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

Informations- und Datenschutzrecht II

Modul 3

(im WS 07/08: Modul 6)

DATUM	MODUL	TITEL
19.06.2007	3	IT-Sicherheit – die Convention on Cybercrime - Mit Aktualisierung in der Vorlesung -

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 „Staat **e n** recht" 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 Vertragsrechtskonvention[2].

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/BGBl/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

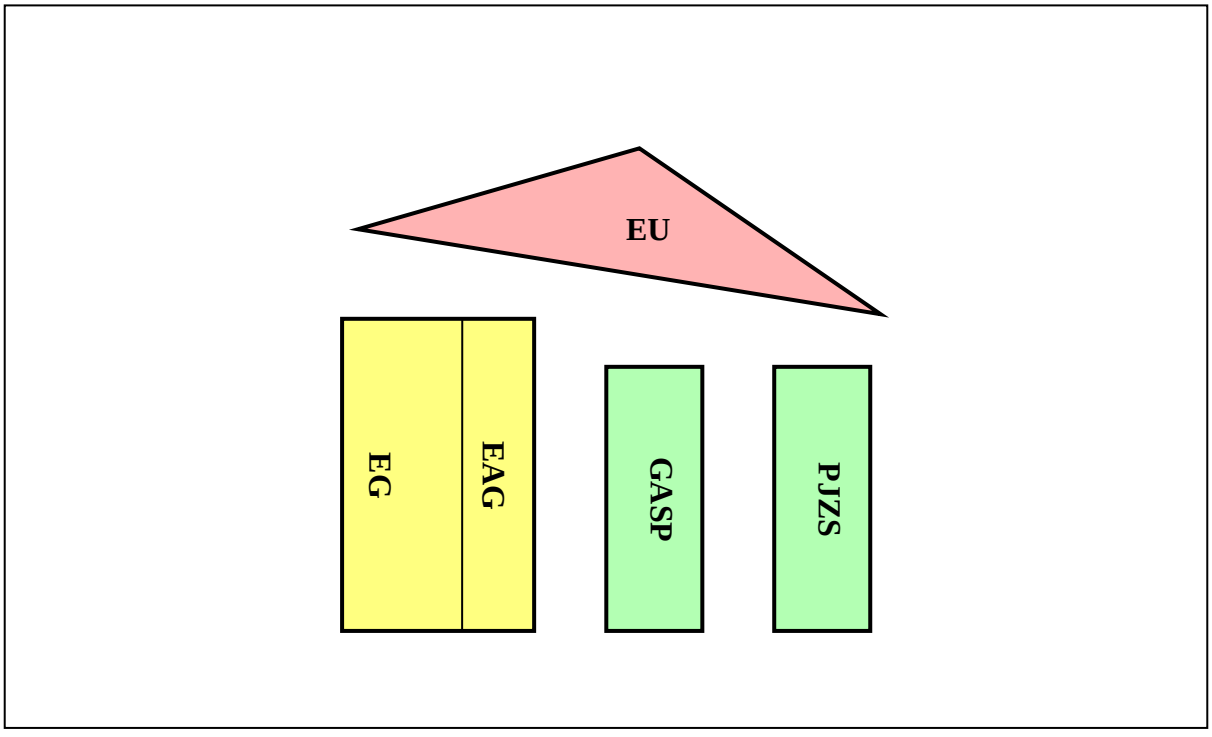
- Supranationalität: Schaffung einer eigenständigen Rechtsordnung, d.h. zwischen den Mitgliedsstaaten finden eigene Regeln Anwendung, welche zum einen die Regeln des allgemeinen, globalen Völkerrechts und zum anderen die innerstaatlichen Regeln der Mitgliedsstaaten ersetzen.
- Mehrheitsentscheidungen: 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 EG[4] 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 43 Staaten unterzeichnet worden, und von 21 Staaten ratifiziert 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 Europarat 47 Mitglieder. Er arbeitet eng mit der EU, den Vereinten Nationen und der OECD zusammen. Sitz des Europarats ist Straßburg.

Bis heute hat der Europarat ca. 200 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 Mitliedsstaaten zusammen. Die Zahl der Abgeordneten, die jedes Mitgliedsland entsenden darf, richtet sich nach der Bevölkerungszahl. Derzeit hat die Versammlung 636 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 allen 47 Mitgliedstaaten des Europarates ratifiziert worden. 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.

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 oderöffentliche 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)[5]

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 (…).

[5] „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

deutsche 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 CompuServe[6] nicht die CompuServe Information Services GmbH zur strafrechtlichen Verantwortung gezogen worden, sondern der Geschäftsführer.

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.

[6] 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.

