Prof. Dr. Viola Schmid, LL.M.

Fachgebiet Öffentliches Recht

Informations- und Datenschutzrecht

Modul 4

A. Grundlagen

B. Deutsches Strafrecht

C. Convention on Cybercrime

*FÖR- Fachgebiet Öffentliches Recht cyberlaw@jus.tu-darmstadt.de

Fundstellen Convention on Cybercrime (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

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

Art. 31 Wiener Vertragsrechtskonvention [Allgemeine Auslegungsregel]
(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. (...)
(http://www.jura.uni-sb.de/BGBl/TEIL2/1990/19901431.2.HTML)

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

(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.

(http://www.jura.uni-sb.de/BGBl/TEIL2/1990/19901432.2.HTML)

Art. 48 Convention on Cybercrime [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. (...)

§ 43 Bundesdatenschutzgesetz (BDSG) [Strafvorschriften]

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

speichert, verändert oder übermittelt,

zum Abruf mittels automatisierten Verfahrens bereithält oder

abruft oder sich oder einem anderen aus Dateien verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. (...)

§ 148 Telekommunikationsgesetz (TKG) [Strafvorschriften]

(...)

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

- Gleichstellung mit Strafgesetzen des Strafgesetzbuchs (StGB)

→ Regeln des Allgemeinen Teils des StGB finden Anwendung

Geltungsbereich des deutschen Strafrechts (1)

Regel: Territorialprinzip

§ 3 StGB [Territorialprinzip]
Das deutsche Strafrecht gilt für die Taten, die im Inland begangen werden.

Anknüpfungspunkt: Tatort

§ 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 (...).

Erweiterung des Inlandsbegriffes: Flaggenprinzip

§ 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 tragen.

Geltungsbereich des deutschen Strafrechts (2)

Ausnahme 1: Personalitätsprinzip

§ 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 Deutsche 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 (...)

Geltungsbereich des deutschen Strafrechts (3)

Ausnahme 2: Schutzprinzip

§ 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 Täter keiner Strafgewalt unterliegt.

Geltungsbereich des deutschen Strafrechts (4)

Ausnahme 3: Weltrechtsprinzip

§ 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 des § 184 Abs. 3 und 4 :
(..)
9. Taten, die auf Grund eines für die Bundesrepublik Deutschland verbindlichen zwischenstaatlichen Abkommens auch dann zu verfolgen sind, wenn sie im Ausland begangen werden.

Strafbarkeit des Täters

§ 25 Abs. 1 StGB [Täterschaft]
Als Täter wird bestraft, wer die Straftat selbst oder durch einen anderen begeht.

→ nur natürliche Personen können sich strafbar machen,
Unternehmen nur durch vertretungsberechtigte Personen, etwa Geschäftsführer
(Beispiel: CompuServe, LG München I, MMR 2000,171ff.)

Strafbarkeit der Teilnahme

§ 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.

A. Geltungsbereich des deutschen Strafrechts eröffnet?
B. Tatbestand
1. Objektiver Tatbestand (Äußere Merkmale): Täter, Tathandlung,Tatobjekt, Erfolg (bei Erfolgsdelikten), Kausalität und objektive Zurechenbarkeit
2. Subjektiver Tatbestand (Innere Merkmale): Vorsatz, Absichten, Motive
C. Rechtswidrigkeit
Diese ist grundsätzlich indiziert.
D. Schuld
Schuldfähigkeit
Unrechtsbewusstsein
Spezielle strafschärfende oder -mildernde Schuldmerkmale
Fehlen von Schuldausschließungsgründen
E. Strafaufhebungs- und -ausschließungsgründe
Rücktritt vom Versuch
Tätige Reue

Szenario

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

§ 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.

(...)

(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 Völkerstrafgesetzbuch

(1) 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.

(2) In minder schweren Fällen des Absatzes 1 Nr. 2 bis 5 ist die Strafe Freiheitsstrafe nicht unter fünf Jahren.

