

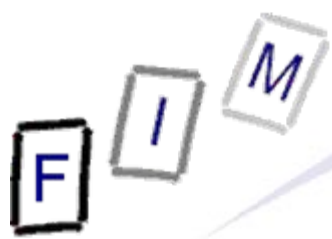


E-Business Recht

Computerstrafrecht

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)
Johannes Kepler Universität Linz, Österreich

E-Mail: sonntag@fim.uni-linz.ac.at
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



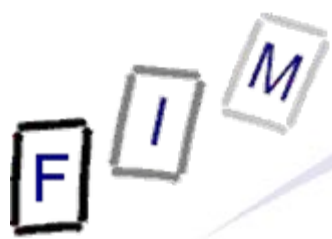
- Delikte des eigentlichen Computerstrafrechts
 - Beispiel: Computerbetrug, Datenbeschädigung/-fälschung, ...
- Delikte, die im Internet "wichtig" sind
 - Als wichtig angesehen oder häufiges Auftreten
 - Beispiel: Kinderpornographie, Üble Nachrede

Hier **nicht** behandelt: Strafrechtliche Delikte in anderen Themenbereichen (zB Datenschutz, Urheberrecht)!



Warum ist Strafrecht nötig?

- Die "ultima ratio": Wenn sich die Leute nicht "entsprechend" verhalten, dann gibt es noch die staatliche Zwangsgewalt
 - Was "entsprechend" ist, bestimmt (im Grundsatz) das Volk
 - » EU-Recht hier unbedeutend! VO, RL, etc. bestimmen nur "ist unter Strafe zu stellen", aber nicht wie (Verwaltung, Gericht), bzw. wie viel (Geld, Haft, Geld+Haft; Ausmaß etc.)
- Strafrecht hat drei Hauptzwecke
 - Generalprävention: Abschreckung potentieller Täter
 - Spezialprävention: Verhinderung des Wieder-Begehens
 - Vergeltung
 - » Dieser Punkt ist umstritten!
- Teilweise Internationale Angleichung: "Convention on Cybercrime"
 - Grund: "Traditionelle" Straftaten sind meist lokal, während Internet-Straftaten meist über (große) Distanz erfolgen



- Daten im Strafrecht: Unabhängig von Personenbezug
 - Keine Verbindung zu Datenschutzgesetz
 - Personenbezogene, Maschinenbezogene, Anonyme, ...
Daten sind alles Daten im strafrechtlichen Sinne
- Daten als Beweise:
 - Daten sind keine eigene Beweismittelkategorie
 - Augenschein oder Gutachten problemlos möglich!
 - » Augenschein oft nicht sehr vielsagend
 - Grundsatz der freien Beweiswürdigung
 - » Beispiel unsigned E-Mail: Kann wertlos oder sehr gut sein
 - Bsp.: Vor ? Jahren (auch) gedruckt, auf Dritt-Server protokolliert, ...
- Urkunden: El. Daten sind in Ö keine Urkunden
 - Schriftlichkeit = Mit freiem Auge lesbar
 - Ausdrucken → Urkunde
 - » Achtung: Urkundendelikte setzen uU zusätzliches voraus!



Geltung österr. Strafrechts

- Distanzdelikte → Problematik der Geltung
 - Zeitlich: Kein besonderes Problem
 - » Strafrecht: Rückwirkung ist niemals erlaubt!
 - Persönlich: Welche Personen sind unterworfen
 - » Meist kein Problem
 - Örtlich: Komplex! Je nach Delikt verschieden
- Örtliche Geltung:
 - Schlichte Tätigkeitsdelikte (selten): Ort der Handlung
 - Erfolgsdelikte: Wo der Täter gehandelt hat, bzw. wo der Erfolg eingetreten ist
 - » Erfolg in Österreich → Österreichisches Recht
 - Zusätzlich: Wenn im Handlungs-Land verboten → Auch dort strafbar
 - Sonstige Ausnahmen: ZB gegen Österr. Geheimnisse
 - » Problem des Erkennens und Durchsetzens
 - Beteiligung: Mitwirkung an Inlandstat vom Ausland aus



Widerrechtlicher Zugriff auf ein Computersystem: § 118a StGB

- Absicht zur Kenntnis-Verschaffung
 - Daten
 - Nicht für ihn bestimmt
 - benützen, zugänglich machen, veröffentlichen der Daten
 - Vermögensvorteil für sich/anderen oder Vermögensnachteil
- Keine Alleinverfügungsberechtigung
- Zugang verschaffen
- Verletzung spezifischer Sicherheitsvorkehrungen im Computersystem
- Verletzung = Hacken, umgehen
 - Wohl: Nicht vorgesehene Bedienung
 - » Nicht: Einloggen mit Gast-Account ohne Passwort
- Sicherheitsvorkehrungen = Schutz gegen Eindringen
 - Backup, Logs, etc. zählen nicht dazu!



