ist zwar zulässig. 16-jährige sollen aber jedenfalls noch geschützt sein.

Im deutschen Strafrecht bestimmt § 184b StGB die Strafbarkeit der Kinderpornographie. Allerdings ist nach deutschem Strafrecht ein „Kind“ eine Person unter 14 Jahren (§ 176 StGB), so dass insoweit Anpassungsbedarf bestehen könnte.

4. Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte

Article 10 – Offences related to infringements of copyright and related rights

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

(2) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

(3) A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Hinsichtlich der Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Rechte verweist Artikel 10 CCC auf drei diesbezügliche internationale Übereinkommen. Im deutschen Recht ist auf das Urheberrechtsgesetz zu verweisen.

V. Cybercrime – Konvention: Strafverfolgung

Die CCC enthält neben den genannten Straftatbeständen auch Normen, die eine effektive Strafverfolgung sicherstellen sollen.

1. Artikel 16 und 17 CCC, Rasche Sicherung und Weitergabe gespeicherter Daten (expedited preservation and partial disclosure of stored computer data)

Article 16 – Expedited preservation of stored computer data

(1) Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

(2) Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

(1) Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

- (a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
- (b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Gemäß Art. 16 CCC müssen die Vertragsparteien für die rasche Sicherung von Computerdaten sorgen, die bereits gespeichert wurden (stored computer data). Betroffen sind also nur Daten, die von den Diensteanbietern bereits erhalten und erfasst wurden. Ausdrücklich genannt sind auch Verbindungs- oder Verkehrsdaten (traffic data), also etwa: Zu welchen Zeiten und wie lange war der Nutzer online? - Welchen Provider hat er zur Einwahl genutzt? - Welche Datenmengen hat er empfangen/verschickt?

Die Anordnung zur Sicherung der Daten erfolgt durch die zuständige Behörde gegenüber demjenigen, in dessen Besitz oder Verfügungsgewalt sich die Daten befinden. Das ist bei den Verbindungsdaten in der Regel der Service – Provider. Die Sicherung kann bis zur Dauer von 90 Tagen angeordnet werden.

2. Artikel 18 CCC, Herausgabeordnung (production order)

Article 18 – Production order

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

- (a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
- (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

(3) For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

- (a) the type of communication service used, the technical provisions taken thereto and the period of service;
- (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
- (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Gemäß Art. 18 CCC kann die Herausgabe von gespeicherten Computerdaten gegenüber demjenigen, welcher die Verfügungsgewalt über die Daten hat, angeordnet werden. Gesondert erwähnt ist die Pflicht zur Herausgabe von „Kundendaten“, da diese Daten mehr beinhalten als der in Art.1 b) CCC definierte Begriff der „Computerdaten“. Umfasst sind etwa auch die Postanschrift und die Telefonnummer des Kunden.

3. Artikel 19 CCC, Durchsuchung und Beschlagnahme gespeicherter Computerdaten (search and seizure of stored computer data)

Article 19 – Search and seizure of stored computer data

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

- (a) a computer system or part of it and computer data stored therein; and
- (b) a computer-data storage medium in which computer data may be stored in its territory.

(2) Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

(3) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

- (a) seize or similarly secure a computer system or part of it or a computer-data storage medium;

- (b) make and retain a copy of those computer data;
- (c) maintain the integrity of the relevant stored computer data;
- (d) render inaccessible or remove those computer data in the accessed computer system.
- (4) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- (5) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

In Art. 19 CCC sind die klassischen Maßnahmen der Strafverfolgungsbehörden, Durchsuchung und Beschlagnahme, normiert. Sie kommen dann in Betracht, wenn eine Herausgabeanordnung nach Art. 18 CCC nicht den erwünschten Erfolg zeitigt hat.

In der Praxis kann den Ermittlungsbehörden der Zugriff auf das Computersystem erschwert oder nicht möglich sein, weil das System speziell gesichert oder einfach zu komplex ist. Deshalb sieht Art. 19 Abs. 4 CCC die Möglichkeit vor, Systemverwalter, die mit der Funktionsweise des Systems vertraut sind, in die Pflicht zu nehmen, um den Ermittlungsbehörden behilflich zu sein.

4. Artikel 20 CCC, Echtzeit – Erhebung von Verbindungsdaten (real – time collection of traffic data)

Article 20 – Real-time collection of traffic data

- (1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
 - (a) collect or record through the application of technical means on the territory of that Party, and
 - (b) compel a service provider, within its existing technical capability:
 - (i) to collect or record through the application of technical means on the territory of that Party; or
 - (ii) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
- (2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
- (3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- (4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Art. 20 CCC eröffnet die Möglichkeit, Verbindungsdaten im Zeitpunkt der Datenübertragung zu erheben oder zu speichern (d.h. in Echtzeit, real time). Die Erfassung von Inhaltsdaten ist

von dieser Norm nicht umfasst. Art. 20 Abs. 1 a) CCC betrifft die Erfassung durch die zuständigen Behörden selbst, während in Abs. 1 b) die Möglichkeit geregelt ist, einen Dienstanbieter zu zwingen, zugunsten der Strafverfolgungsbehörden die Daten zu erheben.

Art. 20 Abs. 4 CCC verweist auf die Artikel 14 und 15 CCC. Hervorzuheben ist Art. 14 Abs. 2 CCC, wonach eine Vertragspartei vorsehen kann, dass Maßnahmen nach Art. 20 CCC nur bei bestimmten Arten von Straftaten angewandt werden dürfen. Art. 15 CCC verweist neben den Menschenrechtsgarantien (Datenschutz!) auf den Grundsatz der Verhältnismäßigkeit und die Möglichkeit der gerichtlichen Kontrolle der Maßnahme und ihrer Begrenzung nach Umfang und Dauer.

5. Artikel 21 CCC, Abfangen von Verbindungsdaten (interception of content data)

Article 21 – Interception of content data

(1) Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

(a) collect or record through the application of technical means on the territory of that Party, and

(b) compel a service provider, within its existing technical capability:

(i) to collect or record through the application of technical means on the territory of that Party, or

(ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Art. 21 CCC soll den Strafverfolgungsbehörden die Möglichkeit eröffnen, inhaltsbezogene Daten zu erheben oder zu speichern. Während Art. 20 CCC also die Erhebung von Verbindungsdaten betrifft, ist Art. 21 CCC Spezialnorm für die Erhebung von Inhaltsdaten. Für beide Arten von Daten benutzt die Konvention dieselben Begriffe, nämlich erheben und speichern (collect; record). In der Praxis ergibt sich für beide Maßnahmen technisch auch kein Unterschied. Dennoch sind die Normen unterschiedlich bezeichnet. Art. 20 ist bezeichnet als „Erhebung (collection) von Verbindungsdaten“, während Art. 21 als „Abfangen (interception) von Inhaltsdaten“ firmiert. Auch wenn diese unterschiedliche Begrifflichkeit eher verwirrt,

könnte sie dazu dienen, deutlich zu machen, dass an die Erhebung von Inhaltsdaten strengere Voraussetzungen geknüpft sind. Im Gegensatz zu Art. 20 enthält Art. 21 schon im Tatbestand, und nicht lediglich als Option, die Einschränkung, dass Inhaltsdaten nur in Bezug auf eine „Reihe schwerer Straftaten, die nach dem innerstaatlichen Recht zu bestimmen sind“, erhoben werden dürfen.

F. Rahmenbeschluss 2005/222/JI des Rates der Europäischen Union über Angriffe auf Informationssysteme

I. Zur rechtlichen Bedeutung von Rahmenbeschlüssen

Ergänzt wird die völkerrechtliche CCC durch einen europarechtlichen Rahmenbeschluss.

Artikel 34 des Vertrages über die Europäische Union [EUV]

(1) In den Bereichen dieses Titels unterrichten und konsultieren die Mitgliedstaaten einander im Rat, um ihr Vorgehen zu koordinieren. Sie begründen hierfür eine Zusammenarbeit zwischen ihren zuständigen Verwaltungsstellen.

(2) Der Rat ergreift Maßnahmen und fördert in der geeigneten Form und nach den geeigneten Verfahren, die in diesem Titel festgelegt sind, eine Zusammenarbeit, die den Zielen der Union dient. Hierzu kann er auf Initiative eines Mitgliedstaats oder der Kommission einstimmig

a) gemeinsame Standpunkte annehmen, durch die das Vorgehen der Union in einer gegebenen Frage bestimmt wird;

b) Rahmenbeschlüsse zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten annehmen. Rahmenbeschlüsse sind für die Mitgliedstaaten hinsichtlich des zu erreichenden Ziels verbindlich, überlassen jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel. Sie sind nicht unmittelbar wirksam;

(...)

Diese Rahmenbeschlüsse können über den Wortlaut hinaus für die Auslegung mitgliedstaatlichen Rechts Bedeutung beanspruchen.¹⁶

II. Inkrafttreten

Der Rahmenbeschluss ist am Tag seiner Veröffentlichung im Amtsblatt der Europäischen Union am 16.03.2005 in Kraft getreten (Art 13. des Rahmenbeschlusses 2005222/JI).

Er entfaltet aber keine unmittelbaren Wirkungen in den einzelnen Mitgliedstaaten, sondern muss erst noch vom Gesetzgeber des jeweiligen Mitgliedstaats umgesetzt werden. Dabei ist der Mitgliedstaat in der Wahl der Form und der Mittel frei (Art. 34 Abs. 2 Litera b EUV). Die

¹⁶ Zur Bedeutung von Rahmenbeschlüssen siehe Urteil des EuGH vom 16.06.2005 in der Rechtsache Pupino , [C-105/03](#).

Mitgliedstaaten sind verpflichtet, den Rahmenbeschluss 2005/222/JI bis zum 16.03.2007 umzusetzen (Art. 12 des Rahmenbeschlusses 2005/222/JI).

III. Sanktionen bei Angriffen auf Informationssysteme im einzelnen

Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme¹⁷

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 29, Artikel 30 Absatz 1 Buchstabe a), Artikel 31 Absatz 1 Buchstabe e) und Artikel 34 Absatz 2 Buchstabe b),

auf Vorschlag der Kommission,

nach Stellungnahme des Europäischen Parlaments,

in Erwägung nachstehender Gründe:

(1) Dieser Rahmenbeschluss stellt darauf ab, durch Angleichung der einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme die Zusammenarbeit zwischen den Justiz- und sonstigen zuständigen Behörden, einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten, zu verbessern.

(2) Es finden nachweislich — und insbesondere im Rahmen der organisierten Kriminalität — Angriffe auf Informationssysteme statt, und es wächst die Besorgnis über das Potenzial an Terroranschlägen auf Informationssysteme, die Teil der kritischen Infrastruktur der Mitgliedstaaten sind. Das Ziel des Aufbaus einer sichereren Informationsgesellschaft und eines Raumes der Freiheit, der Sicherheit und des Rechts wird hierdurch gefährdet; daher bedarf es Gegenmaßnahmen auf Ebene der Europäischen Union.

