

Computerstrafrecht

**(Kurzfassung des Vortrages am 28.03.2001 beim
Landeskriminalamt Baden-Württemberg
im Rahmen der
Aus- und Weiterbildung
für IuK-Sachbearbeiterinnen
und IuK-Sachbearbeiter)**

Zu den Bestimmungen des Strafrechtes und Nebenstrafrechtes in Bezug auf die sog. Computerkriminalität mit Hinweisen zu Fragen der Beweisführung.

Mit Beispielen aus der Praxis unter Darstellung der Zuständigkeiten und der Möglichkeiten der Rechtshilfe und der Ermittlungen im Ausland.

1. Begriffe zum Internet und WWW (World Wide Web)

Das World Wide Web (WWW) ist der jüngste Dienst innerhalb des Internet. Das Web zeichnet sich dadurch aus, dass es auch ungeübteren Anwendern erlaubt, sich im Informationsangebot zu bewegen. Im WWW erscheinen Informationen gleich beim Aufruf am Bildschirm. Das bequeme Navigieren mit Hilfe einfacher Mausklicks wird auch als "Surfen im Netz" bezeichnet.

Die nachfolgenden Begriffe sind in der empfehlenswerten Darstellung von *Munz, selfHTML*, <http://www.teamone.de>, ausführlich erläutert. *SelfHTML* findet sich auf zahlreichen CD-ROM, die als Beilage zu Computerzeitschriften erhältlich sind, oder im WWW (testen Sie doch mal die Suchmaschine www.google.com).

Begriffe zum WWW von A bis Z in deutsch und anderen Sprachen finden sich unter <http://www.wvli.com/translation/netglos/glossary/german.html>

1.1 E-Mail

E-Mail (elektronische Post) ist wohl der am meisten genutzte Internet-Dienst. Eine E-Mail-Adresse ist am Aufbau *name@domain.de* erkennbar. Der „Klammeraffe“ @ bedeutet englisch "at", also "bei".

1.2 Telnet

Telnet dient zur Fernbedienung von Rechnern im Internet.

1.3 File Transfer (FTP)

FTP dient dazu, sich auf einem bestimmten Server-Rechner im Internet einzuwählen und von dort Dateien auf den eigenen Rechner zu übertragen (Download) oder eigene Dateien an den Server-Rechner zu übertragen (Upload).

1.4 Gopher

Gopher gilt heute als der Vorläufer des World Wide Web. Der Name kommt von "go for" und drückt damit aus, was der wichtigste Zweck dieses Dienstes ist: nämlich große Informationsbestände leichter durchsuchbar zu machen.

1.5 Chat (IRC – Internet Relay Chat)

Wer sich einsam fühlt oder einfach "in" sein will, geht im Internet chatten (ratschen, quatschen).

1.6 Newsgroups (News)

Eine Newsgroup ist einem schwarzes Brett vergleichbar, wo Sie Nachrichten zu bestimmten Themenbereichen „posten“ können, die alle Besucher lesen können.

Der Themenkreis ist der News-Kennung zu entnehmen:

alt = alternativ, bunt, verrückt, abgefahren

biz = Kommerzielles, jedoch keine Werbung

comp = Computer

de = deutschsprachig

misc = Sonstiges
 news = Newsgroups zum Thema Newsgroups
 rec = Freizeit, Hobby und Kunst
 sci = Wissenschaften
 soc = Soziales, Kultur, Politik
 talk = Klatsch und Tratsch

1.7 Entwicklung

Auch hier wird auf *Munz*, *selfHTML*, verwiesen. Die nachfolgenden Schlagworte ermöglichen die Suche zu weiterführenden Informationen im WWW.

Die Anfänge

Tim Berners-Lee – CERN - HTML (Hypertext Markup Language) - HTTP (Hypertext Transfer Protocol) -WWW-Browser.

Der Boom

Marc Andreessen - Browser Mosaic – Netscape - CompuServe - Internet-Provider - W3-Konsortium.

1.8 Technik

TCP/IP-Protokoll

TCP/IP - Transmission Control Protocol (Protokoll für Übertragungskontrolle), IP bedeutet Internet Protocol - IP-Adresse - Hosts oder Hostrechner - Zugangs-Provider – AOL - winsock.dll.

IP-Adressierung

Eine typische IP-Adresse sieht in Dezimalschreibweise so aus: 149.174.211.5.

Client-Server-Technologie

DNS - Domain Name Service

DNS setzen die numerischen IP-Adressen für die Endanwender in anschauliche Namensadressen um.

Top-Level-Domains stehen in einem Domain-Namen an letzter Stelle und entsprechen Landes- oder Typenkennungen:

com = Kommerziell orientierter Namensinhaber
 org = Organisation
 net = Allgemeines Netz
 edu = amerikanische Hochschulen
 gov = amerikanische Behörden
 mil = amerikanische Militäreinrichtungen

Routing und Gateways

1.9 Provider

1. Content-Provider

Der für strafbare Inhalte in Computernetzen primär Verantwortliche ist der Content-Provider (Inhaltsanbieter), also der Urheber der jeweiligen Information. Dabei kann es sich z.B. um den Ersteller einer Datenbank, den Verfasser eines Beitrags oder den Verleger handeln, der Teile seiner Zeitschriftenausgabe im Internet anbietet. Die fundamentale Umwälzung durch das Internet resultiert allerdings daraus, dass nicht nur gewerbliche Anbieter Informationen an die Öffentlichkeit tragen. Vielmehr kann jeder Privatmann durch einen Beitrag an eine Newsgroup oder durch eine eigene Web-Seite zum weltweiten Inhaltsanbieter werden. Der Teilnehmer im Internet erreicht dadurch heute - bei einem potentiellen "Leser"-Kreis von rund 40 Millionen Nutzern weltweit - ohne großen Aufwand und in gezielter Weise einen weit größeren Adressatenkreis als regionale Radio- oder Fernsehstationen.

2. Service-Provider

Als strafrechtlich (Mit-)Verantwortliche kommen darüber hinaus die Service-Provider in Betracht, die ihren Teilnehmern eine Zugangsmöglichkeit zum Internet verschaffen. Dabei spielt es grundsätzlich keine Rolle, ob es sich dabei z.B. um einen Online-Dienst, ein sonstiges Wirtschaftsunternehmen, eine Universität oder eine Schule handelt. In allen genannten Fällen verschafft der Service-Provider dem Teilnehmer die Möglichkeit, auf die Dienste des Internet zugreifen zu können. Unterschiede gibt es dabei nur in der technischen Umsetzung der Zugangsmöglichkeit zum Internet.

Im Hinblick auf die rechtliche Bewertung lassen sich dabei verschiedene Tätigkeitsbereiche des Service-Providers unterscheiden, die im folgenden differenziert werden sollen. Die Reihenfolge der Darstellung orientiert sich dabei nicht an der praktischen Bedeutung dieser Tätigkeitsbereiche für den Service-Provider. Sie bestimmt sich vielmehr - bereits mit Blick auf die nachfolgende rechtliche Analyse - nach den abnehmenden Einflussmöglichkeiten des Service-Providers auf die übertragenen Dateninhalte.