A. Geltungsbereich des deutschen Strafrechts eröffnet?

B. Tatbestand

1. Objektiver Tatbestand (Äußere Merkmale): Täter: Jeder, Tathandlung: leugnen, Tatobjekt: Äußerung im Zusammenhang mit Handlungen des Nationalsozialismus nach § 6 Abs. 1 VStGB, Erfolg: konkrete Eignung zur Friedensstörung in der BRD
2. Subjektiver Tatbestand (Innere Merkmale): Vorsatz

C. Rechtswidrigkeit

Diese ist grundsätzlich indiziert.

D. Schuld

E. Strafaufhebungs- und -ausschließungsgründe

Szenario (nach BGH St 46, 212, Az. 1 Str 184/00)

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

Prüfung:

- Geltungsbereich des deutschen Strafrechts eröffnet?

§ 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“)

„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.

(Im Übrigen wie beim Grundszenario)

*FEX: „abstrakt-konkretes Gefährdungsdelikt“, wobei strittig ist, ob es hier einen Erfolgsort geben kann; vergleiche BGH-Entscheidung

§ 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.

A. Grundlagen
- I. Fundstellen
- II. Auslegung völkerrechtlicher Verträge

B. Deutsches Strafrecht
- I. Nebenstrafrecht
- II. Geltungsbereich des deutschen Strafrechts
- III. Täterschaft und Teilnahme
- IV. Strafrechtliches Prüfungsschema
- V. Beispielsfall „Qualifizierte Auschwitzlüge“
- VI. Informationsspezifische Delikte

C. Convention on Cybercrime
- I. Grundlagen
- II. Informationspezifische Delikte
- III. Strafverfolgung

Informationsspezifische Delikte

§ 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.

§ 184 b 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) Ebenso wird bestraft, wer es unternimmt, einem anderen den Besitz von kinderpornographischen Schriften zu verschaffen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben.

(...)

§ 184 c StGB [Verbreitung pornographischer Darbietungen durch Rundfunk, Medien- oder Teledienste]

Nach den §§ 184 bis 184b wird auch bestraft, wer eine pornographische Darbietung durch Rundfunk, Medien- oder Teledienste verbreitet. In den Fällen des § 184 Abs. 1 ist Satz 1 bei einer Verbreitung durch Medien- oder Teledienste nicht anzuwenden, wenn durch technische oder sonstige Vorkehrungen sicher-gestellt ist, dass die pornographische Darbietung Personen unter achtzehn Jahren nicht zugänglich ist.

§ 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;

Schema (1)

A. Grundlagen | B. Deutsches Strafrecht | C. Convention on Cybercrime

1.	**Personal-aktiv**	➢"Berufsgruppen", die in einer prozeduralen Betrachtung für den Informationstransfer von Bedeutung sind (§ 206 StGB - Verletzung des Postgeheimnisses) ➢"Berufsgruppen" (etwa Arzt in § 203 StGB, Amtsträger in § 353b StGB und in Steuersachen § 355 StGB), die in einer inhaltlichen Betrachtung "Geheimnisnähe" haben
2a)	**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

Schema (2)

A. Grundlagen | B. Deutsches Strafrecht | C. Convention on Cybercrime

2 b)	**Personal - passiv** **Datenschutz professionell**	➢§ 203 StGB Verletzung von Privatgeheimnissen ➢§ 206 StGB Verletzung des Post- oder Fernmelde-geheimnisses ➢§ 303b StGB Computersabotage ➢§ 353b StGB Verletzung von Dienstgeheimnissen ➢§ 355 StGB Verletzung des Steuergeheimnisses
2 c)	**Personal-passiv** **Informationskosten**	➢Infomationsvorhaltekosten: Strafverfolgung „Informationsbeschaffungskosten: für die Täter: evtl. Strafbarkeit
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

Schema (3)

A. Grundlagen | B. Deutsches Strafrecht | C. Convention on Cybercrime

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 die Module 1 und 2, in denen der verfassungsrechtliche Schutz von Daten vorgestellt wurde

Tatbestände Personal-aktiv (1)

A. Grundlagen | B. Deutsches Strafrecht | C. Convention on Cybercrime

§ 203 StGB [Verletzung von Privatgeheimnissen]

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker (...),
2. Berufspsychologen (...),
3. Rechtsanwalt, (...)