Verletzung des Telekommunikations- geheimnisses: § 119 StGB

- Absicht zur Kenntnis-Verschaffung
 - Inhalt einer Telekommunikations-Nachricht
 - Nicht für ihn bestimmt
- Benützung einer Vorrichtung an einem Computersystem oder einer Telekommunikationsanlage
- Analog zum Briefgeheimnis:
 - Nachricht = Von Menschen an Menschen
 - » E-Mails, SMS, Telefonate, ...
 - » Nicht: Zeitsynchronisation, automat. Überweisungen, ...
- Anbringen der Vorrichtung ist nicht strafbar, erst Benützung!
- Praxis: Problem bei Einsatz von Netzwerk-Sniffen!
- "Vorrichtung": Geräte, Programm etc.



Missbräuchliches Abfangen von Daten: § 119a StGB

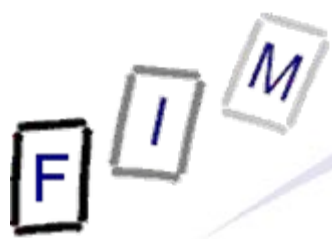
- Absicht zur Kenntnis-Verschaffung
 - Daten
 - Nicht für ihn bestimmt
 - benützen, zugänglich machen, veröffentlichen der Daten
 - Vermögensvorteil für sich/anderen oder Vermögensnachteil
- Benützen einer Vorrichtung an einem Computersystem
 - Oder einer Empfangsvorrichtung (el.-magn. Abstrahlung)
- Hierdurch sind **alle** Daten geschützt!
 - Nicht nur Nachrichten, wie bei § 119
- Dafür ist ein erweiterter Vorsatz nötig
- § 120a: Mithören, wenn Nachrichten "ohnehin vorbeikommen"



Datenbeschädigung: § 126a StGB

- Schädigung eines Anderen durch
- Löschen, verändern, unbrauchbaren machen, unterdrücken
- von Daten ohne Alleinverfügungsberechtigung

- Österreich: Sache = Körperlicher Gegenstand
 - Sachbeschädigung betrifft daher niemals Daten!
 - » Bestenfalls (wertlosen) Datenträger (CD, Festplatte etc.)!
- Löschen etc.: Verhinderung des unmittelbaren Gebrauchs
- Alleinverfügungsberechtigung: Sobald jemand anderer (auch) Rechte an den Daten besitzt, fällt diese weg
- Schaden: Wiederbeschaffung der Daten
 - Problem: Folgeschäden sind nicht enthalten!
 - » Beispiel: Geschäftsentgang
 - » Anders bei einem Schadenersatzprozess!



Störung der Funktionsfähigkeit eines Computersystems: § 126b StGB

- Schwere Störung der Funktionsfähigkeit eines Systems
- Keine Alleinverfügungsberechtigung
- Durch Eingabe oder Übermittlung von Daten

- Schwere Störung: Gravierende Einschränkungen der Funktionalität des Computersystems
- Subsidiär zur Datenbeschädigung
 - Schädigung besteht im Wert der Daten → § 126a
 - Schädigung besteht in schlechterer Funktion → § 126b
- Schädigungsabsicht muss nicht vorliegen, es reicht Vorsatz der schweren Störung!