- a) Eine volle Einflussnahme auf den Inhalt der Daten nimmt der Service-Provider nur wahr, wenn er eigene Daten als Content-Provider anbietet. Dies ist lediglich in seltenen Konstellationen der Fall, z.B. wenn er eigene Informationen im WWW zur Verfügung stellt.
- b) Eine begrenzte Beeinflussung des Dateninhalts durch den Service-Provider erfolgt bei der Moderation (= Auswahl) fremder Daten. Dies ist insbesondere bei moderierten Newsgroups und Mailing Lists, die der Service-Provider selbst moderiert, sowie regelmäßig beim Betrieb eines FTP-Servers gegeben. In diesen Fällen sichtet der Service-Provider den Datenbestand und entscheidet, welche Daten er allgemein zugänglich machen will.
- c) Eine bloß formale technische Unterstützung bei der Verbreitung fremder Informationen übt der Service-Provider dagegen aus, wenn er seine Server für die Speicherung fremder Daten zur Verfügung stellt (sogenanntes "Hosting"). Diese - für die meisten Service-Provider typische - Funktionstätigkeit erfolgt insbesondere beim Betrieb eines Mail-Servers, beim Zugänglichmachen fremder Newsgroups auf dem provider-eigenen News-Server und beim Zurverfügungstellen des eigenen List-Servers für fremde Mailing Lists.
- d) In vielen Fällen dient das Zurverfügungstellen von Speicherplatz jedoch - ebenso wie die Bereitstellung von Leitungskapazitäten - nur dem technischen Transport von bereits gespeicherten Daten. Derartige Transportfunktionen erfüllen insbesondere Netzknotenrechner und Proxy-Cache-Server. Die Einflussmöglichkeiten des Service-Providers auf die Daten sind in diesen Fällen - ebenso wie bei der bloß formalen technischen Unterstützung - gering.
- e) Ein weiterer - für alle Service-Provider zentraler - Tätigkeitsbereich ist die Bereitstellung des Zugangs zum Internet und seinen Diensten. Diese Funktion beinhaltet die technische Realisierung des Internet-Zugangs. Soweit ein Teilnehmer z.B. das WWW ohne Unterstützung eines Proxy-Cache-Servers nutzt, beschränkt sich die Funktion des Service-Providers auf das bloße Zurverfügungstellen des "Gateways".

Diese Differenzierung der Tätigkeit des Service-Providers nach Funktionsgesichtspunkten bietet die Chance, die strafrechtliche Verantwortlichkeit der Beteiligten im Internet im Ein-

klang mit vergleichbaren klassischen Fallgestaltungen zu lösen. Die folgenden Ausführungen untersuchen daher zunächst Lösungsansätze und Präjudizien für ähnliche Funktionen aus dem Bereich der klassischen "Datenvermittlung".

Quelle: Sieber, JZ 1996, 429, 494

1.10 Top-Level-Domains

| Domain | Land |
|--------|------------------------------|
| .ad | Andorra |
| .ae | Vereinigte Arabische Emirate |
| .af | Afghanistan |
| .ag | Antigua |
| .ai | Anguilla |
| .al | Albanien |
| .am | Armenien |
| .an | Niederländische Antillen |
| .ao | Angola |
| .aq | Antarktis |
| .ar | Argentinien |
| .as | Amerikanisch-Samoa |
| .at | Österreich |
| .au | Australien |
| .aw | Aruba |
| .az | Aserbeidschan |
| .ba | Bosnien-Herzegowina |
| .bb | Barbados |
| .bd | Bangladesch |
| .be | Belgien |
| .bf | Burkina |
| .bg | Bulgarien |
| .bh | Bahrain |
| .bi | Burundi |
| .bj | Benin |

| | |
|-----|------------------------------|
| .bm | Bermuda |
| .bn | Brunei |
| .bo | Bolivien |
| .br | Brasilien |
| .bs | Bahamas |
| .bt | Bhutan |
| .bv | Bouvet Island |
| .bw | Botswana |
| .by | Belarus |
| .bz | Belize |
| .ca | Kanada |
| .cc | Cocos-Inseln |
| .cf | Zentralafrikanische Republik |
| .cg | Kongo |
| .ch | Schweiz |
| .ci | Elfenbeinküste |
| .ck | Cook Inseln |
| .cl | Chile |
| .cm | Kamerun |
| .cn | China |
| .co | Kolumbien |
| .cr | Costa Rica |
| .cu | Kuba |
| .cv | Kapverdische Inseln |
| .cx | Weihnachts-Inseln |
| .cy | Zypern |

| | |
|-----|------------------------------------|
| .cz | Tschechien |
| .de | Deutschland |
| .dj | Dschibuti |
| .dk | Dänemark |
| .dm | Dominica |
| .do | Dominikanische Republik |
| .dz | Algerien |
| .ec | Ecuador |
| .ee | Estland |
| .eg | Ägypten |
| .eh | West-Sahara |
| .er | Eritrea |
| .es | Spanien |
| .et | Äthiopien |
| .fi | Finnland |
| .fj | Fidschi-Inseln |
| .fk | Falkland-Inseln |
| .fm | Mikronesien |
| .fo | Färöer-Inseln |
| .fr | Frankreich |
| .fx | Frankreich, zu Frankreich gehörend |
| .ga | Gabun |
| .gb | Großbritannien |
| .gd | Grenada |
| .ge | Georgien |
| .gf | Französisch-Guyana |
| .gh | Ghana |
| .gi | Gibraltar |
| .gl | Grönland |
| .gm | Gambia |

| | |
|-----|--|
| .gn | Guinea |
| .gp | Guadeloupe |
| .gq | Äquatorial-Guinea |
| .gr | Griechenland |
| .gs | Süd-Georgien/Sandwich-Inseln |
| .gt | Guatemala |
| .gu | Guam |
| .gw | Guinea |
| .gy | Guyana |
| .hk | Hong Kong |
| .hm | Heard- /MacDonald-Inseln |
| .hn | Honduras |
| .hr | Kroatien |
| .ht | Haiti |
| .hu | Ungarn |
| .id | Indonesien |
| .ie | Irland |
| .ii | International, für den SSGFI - Gebrauch. |
| .il | Israel |
| .in | Indien |
| .io | "British Indian Ocean Territory" |
| .iq | Irak |
| .ir | Iran |
| .is | Island |
| .it | Italien |
| .jm | Jamaica |
| .jo | Jordanien |
| .jp | Japan |
| .ke | Kenia |
| .kg | Kirgisistan |