- Schuld
  - Schuldfähigkeit
  - Unrechtsbewusstsein
  - Spezielle strafschärfende 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 Völkerstrafgesetzbuches 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, anschlägt, 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 oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben,
1. verbreitet,
2. öffentlich ausstellt, anschlägt, 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, anschlägt, 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	"Berufsgruppen" (etwa Arzt in § 203 StGB, Amtsträger in § 353b StGB und in Steuersachen § 355 StGB), die in einer inhaltlichen Betrachtung "Geheimnisnähe" haben "Berufsgruppen", die in einer prozeduralen Betrachtung für den Informationstransfer von Bedeutung sind (§ 206 StGB – Verletzung des Postgeheimnisses)
2 a)	Personal – passiv Datenschutz allgemein	§ 201 StGB Verletzung der Vertraulichkeit des Wortes § 202a StGB Ausspähen von Daten § 263a StGB Computerbetrug § 269, 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung § 95 ff StGB Offenbarung von Staatsgeheimnissen
2b)	Personal – passiv Datenschutz professionell	§ 203 StGB Verletzung von Privatgeheimnissen § 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses § 303b StGB Computersabotage § 353b StGB Verletzung von Dienstgeheimnissen § 355 StGB Verletzung des Steuergeheimnisses
3.	Objekt	Staatsgeheimnis, 93 StGB Vertraulichkeit des Wortes, § 201 StGB Briefgeheimnis, § 202 StGB Privatgeheimnis, § 203 StGB Post- oder Fernmeldegeheimnis § 206 StGB Datenverarbeitungsvorgang, §§ 263a, 270 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) 1Die 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 mir 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 tätigem 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.
(..)

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)[7] 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.

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

2. Auslegung von völkerrechtlichen Verträgen

Art. 31 Wiener Vertragsrechtskonvention [Allgemeine Auslegungsregel][8]
(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)[9] 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][10]
(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.

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. (…)

[8] http://www.jura.uni-sb.de/BGBl/TEIL2/1990/19901431.2.HTML
[9] im Volltext unter http://www.jura.uni-sb.de/BGBl/TEIL2/1990/19901415.A20.HTML
[10] http://www.jura.uni-sb.de/BGBl/TEIL2/1990/19901432.2.HTML

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. Kugelmann, 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 Rechte[11] 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.

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 unredli-

[11] http://www.auswaertiges-amt.de/www/de/infoservice/download/pdf/mr/zivilpakt.pdf

che 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.[12]

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 § 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.

[12] 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.

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 (missuse 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 beweiserheblicher 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 neces-

sary, 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, Herausgabeanordnung (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 Erfolgt gezeitigt 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) ompel 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.[13]

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

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

III. Sanktionen bei Angriffen auf Informationssysteme im Einzelnen

Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme[14]

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 Sicherheit 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 Entschließung 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

[14] veröffentlicht im Amtsblatt:. L 69/67.

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 vereinbarender 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, verhält-

nismäßige 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. Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten

Auf europäischer Ebene wurde am 15. März 2006 eine „Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“[15] erlassen.

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 in der Richtlinie nicht legal definiert. Aus den Regelungen 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.[16]

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.

[15] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG vom 15.03.2006, ABl. L 105, 54.
[16] Vergleiche Art. 1-5 der Richtlinie.

III. Überblick über die Richtlinie zur Vorratsdatenspeicherung

Artikel 3 der Richtlinie sieht eine Vorratsspeicherungspflicht der Mitgliedstaaten vor.

Art. 3 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten [Vorratsspeicherungspflicht]
(1) Abweichend von den Artikeln 5, 6 und 9 der Richtlinie 2002/58/EG tragen die Mitgliedstaaten durch entsprechende Maßnahmen dafür Sorge, dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen der vorliegenden Richtlinie auf Vorrat gespeichert werden.
(2) Die Verpflichtung zur Vorratsspeicherung nach Absatz 1 schließt die Vorratsspeicherung von in Artikel 5 genannten Daten im Zusammenhang mit erfolglosen Anrufversuchen ein, wenn diese Daten von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes im Rahmen der Zuständigkeit des betreffenden Mitgliedstaats im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet und gespeichert (bei Telefoniedaten) oder protokolliert (bei Internetdaten) werden. Nach dieser Richtlinie ist die Vorratsspeicherung von Daten im Zusammenhang mit Anrufen, bei denen keine Verbindung zustande kommt, nicht erforderlich.

Die jeweils zu speichernden Daten nennt Artikel 5 der Richtlinie.

Art. 5 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten [Kategorien von auf Vorrat zu speichernden Daten]
(1) Die Mitgliedstaaten stellen sicher, dass gemäß dieser Richtlinie die folgenden Datenkategorien auf Vorrat gespeichert werden:
a) zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten:
1. betreffend Telefonfestnetz und Mobilfunk:
i) die Rufnummer des anrufenden Anschlusses,
ii) der Name und die Anschrift des Teilnehmers oder registrierten Benutzers;
2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
i) die zugewiesene(n) Benutzerkennung(en),
ii) die Benutzerkennung und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden,
iii) der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine Internetprotokoll- Adresse (IP-Adresse), Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war;
b) zur Identifizierung des Adressaten einer Nachricht benötigte Daten:
1. betreffend Telefonfestnetz und Mobilfunk:
i) die angewählte(n) Nummer(n) (die Rufnummer(n) des angerufenen Anschlusses) und bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Nummer(n), an die der Anruf geleitet wird,
ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer;
2. betreffend Internet-E-Mail und Internet-Telefonie:
i) die Benutzerkennung oder Rufnummer des vorgesehenen Empfängers eines Anrufs mittels Internet-Telefonie,
ii) die Namen und Anschriften der Teilnehmer oder registrierten Benutzer und die Benutzerkennung des vorgesehenen Empfängers einer Nachricht;

c) zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten:
1. betreffend Telefonfestnetz und Mobilfunk: Datum und Uhrzeit des Beginns und Endes eines Kommunikationsvorgangs;
2. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
i) Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers,
ii) Datum und Uhrzeit der An- und Abmeldung beim Internet-E-Mail-Dienst oder Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone;
d) zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:
1. betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;
2. betreffend Internet-E-Mail und Internet-Telefonie: der in Anspruch genommene Internetdienst;
e) zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten:
1. betreffend Telefonfestnetz: die Rufnummern des anrufenden und des angerufenen Anschlusses;
2. betreffend Mobilfunk:
i) die Rufnummern des anrufenden und des angerufenen Anschlusses,
ii) die internationale Mobilteilnehmerkennung (IMSI) des anrufenden Anschlusses,
iii) die internationale Mobilfunkgerätekennung (IMEI) des anrufenden Anschlusses,
iv) die IMSI des angerufenen Anschlusses,
v) die IMEI des angerufenen Anschlusses,
vi) im Falle vorbezahlter anonymer Dienste: Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde;
3. betreffend Internetzugang, Internet-E-Mail und Internet-Telefonie:
i) die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss,
ii) der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs;
f) zur Bestimmung des Standorts mobiler Geräte benötigte Daten:
1. die Standortkennung (Cell-ID) bei Beginn der Verbindung,
2. Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt.
(2) Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden.

Diese Daten sind mindestens 6 Monate zu speichern:

Art. 6 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten [Speicherungsfristen]
Die Mitgliedstaaten sorgen dafür, dass die in Artikel 5 angegebenen Datenkategorien für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden.

Die Richtlinie enthält außerdem besondere Anforderungen an die Datensicherheit:

Art. 7 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten [Datenschutz und Datensicherheit]
Unbeschadet der zur Umsetzung der Richtlinien 95/46/EG und 2002/58/EG erlassenen Vorschriften stellt jeder Mitgliedstaat sicher, dass Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes in Bezug auf die nach Maßgabe der vorliegenden Richtlinie auf Vorrat gespeicherten Daten zumindest die folgenden Grundsätze der Datensicherheit einhalten:
a) Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten,
b) in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen,
c) in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist,
und
d) die Daten werden am Ende der Vorratsspeicherungsfrist vernichtet, mit Ausnahme jener Daten, die abgerufen und gesichert worden sind.

Irland hat beim EuGH Nichtigkeitsklage[17] gegen die Richtlinie erhoben, da sich aus dem EG-Vertrag keine Kompetenz zum Erlass der Richtlinie ergebe.

IV. Rechtslage in Deutschland

Zur gegenwärtigen Rechtslage bei der Speicherung dynamischer IP-Adressen siehe folgende Entscheidungen:

- Entscheidung des BVerfG vom 27.10.2006, Az.: 1 BvR 1811/99.[18]
- Entscheidung des AG Darmstadt vom 30.06.2005, Az.: 300 C 397/04.[19]
- 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.[20]

Zur Umsetzung der Richtlinie über die Vorratsspeicherung von Daten sollen die folgenden Normen in das TKG eingefügt werden:[21]

§ 113a TKG [Speicherungspflichten für Daten]
(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten

[17] Rs. C-301/06, ABl. C 237/5 vom 30.09.2006.
[18] Entscheidung des BVerfG vom 27.10.2006, Az.: 1 BvR 1811/99.
[19] Siehe CyLaw-Report I: „Speicherung von IP-Adressen“.
[20] Siehe CyLaw-Report III: „Auskunftspflichten von Acces-Providern I“.
[21] Gesetzesentwurf der Bundesregierung zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung de Richtlinie 2006/24/EG vom 27.04.2007, BR-Drs. 275/07.

nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.
(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:
1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,
3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,
4. im Fall mobiler Telefondienste ferner:
a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,
b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,
c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,
d) im Falle im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,
5. im Falle von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.
Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.
(3) Die Anbieter von Diensten der elektronischen Post speichern:
1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,
2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,
3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll- Adresse des Abrufenden,
4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.
(4) Die Anbieter von Internetzugangsdiensten speichern:
1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll- Adresse,
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,
3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.
(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.
(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.
(7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten,

aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.
(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.
(9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.
(10) Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Er hat durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu besonders ermächtigten Personen möglich ist.
(11) Der nach dieser Vorschrift Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten innerhalb eines Monats nach Ablauf der in Absatz 1 genannten Frist zu löschen oder die Löschung sicherzustellen.

§ 113b TKG [Verwendung der nach § 113a gespeicherten Daten]
Der nach § 113a Verpflichtete darf die allein auf Grund der Speicherungsverpflichtung nach § 113a gespeicherten Daten
1. zur Verfolgung von Straftaten,
2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder
3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes
an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke darf er die Daten nicht verwenden. § 113 Abs. 1 Satz 4 gilt entsprechend.