(3) Um diesen Gefahren wirksam begegnen zu können, ist ein umfassender Ansatz zur Gewährleistung der Sicherheit der Netze und Informationen erforderlich, wie dies im Aktionsplan "eEurope", in der Mitteilung der Kommission "Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz" und in der Entschließung des Rates vom 28. Januar 2002 zu einem gemeinsamen Ansatz und spezifischen Maßnahmen im Bereich der Netz- und Informationssicherheit [2] hervorgehoben wurde.

(4) Das Europäische Parlament hat in seiner Entschließung vom 5. September 2001 auf die Notwendigkeit einer stärkeren Sensibilisierung für die Probleme der Informationsgesellschaft und der Gewährung von praktischer Hilfe hingewiesen.

(5) Die Bekämpfung der organisierten Kriminalität und des Terrorismus könnte durch beträchtliche Unterschiede und Diskrepanzen zwischen den einschlägigen Rechtsvorschriften der Mitgliedstaaten behindert werden, die eine wirksame polizeiliche und justizielle Zusammenarbeit beim Abwehren von Angriffen auf Informationssysteme erschweren könnten. Der länder- und grenzübergreifende Charakter moderner Informationssysteme führt dazu, dass Angriffe auf solche Systeme häufig eine grenzüberschreitende Dimension annehmen, was den dringenden Bedarf an weiteren Maßnahmen zur Angleichung der einschlägigen Strafrechtsvorschriften unterstreicht.

(6) Der Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raumes der Freiheit, der Si-

¹⁷ veröffentlicht im Amtsblatt: [L 69/67](#).

cherheit und des Rechts [3], der Europäische Rat (Tampere, 15./ 16. Oktober 1999 und Santa Maria da Feira, 19./ 20. Juni 2000), die Kommission im "Anzeiger der Fortschritte" und das Europäische Parlament in seiner EntschlieÙung vom 19. Mai 2000 haben legislative Maßnahmen (einschließlich gemeinsamer Definitionen, Tatbestandsmerkmale und Sanktionen) gegen die Hightech-Kriminalität genannt oder gefordert. (7) Die von internationalen Organisationen und insbesondere vom Europarat geleisteten Arbeiten zur Angleichung des Strafrechts sowie die Arbeiten der G8 zum Thema grenzüberschreitende Zusammenarbeit im Bereich der Hightech-Kriminalität müssen durch einen gemeinsamen Ansatz der Europäischen Union für diesen Bereich ergänzt werden. Diese Anforderung wurde in der Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zur "Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" näher ausgeführt.

(8) Das Strafrecht im Bereich der Angriffe auf Informationssysteme sollte angeglichen werden, um eine möglichst effiziente polizeiliche und justizielle Zusammenarbeit bei Straftaten in Verbindung mit Angriffen auf Informationssysteme sicherzustellen und einen Beitrag zur Bekämpfung der organisierten Kriminalität und des Terrorismus zu leisten.

(9) Alle Mitgliedstaaten haben das Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ratifiziert. Die im Zusammenhang mit der Umsetzung dieses Rahmenbeschlusses verarbeiteten Daten sollten gemäß den Grundsätzen des Übereinkommens geschützt werden.

(10) Gemeinsame Definitionen in diesem Bereich und insbesondere Definitionen von Informationssystemen und Computerdaten sind im Hinblick auf einen einheitlichen Ansatz in den Mitgliedstaaten für die Umsetzung dieses Rahmenbeschlusses von großer Bedeutung.

(11) Es gilt, gemeinsame Strafbestände des rechtswidrigen Zugangs zu Informationssystemen, des rechtswidrigen Systemeingriffs und der rechtswidrigen Bearbeitung von Daten vorzusehen, um so zu einem gemeinsamen Ansatz im Hinblick auf die Tatbestandsmerkmale von Straftaten zu gelangen.

(12) Zum Zwecke der besseren Bekämpfung der Cyber-Kriminalität sollte jeder Mitgliedstaat eine wirksame justizielle Zusammenarbeit bei Straftaten, die auf den in den Artikeln 2, 3, 4 und 5 beschriebenen Vorgehensweisen beruhen, gewährleisten.

(13) Eine Überkriminalisierung insbesondere von Bagatellfällen ist zu vermeiden; ebenso gilt es zu verhindern, dass Rechteinhaber und Zugangsberechtigte als Kriminelle eingestuft werden.

(14) Die Mitgliedstaaten müssen Angriffe auf Informationssysteme mit Sanktionen bedrohen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(15) Schwerere Strafen sollten für Fälle vorgesehen werden, in denen ein Angriff auf ein Informationssystem im Rahmen einer kriminellen Vereinigung im Sinne der Gemeinsamen Maßnahme 98/733/JI vom 21. Dezember 1998 betreffend die Strafbarkeit der Beteiligung an einer kriminellen Vereinigung in den Mitgliedstaaten der Europäischen Union [4] begangen wurde. Es ist ferner angemessen, schwerere Strafen vorzusehen, wenn ein solcher Angriff schwere Schäden verursacht oder wesentliche Interessen beeinträchtigt hat.

(16) Ferner sind Maßnahmen zur Zusammenarbeit zwischen den Mitgliedstaaten im Hinblick auf eine wirksame Vorgehensweise gegen Angriffe auf Informationssysteme vorzusehen. Die Mitgliedstaaten sollten daher das bestehende Netz der operativen Kontaktstellen für den Informationsaustausch, auf das in der Empfehlung des Rates vom 25. Juni 2001 über Kontaktstellen mit einem rund um die Uhr erreichbaren Dauerdienst zur Bekämpfung der Hightech-Kriminalität [5] verwiesen wird, nutzen.

(17) Da die Ziele dieses Rahmenbeschlusses, nämlich Angriffe auf Informationssysteme in allen Mitgliedstaaten mit wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen

Sanktionen zu ahnden und die justizielle Zusammenarbeit durch Beseitigung möglicher Hemmnisse in ausreichendem Maße zu verbessern und zu fördern, auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können, und — da es dazu gemeinsamer, miteinander zu vereinbarenden Regeln bedarf — besser auf Unionsebene zu erreichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Verhältnismäßigkeitsprinzip geht dieser Rahmenbeschluss nicht über das zur Erreichung dieser Ziele erforderliche Maß hinaus.

(18) Dieser Rahmenbeschluss wahrt die Grundrechte und achtet die Grundsätze, die in Artikel 6 des Vertrags über die Europäische Union und in der Charta der Grundrechte der Europäischen Union, vor allem in den Kapiteln II und VI, anerkannt werden —

HAT FOLGENDEN RAHMENBESCHLUSS ANGENOMMEN:

Artikel 1

Begriffsbestimmungen

Im Sinne dieses Rahmenbeschlusses bezeichnet der Ausdruck

- a) "Informationssystem" eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten oder übertragenen Computerdaten;
- b) "Computerdaten" die Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann;
- c) "juristische Person" jedes Rechtssubjekt, das diesen Status nach geltendem Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung ihrer hoheitlichen Rechte, und von öffentlich-rechtlichen internationalen Organisationen;
- d) "unbefugt" einen Zugang oder Eingriff, der vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder eines Teils des Systems nicht gestattet wurde, oder der nach den einzelstaatlichen Rechtsvorschriften nicht zulässig ist.

Artikel 2

Rechtswidriger Zugang zu Informationssystemen

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche und unbefugte Zugang zu einem Informationssystem als Ganzes oder zu einem Teil eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

(2) Jeder Mitgliedstaat kann beschließen, dass Handlungen nach Absatz 1 nur geahndet werden, sofern sie durch eine Verletzung von Sicherheitsmaßnahmen erfolgen.

Artikel 3

Rechtswidriger Systemeingriff

Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die unbefugte vorsätzliche schwere Behinderung oder Störung des Betriebs eines Informationssystems, durch Eingeben, Übermitteln, Beschädigen, Löschen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

*Artikel 4***Rechtswidriger Eingriff in Daten**

Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass das unbefugte vorsätzliche Löschen, Beschädigen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

*Artikel 5***Anstiftung, Beihilfe und Versuch**

(1) Jeder Mitgliedstaat stellt sicher, dass die Anstiftung oder Beihilfe zur Begehung einer der in den Artikeln 2, 3 und 4 beschriebenen Straftaten unter Strafe gestellt wird.

(2) Jeder Mitgliedstaat stellt sicher, dass der Versuch der Begehung einer der in den Artikeln 2, 3 und 4 beschriebenen Straftaten unter Strafe gestellt wird.

(3) Jeder Mitgliedstaat kann beschließen, Absatz 2 auf die in Artikel 2 genannten Straftaten nicht anzuwenden.

*Artikel 6***Sanktionen**

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten nach den Artikeln 2, 3, 4 und 5 mit wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen Sanktionen bedroht werden.

(2) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten nach Artikel 3 und 4 mit einer Freiheitsstrafe im Höchstmaß von mindestens einem bis drei Jahren geahndet werden.

*Artikel 7***Erschwerende Umstände**

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten nach Artikel 2 Absatz 2 sowie die Straftaten nach den Artikeln 3 und 4 mit einer Freiheitsstrafe im Höchstmaß von mindestens zwei bis fünf Jahren geahndet werden, wenn sie im Rahmen einer kriminellen Vereinigung im Sinne der Gemeinsamen Maßnahme 98/733/JI begangen wurden, unabhängig von dem dort vorgesehenen Strafmaß.

(2) Ein Mitgliedstaat kann die in Absatz 1 genannten Maßnahmen auch treffen, wenn durch die Straftaten schwere Schäden verursacht oder wesentliche Interessen beeinträchtigt wurden.

*Artikel 8***Verantwortlichkeit juristischer Personen**

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person für die in den Artikeln 2, 3, 4 und 5 aufgeführten Straftaten verantwortlich gemacht werden kann, die zu ihren Gunsten von einer Person begangen werden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt hat und die eine Führungsposition innerhalb der juristischen Person innehat aufgrund

a) einer Befugnis zur Vertretung der juristischen Person oder

b) einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder

c) einer Kontrollbefugnis innerhalb der juristischen Person.

(2) Neben den in Absatz 1 vorgesehenen Fällen trifft jeder Mitgliedstaat die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch die in Absatz 1 genannte Person die Begehung der in den Artikeln 2, 3, 4 und 5 genannten Straftaten zugunsten der juristischen Person durch eine ihr unterstellte Person ermöglicht hat.

(3) Die Verantwortlichkeit der juristischen Personen nach den Absätzen 1 und 2 schließt die strafrechtliche Verfolgung natürlicher Personen nicht aus, die als Täter, Anstifter oder Gehilfe an der Begehung der in den Artikeln 2, 3, 4 und 5 genannten Straftaten beteiligt sind.

Artikel 9

Sanktionen gegen juristische Personen

(1) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 8 Absatz 1 verantwortliche juristische Person wirksame, verhältnismäßige und abschreckende Sanktionen verhängt werden können, zu denen Geldbußen oder Geldstrafen gehören und zu denen andere Sanktionen gehören können, beispielsweise:

- a) Ausschluss von öffentlichen Zuwendungen oder Hilfen,
- b) vorübergehendes oder ständiges Verbot der Ausübung einer Handelstätigkeit,
- c) richterliche Aufsicht oder
- d) richterlich angeordnete Eröffnung des Liquidationsverfahrens.