| | |
|-----|---------------------------|
| .kh | Kambodscha |
| .ki | Kiribati |
| .km | Komoren |
| .kn | St.Kitts, Nevis, Anguilla |
| .kp | Nord-Korea |
| .kr | Süd-Korea |
| .kw | Kuwait |
| .ky | Kaiman-Inseln |
| .kz | Kasachstan |
| .la | Laos |
| .lb | Libanon |
| .lc | Santa Lucia |
| .li | Liechtenstein |
| .lk | Sri Lanka |
| .lr | Liberia |
| .ls | Lesotho |
| .lt | Litauen |
| .lu | Luxemburg |
| .lv | Lettland |
| .ly | Lybien |
| .ma | Marokko |
| .mc | Monaco |
| .md | Moldawien |
| .mg | Madagaskar |
| .mh | Marshall-Inseln |
| .mk | Mazedonien |
| .ml | Mali |
| .mm | Myanmar |
| .mn | Mongolei |
| .mo | Macao |
| .mp | Marianen-Inseln |

| | |
|-----|------------------------|
| .mq | Martinique |
| .mr | Mauretanien |
| .ms | Montserrat |
| .mt | Malta |
| .mu | Mauritius |
| .mv | Malediven |
| .mw | Malawi |
| .mx | Mexiko |
| .my | Malaysia |
| .mz | Mozambique |
| .na | Namibia |
| .nc | Neu-Kaledonien |
| .ne | Niger |
| .nf | Norfolk Islands |
| .ng | Nigeria |
| .ni | Nicaragua |
| .nl | Niederlande |
| .no | Norwegen |
| .np | Nepal |
| .nr | Nauru |
| .nu | Niue |
| .nz | Neuseeland |
| .om | Oman |
| .pa | Panama |
| .pe | Peru |
| .pf | Französisch Polynesien |
| .pg | Papua-Neuguinea |
| .ph | Philippinen |
| .pk | Pakistan |
| .pl | Polen |
| .pm | St.Pierre, Miquelon |

| | |
|-----|---|
| .pn | Pitcairn |
| .pr | Puerto Rico |
| .ps | Palästina (In Vorbereitung, Stand: 10/1999) |
| .pt | Portugal |
| .pw | Palau |
| .py | Paraguay |
| .qa | Katar |
| .re | Reunion |
| .ro | Rumänien |
| .ru | Russland |
| .rw | Ruanda |
| .sa | Saudi-Arabien |
| .sb | Solomon-Inseln |
| .sc | Seychellen |
| .sd | Sudan |
| .se | Schweden |
| .sg | Singapur |
| .sh | St. Helena |
| .si | Slowenien |
| .sj | Svalbard und die Jan Mayen Inseln |
| .sk | Slowakien |
| .sl | Sierra Leone |
| .sm | San Marino |
| .sn | Senegal |
| .so | Somalia |
| .sr | Surinam |
| .st | St. Tome, Principe |
| .su | Sowjetunion |
| .sv | El Salvador |

| | |
|-----|-----------------------------|
| .sy | Syrien |
| .sz | Swaziland |
| .tc | Turks- und Caicos-Inseln |
| .td | Tschad |
| .tf | French Southern Territories |
| .tg | Togo |
| .th | Thailand |
| .tj | Tadschikistan |
| .tk | Tokelau |
| .tm | Turkmenistan |
| .tn | Tunesien |
| .to | Tonga |
| .tp | Ost-Timor |
| .tr | Türkei |
| .tt | Trinidad und Tobago |
| .tv | Tuvalu |
| .tw | Taiwan |
| .tz | Tansania |
| .ua | Ukraine |
| .ug | Uganda |
| .uk | United Kingdom |
| .um | US Minor Outlying Islands |
| .us | Vereinigte Staaten |
| .uy | Uruguay |
| .uz | Usbekistan |
| .va | Vatikan |
| .vc | St. Vincent und Grenadine |
| .ve | Venezuela |
| .vg | Virgin-Islands (Britisch) |
| .vi | Virgin-Islands (US) |
| .vn | Vietnam |

| | |
|-----|--------------------------|
| .vu | Vanuatu |
| .wf | Wallis und Futuna-Inseln |
| .wg | Westjordanland |
| .ws | Samoa |
| .ye | Jemen |
| .yt | Mayotte |
| .yu | Jugoslawien |
| .za | Südafrika |
| .zm | Sambia |
| .zr | Zaire |
| .zw | Zimbabwe |

2. Fallbeispiele¹


BKA, Bericht zur IuK-Kriminalität (Kriminalität in Verbindung mit der Informations- und Kommunikationstechnologie), IuK-Mitteilungsblatt 2/00, August 2000

Bischoff, Dirty Tricks im Internet, PC-Welt 10/2000, 58



2.1 Raubkopien: "warez" und "appz"

Z ist eines der Kennzeichen der "Hackerszene" u.a. für raubkopierte Software. Man

findet sie überall, denn:  hilft suchen: in weniger als 1 Minute findet Google (oder jede andere Suchmaschine) mehr als 10.000 Internetseiten mit Raubkopien und Seriennummern oder Linkseiten, die ihrerseits auf entsprechende Seiten verweisen.

"Bekannt" aus der Tagespresse ist auch "Cosmo Conner"

2.1.1 Identfälschung

Marktgängige Software wird von oftmals unbekanntem Tätern im Ausland, möglicherweise unter Benutzung der Fertigungsstätten des Originalherstellers ("Überproduk-

¹ Der Vortrag beschränkt sich auf Taten mit wirtschaftlichem Einschlag.

tion"), so kopiert, dass für den unerfahrenen Käufer ein Unterschied zum Original erkennbar ist. Der Käufer erhält mit dem Original verwechselbare Datenträger und Handbücher, die das Logo usw. des Originalherstellers tragen.

2.1.2 "Selbstgebranntes"

Mit "selbstgebrannten" CD-R wird nicht nur von Jugendlichen ein schwunghafter Handel oder Tausch auf dem Schulhof getrieben. Auch der semiprofessionelle Handel mit raubkopierter Software reißt nicht ab. Motive sind u.a. der Wunsch, Geld zu sparen, dieses oder jenes Programm auch noch zu besitzen oder es dem großen Hersteller zu "zeigen".

2.1.3 Online-Vertrieb I

A unterhält auf einem der zahlreichen Webspaces-Anbieter im Ausland eine Homepage, auf der er Interessenten gegen eine Unkostenerstattung von DM 30,00 und DM 10,00 Porto anbietet, eine CD-R mit Software zu brennen. Die Software wird aus einer Liste ausgesucht, wobei die Zusammenstellung nur durch den Speicherplatz der CD-R (650 MB) begrenzt ist. Daneben bietet er 1:1-Kopien von Software-CD's an. Selbstverständlich liefert er die notwendigen Seriennummern oder Aktivierungsschlüssel mit.

Die Korrespondenz wickelt A über einen Account bei Hotmail / USA (Tochter von Microsoft) an. Die CD-R versendet er über die Deutsche Post, nachdem der Käufer seinen Obulus in bar an ein Postlagerfach entrichtet hat.

Nach Sicherstellung seines PC werden bei der Auswertung des Programmes Outlook-Express ca. 400 Emails aufgefunden, die zur Identifizierung von ca. 200 Abnehmern führen.

2.1.4 Online-Vertrieb II

B unterhält auf einem der zahlreichen Webspaces-Anbieter im Ausland eine Homepage, auf der er Interessenten anbietet, Software "herunterzuladen". Hierzu hat er die Software installationsfähig auf Rechner verschiedener Webspaces-Anbieter hochgeladen. Die Software kann aus Listen ausgesucht werden.