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. (...)

§ 353b StGB [Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht]

(1) Wer ein Geheimnis, das ihm als

1. Amtsträger, (...)
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

anvertraut worden oder sonst bekanntgeworden ist, unbefugt offenbart und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. (...)

Tatbestände Personal-aktiv (2)

§ 355 StGB [Verletzung des Steuergeheimnisses]

(1) Wer unbefugt

1. Verhältnisse eines anderen, die ihm als Amtsträger

a) in einem Verwaltungsverfahren oder einem gerichtlichen Verfahren in Steuersachen, (…)

2. ein fremdes Betriebs- oder Geschäftsgeheimnis, das ihm als Amtsträger in einem der in Nummer 1 genannten Verfahren bekanntgeworden ist,

offenbart oder verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. (…)

§ 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. (…)

Tatbestände Personal-passiv (Datenschutz allgemein) (1)

§ 201 StGB [Verletzung der Vertraulichkeit des Wortes]

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

Tatbestände Personal-passiv (Datenschutz allgemein) (2)

§ 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.

§ 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.

(..)

Tatbestände Personal-passiv (Datenschutz allgemein) (3)

§ 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.

(…)

Tatbestände Personal-passiv (Datenschutz allgemein) (4)

§ 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.

§ 95 StGB [Offenbaren von Staatsgeheimnissen]

(1) Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, an einen Unbefugten gelangen läßt oder öffentlich bekanntmacht und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft, wenn die Tat nicht in § 94 mit Strafe bedroht ist.

Tatbestände 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.

Tatbestände Personal-passiv (Objekt)

§ 93 StGB [Begriff des Staatsgeheimnisses]

(1) Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheimgehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden.

§ 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.

(...)

Qualität der Informationstechnik (1)

Qualität der Informationstechnik in einer detaillierten Betrachtung		
1.	**Personal-aktiv**	➢Personen, die über spezifische Kenntnisse und Tools verfügen
2 a)	**Personal - passiv** **Datenschutz allgemein**	➢§ 202a StGB Ausspähen von Daten (Hacken ist zunächst strafrechtlich irrelevant, solange es beim Eindringen in die fremde Datenbank bleibt. Erst beim Sichverschaffen der Daten ist § 202a StGB einschlägig) ➢§ 263a StGB Computerbetrug ➢§§ 269, 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung ➢§ 303a Datenveränderung
2b)	**Personal - passiv** **Datenschutz professionell**	➢§ 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses ➢§ 303b StGB Computersabotage

Qualität der Informationstechnik (2)

2 b)	**Personal-passiv** **Informationskosten**	➢Infomationsvorhaltekosten: Strafverfolgung (späteres Modul) ➢„Informationsbeschaffungskosten“: für die Täter: evtl. Strafbarkeit
3.	**Objekt**	➢Persönlicher Lebens- und Geheimnis-bereich § 202a StGB ➢Post- oder Fernmeldegeheimnis, § 206 StGB ➢Datenverarbeitungsvorgang, §§ 263a, 270 StGB ➢Datenverarbeitungsanlage und -träger, § 303b StGB ➢Telekommunikationsanlage, § 317 StGB

Qualität der Informationstechnik (3)