(2) Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 8 Absatz 2 verantwortliche juristische Person wirksame, verhältnismäßige und abschreckende Sanktionen oder Maßnahmen verhängt werden können.

Artikel 10

Gerichtliche Zuständigkeit

(1) Jeder Mitgliedstaat begründet seine gerichtliche Zuständigkeit in Bezug auf die Straftaten nach den Artikeln 2, 3, 4 und 5, wenn diese

- a) ganz oder teilweise in seinem Hoheitsgebiet oder
- b) von einem seiner eigenen Staatsangehörigen oder
- c) zugunsten einer juristischen Personen, deren Hauptsitz sich im Hoheitsgebiet dieses Mitgliedstaats befindet, begangen wurden.

(2) Bei der Begründung seiner Zuständigkeit gemäß Absatz 1 Buchstabe a) stellt jeder Mitgliedstaat sicher, dass sich die Zuständigkeit auch auf Fälle erstreckt, in denen

- a) der Täter die Straftat begeht, während er sich physisch im Hoheitsgebiet dieses Staates aufhält, unabhängig davon, ob sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, oder
- b) sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, unabhängig davon, ob der Täter die Straftat begeht, während er sich physisch im Hoheitsgebiet dieses Staates aufhält.

(3) Ein Mitgliedstaat, der aufgrund seiner Rechtsvorschriften eigene Staatsangehörige noch nicht ausliefert oder überstellt, trifft die erforderlichen Maßnahmen, um seine gerichtliche Zuständigkeit in Bezug auf die in den Artikeln 2, 3, 4 und 5 genannten Straftaten zu begründen und gegebenenfalls die Strafverfolgung einzuleiten, sofern sie von einem seiner Staatsangehörigen außerhalb seines Hoheitsgebiets begangen wurden.

(4) Fällt eine Straftat in die gerichtliche Zuständigkeit von mehreren Mitgliedstaaten und kann jeder dieser Staaten auf der Grundlage desselben Sachverhalts die Strafverfolgung übernehmen, so entscheiden diese Mitgliedstaaten gemeinsam, welcher von ihnen die Strafverfolgung gegen den Täter vornimmt, um das Verfahren nach Möglichkeit auf einen Mitgliedstaat zu konzentrieren. Zu diesem Zweck können die Mitgliedstaaten auf jedes Gremium oder jeden Mechanismus auf Ebene der Europäischen Union zurückgreifen, um die Zusammenarbeit zwischen ihren Justizbehörden und die Koordinierung ihrer Maßnahmen zu erleichtern. Nacheinander kann nachstehenden Anknüpfungspunkten Rechnung getragen werden:

- es handelt sich um den Mitgliedstaat, in dessen Hoheitsgebiet die Straftat begangen wurde, nach Maßgabe von Absatz 1 Buchstabe a) und Absatz 2;
- es handelt sich um den Mitgliedstaat, dessen Staatsangehöriger der Täter ist;

- es handelt sich um den Mitgliedstaat, in dem der Täter ergriffen wurde.

(5) Ein Mitgliedstaat kann beschließen, die Zuständigkeitsregelung gemäß Absatz 1 Buchstaben b) und c) nicht oder nur in bestimmten Fällen oder unter bestimmten Umständen anzuwenden.

(6) Beschließen die Mitgliedstaaten die Anwendung des Absatzes 5, so unterrichten sie das Generalsekretariat des Rates und die Kommission und teilen gegebenenfalls mit, in welchen speziellen Fällen oder unter welchen speziellen Umständen der Beschluss gilt.

Artikel 11

Informationsaustausch

(1) Zum Zwecke des Informationsaustauschs über die in den Artikeln 2, 3, 4 und 5 genannten Straftaten und im Einklang mit den Datenschutzbestimmungen nutzen die Mitgliedstaaten das bestehende Netz der operativen Kontaktstellen, die rund um die Uhr und sieben Tage pro Woche erreichbar sind.

(2) Jeder Mitgliedstaat setzt das Generalsekretariat des Rates und die Kommission darüber in Kenntnis, welche Kontaktstelle für den Informationsaustausch über Straftaten im Zusammenhang mit Angriffen auf Informationssysteme benannt wurde. Das Generalsekretariat leitet diese Informationen an die übrigen Mitgliedstaaten weiter.

Artikel 12

Umsetzung

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um den Bestimmungen dieses Rahmenbeschlusses bis zum 16. März 2007 nachzukommen.

(2) Die Mitgliedstaaten übermitteln dem Generalsekretariat des Rates und der Kommission bis zum 16. März 2007 den Wortlaut der Vorschriften, mit denen ihre Verpflichtungen aus diesem Rahmenbeschluss in innerstaatliches Recht umgesetzt werden. Der Rat prüft bis zum 16. September 2007 anhand eines auf der Grundlage der Informationen und eines schriftlichen Berichts der Kommission erstellten Berichts, inwieweit die Mitgliedstaaten den Bestimmungen dieses Rahmenbeschlusses nachgekommen sind.

Artikel 13

Inkrafttreten

Dieser Rahmenbeschluss tritt am Tag seiner Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Geschehen zu Brüssel am 24. Februar 2005.

Im Namen des Rates

Der Präsident

N. Schmit

G. Vorschläge für eine Richtlinie über die Vorratsspeicherung von Daten

Auf europäischer Ebene wurde außerdem eine „Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden“¹⁸ vorgeschlagen.

I. Zur rechtlichen Bedeutung einer Richtlinie

Art 249 EGV

Zur Erfüllung ihrer Aufgaben und nach Maßgabe dieses Vertrags erlassen das Europäische Parlament und der Rat gemeinsam, der Rat und die Kommission Verordnungen, Richtlinien und Entscheidungen, sprechen Empfehlungen aus oder geben Stellungnahmen ab.

Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.

Die Entscheidung ist in allen ihren Teilen für diejenigen verbindlich, die sie bezeichnet.

Die Empfehlungen und Stellungnahmen sind nicht verbindlich.

II. Definition der Vorratsdatenspeicherung

Der Begriff Vorratsdatenspeicherung ist im Richtlinienvorschlag nicht legal definiert. Aus den Regelungen des Richtlinienvorschlags ergibt sich, dass der Begriff Vorratsdatenspeicherung

- die Speicherung von Verkehrs- und Standortdaten sowie alle damit in Zusammenhang stehenden Daten, die zu Feststellung des Teilnehmers oder Nutzers erforderlich sind
- durch Telekommunikationsdiensteanbieter
- zur Bestimmung von Quelle, Adressat, Zeitpunkt, Dauer, Art etc. einer Nachricht bezeichnet.¹⁹

Die Speicherung von Daten auf Vorrat (FÖR-Terminologie: „Vorratsdatenorganisation“) ist dadurch gekennzeichnet, dass

- die Speicherung (temporal) über den eigentlichen Zweck hinaus und/oder
- für weitere Zwecke als für den ursprünglichen Zweck der Erhebung erfolgt.

¹⁸ Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, vom 21.09.2005, [KOM\(2005\) 438 endgültig](#)

¹⁹ Siehe Art. 2-4 des Richtlinienvorschlags.

III. Gegenwärtige Rechtslage bei der Speicherung dynamischer IP-Adressen

Siehe dazu die folgenden Entscheidungen:

- Entscheidung des AG Darmstadt vom 30.06.2005, Az.: 300 C 397/04.
- Entscheidungen des LG Bonn vom 21.05.2004, Az.: 31 Qs 65/04, und des LG Stuttgart vom 04.01.2005, Az.: 13 Qs 89/04.

Die Entscheidungen wurden vom Fachgebiet Öffentliches Recht im Rahmen der CyLaw-Reports bearbeitet und dargestellt. Die entsprechenden CyLaw-Reports I und III sind im Anhang an dieses Modul zu finden und im Internet unter folgender URL:

<http://www.sicari.de/veroeffentlichungen/projektarbeiten/cyberlaw/index.en.html>

IV. Zusammenfassung des Richtlinienvorschlags zur Vorratsdatenspeicherung

Der Richtlinienvorschlag über die Vorratsdatenspeicherung legt fest, dass bestimmte Verkehrs- und Standortdaten auf Vorrat zu speichern sind. Die Richtlinie nennt verschiedene Kategorien von Daten, die auf Vorrat zu speichern sind:

Art. 4 des Richtlinienvorschlags [Für die Vorratsspeicherung in Frage kommende Datenkategorien]

Die Mitgliedstaaten stellen sicher, dass gemäß dieser Richtlinie folgende Datenkategorien auf Vorrat gespeichert werden:

1. zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten
2. zur Rückverfolgung und Identifizierung des Adressaten einer Nachricht benötigte Daten
3. zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten
4. zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten
5. zur Bestimmung der (mutmaßlichen) Endeinrichtung benötigte Daten
6. zur Bestimmung des Standorts mobiler Geräte benötigte Daten.

Die gemäß den oben genannten Datenkategorien auf Vorrat zu speichernden Datentypen sind im Anhang im Einzelnen aufgeführt.

Im Hinblick auf den Zweck der Richtlinie – den Behörden zur Verfolgung und Verhütung von Straftaten den Zugriff auf in diesem Zusammenhang wichtige Daten zu sichern – werden auch an die Art der Vorratsdatenspeicherung Anforderungen geknüpft:

Art. 8 des Richtlinienvorschlags [Anforderungen an die Vorratsdatenspeicherung]

Die Mitgliedstaaten stellen sicher, dass die Daten gemäß den Bestimmungen dieser Richtlinie so gespeichert werden, dass sie und alle sonstigen damit zusammenhängenden erforderlichen Informationen unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können.

Die Speicherungsfrist beträgt sechs Monate bzw. ein Jahr.

Art. 7 des Richtlinienvorschlags [Speicherungsfristen]

Die Mitgliedstaaten sorgen dafür, dass die in Artikel 4 genannten Datenkategorien für den Zeitraum eines Jahres ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden. Dies gilt nicht für Daten, die ganz oder überwiegend unter Verwendung des Internet-Protokolls vorgenommen werden. Für letztgenannte Daten beträgt die Speicherungsfrist sechs Monate.

Die Mitgliedstaaten werden verpflichtet, die Richtlinie innerhalb von 15 Monaten nach ihrer Annahme in innerstaatliches Recht umzusetzen.

Art. 13 des Richtlinienvorschlags [Umsetzung]

1. Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie bis spätestens fünfzehn Monate nach ihrer Annahme nachzukommen. (...)

Der Anhang des Richtlinienvorschlags listet schließlich die Datentypen auf, die auf Vorrat zu speichern sind.

Dies sind für die Bereiche Internetzugang, E-Mail per Internet und Sprachübermittlung per Internet:

Anhang des Richtlinienvorschlags

Auf Vorrat zu speichernde Datentypen, aufgeschlüsselt nach den in Artikel 4 dieser Richtlinie genannten Datenkategorien:

a) zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten: (...)