B hat zu seinen "Kunden" keinen Kontakt. Weder Geld noch CD-R werden verschickt. Vielmehr finanziert er sich durch Werbebanner auf den Webseiten. Abhängig von der Zahl der "Clicks" erhält er eine Vergütung.

Auffällig wird B, weil er Internetzugangsdaten unbefugt nutzt. Durch die Auswertung des PC - und sein Geständnis - wird der Online-Softwarevertrieb bekannt.

Nebenbei beschäftigt er sich auch mit der Freischaltung von Pay-TV-Karten - für den Heimgebrauch.

2.2 Erpressung, Nötigung

C hat für U ein Programm zur Abwicklung von Kundenbestellungen erstellt, das U in seinem Betrieb verwendet. Kundendaten werden in verschiedenen Dateien gespeichert. C nimmt auftragsgemäß Änderungen am Programm vor, teilweise sind "Bugs" zu beseitigen. U zahlt eine Rechnung von DM 2.400,00 nicht, worüber C verärgert ist. U meint, die Programmierarbeiten seien fehlerhaft; C ist der Auffassung, seine Arbeit sei in Ordnung, es handele sich vielmehr um Bedienerfehler.

C lässt U eine Diskette zukommen, die als Update bezeichnet ist. In der Anleitung wird die Installation beschrieben, die U ausführt. Danach ist das Programm nicht mehr lauffähig, die Kundendaten sind "weg".

U wendet sich daraufhin an C, der mitteilt, dass er erst nach Zahlung der Rechnung das Programm (wieder) lauffähig machen werde.

2.3 Computerbetrug

Computerbetrug ist ein Tatbestand, der in vielen Fallkonstellationen Anwendung findet.

In Presseberichten wird teilweise über astronomische Schadenssummen berichtet.

2.3.1 Zahlungsverkehr

ST 17.3.2001

COMPUTERBETRUG / Zwei Jahre Haft auf Bewährung

Millionen umgebucht

Schwindel am Heimcomputer: Ein Reutlinger Gastwirt konnte Millionen auf sein Konto buchen, bevor die Banken misstrauisch wurden.

MATTHIAS REICHERT

REUTLINGEN ■ „Bis zum Geht-nicht-mehr“ habe er den Geldsegen ausreizen wollen, sagte ein Reutlinger Gastwirt vor Gericht. Der 52-Jährige hatte im vergangenen Oktober mit Tele-Cash-Gerät und Kundenkarte innerhalb von vier Tagen 376 Millionen Mark vom Privat- aufs Geschäftskonto umgebucht. 8,2 Millionen überwies die Bank tatsächlich.

Das Reutlinger Amtsgericht verurteilte den Mann gestern wegen Computerbetrugs zu zwei Jahren Haft auf Bewährung und 200 Stunden gemeinnütziger Arbeit. „Aus einer Schnapsidee wurde eine bierernste

Sache“, begründete Richter Eberhard Hausch das Urteil.

An einem Oktoberabend holte der Gastwirt auf Anhieb 8,2 Millionen Mark aufs Geschäftskonto – von einem Privatkonto mit nur wenigen hundert Mark Guthaben. Er sei im Internet auf eine seltene Briefmarke gestoßen und so zum Geld gekommen, sagte er der Bank. In den nächsten Tagen startete er fast 600 weitere Buchungen. Beim Eintippen halfen zeitweise zwei Kellnerinnen. Verfahren wegen Beihilfe gegen die beiden wurden eingestellt.

Irgendwann wurden die Banken misstrauisch und überwiesen keine müde Mark mehr. Auch die 8,2 Millionen wurden sichergestellt. Der 52-Jährige machte eine Alkohol-Entziehungskur. Der Schwindel kostete den Mann sein gesamtes Vermögen. Allein für entgangene Zinsen durch die Buchungen stellten ihm die Banken 5000 Mark in Rechnung.

Schwäbisches Tagblatt 17.3.2001

Kaiserpassage 13

Kurzzeit-Millionär

Wie er es genau hingekriegt hat, weiß er wohl selbst nicht. Ein Reutlinger Wirt entdeckte – angeblich aus einer Schnapslaune – das Geheimnis, aus nichts Geld zu zaubern. Seine Reutlinger Geschäftsbank hatte ihn leichtsinnigerweise mit einem Tele-Cash-Gerät ausgestattet, von einem anderen Geldinstitut war er mit einer Kundenkarte fürs Privatkonto ausgestattet. Simsalabim, vergangenen Oktober buchte er mit diesen spärlichen Utensilien über 376 Millionen Mark vom Geschäftsaufs Privatkonto. Insgesamt 600 Mal betätigte er die Wundermaschine, alles in vier Tagen.

Gleich beim ersten Versuch in einer nebligen Oktobernacht wanderten 8,2 Millionen von einem Konto aufs andere. „Kaum zu glauben, dass sich das Zentrum der Finanzwelt in dieser Wirtschaft befand“, staunte Staatsanwalt Guido Zöllner vor dem Reutlinger Amtsgericht, wo sich der 52-Jährige diese Woche wegen Computerbetrugs verantworten musste. Zum Glück entdeckte die Bank rechtzeitig, dass nicht alles mit rechten Dingen zugeht – Schaden richtete der Zahlenjongleur keinen an. Bevor er das Geld ausgeben konnte, wanderte er in eine Alkohol-Entziehungskur.

Mehr als die 8,2 Millionen bekam er nicht aufs Konto, so oft er es auch versuchte. „Ausreizen bis zum Geht-nicht-mehr“ habe er

den Geldsegen wollen, sagte er vor Gericht. Der Staatsanwalt hatte die ungeheuerlichen Geldbewegungen detailliert aufgelistet. Einmal verbuchte der trickreiche Wirt in wenigen Stunden mit 360 Überweisungen satte 260 Millionen Mark. Doch das Geld blieb diesmal bei der Bank, der Betrag belastete nur sein Sündenkonto. Teilweise ließ er auch seine Kellnerinnen die vielen Zahlen eintippen, jetzt waren die Aushilfen wegen Beihilfe angeklagt. „Ich habe nicht eine Minute gedacht, dass das strafbar ist“, sagte die eine. „Ich dachte, dass die Karte nicht funktioniert“, beteuerte die andere. Die Verfahren gegen sie wurden eingestellt. Dass ihnen der Wirt den Lohn schuldig blieb, sei Strafe genug.

Der Wirt erzählte den Frauen die gleiche Geschichte wie der Geschäftsbank, die sich über den Geldregen wunderte: Er sei durch eine seltene Briefmarke aus dem Internet reich geworden. Den Kneipen-Job hat der Mann mittlerweile an den Nagel gehängt, sein spärliches Vermögen ist futsch – unter anderem buchten ihm die Banken 5000 Mark Zinsen ab.