Missbrauch von Computerprogrammen oder Zugangsdaten: § 126c StGB

- Spezielle Computerprogramme oder Zugangscodes
 - Ersichtlich zur Begehung bestimmter Straftaten (§ 118a, 119, 119a, 126a, 126b, 148a) geschaffen oder adaptiert
- Herstellen, einführen, vertreiben, veräußern, zugänglich machen, verschaffen, **besitzen**
- Vorsatz zur Verwendung bei Begehung best. (s.o.) Straftaten
- Schon die Vorbereitung auf bestimmte Straftaten bzw. dafür erforderliche Mittel werden unter Strafe gestellt
- Computerprogramme: **Objektiver** Maßstab
 - Sicherheitsprogramme fallen darunter
 - Es kommt dann nur mehr auf den Vorsatz an!
- "Besitz" war anfangs nicht enthalten, wurde dann eingefügt



Betrügerischer Datenverarbeitungsmissbrauch: § 148a StGB

- Unrechtm. Bereicherungs- oder Schädigungsvorsatz
- Ergebnis-Veränderung einer autom. Datenverarbeitung
 - Durch Programmgestaltung, Eingabe, Veränderung, Löschung, Unterdrückung oder sonstige Einwirkung
- Betrug: Ein **Mensch** muss getäuscht werden
- Manipulation muss Ergebnis verändern
 - Hacken, Zeitediebstahl, Verspätung, etc. → Nicht relevant!
- Dieses Ergebnis muss Vermögensschaden verursachen
- Die Bereicherung muss aus dem Schaden stammen
- Mögliche Manipulationen:
 - Eingabe falscher Daten
 - Unbefugte Eingabe richtiger Daten
 - Veränderung von Programm oder dessen Ablauf



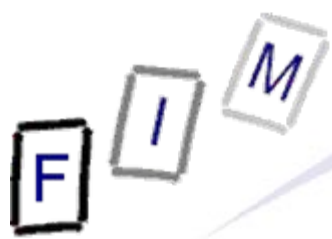
Datenfälschung: § 225a StGB

- Herstellung falscher oder Verfälschung echter Daten
- Eingabe, Veränderung, Löschung oder Unterdrückung
- Vorsatz der Verwendung zum Beweis eines Rechts oder einer Tatsache im Rechtsverkehr

- Analog der Urkundenfälschung
 - Daten sind ja keine Urkunden!
- "Falsche" Daten = Täuschung über den **Urheber**
 - Ob der Inhalt den Tatsachen entspricht ist hier egal!
- "Verfälschung" von Daten: Änderung von **Inhalt** oder **Urheber**
- Verwendung als Beweis
 - Spuren verwischen fällt nicht darunter!
 - Muss aber kein Gerichtsverfahren sein; überall reicht
 - » Auch zur Vortäuschung eines Garantiefalles



- Die folgenden Delikte sind keine **echten** Computerdelikte, d.h. sie haben nichts besonderes mit der IT zu tun
- Sie sind aber in diesem Bereich besonders wichtig!
 - Kommen häufig vor
 - Werden als besonders wichtig angesehen



Üble Nachrede: § 111 StGB

- Vorwurf gegen den Charakter einer Person
- Vorwurf einer unehrenhaften oder unsittlichen Handlung
 - Nicht: Vorwurf einer Straftat (→ § 297 Verleumdung)!
- Möglichkeit der Abwendung: Wahrheitsbeweis
 - Alternativmöglichkeit: Beweis des guten Glaubens
 - » Sachliche und glaubhafte Anhaltspunkte für die Äußerung
 - Nicht erlaubt bei Tatsachen des Privat- und Familienlebens
 - » Herabsetzende Äußerungen sind in diesem Bereich auch dann verboten, wenn sie der Wahrheit entsprechen!
- Erhöhte Strafdrohung bei breiter Öffentlichkeit
 - Beispiel: Gut besuchte Web-Site oder Blog
- Erforderlich ist nur die Möglichkeit der Kenntnisnahme für zumindest einen Dritten (d.h. nicht den/die Beleidigten)
- Praktisches Problem: Prozess = Noch größere Öffentlichkeit!



Beleidigung: § 115 StGB

- Im Gegensatz zur Üblen Nachrede hier reine Werturteile
 - Beschimpfung, Verspottung, Androhung von Misshandlung
 - Daher kein Wahrheitsbeweis/Gutgläubensbeweis möglich!
- Muss aber öffentlich oder vor mehreren begangen werden
 - Mehrere = Mindestens drei Personen!
 - » Ohne Beleidiger/Beleidigte(n)
 - Es reicht die Wahrnehmbarkeit; tatsächliche Wahrnehmung ist nicht erforderlich
- Früher: Beleidigung privat gegenüber einer Person war ein Verwaltungsdelikt
 - » Beispiel: Autofahrer zeigt einem anderen den Vogel
 - Würde inzwischen abgeschafft!