4.	**Kausal/Zweck**	➢Interesse an und Schutz der Daten und des Datenverarbeitungsvorganges
5.	**Qualität der Information(stechnik)**	➢Ausspähen von Daten (Zugriffverschaffen) ➢Verfälschung von Daten ➢Eingriff in den Datenverarbeitungsvorgang ➢Datenveränderung, -unterdrückung und –unbrauchbarmachung ➢Zerstörung der Anlagen
6.	**Verfahren**	Die Straftaten werden nach der Strafprozessordnung (StPO) verfolgt.
7.	**Rechtfertigung/ Verhältnismäßigkeit**	Siehe Vorlesung und die Module 1 und 2, in denen der verfassungsrechtliche Schutz von Daten und Anlagen vorgestellt wurde

Gliederung

CCC- Grundlagen - Geltungsbereich (1)

Article 22 [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.

CCC -Grundlagen - Geltungsbereich (2)

A. Grundlagen | B. Deutsches Strafrecht | C. Convention on Cybercrime

Article 22 [Jurisdiction]

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.

CCC - Grundlagen - Geltungsbereich (3)

A. Grundlagen | B. Deutsches Strafrecht | C. Convention on Cybercrime

Geltungsbereich eröffnet, wenn Straftat

I. auf dem Hoheitsgebiet einer Vertragspartei,
(Art. 22 Abs. 1 a) CCC). (→ Territorialprinzip des § 3 StGB)

II. an Bord eines Schiffes, das die Flagge eines Vertragsstaats führt (Art.22 Abs.1b)CCC)
bzw. an Bord eines Flugzeugs eines Vertragsstaats (Art.22 Abs.1 c)CCC).
(→ Territiorialprinzip des § 4 StGB)

III. von einem Staatsangehörigen eines Vertragsstaats, wenn die Tat am Tatort strafbar ist oder der Ort keiner Strafgewalt unterliegt, (Art. 22 Abs. 1 d) CCC).
(→ Personalitätsprinzip § 7 Abs. 1 StGB)

→ Falls Zuständigkeiten (jurisdiction) verschiedener Vertragsstaaten begründet sind, ist eine gegenseitige Konsultation und Abstimmung der Vertragsstaaten (Art. 22 Abs. 5 CCC) gefordert

Geltungsbereich des deutschen Strafrechts - RERUN

A. Grundlagen | B. Deutsches Strafrecht | C. Convention on Cybercrime

Regel: Territorialprinzip

§ 3 StGB [Territorialprinzip]

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

Erweiterung des Inlandsbegriffes: Flaggenprinzip

§ 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 tragen.

CCC - Grundlagen - Geltungsbereich (3)

A. Grundlagen | B. Deutsches Strafrecht | C. Convention on Cybercrime

Geltungsbereich eröffnet, wenn Straftat

I. auf dem Hoheitsgebiet einer Vertragspartei,
(Art. 22 Abs. 1 a) CCC). (→ Territorialprinzip des § 3 StGB)

II. an Bord eines Schiffes, das die Flagge eines Vertragsstaats führt (Art.22 Abs.1b)CCC)
bzw. an Bord eines Flugzeugs eines Vertragsstaats (Art.22 Abs.1 c)CCC).
(→ Territiorialprinzip des § 4 StGB)

III. von einem Staatsangehörigen eines Vertragsstaats, wenn die Tat am Tatort strafbar ist oder der Ort keiner Strafgewalt unterliegt, (Art. 22 Abs. 1 d) CCC).
(→ Personalitätsprinzip § 7 Abs. 1 StGB)

→ Falls Zuständigkeiten (jurisdiction) verschiedener Vertragsstaaten begründet sind, ist eine gegenseitige Konsultation und Abstimmung der Vertragsstaaten (Art. 22 Abs. 5 CCC) gefordert

CCC- Grundlagen – Vorsatz und fehlende Berechtigung

I. Vorsatz

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

II. Fehlende „Berechtigung“

Zudem fordern alle Tatbestände der Konvention ein „unbefugtes“ Verhalten (without right). Grundlagen einer Berechtigung sind:

- 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

→ „unbefugt“ kann als Tatbestands- oder Rechtswidrigkeitsmerkmal ausgelegt werden.