Richter Eberhard Hausch verurteilte ihn, wie vom Staatsanwalt beantragt, zu zwei Jahren Haft auf Bewährung. Als Auflage muss der 52-Jährige 200 Stunden gemeinnützige Arbeit leisten. „Aus einer Schnapsidee wurde eine bierernste Sache“, sagte Hausch und warnte vor Nachahmung. Richterlicher Rat, falls es doch jemand in den Fingern juckt: Gleich der Presse stecken, wo solche Un-Summen fließen. Wir sagen's auch bestimmt nicht weiter! Matthias Reichert

2.3.2 Kreditkarten

INTERNETBETRUG / Zum Schluss übertrieben *St 12/01*

Da staunt die Polizei

Gefahr Internet: Ein Amerikaner hat sich über das Internet Daten über die Identität von reichen Landsleuten besorgt und auf deren Kosten Teures eingekauft.

PETER DE THIER

WASHINGTON ■ Sechs Monate lang hat der 31-jährige Abraham Abdallah an Computern in einer öffentlichen Bibliothek und mit Internet-fähigen Handys Informationen über die Reichsten im Lande gesammelt. Völlig ungeniert belastete er Kreditkarten von Hollywood-Größen wie Regisseur Stephen Spielberg und anderen Super-Reichen wie dem Medienzar Ted Turner.

Es schwingt geradezu ein wenig Bewunderung mit, wenn Polizeichef William Alee von dem „ambitio-

niertesten Internet-Betrug, den ich jemals erlebt habe" spricht. Von insgesamt 217 Spitzenbossen hatte sich der inzwischen festgenommene frühere Kellner die Sozialversicherungsnummern, Privatadressen und Kreditkartennummern ergaunert.

Mit seinem letzten Coup schlug der findige Betrüger dann allerdings über die Stränge. 21 Millionen Mark wollte er vom Konto des Software-Unternehmers Thomas Siebel abheben. Da der Betrag aber nicht gedeckt war, erkundigte sich die Bank beim Unternehmer. Der fiel aus allen Wolken, und bald führte die Spur zum Auftraggeber.

Es kann lange dauern, bis der endgültige Schaden, den Abdallah anrichtete, feststehen wird. Ironie: Der Festgenommene jobbte früher als Sicherheitsexperte, der in Videofilmen vor Internet-Kriminalität warnte und Tipps gab.

2.3.3 Computerbetrug: "realz" und "fakez"

U wählte sich von zuhause unter Nutzung seines Telefonanschlusses (Calling-ID) bei der Fa. X ein, wobei er bewußt die anderweitig - im Internet - erlangten Zugangsdaten des A ("realz") sowie die von ihm als einer fiktiven Person zugeordneten Zugangsdaten ("fakez") benutzte, um so - letztlich nur vorläufig - die Telekommunikationsgebühren zu sparen.

ST

Dienstag, 16. Januar 2001

COMPUTER**Hacker greifen
Privatleute an**

SCHWEINFURT ■ Auf Kosten anderer Internet-Kunden haben sich sechs junge Männer im Alter von 17 bis 21 Jahren Zugang ins Internet verschafft. Die betroffenen Anschluss-Inhaber waren wegen immens hoher Telefonrechnungen auf den Missbrauch ihrer Passwörter aufmerksam geworden. Insgesamt sei dadurch rund 45 Betroffenen ein Schaden von zusammen 5500 Mark entstanden, berichtet die Polizei.

Doch der Fall hat einen größeren Hintergrund, denn die Zugangsdaten hatten sich die sechs Surfer einfach im Internet beschafft. Laut Polizei hatten unbekannte Hacker diese Daten auf den Festplatten fremder Internet-Nutzer ausspioniert und dann auf einer Internetseite veröffentlicht. Angaben zu dieser bundesweit angelegten Hacker-Aktion, bei der ein Gesamtschaden von einer Million Mark entstanden sei, lehnte die Polizei aus ermittlungstaktischen Gründen bislang noch ab.

Die sechs Surfer, die inzwischen ein Geständnis abgelegt haben, erklärten beim Verhör, sie hätten den „günstigen Internet-Zugang“ vor allem für das Herunterladen von Computerspielen genutzt. Dazu sei die illegale Internet-Verbindung oft tagelang aufgebaut gewesen. Die Polizei fand bei den sechs Männern etwa 300 selbstgebrannte CD-Roms. dpa

INFO

Auf den **Computerbetrug** der sechs Festgenommenen stehen bis zu fünf Jahre Haft.

2.3.4 Pay-TV

| | | |
|---|--------------------------|---|
| | Samstag, 26. August 2000 | 7 |
| <h2>Pay-TV-Betrüger kommt vor Gericht</h2> | | |
| <p>MANNHEIM (lsw). Die Mannheimer Staatsanwaltschaft hat die erste Anklage gegen einen von etwa 60 Verdächtigen erhoben, die den Pay-TV-Sender „Premiere“ um Millionen geprellt haben sollen. Dem 23 Jahre alten Mann werde gewerbsmäßige Banden-Hehlerei in mindestens 80 Fällen vorgeworfen, teilte die Staatsanwaltschaft mit. Bei der groß angelegten Betrugsaktion soll er systematisch Mittäter angeworben haben, die für ihn Pay-TV-Decoder anmieteten, aber die Miete nicht zahlten. Die Decoder verkaufte der 23-Jährige dann weiter. Seine Staatsangehörigkeit sei unklar, hieß es bei der Staatsanwaltschaft.</p> <p>Abnehmer soll unter anderem ein 41 Jahre alter indischer Ladeninhaber aus Mannheim gewesen sein, der die Decoder an seine ahnungslosen Kundschaft verscherbelte. Der in Sachen High Tech offenbar begabte Inder fälschte oder manipulierte auch so genannte Smartcards, die zusammen mit den Decodern den Empfang von Pay-TV-Programmen ermöglichen. So konnte seine dankbare Kundschaft sogar ausländische Programme empfangen, die normalerweise nicht im Angebot deutscher Pay-TV-Sender sind.</p> <p>Insgesamt sollen bei dem Fall rund 1000 Decoder auf betrügerische Art und Weise angemietet worden sein. Einige der 60 mutmaßlichen Beteiligten seien untergetaucht, sagte Oberstaatsanwalt Wolfgang Kneip. Neben dem jetzt angeklagten 23-Jährigen saßen noch drei weitere Verdächtige in Untersuchungshaft.</p> | | |

2.4 Computersabotage

S "hostet" als großes Telekommunikationsunternehmen die Internetauftritte bekannter Unternehmen, so auch des in Frankreich ansässigen Parfum- und Modehersteller C. C bemerkt, dass Unbekannte die Webseiten mit Texten und Bildern gegen Tierversuche versehen haben.

Die Anzeige gegen Unbekannt zieht S zurück, nachdem C keine "Publicity" in diesem Zusammenhang wünscht.

2.5 Hacker: Portscan

... erst einmal möchte ich um Entschuldigung für den Zugriffsversuch auf Ihr System bitten, obgleich dieser nicht direkt aus unserem Hause erfolgt ist. Der Rechner, der in Ihrem Logfile angezeigt wurde ist ein Server, an dem jedoch zu diesem Zeitpunkt niemand eingeloggt war. Da wir jedoch zeitgleich unsere Firewall zwecks Neukonfiguration zeitweise geöffnet hatten und ansonsten keine User im Hause aktiv waren, sind wir höchstwahrscheinlich selbst Ziel eines Angriffs geworden, bei dem versucht wurde über unsere Server auf Ihr Netzwerk einen getarnten Zugriff zu erhalten.