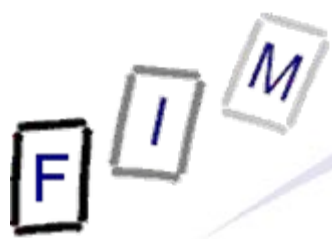
Verletzung des Briefgeheimnisses: § 118 StGB

- "Verschlossene Briefe oder andere solche Schriftstücke"
 - Postkarten gehören nicht dazu!
 - E-Mail daher also auch nicht, da sie nicht "verschlossen" ist
- Ev. möglich: Verschlüsselte E-Mails
 - Immer noch das Problem mit "Schriftstück"
- Daher keine Bedeutung im el. Bereich
 - Datenschutzbestimmungen stattdessen anwenden
 - Siehe § 119 (Verletzung des Telekommunikationsgeheimnisses)

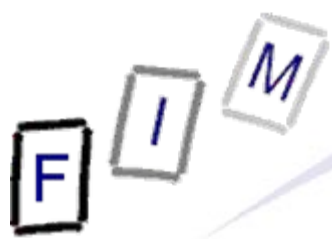


Auskundschaften von Geschäfts- oder Betriebsgeheimnissen: § 123 StGB

- Geschäftsgeheimnisse = Wissen kommerzieller Art, das nur Innenstehenden bekannt ist
- Betriebsgeheimnisse = Technische Einrichtungen oder sachbezogenen Daten
- "Geheimnis" muss kumulativ erfüllen:
 - Beziehung zu Betrieb
 - Nicht offenkundig oder allgemein zugänglich
 - Berechtigtes Interesse an Geheimhaltung
 - Willen zur Geheimhaltung
- Verboten ist die kommerzielle Verwertung der Geheimnisse
 - Schon das Auskundschaften dafür ist ebenfalls verboten!
- **Nicht** darunter fällt die Weitergabe solcher Daten die rechtmäßig erworben wurden ("Verrat" durch Mitarbeiter!)



- Besondere theoretische Bedeutung im Internet, praktische Verurteilungen aber meist nur aus "offline" Bereichen
- Pyramidenspiel:
 - Ein Einsatz ist zu entrichten
 - Dafür wird ein Vermögensvorteil versprochen
 - Der Erfolg hängt davon ab, dass den System weitere Teilnehmer unter gleichen Bedingungen zugeführt werden und sich diese ebenfalls an die Bedingungen halten
- Verboten ist:
 - Veranstalten bzw. In-Gang-Setzen
 - Verbreiten in geeigneter Weise zur Anwerbung Vieler
 - » Zur Anwerbung von mindestens 30 Personen geeignet
 - Gewerbsmäßige Förderung auf sonstige Weise
- Erlaubt ist: Die bloße Teilnahme daran!



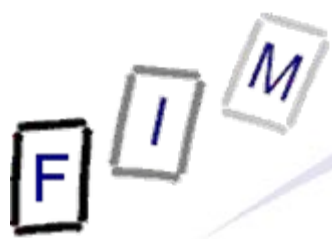
Pornographische Darstellungen Minderjähriger: § 207a StGB

- Bildliche Darstellungen (Bilder, Videos; nicht: Audio, Text)
- Minderjährige Person (Höhere Strafdrohung bei <14 Jahren)
 - Es reicht der Eindruck dafür aus!
 - » Auch "Fakes": Bloßer Eindruck, es wäre geschlechtliche Hdlg.
 - Frau mit 18,1 Jahren, sieht aus/aufgemacht wie 16 → Verbot!
 - Selbst komplett computergenerierte Bilder fallen darunter!
 - » Sofern sie wirklichkeitsnahe sind (Cartoons eher nicht mehr)
 - » Angebot zur Befriedigung entsprechender Wünsche soll ausgedünnt werden; nicht nur tatsächlichen Missbrauch verhindern!
- Verboten ist: Herstellung, anbieten, verschaffen, überlassen, vorführen, zugänglich machen, besitzen
 - Sowie zur Verbreitung einführen, befördern, ausführen
 - Besitz setzt allerdings Besitzwillen voraus, was Wissen darüber verlangt: Unterschobene Bildern sind nicht strafbar!