(3) (a) die vom Internet-Provider für eine Nachrichtenübermittlung zugewiesene dynamische oder statische Internet-Protokoll-Adresse

(b) die Benutzerkennung der Quelle einer Nachricht

(c) die Anschlusskennung oder Rufnummer, die jeder Nachrichtenübermittlung über das öffentliche Telefonnetz zugewiesen wird

(d) Name und Anschrift des Teilnehmers bzw. registrierten Nutzers, dem die IP-Adresse, Anschlusskennung oder Benutzerkennung zum Zeitpunkt der Nachrichtenübermittlung zugewiesen war

b) zur Rückverfolgung und Identifizierung des Adressaten einer Nachricht benötigte Daten: (...)

(3) (a) Anschluss- oder Benutzerkennung des bzw. der geplanten Empfänger einer Nachricht

(b) Name und Anschrift des bzw. der Teilnehmer oder registrierten Nutzer, an die die Nachricht gerichtet ist

c) zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten: (...)

(2) (a) Datum und Uhrzeit der An- und Abmeldung für eine Internet-Sitzung ausgehend von einer bestimmten Zeitzone

(...)

e) zur Bestimmung der (mutmaßlichen) Endeinrichtung benötigte Daten: (...)

(2) (a) die für die Einwahl verwendete Rufnummer

(b) der DSL-Anschluss oder eine andere Endpunktkenung des Urhebers der Nachrichtenübermittlung

(c) die MAC-Adresse (Media Access Control) oder sonstige Gerätekenung des vom Urheber der Nachrichtenübermittlung verwendeten Geräts

(...)

CyLaw-Report I: „Speicherung von IP-Adressen“

Entscheidung des Amtsgerichts Darmstadt vom 30.06.2005 – 300 C 397/04

Das FÖR¹ an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) ist verantwortlich für das SicAri-Teilprojekt * "Cyberlaw"². Mit den CyLaw-Reports soll das rechtswissenschaftliche Diskursangebot L.O.S. (Legal Open Source), das bisher nur Rechtsquellen (SicAri-Cyberlaw) enthält, um Rechtsprechung ergänzt werden. Die CyLaw-Reports-Idee ist es, auch Nicht-Juristen an grundlegender und/oder aktueller Cyberlaw-Rechtsprechung und juristischer Methodik fokussiert teilhaben zu lassen. Fragestellungen, die spezielles juristisches Wissen voraussetzen werden mit dem Kürzel „FEX“ (Für Experten) gekennzeichnet. Hintergrundwissen wird unter der Überschrift „FÖR-Glossar“ ergänzt. Aus Gründen der Präsentationsstrategie wird zwischen „clear cases“, die eine relativ einfache rechtliche Prüfung erfordern, und „hard cases“, die eine vertiefte Diskussion erfordern, unterschieden. In keinem Falle ist mit den CyLaw-Reports die Übernahme von Haftung verbunden. Die Entscheidung des AG Darmstadt wurde in die CyLaw-Reports aufgenommen, weil es sich – soweit ersichtlich – um die erste Entscheidung zur (Nicht-)Speicherung dynamischer IP-Adressen durch einen Access Provider handelt. Bei der Entscheidung eines Amtsgerichts handelt es sich um eine unterinstanzliche Entscheidung, gegen die Rechtsmittel statthaft sind.

* Die Arbeiten am CyLaw-Report werden im Rahmen des Projektes SicAri vom Bundesministerium für Bildung und Forschung gefördert.

Gliederung:

A.	Speicherung von (Verkehrs-)Daten – „Clear Case“	3
I.	Sachverhalt	3
II.	Telekommunikationsdienst oder Teledienst? – Eröffnung des Geltungsbereichs des TKG	3
III.	Erhebung von (Verkehrs-)Daten zur Entgeltermittlung und -abrechnung.....	4
1	Rechtsgrundlage	4
2	(Verkehrs-)Daten?	5
3	Erforderlichkeit	6
B.	Speicherung von IP-Adressen – „Hard Case“	7
I.	Sachverhalt	7
II.	Speicherung von Verkehrsdaten zur Entgeltabrechnung	7
1	Rechtsgrundlage	7
2	Erforderlichkeit	8
III.	Speicherung zur Gewährleistung der Datensicherheit	9
1	Subsidiarität des BDSG.....	9
2	Eignung der Speicherung von IP-Adressen für die Gewährleistung der Datensicherheit	10
3	Erforderlichkeit zur Datensicherheitsgewährleistung.....	11
C.	Schlussfolgerungen aus der Entscheidung des AG Darmstadt.....	12

A. Speicherung von (Verkehrs-)Daten – „Clear Case“

I. Sachverhalt

Der Access-Provider P bietet seinen Kunden unter anderem einen Flatratetarif an. Das Pauschalentgelt für die Flatrate beinhaltet den Zugang zum Internet über einen DSL-Anschluss ohne Begrenzung der zeitlichen Dauer oder des Datenvolumens. Weitere Gebühren fallen nur dann an, wenn ein ISDN-Anschluss für den Zugang benutzt wird oder sonstige entgeltabhängige Angebote (Mehrwertdienste) in Anspruch genommen werden. Um von der Flatrate solche nicht umfassten Nutzungen zu erfassen, möchte P folgende Daten erheben:

- den Beginn und das Ende der Nutzung,
- den Zugangsweg,
- das Volumen der übertragenen Daten und
- die dynamische IP-Adresse, die nach Authentifizierung durch den Kunden für die jeweilige Nutzung vergeben wird.

P möchte wissen, ob er diese Daten auch gegen den Willen seines Kunden K erheben darf.

Die Erhebung von (Verkehrs-)Daten durch Access-Provider wirft zahlreiche Fragen auf:

- Eröffnet die Leistung der Zugangsvermittlung zum Internet (Access - Provider) den Geltungsbereich des Telekommunikationsrechts oder des Telediensterechts?
- Welche Daten dürfen zu welchen Zwecken erhoben werden?
- Welche Daten dürfen zu welchen Zwecken dann auch gespeichert werden?
- Wie lange dürfen Daten gespeichert werden?

II. Telekommunikationsdienst oder Teledienst? – Eröffnung des Geltungsbereichs des TKG

Die Rechtmäßigkeit der Datenerhebung könnte im Telekommunikationsgesetz (TKG) oder im Teledienststedatenschutzgesetz (TDDSG) geregelt sein. Entscheidend ist, ob

die Leistung des Access-Providers einen Telekommunikationsdienst oder einen Teledienst darstellt.

§ 3 Nr. 24 TKG

„Telekommunikationsdienste“ [sind] in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen

§ 2 Abs. 1 TDG

Die nachfolgenden Vorschriften gelten für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).

Der Vergleich beider Normen könnte den Schluss rechtfertigen, dass Telekommunikationsdienstleistungen solche sein sollen, bei denen die Transportfunktion (also das Aussenden, Übermitteln und Empfangen) im Vordergrund steht. Teledienste kennzeichnen sich demgegenüber durch die inhaltliche Komponente. Jedenfalls schließen sich Telekommunikationsdienst einerseits und Teledienst andererseits aus:

§ 2 Abs. 4 TDG

Dieses Gesetz gilt nicht für

1. Telekommunikationsdienstleistungen [...]

P bietet nur den Zugang zum Internet an. Inhalte bietet er als reiner Access-Provider nicht an. Die Übermittlungsfunktion steht im Vordergrund.³ Er ist deshalb - jedenfalls nach Ansicht des AG Darmstadt als Telekommunikationsdienstleister zu qualifizieren.⁴

III. Erhebung von (Verkehrs-)Daten zur Entgeltermittlung und -abrechnung

1 Rechtsgrundlage

Als Rechtsgrundlage für die Erhebung von Verkehrsdaten kommt § 97 Abs. 2 Nr. 1 i.V.m. § 96 Abs. 1 TKG in Betracht.

§ 97 TKG [Entgeltermittlung und Entgeltabrechnung]

(2) Der Diensteanbieter darf zur ordnungsgemäßen Ermittlung und Abrechnung der Entgelte für Telekommunikationsdienste und zum Nachweis der Richtigkeit derselben

folgende personenbezogene Daten nach Maßgabe der Absätze 3 bis 6 erheben und verwenden:

1. die Verkehrsdaten nach § 96 Abs. 1, [...]

§ 96 TKG [Verkehrsdaten]

(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben und verwenden, soweit dies für die in diesem Abschnitt genannten Zwecke erforderlich ist:

1. **die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung**, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartenummer, bei mobilen Anschlüssen auch die Standortdaten
2. **den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,**
3. **den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,**
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

(2) Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke erforderlich sind. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.

[...]

2 (Verkehrs-)Daten?

Bei den Daten, die P erheben möchte, müsste es sich um Verkehrsdaten handeln.

- Beginn und Ende der Nutzung sind ausdrücklich als Verkehrsdaten genannt (§ 97 Abs. 2 Nr. 1 i.V.m. § 96 Abs. 1 Nr. 2 TKG). Ihre Erhebung ist damit rechtmäßig.
- Die Erhebung des Datenvolumens ist rechtmäßig, soweit die Entgelte davon abhängen (§97 Abs. 2 Nr. 1 i.V m. § 96 Abs. 1 Nr. 2 TKG).

K argumentierte, „dass angesichts des vereinbarten Pauschaltarifs eine Speicherung von Abrechnungsdaten grundsätzlich unzulässig sei.“⁵

Grundsätzlich sind bei einer Flatrate, die alle Nutzungen in ihrem Pauschaltarif beinhaltet, keine Daten zur Entgeltabrechnung erforderlich. Das Entgelt steht dann in Form einer Pauschale von Anfang an fest. Gibt es daneben aber auch weitere kostenpflichtige Nutzungen, dann könnte die Erhebung von Daten, die Auskunft über die konkrete Nutzung geben, für die Entgeltermittlung und -abrechnung erforderlich sein. Das AG Darmstadt geht davon aus, dass wegen der möglichen entgeltspflichtigen

Nutzungen auch bei einer Flatrate die Erhebung des Datenvolumens erfolgen kann. Die „Abhängigkeit“ der Entgelte von der Datenmenge wird bejaht.

- Der Zugangsweg stellt ebenfalls ein Verkehrsdatum dar (§ 97 Abs. 2 Nr. 1 i.V.m. § 96 Abs. 1 Nr. 3 TKG). Telekommunikationsdienste sind Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Alle Zugangswege wie etwa DSL oder ISDN übertragen Signale über Telekommunikationsnetze. Sie sind Telekommunikationsdienste und damit Verkehrsdaten, die erhoben werden dürfen.
- Die dynamische IP-Adresse ist nach hier vertretener Auffassung auch Verkehrsdatum (§97 Abs. 2 Nr. 1 i.V.m. § 96 Abs. 1 Nr. 1 TKG), weil es sich um eine Kennung der Endeinrichtung handelt.⁶ Für jede Nutzung wird eine IP-Adresse dem vom Kunden genutzten Rechner oder Router zugewiesen. Jede IP-Adresse ist zur gleichen Zeit nur einmal vergeben. Damit kann auch die dynamische IP-Adresse immer eindeutig zugeordnet werden.
- Die dynamische IP ist auch ein personenbezogenes Datum (§ 97 Abs. 2 TKG). Ein außen stehender Dritter kann die dynamische IP-Adresse zwar nicht einem bestimmten Nutzer zuordnen. P als Zugangsvermittler kann dies aber. Die dynamische IP-Adresse wird nach erfolgreicher Authentifizierung vergeben. Damit kann P eine dynamische IP eindeutig einem Kunden zuordnen.