Bitte informieren Sie mich umgehend, wenn dieses nochmals vorkommen sollte. In diesem Falle werden wir zudem testen, ob IP Pakete fehlgeleitet werden (Wir haben gerade ein neues IP Adress-Range für unsere Firewall erhalten) oder ein IP Spoofing irgendwo im Internet aktiv ist um sicherzustellen, dass derartige Vorfälle sich nicht wiederholen. Um weitere vorbeugende Maßnahmen auf unserer Seite zu ergreifen und den wahren Verursacher ausfindig zu machen wäre es sehr hilfreich zu wissen welcher Art der Zugriffsversuch war und auf welche IP oder Computernamen er erfolgt ist.

2.5.1 Programme für Hacker

Verschiedene Literatur und Software aus dem Internet, z.B.:

Superscan 2.06:

Das Utility ergänzt Windows um einen TCP/IP-Portscanner, der Port-Scans anhand verschiedener Vorgaben durchführt. Zum einen sucht SuperScan einen vorgegebenen Adressbereich ab, nachdem die Anfangs- und End-IP-Adresse angegeben wurde. Außerdem kann das Programm mit Hilfe einer Steuerdatei bestimmte IP-Adressen überprüfen. Dabei protokolliert SuperScan die Reaktion der Gegenstelle im Klartext. Mit einem Mausklick stellt das Tool eine Verbindung zu gewünschter Adresse her. Mit eingebaut ist ein Pinger und Hostname-Resolver. (Freeware, keine Registrierungsgebühr).

Datenschutz-CD: Im Buchhandel erhältlich!

2.5.2 Programme gegen Hacker

Virenschutzprogramme, Firewalls, z.B.

The Cleaner 3.1:

The Cleaner spürt Trojanische Pferde in Ihrem System auf und eliminiert diese, bevor Sie Unheil anrichten können. Dem Programm liegt eine umfangreiche Datenbank zugrunde, die alle bekannten Trojaner mit ihren Angriffszielen und -methoden enthält.

Um immer auf dem neuesten Stand und damit auch vor gerade erschienen Angreifern gefeit zu sein, lässt sich The Cleaner über eine Internet-Verbindung aktualisieren. Da sich der Hersteller voll und ganz der Bekämpfung der Trojaner verschrieben hat, geht die Treffsicherheit beim Auffinden über die Quote der Virenscanner hinaus. Zu den Stärken des Programms zählt das Erkennen der gefährlichsten Trojaner BackOrifice, NetBus, Masters Paradise, ICQ-Killer, Girlfriend, Mirc Script und viele andere mehr. Sie können das System einmalig untersuchen und so konfigurieren, dass es Ihren Rechner dauerhaft im Auge behält. (Shareware 20 Dollar Registrierungsgebühr) .

2.6 Virus, Trojaner

U versendet mit Email Anhänge, die als "schädliche Software" auf dem Empfängersystem Daten löschen oder verändern soll.

Um ein Computerspiel im Rahmen eines privaten Netzwerks spielen zu können, schließen Computerfreunde ihre PC zusammen. X spielt dem Y erforderliche Programme sowie "Back Orifice" auf. Während des Spieles benutzt X die Möglichkeiten von "BO", um ein bisschen auf dem PC des Y herumzustöbern. Nach Beendigung des Spieles teilt X dem Y mit, dass auf dem PC "BO" installiert sei. Y kann mit diesem Hinweis nichts anfangen.

Einige Zeit später bekommt Y hohe Rechnungen seines Internetproviders. Im Rahmen der Ermittlungen wird bekannt, dass durch "BO" von unbekanntem Tätern die Passwörter des Y ausgespäht und im Internet auf entsprechenden Seiten veröffentlicht wurden.

Literatur:

Frhr. von **Gravenreuth**, Computerviren, 2. Aufl. 1998

2.7 Spamming

Unbekannte Täter stehen im Verdacht, den Mailserver der Anzeigerstatterin, der sich in den Räumen des Netzwerkbetriebsunternehmens, in der Weise manipuliert zu haben, dass im wesentlichen unbemerkt Emails von Unbekannten über den Mailserver der Anzeigerstatterin versandt werden. Nach den bisherigen Ermittlungen hat sich der Verdacht, es seien hierbei Daten der Anzeigerstatterin ausgespäht oder Geschäftsgeheimnisse entwendet worden, nicht bestätigt. Ebenso hat sich der Verdacht, der Anzeigerstatterin solle durch den Mailverkehr ein sonstiger Schaden (z.B. durch beleidigende Emails an Dritte o.ä.) zugefügt werden, nicht verfestigt.

Vielmehr ist der Anzeigerstatterin durch den Mailversand („Spamming“) ein Schaden in der Weise zugefügt worden, dass sie für den erhöhten „Traffic“, d.h. den Datentransport

über die von ihr zu bezahlenden Leitungen, einen bislang nicht messbaren Schaden erlitten hat.

2.7.1 Anonymisierer

Neben web-basierten Anonymisierern gibt es auch verschiedene Programme zum Verschleiern der Identität im Internet, z.B.:

Secretmaker:

frage 4: für wen ist secretmaker entwickelt worden?

für jeden benutzer der über einen internetanschluss verfügt und sich im web geschützt bewegen möchte.

frage 6: wie kann man feststellen, dass secretmaker die anonymität schützt?

klicken sie das secretmaker icon in der taskbar doppelt an und danach den "stop" button. nun sind sie mit ihren eindeutigen benutzerdaten identifizierbar und können profiliert werden.

für anwender, die mit windows 95,98 oder ME arbeiten:

drücken sie den windows "start" button und den "ausführen" button, und geben sie dann "command" ein. anschliessend geben sie auf dem DOS-prompt "winipcfg" ein und drücken "enter". danach sehen sie das fenster welches ihre IP-adresse angibt: z.b. 193.216.23.48. geben sie nun in dieses fenster das kommando "nbtstat -A 193.216.23.48" ein und drücken enter. sie sehen jetzt die information ihres persönlichen benutzer accounts und ihrer einmaligen mac adresse, welche es erlaubt sie im internet eindeutig zu identifizieren. alle ihre bewegungen im web können ihnen zugeordnet werden.

für alle anwender:

um secretmaker wieder zu aktivieren drücken sie den "start/stop" button, es erscheint dann das label "stop". geben sie jetzt mehrere male nacheinander den befehl "nbtstat -A 193.216.23.48" ein, um das funktionieren der software zu prüfen. bei jeder befehlseingabe werden sie neue phantomdaten erhalten. keine dieser phantomdaten entspricht aber ihren wahren benutzerdaten, sie können sich frei und unerkannt im internet bewegen.