Delikte gegen Geld: § 232, 241a-g StGB

- Geldfälschung (§ 232): Keine Bedeutung, da es kein echtes "e-Geld" gibt
 - Giralgeld, PayPal-Guthaben, Kreditkarten → Kein "Geld"!
- Delikte gegen "Unbare Zahlungsmittel" (§ 241a-g)
 - **Körperliche Zahlungsmittel**
 - » Daher hier auch keine große Bedeutung!
 - Aussteller erkennbar
 - Gegen Fälschung/missbräuchliche Verwendung geschützt
 - Bargeldvertretende Funktion/zur Ausgabe von Bargeld
 - Beispiele: Quick, Bankomat, Kreditkarte, Prepaid-Karten, Wechsel, Schecks, ...
 - Verboten ist: Fälschung, Annahme/Weitergabe/Besitz gefälschter Zahlungsmittel, Vorbereitung der Fälschung, ...
 - » Nicht enthalten: Einsatz gefälschter/gestohlener Mittel
 - Dafür gibt es Betrug, Computerbetrug etc.!



Beweismittelfälschung: § 293 StGB

- Beweismittel = Geeignet, in einem behördlichen Verfahren einen Sachverhalt zu belegen
 - Logfiles, Dateninhalte, E-Mails etc.
- Jegliche Änderung verboten, um einen anderen Sachverhalt glaubhaft(er) zu machen
 - Wenn es in einem gerichtlichen oder verwaltungsbehördlichen Verfahren verwendet werden soll
 - » Von wem auch immer!
- Achtung: Konkurrenz zu Datenfälschung!
- Problem: Nachweis der Veränderung in der Praxis
 - Beispiel: Es gibt weitere Kopien, die zu verändern vergessen wurde (zB wiederherstellbare gelöschte alte Versionen)



- Spezialität in Österreich/Deutschland
 - USA: Geschützt durch "Freie Meinungsäußerung"!
 - Problem der Zuständigkeit
- Nationalsozialistische Propaganda bzw. Unterstützung in verschiedensten Ausprägungen ist verboten
 - Aufforderung, Wiederbetätigung, Verharmlosung, Darstellung entsprechender Symbole, ...
- Einer der Punkte, von denen jeder Österreicher (**auch juristische Laien!**) wissen muss, dass sie verboten sind!



Pornographieggesetz

- Dies betrifft **nicht** die Kinderpornographie (siehe oben!)
- Hier ist der Besitz erlaubt, aber die Verbreitung verboten oder beschränkt (insb. an Jugendliche)
- Einteilung in "harte" und "normale" Pornographie
 - **"Hart": Bei Gewinnabsicht grundsätzlich verboten**
 - » Sexuelle Gewalttätigkeiten, Unzucht mit Tieren etc.
 - » Keine exakte Definition im Gesetz; die Gerichte urteilen verschieden, insb ändert sich die Rechtsprechung über die Zeit
 - Beispiel: Homosexualität
 - **"Normal": Darf auch verkauft werden, sofern sie nicht öffentlich in Erscheinung tritt und Jugendlichen der Zutritt verwehrt wird**
 - » Verkauf nur "unter dem Ladentisch"
 - » Internet: Wirksame Alterskontrolle erforderlich
 - In D existieren dazu strenge und genaue Vorgaben, in Ö nicht



- In weiten Teilen "graue Theorie", denn
 - Viele Delikte sind schwer erkennbar
 - Viele Delikte sind schwer zu beweisen
 - Viele Täter sind (für Österreich) nicht greifbar
 - Betroffene Firmen haben oft kein Interesse an Publizität
 - » Schadenersatz ist von Tätern meist ohnehin nicht zu erlangen
 - Einige Delikte sind Privatanklagedelikte
 - Meist professionelles Vorgehen (Org. Kriminalität)
- Praktische Bedeutung oft im Gegensatz zu Volksempfinden
 - Kinderpornographie gegenüber Betrug verschwindend gering!
- Polizei in EDV-Hinsicht bisher schwer unterbesetzt
 - Wird sehr viel besser, sowohl hinsichtlich Ausbildung als auch Ausstattung mit Personal und Geräten

F I M

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!