3 Erforderlichkeit

Die Erhebung der Daten muss für die Entgeltermittlung und -abrechnung erforderlich sein. Mit Hilfe der IP-Adresse werden einzelne Nutzungen bestimmten Kunden zugeordnet. Durch den Zugangsweg wird bestimmt, ob die Nutzung von der Flatrate umfasst wird. Beginn und Ende der Nutzung wie Datenvolumen werden bei der Nutzung und Abrechnung von Mehrwertdiensten nach Ansicht des Amtsgerichts Darmstadt benötigt. Die Datenerhebung ist daher für die Entgeltermittlung und -abrechnung erforderlich.

- Ergebnis:

P darf die Daten nach Ansicht des AG Darmstadt erheben.

B. Speicherung von IP-Adressen – „Hard Case“

I. Sachverhalt

Der vorliegende Sachverhalt weicht hauptsächlich hinsichtlich der möglichen Dauer der Speicherung von dem vom AG Darmstadt am 30. Juni 2005⁷ entschiedenen Fall ab. Dort war eine Speicherdauer von 80 Tagen Entscheidungsgegenstand, was der früheren Rechtslage im TKG entsprach. Mittlerweile liegt die Speicherdauer bei sechs Monaten.

K ist Kunde beim Access-Provider P. K nutzt den Flatratetarif von P. P erhebt und speichert bei jeder Nutzung durch K Beginn und Ende der Nutzung, den Zugangsweg, das Datenvolumen und die dynamische IP-Adresse. Diese Daten werden innerhalb weniger Tage nach der jeweiligen Nutzung im Abrechnungssystem von P verarbeitet. Die zusätzlichen, von der Flatrate nicht umfassten Nutzungen werden ermittelt. P speichert die erhobenen Daten auch nach der Ermittlung der Abrechnungsdaten.

K hält die Speicherung für rechtswidrig. P hält eine Speicherung für notwendig und bis zum Ablauf von sechs Monaten auch für rechtmäßig

II. Speicherung von Verkehrsdaten zur Entgeltabrechnung

1 Rechtsgrundlage

Als Rechtsgrundlage für die Speicherung von Verkehrsdaten kommt § 97 Abs. 3 S. 3 TKG in Betracht.

§ 97 TKG

(3) Der Diensteanbieter hat nach Beendigung der Verbindung aus den Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 3 und 5 unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Nicht erforderliche Daten sind unverzüglich zu löschen. Die Verkehrsdaten dürfen - vorbehaltlich des Absatzes 4 Satz 1 Nr. 2 - höchstens sechs Monate nach Versendung der Rechnung gespeichert werden. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 3 Einwendungen erhoben, dürfen die Verkehrsdaten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

(4) Nach Wahl des Teilnehmers hat der rechnungsstellende Diensteanbieter die Zielnummer

1. vollständig oder unter Kürzung um die letzten drei Ziffern zu speichern oder
 2. mit Versendung der Rechnung an den Teilnehmer vollständig zu löschen.
- [...]

Verkehrsdaten dürfen sechs Monate gespeichert werden. Nur bei den Zielnummern besteht die Einschränkung, dass K nicht die Löschung gewählt haben darf (§ 97 Abs. 4 S. 1 Nr. 2 TKG). Für den vorliegenden Fall wird davon ausgegangen, dass K nicht die Löschung beantragt hat.

Nicht erforderliche Daten sind unverzüglich zu löschen (§ 97 Abs. 3 S. 2 TKG).

Es stellt sich deshalb die Frage, in welchem Verhältnis § 97 Abs. 3 S. 3 und S. 2 TKG zu einander stehen.

Grundsätzlich erlaubt § 97 Abs. 3 S. 3 TKG die Verkehrsdatenspeicherung auf sechs Monate. Bei sämtlichen im Sachverhalt angesprochenen Daten handelt es sich um Verkehrsdaten (siehe oben unter A III 2). Nach hier vertretener Ansicht handelt es sich bei § 97 Abs. 3 S. 2 TKG um eine Ausnahme von § 97 Abs. 3 S. 3 TKG - d.h. die (Verkehrs-)Daten, die nicht (mehr) erforderlich sind, sind zu löschen.

2 Erforderlichkeit

In der Entscheidung des AG Darmstadt wird nur problematisiert, inwieweit dynamische IP-Adressen gespeichert werden können.⁸

P argumentierte:

„Zur Vermeidung von Abrechnungsschwierigkeiten sei es allerdings notwendig, die IP-Adressen weiterhin zu speichern, um Einwendungen der Nutzer hinsichtlich der Nutzung des Internets begegnen zu können und nachweisen zu können, dass die in Rechnung gestellten Beträge ordnungsgemäß abgerechnet worden seien.“⁹

Hintergrund der Argumentation von P ist also, dass Flatratekunden Einwendungen gegen die Abrechnung von Zusatzdiensten erheben könnten.

Anderer Ansicht ist das AG Darmstadt, das, sobald entgeltliche und unentgeltliche Nutzungen getrennt worden sind, nicht mehr von einer Erforderlichkeit ausgeht. Die Speicherung der Daten wäre danach rechtswidrig. Der Gesetzgeber habe deutlich gemacht, dass sich das Erforderlichkeitskriterium allein auf die Abrechnung bezieht. Sonstige Zwecke, für die Daten erforderlich sein könnten, blieben nach dem klaren Wortlaut der Norm außer Betracht.¹⁰ Der Begriff der Erforderlichkeit sei eng auszulegen. Erforderlich für die Berechnung des Entgelts sind daher nur Daten, die zur Abrechnung unerlässlich sind. Dies beruht auf der hohen Sensibilität von Telekommuni-

kationsnutzungsdaten. Die dynamischen IP-Adressen stellen Telekommunikationsnutzungsdaten dar. Dynamische IP-Adressen können dazu führen,

„[...] das Nutzerverhalten im Internet transparent zu machen und mit weiteren Daten einen Personenbezug herzustellen, so dass nachvollzogen werden kann, welche Aktivitäten bestimmte Personen im Internet entfaltet haben.“¹¹

Dieser massive Eingriff könne nicht dadurch gerechtfertigt werden, dass die Nutzungsdaten den späteren Nachweis der Richtigkeit der Abrechnung ermöglichen.

„Die Speicherung von Nutzungsdaten kann daher nicht damit gerechtfertigt werden, dass die Nutzung des Dienstes im Streitfall mit den gespeicherten Daten plausibel gemacht oder nachgewiesen werden kann. Mit diesem Argument wäre auch etwa die Speicherung der einzelnen Internetseiten, die der Nutzer aufruft, zulässig. Auch damit könnte nämlich im Einzelfall nachgewiesen werden, dass ein Nutzer den Dienst benutzt hat. Selbst eine Speicherung von Inhaltsdaten könnte mit diesem Argument gerechtfertigt werden.“¹²

Die Erhebung und vorübergehende Speicherung von IP-Adressen ist eben nur so lange unerlässlich, bis die einzelnen Nutzungen über die dynamischen IP-Adressen bestimmten Kunden zugeordnet worden sind. Nur bis zu diesem Zeitpunkt dient die Erhebung und Speicherung der Entgeltabrechnung.

Daher ist die Speicherung der dynamischen IP-Adressen über diesen Zeitpunkt hinaus unzulässig. P muss die IP-Adressen dann unverzüglich löschen (§ 97 Abs. 3 S.2).

III. Speicherung zur Gewährleistung der Datensicherheit

Hinsichtlich der Speicherung der dynamischen IP-Adressen kommt § 9 Bundesdatenschutzgesetz (BDSG) als Rechtsgrundlage in Betracht:

§ 9 BDSG

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1 Subsidiarität des BDSG

Das BDSG ist nur subsidiär anwendbar (§ 1 Abs. 3 S. 1 BDSG).

§ 1 BDSG

(III) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. [...]

Das TKG ist eine andere Rechtsvorschrift des Bundes. Mit den §§ 96 und 97 TKG enthält es Regelungen über den Umgang mit personenbezogenen Daten. Deshalb wäre es vertretbar, das TKG als „andere Rechtsvorschrift“ zu qualifizieren und die Eröffnung des Geltungsbereichs des BDSG zu verneinen. Anderer Meinung scheint das AG Darmstadt zu sein, das die Anwendbarkeit des BDSG neben dem TKG in einem Satz bejaht.¹³ Für diese Auffassung könnte sprechen, dass die Regelungen des TKG nicht die Gewährleistung der Datensicherheit umfassen. So gibt es im TKG keine Norm, die sich mit Datensicherheit im Sinne von Zutritts-, Zugangs-, Zugriffs-, Eingabe-, Weitergabe-, Auftrags- und Verfügbarkeitskontrolle¹⁴ beschäftigt.

Damit gibt es keine deckungsgleiche Norm im TKG, die § 9 BDSG entspricht. Nur eine von ihrem Regelungsgegenstand her deckungsgleiche Norm im TKG kann die Anwendbarkeit einer entsprechenden Norm im BDSG ausschließen. Dies könnte sich aus dem Wortlaut der Vorschrift auf Grund des Wortes „soweit“ ergeben. Eine andere Meinung ist aber vertretbar, weil § 109 TKG sehr wohl die Einhaltung der Datensicherheit vom Diensteanbieter verlangt.

§ 109 Abs. 1 TKG

Jeder Diensteanbieter hat angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

1. des Fernmeldegeheimnisses und personenbezogener Daten und
2. der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen.

Für die weitere Prüfung wird hier der Entscheidungsweg des AG Darmstadt nachgezeichnet.

2 Eignung der Speicherung von IP-Adressen für die Gewährleistung der Datensicherheit

Nach Ansicht des AG Darmstadts ist die Eignung zu bejahen:

„Es mag durchaus sein, dass eine effektive Zugriffskontrolle zwingend voraussetzt, dass die Information darüber verfügbar ist, wem die fragliche IP-Adresse zum kon-

kreten Zeitpunkt zugeteilt war. Auch mag die Vielzahl der möglichen Angriffe auf ihr System einen entsprechenden Schutz erfordern.“¹⁵

3 Erforderlichkeit zur Datensicherheitsgewährleistung

Die Speicherung der IP-Adressen muss zur Gewährleistung der Datensicherheit erforderlich sein.