2.7.2 TU Dresden: JAP - JAVA ANON PROXY

Mit dem **Java Anon Proxy (JAP)** ist es möglich, Webseiten unbeobachtbar aufzurufen. Das bedeutet, daß weder der angefragte Server noch ein Lauscher auf den Verbindungen mitbekommt, welcher Benutzer welche Webseite aufgerufen hat.

Funktion

Diese Funktion wird dadurch erreicht, daß die Kommunikationsverbindung nicht direkt an den Webserver geschickt wird, sondern über eine sogenannte Mix Proxy Kaskade geschickt wird.

Da viele Benutzer gleichzeitig den Anonymitätsdienst nutzen, werden die Internetverbindungen jedes Benutzers unter denen aller anderer Benutzer versteckt: Jeder Benutzer könnte der Urheber einer Verbindung gewesen sein. Niemand, kein Außenstehender, kein anderer Benutzer, nicht einmal der Betreiber des Anonymitätsdienstes kann herausbekommen, welche Verbindungen ein bestimmter Benutzer hat.

Im Regelfall werden in einer Kaskade mindestens drei Mix Proxies arbeiten, die von unabhängigen Institutionen betrieben werden und die in einer Selbstverpflichtung erklären, daß sie weder Log-Files über die transportierten Verbindungen speichern, noch

mit den anderen Mix Proxy Betreibern Daten austauschen, die dazu führen könnten, daß ein Benutzer von JAP enttarnt wird.

Mit dem Java Anon Proxy (JAP) ist es möglich, Webseiten unbeobachtbar aufzurufen. Das bedeutet, daß weder der angefragte Server noch ein Lauscher auf den Verbindungen mitbekommt, welcher Benutzer welche Webseite aufgerufen hat.

Im Regelfall werden in einer Kaskade mindestens drei Mix Proxies arbeiten, die von unabhängigen Institutionen betrieben werden und die in einer Selbstverpflichtung erklären, daß sie weder Log-Files über die transportierten Verbindungen speichern, noch mit den anderen Mix Proxy Betreibern Daten austauschen, die dazu führen könnten, daß ein Benutzer von JAP enttarnt wird.

Ist die Rück- bzw. Strafverfolgung einer durch JAP anonymisierten Verbindung möglich, wenn ein entsprechender Gerichtsbeschuß vorliegt?

Der Gesetzgeber zwingt einen Anbieter von TK-Dienstleistungen dazu, Daten, die er sowieso speichert, für die Strafverfolgung herauszugeben. Der Gesetzgeber zwingt aber niemanden dazu, Daten zu speichern, die für den Betrieb nicht erhoben oder verarbeitet werden müssen.

Eine Offline-Überwachung ist nahezu unmöglich: Wenn ein sogenannter Bedarfsträger die nachträgliche Aufdeckung einer Verbindung wünscht, muß er alle eingehenden und ausgehenden Nachrichten aller Mixe aufzeichnen und dem jeweiligen Mix zur Deanononymisierung vorlegen. Dies hätte allerdings nur Sinn, solange der öffentliche Schlüssel des Mix noch gültig ist. Nach einem Schlüsselwechsel kann selbst der Mix die alten Nachrichten nicht mehr entschlüsseln, da der private Schlüssel vernichtet wird. Im derzeitigen Zustand ist das allerdings noch nicht implementiert. Wie oft der öffentliche Schlüssel gewechselt wird, hängt vom Mix-Bereiber ab. Im Endausbau des Systems kann dies alle paar Stunden geschehen.

Eine Online-Überwachung, d.h. der Bedarfsträger wünscht die sofortige Deanononymisierung einer Verbindung, setzt voraus, daß per Gerichtsbeschuß jeder Mix dazu gezwungen wird, die Deanononymisierung einer bestimmten Nachricht sofort vorzunehmen. Hierzu muß der zunächst der erste Mix die Ein-Ausgabe-Zuordnung des betreffenden Kanals mitloggen und dem zweiten Mix mitteilen, welche Eingabenachricht vom zweiten Mix aufgedeckt werden soll u.s.w., ähnlich der "Fangschaltung" in der analogen Telefonie. Das Loggen der Ein-Ausgabezuordnungen aller Kanäle aller Mixe dürfte dem Datenschutz widersprechen, da es einer Massenüberwachung gleich kommt.

Kann der Anonymisierungsdienst nicht zum staatlichen Kontrolldienst werden?

Im Gegensatz zu einfachen anonymisierenden Proxies, die nicht gegen den Betreiber des Proxys schützen, sind bei JAP nicht einmal die Betreiber eines Mix in der Lage, Benutzer zu beobachten. Insofern wird jegliche Überwachung der Internetnutzer, also auch die staatliche, durch JAP nicht einfacher, sondern erheblich schwerer.

Mißtrauen ist vor allem bei den sehr einfach zu benutzenden ("ohne Installation von Software") web-basierten anonymisierenden Proxies angesagt, wenn es sich um einen ihnen unbekanntem Betreiber handelt. Er kann schließlich alle Ihre Zugriffe überwachen!

Quelle:

Technische Universität Dresden, Institut Systemarchitektur, Dr. Hannes Federrath, D-01062 Dresden, E-Mail: jap@inf.tu-dresden.de, WWW: <http://anon.inf.tu-dresden.de>

„JAP ist eine Entwicklung im Projekt Anonymität im Internet, das von der Deutschen Forschungsgemeinschaft und vom Bundesministerium für Wirtschaft und Technologie (BmWi) gefördert wird. Das Projekt arbeitet eng mit dem Unabhängigen Landeszentrum für den Datenschutz Schleswig-Holstein zusammen. Mehr über den Datenschutz erfahren Sie auch im Virtuellen Datenschutzbüro.“

2.8 Markenrechtsverstöße

Bei der Identfälschung von Software wird – um den Eindruck der Echtheit zu erzeugen – das Logo (Markenzeichen) des Herstellers benutzt.

Bei der Registrierung von Domains werden Markennamen (vgl. den aktuellen zivilrechtlichen Streitfall „Explorer“) benutzt.

Bei der Bekanntmachung von Webseiten oder zur Beeinflussung von sog. Suchmaschinen werden Markenzeichen offen oder versteckt (Meta-Tags) benutzt.

2.9 Entsperrten von Handy´s

A erwirbt palettenweise preisgünstige Handy´s mit sog. Prepaidkarten, die nach den vertraglichen Vereinbarungen aller Anbieter nur mit dem jeweils zugehörigen Handy gehören (SIM-Lock). Die Prepaid-Karten "vertelefontiert" A mit von ihm eingerichteten 0190-Nummern, wodurch ihm ein (hälftiger) Anteil der Gebühren zufließt. Die Handy´s übergibt er B, der sie für eine sog. Servicegebühr "entsperrt", so dass die Handy´s nun mit allen Kartenarten funktionieren und zum entsprechenden Preis im In- oder Ausland veräußert werden. Zum Entsperrten benutzt B Hacker-Software, die er aus dem Internet bezieht, sowie Programmierungs-Software für Mobiltelefone, die aus der Produktionsstätte entwendet worden war.