CCC- Grundlagen – Beteiligtenstrafbarkeit

Article 11 [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.

→Keine dem deutschen Recht vergleichbare Unterscheidbarkeit der Beteiligungsmodalitäten;
“aiding”: tendiert zu Beihilfe
“abetting”: tendiert zur Ansitiftung

„“Aid“ within aider and abettor statute means to help, to assist, or to strengthen while „abet“ means to counsel, to encourage, to incite or to assist in commission of criminal act.“ (Quelle: Black‘s Law-Dictionary)

CCC- Grundlagen – Versuch

Article 11 [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, an 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.

CCC-Grundlagen – Verantwortlichkeit juristischer Personen (1)

Article 12 [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.

- Juristische Personen können neben natürlichen Personen verantwortlich sein.

- Verantwortlichkeit der juristischen kann Person straf-, zivil- oder verwaltungsrechtlicher Art sein.

→ Anpassungsbedarf in Deutschland?

Article 15 [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.

Article 15 [Conditions and safeguards]

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.

Informationsspezifische Delikte

➢Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen

➢Computerstraftaten

➢Kinderpornographie

➢Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte

Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen (1)

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.

→ Vgl. § 202a StGB (Ausspähen von Daten9

Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen (2)

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.

→ Vgl. § 202a StGB (Ausspähen von Daten)

Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen (3)

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.

→ Vgl. § 303a StGB (Datenveränderung)

Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen (4)

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.

→ Vgl. § 303b StGB (Computersabotage)

Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen (5)

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.

Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen (6)

Article 6 [Misuse of devices]

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.

Computerstraftaten (1)

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.

→Vgl. § 269 StGB (Fälschung beweiserheblicher Daten) und
§ 270 StGB (Täuschung im Rechtsverkehr bei Datenverarbeitung

Computerstraftaten (2)

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.

→Vgl. § 263 StGB (Computerbetrug)

Kinderpornographie (1)

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.

Kinderpornographie (2)

Article 9 [Offences related to child pornography]

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.

→ Vgl. § 184 b StGB (Verbreitung,..., kinderpornographischer Schriften)
→ bislang im deutschen Strafrecht: Minderjährig = bis 14 Jahre
→ Anpassungsbedarf?

Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (1)

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.

Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (2)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

Article 10 [Offences related to infringements of copyright and related rights]

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.

→ Vgl. deutsches Urheberrecht (Urhebergesetz)

Gliederung

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

Strafverfolgung (1)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

Article 16 [Expedited preservation of stored computer data]

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

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

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

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

Strafverfolgung (2)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

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.

→ Sicherung von „stored computer data", „traffic data"
→ bis zu 90 Tage

Strafverfolgung (3)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

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.

→ Herausgabeanordnung

Strafverfolgung (4)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

Article 18 [Production order]

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.

Strafverfolgung (5)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

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.

Strafverfolgung (6)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

Article 19 [Search and seizure of stored computer data]

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.

Strafverfolgung (7)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

Article 19 [Search and seizure of stored computer data]

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.

→ Durchsuchung und Beschlagnahme (klassische Maßnahmen der Strafverfolgungsbehörden)

→ Inpflichtnahme des Systemverwalters möglich (Art. 19 Abs. 4 CCC)

Strafverfolgung (8)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

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.

Strafverfolgung (9)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

Article 20 [Real-time collection of traffic data]

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.

Strafverfolgung (10)

A. Grundlagen B. Deutsches Strafrecht C. Convention on Cybercrime

Article 21 [Interception of content data]

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

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

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

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

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

Article 21 [Interception of content data]

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.

Prof. Dr. Viola Schmid, LL.M.

Fachgebiet Öffentliches Recht

Informations- und Datenschutzrecht

Modul 4

A. Grundlagen

B. Deutsches Strafrecht

C. Convention on Cybercrime