Das AG Darmstadt verneint eine Erforderlichkeit (§ 9 S. 2 BDSG):

“Dennoch ist damit der Anwendungsbereich des § 9 BDSG deutlich überschritten. Denn man würde den Zweck der Vorschrift, die bei einer Stelle gespeicherten personenbezogenen Daten vor unberechtigten Zugriffen zu schützen, genau in sein Gegenteil verkehren, wenn man daraus die Befugnis zur Speicherung weiterer personenbezogener Daten ableiten wollte. Eine solche Mehrspeicherung würde nämlich noch weitere Daten über den Betroffenen der Gefahr missbräuchlicher Zugriffe aussetzen. Nach dem Grundsatz der Datensparsamkeit (§ 3a BDSG) stellt den besten Schutz vor missbräuchlichen Zugriffen auf persönliche Daten dar, diese erst gar nicht zu speichern. Dann ist es auch überflüssig, Vorkehrungen zu ihrem Schutz zu treffen, wobei die Ausführungen der Beklagten [des P, Anm. d. Verf.] zur Größe des Personenkreises, der Zugriff auf die gespeicherten IP-Adressen hat, mehr als dürftig gewesen sind.“¹⁶

Nach Ansicht des AG Darmstadt steht also der Grundsatz der Datenvermeidung und der Datensparsamkeit (§ 3a S. 1 BDSG) entgegen.

§ 3a Satz 1 BDSG

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

Dem Grundsatz der Datensparsamkeit liegt der Gedanke zugrunde, dass auf nicht gespeicherte Daten auch nicht missbräuchlich zugegriffen werden kann. Datenvermeidung sei der beste Schutz vor Datenmissbrauch.

Unter Beachtung des Grundsatzes der Datensparsamkeit ist eine Speicherung der IP-Adressen zur Gewährleistung der Datensicherheit (§ 9 BDSG) nach Ansicht des AG Darmstadt nicht gestattet:

➤ Ergebnis

Die IP-Adressen können auch nicht unter dem Gesichtspunkt der Gewährleistung der Datensicherheit von P gespeichert werden.

C. Schlussfolgerungen aus der Entscheidung des AG Darmstadt

- Der Access-Provider erbringt Telekommunikationsdienste.
- Dynamische IP-Adressen sind nicht mehr für die Abrechnung erforderlich, sobald einzelne Nutzungen bestimmten Kunden zugeordnet worden sind. Die Daten sind dann unverzüglich zu löschen.
- Das Bundesdatenschutzgesetz ist zwar neben dem TKG anwendbar, gestattet eine Speicherung von IP-Adressen aber nach dem Grundsatz der Datensparsamkeit ebenfalls nicht.

¹ Informationen zu FÖR (Fachgebiet Öffentliches Recht) finden Sie unter <http://www.bwl.tu-darmstadt.de/jus4/?FG=jus>.

² Cyberlaw (in einer öffentlich-rechtlichen Betrachtung) ist ein Oberbegriff für Medien-, Telekommunikations-, Computer-, Internet-, Informations-, Datensicherheits- und Datenschutzrechte, die sich mit den Themen des Cyberspace und der Cyberworld befassen.

³ FEX (Für Experten): Daran ändert nach der vom AG Darmstadt vertretenen Ansicht auch § 2 Abs. 2 Nr. 3 TDG nichts, wonach insbesondere „Angebote zur Nutzung des Internets [...]“ Teledienste sind. Darunter fällt zwar nach dem Wortlaut auch die Leistung des Access-Providers. Gedacht wurde bei dieser Formulierung aber an Suchmaschinen o. ä. Jedenfalls steht bei der Zugangsvermittlung der Transport klar im Vordergrund, so dass Einigkeit herrscht, dass ein Telekommunikationsdienst vorliegt.

⁴ So jedenfalls AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 9

Sieht man dies anders und qualifiziert P als Telediensteanbieter, würde sich nach dem Urteil des AG Darmstadt in der Sache nichts ändern. § 6 Abs. 1 TDDSG gestattet die Datenerhebung zu Abrechnungszwecken. Nutzungsdaten dürfen gespeichert werden, soweit sie für die Abrechnung erforderlich sind (§ 6 Abs. 4 TDDSG). Auch hier reicht nach Ansicht des AG Darmstadt für die Speicherung von IP-Adressen nicht aus, mit den Daten die Richtigkeit der Abrechnung beweisen zu können.

⁵ AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 5

⁶ Das AG Darmstadt nimmt keine nähere Subsumtion vor und lässt mit der Feststellung, es handle sich um ein personenbezogenes Datum offen, ob es sich um ein Verkehrsdatum nach § 96 Abs. 1 Nr. 1 oder § 96 Abs. 1 Nr. 5 handelt.

⁷ AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04

⁸ Unproblematisch bejaht für sechs Monate für Datenmenge, Beginn und Ende der Nutzung und den Zugangsweg (AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 13). Die hier anzuführende Vorschrift wäre § 97 Abs. 3 S. 3 TKG.

⁹ AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 6

¹⁰ Dies ergibt sich aus einer Zusammenschau von § 97 Abs. 3 Sätze 1 und 2 TKG. Danach ist Satz 2 wie folgt zu lesen: Nicht für die Berechnung des Entgelts erforderliche Daten sind unverzüglich zu löschen.

¹¹ AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 9

¹² AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 10

¹³ AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 12

¹⁴ Die Begriffe stammen aus der Anlage zu § 9 S. 1 BDSG

¹⁵ AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 13

¹⁶ AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04, S. 13

CyLaw-Report III : „Auskunftspflichten von Access-Providern I“

Entscheidungen des LG Bonn vom 21.05.2004 - 31 Qs 65/04 - und des LG Stuttgart vom 04.01.2005 - 13 Qs 89/04 -

Das FÖR¹ an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) ist verantwortlich für das SicAri-Teilprojekt * "Cyberlaw"². Mit den CyLaw-Reports soll das rechtswissenschaftliche Diskursangebot L.O.S. (Legal Open Source), das bisher nur Rechtsquellen (SicAri-Cyberlaw) enthält, um Rechtsprechung ergänzt werden. Die CyLaw-Reports-Idee ist es, auch Nicht-Juristen an grundlegender und/oder aktueller Cyberlaw-Rechtsprechung und juristischer Methodik fokussiert teilhaben zu lassen. Fragestellungen, die spezielles juristisches Wissen voraussetzen werden mit dem Kürzel „FEX“ (Für Experten) gekennzeichnet. Hintergrundwissen wird unter der Überschrift „FÖR-Glossar“ ergänzt. Aus Gründen der Präsentationsstrategie wird zwischen „clear cases“, die eine relativ einfache rechtliche Prüfung erfordern, und „hard cases“, die eine vertiefte Diskussion erfordern, unterschieden. In keinem Fall ist mit den CyLaw-Reports die Übernahme von Haftung verbunden. Die beiden landgerichtlichen Entscheidungen³ wurden in die CyLaw-Reports aufgenommen, da sie sich jeweils mit der Auskunftspflicht von Access-Providern über Kundendaten beschäftigen. Der Umfang und Geltungsbereich dieser Auskunftspflichtung ist richterlich noch nicht abschließend geklärt. Die beiden zentralen hierzu vertretenen Positionen werden durch die ausgewählten Entscheidungen repräsentiert.

* Die Arbeiten am CyLaw-Report werden im Rahmen des Projektes SicAri vom Bundesministerium für Bildung und Forschung gefördert.

Gliederung:

A.	Auskunftspflichten von Access-Providern – „Clear Case“	3
I.	Sachverhalt	3
II.	Rechtsgrundlage	3
III.	Telekommunikationsdienst oder Teledienst – Eröffnung des Geltungsbereich des TKG	4
IV.	Auskunft über Bestands- oder Verbindungsdaten?	5
V.	Ergebnis	6
B.	Auskunftspflichten von Access-Providern – „Hard Case“	7
I.	Sachverhalt	7
II.	Rechtsgrundlage	7
III.	Auskunft über Bestands- oder Verbindungsdatum?	7
1.	Namens- und Anschriftersuchen aufgrund dynamischer IP-Adressen als Bestandsdatenabfrage?	7
2.	Namens- und Anschriftersuchen aufgrund dynamischer IP-Adressen als Verbindungsdatenabfrage?	9
3.	Ergebnis	11
IV.	Vereinbarkeit mit den Grundrechten.....	11
1.	Recht.....	11
2.	Eingriff	12
3.	Ergebnis:	13
C.	Schlussfolgerungen	14

A. Auskunftspflichten von Access-Providern – „Clear Case“

I. Sachverhalt

Der Staatsanwalt S ermittelt wegen Verbreitens pornographischer Schriften über das Internet. In diesem Rahmen entsteht der Verdacht des Verbreitens pornographischer Schriften gegenüber dem Inhaber einer bestimmten statischen IP-Adresse. S möchte jetzt den Namen und die Anschrift des Inhabers der IP-Adresse herausfinden.

S fragt sich, ob er sich mit seinem Auskunftersuchen direkt an den Access-Provider P wenden kann und dieser ihm Auskunft geben muss oder ob er erst einen richterlichen Beschluss benötigt.

II. Rechtsgrundlage

Rechtsgrundlage für das Auskunftsbegehren des S könnte entweder § 113 Abs. 1 S. 1 Telekommunikationsgesetz (TKG)⁴ oder § 100g Abs. 1 S. 1 Strafprozessordnung (StPO) sein.

§ 113 TKG [Manuelles Auskunftsverfahren]

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat im Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte über die nach den §§ 95 und 111 erhobenen Daten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. (...) Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig. Über die Auskunftserteilung hat der Verpflichtete gegenüber seinen Kundinnen und Kunden sowie Dritten gegenüber Stillschweigen zu wahren.
(...)

§ 100g [Auskunft über Telekommunikationsverbindungsdaten]

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine Straftat von erheblicher Bedeutung, insbesondere eine der in § 100a Satz 1 genannten Straftaten, oder mittels einer Endeinrichtung (§ 3 Nr. 3 des Telekommunikationsgesetzes) begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, darf angeordnet werden,

dass diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, unverzüglich Auskunft über die in Absatz 3 bezeichneten Telekommunikationsverbindungsdaten zu erteilen haben, soweit die Auskunft für die Untersuchung erforderlich ist. Dies gilt nur, soweit diese Verbindungsdaten den Beschuldigten oder die sonstigen in § 100a Satz 2 bezeichneten Personen betreffen. Die Auskunft darf auch über zukünftige Telekommunikationsverbindungen angeordnet werden.

(2) Die Erteilung einer Auskunft darüber, ob von einem Telekommunikationsanschluss Telekommunikationsverbindungen zu den in Absatz 1 Satz 2 genannten Personen hergestellt worden sind, darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Telekommunikationsverbindungsdaten sind:

1. im Falle einer Verbindung Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung,
2. Beginn und Ende der Verbindung nach Datum und Uhrzeit,
3. vom Kunden in Anspruch genommene Telekommunikationsdienstleistung,
4. Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit.

III. Telekommunikationsdienst oder Teledienst – Eröffnung des Geltungsbereich des TKG

Fraglich ist, ob überhaupt der Geltungsbereich des TKG eröffnet ist. Mangelt es daran, muss Staatsanwalt S nach der StPO vorgehen. Nur das TKG sieht eine spezielle Auskunftspflichtung des Diensteanbieters vor – im Gegensatz zu Teledienstgesetz (TDG) und Teledienststedatenschutzgesetz (TDDSG)⁵. Im Rahmen von TDG/TDDSG bliebe nur ein Rückgriff auf die Regeln der StPO.

Entscheidend für die Abgrenzung ist, ob die Leistung des Access-Providers P einen Telekommunikationsdienst oder einen Teledienst darstellt.

§ 3 Nr. 24 TKG

„Telekommunikationsdienste“ [sind] in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen

§ 2 Abs. 1 TDG

Die nachfolgenden Vorschriften gelten für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten

wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).

Der Vergleich beider Normen könnte den Schluss rechtfertigen, dass Telekommunikationsdienstleistungen solche sein sollen, bei denen die Transportfunktion (also das Aussenden, Übermitteln und Empfangen) im Vordergrund steht. Teledienste kennzeichnen sich demgegenüber durch die inhaltliche Komponente. Jedenfalls schließen sich Telekommunikationsdienst einerseits und Teledienst andererseits aus:

§ 2 Abs. 4 TDG

Dieses Gesetz gilt nicht für

1. Telekommunikationsdienstleistungen [...]

Weder das LG Bonn noch das LG Stuttgart problematisieren diese Frage in ihren Entscheidungen und scheinen selbstverständlich von der Eröffnung des Geltungsbereichs des TKG auszugehen. Dafür spricht zwar das Argument, dass der Access-Provider eine reine Übermittlungsleistung ohne inhaltliche Komponente erbringt. Allerdings wäre dies zu diskutieren gewesen - schon allein im Hinblick darauf, dass TDG und TDDSG eine § 113 Abs. 1 S. 1 TKG verwandte Auskunftregelung nicht kennen.

Der Geltungsbereich des TKG ist nach Ansicht sowohl des LG Bonn wie des LG Stuttgart eröffnet.

IV. Auskunft über Bestands- oder Verbindungsdaten?

§ 95 TKG [Vertragsverhältnisse]

(1) Der Diensteanbieter darf Bestandsdaten erheben und verwenden, soweit dieses zur Erreichung des in § 3 Nr. 3 genannten Zweckes erforderlich ist. (...)

§ 3 TKG [Begriffsbestimmungen]

Im Sinne dieses Gesetzes ist oder sind

(...)

3. „Bestandsdaten“ Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden; (...)

§ 111 TKG [Daten für Auskunftersuchen der Sicherheitsbehörden]

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern vergibt oder Telekommunikationsanschlüsse für von anderen

vergebene Rufnummern bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113 die Rufnummern, den Namen und die Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum, sowie bei Festnetzanschlüssen auch die Anschrift des Anschlusses vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. (...)

§ 113 Abs. 1 S. 1 TKG sieht eine Auskunftspflicht nur über Bestandsdaten vor (§§ 95 Abs. 1 S. 1, 111 Abs. 1 S. 1 TKG). § 100g StPO sieht eine Auskunftspflicht nur über Verbindungsdaten (§ 100g Abs. 3 StPO)⁶ vor. Fraglich ist daher, ob sich die von S beehrte Auskunft auf Bestands- oder auf Verbindungsdaten bezieht.

Die von Staatsanwalt S gewünschten Auskünfte, nämlich **Name und Anschrift** eines bestimmten Kunden des P, stellen grundsätzlich Bestandsdaten dar. Die Daten sind bereits für die Begründung eines Vertragsverhältnisses erforderlich und bleiben dies auch für die gesamte Vertragsdauer bis zur Beendigung des Vertragsverhältnisses (§ 3 Nr. 3 TKG). Diese Qualifizierung als Bestandsdaten wird auch durch § 111 Abs. 1 S. 1 TKG bestätigt, der den Namen und die Anschrift ausdrücklich nennt. Demgegenüber sind Name und Anschrift in § 100g Abs. 3 StPO gerade nicht als Verbindungsdaten genannt.

Fraglich ist, ob sich an dieser Beurteilung etwas ändert, weil Name und Anschrift unter Berufung auf die statische IP-Adresse erfragt werden. Nach Auffassung beider Landgerichte⁷ handelt es sich in diesem Fall um eine Bestandsdatenabfrage, die nach TKG erfolgt.

V. Ergebnis

Da es sich bei Namen und Anschrift, auch wenn sie „hinter einer“ statischen IP-Adresse stehen, um Bestandsdaten handelt, ist § 113 Abs. 1 S. 1 TK die richtige Rechtsgrundlage. Staatsanwalt S kann sich direkt und ohne richterlichen Beschluss an den Access-Provider P wenden. Dieser ist verpflichtet, den Namen und die Anschrift mitzuteilen.

B. Auskunftspflichten von Access-Providern – „Hard Case“

I. Sachverhalt

Der Sachverhalt entspricht dem Beschluss des LG Stuttgart vom 04.01.2005⁸.

Im Rahmen des von Staatsanwalt S geführten Ermittlungsverfahrens wegen Verbreitens pornographischer Schriften gerät ein (noch) unbekannter Kunde K des Access-Providers P in Verdacht. Staatsanwalt S verlangt von P Auskunft über Namen und Anschrift dieses Kunden K, dessen Internetzugang am 30.08.2004 um 16:14:47 Uhr MEZ die dynamische IP-Adresse 217.94.XXX.XXX zugeteilt war.

P möchte wissen, ob er zur Erteilung dieser Auskunft verpflichtet ist.

II. Rechtsgrundlage

Als Rechtsgrundlage für das Auskunftsbegehren kommt wie im „Clear Case“ bei der statischen IP-Adresse § 113 Abs. 1 S. 1 TKG in Betracht. Von einer Eröffnung des Geltungsbereichs des TKG wird ausgegangen (siehe oben unter A III).

III. Auskunft über Bestands- oder Verbindungsdatum?

1. Namens- und Anschriftersuchen aufgrund dynamischer IP-Adressen als Bestandsdatenabfrage?

Fraglich ist, wie das Auskunftersuchen des Staatsanwalts S zu qualifizieren ist – als reine Abfrage von Bestandsdaten (da Name und Anschrift Bestandsdaten sind) oder als Abfrage von Verbindungsdaten (da die dynamische IP-Adresse ein Verbindungsdatum („Kennung...der Endeinrichtung“) im Sinne von 100g Abs. 3 StPO darstellt)?

Für die Qualifizierung des Auskunftersuchens als Abfrage von Bestandsdaten könnte folgendes sprechen:

- Dynamische und statische IP-Adresse unterscheiden sich weder in ihrer Funktion noch nach der dahinter stehenden Technik. Der einzige Unterschied zwischen

beiden liegt in der zeitlichen Dauer der Vergabe an einen Nutzer: Während die statische IP einem Nutzer über einen längeren Zeitraum zugewiesen ist, wird die dynamische IP einem Nutzer immer nur für einen kurzen Zeitraum zugewiesen. Man könnte daher argumentieren, dass dynamische und statische IP-Adresse im Kern dasselbe seien („clear case“ entspricht „hard case“) und allein der Unterschied in der zeitlichen Dauer der Vergabe eine unterschiedliche Behandlung nicht rechtfertigen könne.

LG Stuttgart:

„Danach ist für die Frage, ob ein Auskunftersuchen der Ermittlungsbehörde unter § 113 Abs. 1 Satz 1 TKG fällt, nicht danach zu differenzieren, ob eine Kennung einem TK-Teilnehmer lang- oder mittelfristig (wie üblicherweise bei Telefonnummern) oder nur kurzfristig (wie üblicherweise bei dynamischen IP-Adressen) zugeteilt ist oder war. Von § 113 Abs. 1 Satz 1 TKG werden vielmehr alle Fälle erfasst, in denen es - wie hier - der Ermittlungsbehörde darum geht, durch die Auskunft des TK-Dienstleistungen erbringenden Unternehmens eine bereits bekannte Kennung (sei es eine dynamische oder statische IP-Adresse oder eine Telefonnummer) zu einem bereits bekannten Zeitpunkt einer natürlichen Person zuzuordnen und diese namhaft zu machen.“⁹

- § 100g Abs. 3 StPO nennt Telekommunikationsverbindungsdaten. Diese Aufzählung könnte als enumerativ (abschließend) angesehen werden. Dementsprechend wären nur die in § 100g Abs. 3 StPO ausdrücklich genannten Daten (dynamische IP-Adressen als „Kennungen...der Endeinrichtung“) Verbindungsdaten – und nicht die in grammatischer Auslegung nicht erwähnte Anschrift bzw. der Name.
- Schließlich könnte die Betroffenheit der dynamischen IP als Verbindungsdatum gänzlich irrelevant sein, da Staatsanwalt S selbst dem P die dynamische IP-Adresse von K nennt. Letztlich gewinnt Staatsanwalt S keine über Namen und Anschrift des K hinausgehende Erkenntnisse durch eine Auskunft des P. Die Anknüpfungspunkte für das Auskunftersuchen, nämlich dynamische IP-Adresse und Zeitpunkt, kennt Staatsanwalt S bereits. Darüber hinaus erfährt S von P nur Namen und Anschrift, also Bestandsdaten.

2. Namens- und Anschriftersuchen aufgrund dynamischer IP-Adressen als Verbindungsdatenabfrage?

Gegen die Qualifizierung des Auskunftersuchens als Abfrage von Bestandsdaten könnte argumentiert werden, dass die Bestandsdaten (Name und Anschrift) nur unter Rückgriff auf Verbindungsdaten (dynamische IP-Adresse) ermittelt werden:

- Der Geltungsbereich des § 100g StPO wurde in Anlehnung an § 6 Abs. 1 Nr. 1 bis 4 Telekommunikationsdatenschutzverordnung (TDSV), dem heute § 96 Abs. 1 Nr. 1 bis 4 TKG entspricht, konzipiert.

§ 96 TKG [Verkehrsdaten]

(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben und verwenden, soweit dies für die in diesem Abschnitt genannten Zwecke erforderlich ist:

- 1, die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
 2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
 3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
 4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
- (...)

Der Gesetzgeber könnte damit zum Ausdruck gebracht haben, dass Daten, die wie die dynamische IP-Adresse bei der Inanspruchnahme von Leistungen erhoben werden, in jedem Fall in den Geltungsbereich von § 100g StPO fallen.

- Statische IP-Adresse und dynamische IP-Adresse unterscheiden sich insoweit, als erstere von der Begründung des Vertragsverhältnisses zwischen Provider und Kunden bis zu dessen Beendigung dem Kunden dauerhaft zugewiesen ist, die dynamische IP aber bei jeder Einwahl neu und jeweils nur für einen kurzen Zeitraum vergeben wird. Die dynamische IP könnte daher als Datum, das bei der Erbringung der Telekommunikationsdienstleistung erhoben wird, anzusehen sein. Dies entspricht der Legaldefinition des Begriffs „Verkehrsdatum“ im TKG, der sich mit dem Begriff „Verbindungsdatum“ deckt (grammatische und systematische Auslegung).

§ 3 TKG [Begriffsbestimmungen]

Im Sinne dieses Gesetzes ist oder sind
(...)

30. „Verkehrsdaten“ Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden;
(...)

Vor diesem Hintergrund könnte in der Vergabedauer – anders als vom LG Stuttgart vertreten - ein signifikanter Unterschied der Abfragen aufgrund einer statischen oder dynamischen IP-Adresse zu sehen sein.

- Bei einer dynamischen IP-Adresse kann der Nutzer, dem diese IP zu einem bestimmten Zeitpunkt zugewiesen war, nur durch Rückgriff auf die Logdatei benannt werden. Diese Logdatei enthält aber nicht nur Bestandsdaten, sondern auch Verbindungsdaten. Man könnte daher die Auffassung vertreten, dass es für die Beantwortung der Frage, ob es sich um eine Abfrage von Bestands- oder von Verbindungsdaten handelt, nicht auf die Einordnung der abgefragten Daten selbst, sondern auf die Betroffenheit anderer Daten bei der Abfrage ankomme.

LG Bonn:

„Bedarf es hingegen zur Auskunftserteilung eines Zugriffs auf bzw. einer Auswertung von – erst – bei der Bereitstellung, Erbringung von Kommunikationsdiensten erhobenen und gespeicherten Daten, so handelt es sich um eine Auskunft über Verbindungsdaten. Diese Auskunft kann in Fällen wie dem vorliegenden – im Ergebnis – die Bekanntgabe des Namens eines Anschlussnehmers zum Gegenstand haben. Maßgeblich für die Differenzierung zwischen personenbezogenen Bestandsdaten einerseits und personenbezogenen Verbindungsdaten andererseits ist nicht, ob das „Endziel“ der Auskunft zu den eigentlichen Bestandsdaten zählt oder nicht, sondern, ob die Auskunftserteilung aufgrund der gespeicherten Vertragsdaten möglich ist oder es vielmehr eines **Zugriffs** auf die Verbindungsdaten bedarf.“¹⁰

- Dieser Argumentation steht auch nicht entgegen, dass wesentliche Daten der Verbindung, wie dynamische IP-Adresse, Datum und Uhrzeit bereits bekannt sind.

LG Bonn:

Diese Daten ermöglichen „vielmehr erst den Erlass eines auf eine konkrete Verbindung zu stützenden Beschlusses nach § 100g StPO.“¹¹

- Gegen eine Einordnung des Auskunftsbegehrens des Staatsanwalts S als von § 113 Abs. 1 S. 1 TKG umfasste Bestandsdatenabfrage könnte auch § 96 Abs. 1 TKG sprechen – auch wenn weder das LG Bonn noch das LG Stuttgart dies thematisieren. Danach ist die Verwendung der in § 96 Abs. 1 TKG genannten Verkehrsdaten nur für die in diesem Abschnitt genannten Zwecke zulässig. Die dynamische IP-

Adresse fällt unter § 96 Abs. 1 Nr. 1 TKG. Der für die Namensermittlung notwendige Rückgriff auf die Logdatei stellt eine Nutzung der Verkehrsdaten dar – ohne dass der betreffende Abschnitt des TKG eine Regelung enthält, wonach die Nutzung zu diesem Zweck zulässig wäre.

3. Ergebnis

Je nachdem, welcher Auffassung letztlich der Vorzug gegeben wird, ist die richtige Rechtsgrundlage für das Auskunftersuchen entweder mit dem LG Stuttgart § 113 Abs. 1 S. 1 TKG oder mit dem LG Bonn § 100g Abs. 1 S. 1 StPO. Im letztgenannten Fall würde Staatsanwalt S einen richterlichen Beschluss benötigen und ohne diesen wäre P auch nicht zur Auskunft verpflichtet.

IV. Vereinbarkeit mit den Grundrechten

1. Recht

Die Erteilung von Auskünften über Kundendaten, die mit Telekommunikationsvorgängen zusammenhängen, könnte in den Geltungsbereich des Fernmeldegeheimnisses (Art. 10 Abs. 1 Grundgesetz, § 88 TKG) fallen.

Art. 10 GG [Brief-, Post- und Fernmeldegeheimnis]

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
(...)

§ 88 TKG [Fernmeldegeheimnis]

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere

Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(...)

Der Geltungsbereich des Fernmeldegeheimnisses umfasst nicht nur die eigentliche Telekommunikation selbst, sondern auch die näheren Umstände der Telekommunikation. Hierin liegt auch der Grund, weswegen für Bestands- und Verbindungsdaten unterschiedliche Regelungen getroffen wurden. Bei Bestandsdaten wurde davon ausgegangen, dass diese nicht telekommunikationsspezifisch seien und daher das Fernmeldegeheimnis durch die Auskunftspflichtung des § 113 Abs. 1 S. 1 TKG auch nicht betroffen sein könne. Verbindungsdaten betreffen dagegen typischerweise die näheren Umstände der Telekommunikation. Eine Auskunft über diese Daten soll daher nur nach richterlicher Anordnung erfolgen.

2. Eingriff

Fraglich ist, ob durch die Erteilung der von S verlangten Auskunft in das Fernmeldegeheimnis des Kunden K eingegriffen wird.

- Für das Vorliegen eines Eingriffs könnte nach Erwägungen des LG Stuttgart sprechen,

„[dass] durch die Erteilung der verlangten Auskunft - Name und Anschrift des Kunden - zugleich und zwangsläufig auch eine Aussage über Zeit, Art und/oder Umfang der vom Kunden in Anspruch genommenen Telekommunikationsdienstleistungen und damit über Verbindungsdaten i.S.d. § 100g Abs. 3 StPO gemacht werde.“¹²

Wegen des sehr engen Bezugs einer dynamischen IP-Adresse zu einem bestimmten Kommunikationsvorgang könnte eine Auskunft über den „hinter einer“ dynamischen IP-Adresse stehenden Kunden grundrechtlich anders zu bewerten sein als eine Auskunft anhand einer statischen IP-Adresse. Bei einer dynamischen IP besteht immer die realistische Möglichkeit, dass nur ein bestimmter Kommunikationsvorgang mit dieser IP durchgeführt wurde. Dieser konkrete Kommunikationsvorgang könnte dann durch die Auskunft des Diensteanbieters mit einer bestimmten

Person in Verbindung gebracht werden. Dies könnte als Eingriff in das Fernmeldegeheimnis zu bewerten sein.

- Gegen das Vorliegen eines Eingriffs könnte sprechen, dass der Kunde K über die dynamische IP-Adresse als unverwechselbare Kennung bereits eindeutig ermittelt ist.

LG Stuttgart:

„Ist aber die Kennung eines an einem zeitlich fixierten TK-Vorgang beteiligten Endgerätenutzers bekannt, hier die dynamische IP-Adresse, die den Vorgang einer ganz bestimmten Person und damit einem Grundrechtsträger zuordnet, so ist der betreffende Anschlussinhaber bereits eindeutig und unverwechselbar individualisiert. Die bürgerliche Identität, d.h. sein Name und seine Anschrift sind hierfür nicht erforderlich. Das nachgelagerte Auskunftersuchen der Ermittlungsbehörde, das die dynamische IP-Adresse und den konkreten Zeitpunkt vorgibt und lediglich die Namhaftmachung des bereits ausreichend individualisierten Endgerätenutzers begehrt, zielt somit auf die Erhebung von Bestandsdaten i.S.v. § 3 Nr. 3 TKG und berührt das Fernmeldegeheimnis nicht (mehr).“¹³

Durch die Auskunft erfährt Staatsanwalt S nicht mehr, als er von vornherein bereits weiß. P erteilt keine über Namen und Anschrift hinausgehende Auskunft, selbst wenn P für diese Auskunft auf Verbindungsdaten in der Logdatei zugreifen muss.

3. Ergebnis:

Folgt man der Auffassung, dass ein Eingriff in das Fernmeldegeheimnis vorliege, dann kann Rechtsgrundlage für das Auskunftersuchen nur § 100g Abs. 1 S. 1 StPO sein. § 113 Abs. 1 S. 3 TKG weist selbst darauf hin, dass ein Eingriff in das Fernmeldegeheimnis nur aufgrund der gesetzlichen Vorschriften erfolgen kann. § 113 Abs. 1 S. 1 TKG kann also einen Grundrechtseingriff in das Fernmeldegeheimnis nicht rechtfertigen. § 100g StPO regelt dagegen gerade die Auskunft über Telekommunikationsverbindungsdaten und rechtfertigt den Eingriff in das Fernmeldegeheimnis.

C. Schlussfolgerungen

- Ein Auskunftsverlangen über Namen und Anschrift aufgrund statischer IP-Adressen stellt unstreitig eine Abfrage von Bestandsdaten dar. Sie kann ohne richterlichen Beschluss direkt beim Provider erfragt werden. Dieser muss die Auskunft erteilen (§ 113 Abs. 1 S. 1 TKG).
- Dynamische IP-Adressen sind als Verbindungs- bzw. Verkehrsdaten anzusehen – nach in beiden landgerichtlichen Entscheidungen vertretener Ansicht.
- Streitig ist, ob das Auskunftsbegehren, mithilfe der dynamischen IP-Adresse den Namen und die Anschrift eines Kunden zu erfahren, eine Auskunft über Bestandsdaten oder eine Auskunft über Verbindungsdaten darstellt. Beide Auffassungen sind insoweit vertretbar.

¹ Informationen zu FÖR (Fachgebiet Öffentliches Recht) finden Sie unter <http://www.bwl.tu-darmstadt.de/jus4/?FG=jus>.

² Cyberlaw (in einer öffentlich-rechtlichen Betrachtung) ist ein Oberbegriff für Medien-, Telekommunikations-, Computer-, Internet-, Informations-, Datensicherheits- und Datenschutzrechte, die sich mit den Themen des Cyberspace und der Cyberworld befassen.

³ LG Bonn, Beschluss vom 21.05.2004, Az.: 31 Qs 65/94, DuD 2004, 628; LG Stuttgart, Beschluss vom 04.01.2005, Az.: 13 Qs 89/04, CR 2005, 598.

⁴ § 113 Abs. 1 S. 1 TKG n.F. entspricht § 89 Abs. 6 S. 1 TKG a.F., auf den sich die Entscheidung des LG Bonn noch bezieht.

⁵ FEX: § 5 S. 2 TDDSG steht zwar einer Auskunftspflicht des Telediensteanbieters nicht im Wege, verweist diesbezüglich aber nur auf Auskunftsverpflichtungen, die sich aus anderen Vorschriften ergeben, etwa die Strafprozessordnung, und schafft gerade keine eigenständige Auskunftspflicht.

⁶ Verbindungsdaten werden in der neuen Fassung des TKG als Verkehrsdaten bezeichnet. Die StPO behält den Terminus Verbindungsdaten bei. Die Begriffe sind aber inhaltsgleich.

⁷ LG Bonn, DuD 2004, 628 (628); LG Stuttgart, CR 2005, 598 (599).

⁸ LG Stuttgart, Beschluss vom 04.01.2005, Az.: 13 Qs 89/04, CR 2005, 598.

⁹ LG Stuttgart, CR 2005, 598 (599).

¹⁰ LG Bonn, DuD 2004, 628 (629).

¹¹ LG Bonn, DuD 2004, 628 (629).

¹² LG Stuttgart, CR 2005, 598 (599).

¹³ LG Stuttgart, CR 2005, 598.