2.10 sonstige Tathandlungen

- Mißbräuchliche Verwendung von EC-Karten mit PIN an Geldausgabeautomaten
- Benutzung von Telefonkartensimulatoren
- Wiederaufladung von Original-Telefonkarten
- 0190-Dialer

3. Strafnormen

Gesetzessammlung Online-Recht: <http://www.netlaw.de/gesetze/index.html>

3.1 StGB

3.1.1 § 73 Voraussetzungen des Verfalls

(1) Ist eine rechtswidrige Tat begangen worden und hat der Täter oder Teilnehmer für die Tat oder aus ihr etwas erlangt, so ordnet das Gericht dessen Verfall an. **Dies gilt nicht, soweit dem Verletzten aus der Tat ein Anspruch erwachsen ist, dessen Erfüllung dem Täter oder Teilnehmer den Wert des aus der Tat Erlangten entziehen würde.**

3.1.2 § 202a 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.

3.1.3 § 261 Geldwäsche; Verschleierung unrechtmäßig erlangter Vermögenswerte

(1) Wer einen Gegenstand, der aus einer in Satz 2 genannten rechtswidrigen Tat herrührt, verbirgt, dessen Herkunft verschleiert oder die Ermittlung der Herkunft, das Auffinden, den Verfall, die Einziehung oder die Sicherstellung eines solchen Gegenstandes vereitelt oder gefährdet, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft. Rechtswidrige Taten im Sinne des Satzes 1 sind

1. ...

2. ...

3. ...

4. Vergehen

a) nach den §§ ... 259, 263 bis 264, 266, 267, 269, ...b) ...

die gewerbsmäßig oder von einem Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, begangen worden sind, und

5. ...

In den Fällen des Satzes 2 Nr. 3 gilt Satz 1 auch für einen Gegenstand, hinsichtlich dessen Abgaben hinterzogen worden sind.

(2) Ebenso wird bestraft, wer einen in Absatz 1 bezeichneten Gegenstand

1. sich oder einem Dritten verschafft oder

2. verwahrt oder für sich oder einen Dritten verwendet, wenn er die Herkunft des Gegenstandes zu dem Zeitpunkt gekannt hat, zu dem er ihn erlangt hat.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung einer Geldwäsche verbunden hat.

(5) Wer in den Fällen des Absatzes 1 oder 2 leichtfertig nicht erkennt, daß der Gegenstand aus einer in Absatz 1 genannten rechtswidrigen Tat herrührt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(6) Die Tat ist nicht nach Absatz 2 strafbar, wenn zuvor ein Dritter den Gegenstand erlangt hat, ohne hierdurch eine Straftat zu begehen.

(7) Gegenstände, auf die sich die Straftat bezieht, können eingezogen werden. § 74a ist anzuwenden. Die §§ 43a, 73d sind anzuwenden, wenn der Täter als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung einer Geldwäsche verbunden hat. § 73d ist auch dann anzuwenden, wenn der Täter gewerbsmäßig handelt.

(8) Den in den Absätzen 1, 2 und 5 bezeichneten Gegenständen stehen solche gleich, die aus einer im Ausland begangenen Tat der in Absatz 1 bezeichneten Art herrühren, wenn die Tat auch am Tatort mit Strafe bedroht ist.

(9) Nach den Absätzen 1 bis 5 wird nicht bestraft, wer

1. die Tat freiwillig bei der zuständigen Behörde anzeigt oder freiwillig eine solche Anzeige veranlaßt, wenn nicht die Tat in diesem Zeitpunkt ganz oder zum Teil bereits entdeckt war und der Täter dies wußte oder bei verständiger Würdigung der Sachlage damit rechnen mußte, und

2. in den Fällen des Absatzes 1 oder 2 unter den in Nummer 1 genannten Voraussetzungen die Sicherstellung des Gegenstandes bewirkt, auf den sich die Straftat bezieht.

Nach den Absätzen 1 bis 5 wird außerdem nicht bestraft, wer wegen Beteiligung an der Vortat strafbar ist.

(10) ...

3.1.4 § 263a 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.

3.1.5 § 265a Erschleichen von Leistungen

(1) Wer die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Telekommunikationsnetzes, die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht erschleicht, das Entgelt nicht zu entrichten, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

(2) Der Versuch ist strafbar.

(3) Die §§ 247 und 248a gelten entsprechend.

3.1.6 § 268 Fälschung technischer Aufzeichnungen

(1) Wer zur Täuschung im Rechtsverkehr

1. eine unechte technische Aufzeichnung herstellt oder eine technische Aufzeichnung verfälscht oder

2. eine unechte oder verfälschte technische Aufzeichnung gebraucht,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Technische Aufzeichnung ist eine Darstellung von Daten, Meß- oder Rechenwerten, Zuständen oder Geschehensabläufen, die durch ein technisches Gerät ganz oder zum Teil selbsttätig bewirkt wird, den Gegenstand der Aufzeichnung allgemein oder für Eingeweihte erkennen läßt und zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist, gleichviel ob ihr die Bestimmung schon bei der Herstellung oder erst später gegeben wird.

(3) Der Herstellung einer unechten technischen Aufzeichnung steht es gleich, wenn der Täter durch störende Einwirkung auf den Aufzeichnungsvorgang das Ergebnis der Aufzeichnung beeinflußt.

(4) Der Versuch ist strafbar.

(5) § 267 Abs. 3 und 4 gilt entsprechend.

3.1.7 § 269 Fälschung beweisheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweishebliche 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.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.

3.1.8 § 270 Täuschung im Rechtsverkehr bei Datenverarbeitung

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

3.1.9 § 303a 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.

3.1.10 § 303b 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.

3.2 UrhG

3.2.1 § 69a Gegenstand des Schutzes

(1) Computerprogramme im Sinne dieses Gesetzes sind Programme in jeder Gestalt, einschließlich des Entwurfsmaterials.

(2) Der gewährte Schutz gilt für alle Ausdrucksformen eines Computerprogramms. Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrundeliegenden Ideen und Grundsätze, sind nicht geschützt.

(3) Computerprogramme werden geschützt, wenn sie individuelle Werke in dem Sinne darstellen, daß sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind. Zur Bestimmung ihrer Schutzfähigkeit sind keine anderen Kriterien, insbesondere nicht qualitative oder ästhetische, anzuwenden.

(4) Auf Computerprogramme finden die für Sprachwerke geltenden Bestimmungen Anwendung, soweit in diesem Abschnitt nichts anderes bestimmt ist.

3.2.2 § 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

3.2.3 § 108a Gewerbsmäßige unerlaubte Verwertung

(1) Handelt der Täter in den Fällen der §§ 106 bis 108 gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(2) Der Versuch ist strafbar.

3.3 BDSG

3.3.1 § 1 [Zweck und Anwendungsbereich des Gesetzes]

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
 - a. Bundesrecht ausführen oder
 - b. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.

(3) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen:

1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§ 5 und 9.
2. Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§ 5, 8, 39 und 40. Außerdem gelten für Dateien öffentlicher Stellen die Regelungen über die Verarbeitung und Nutzung personenbezogener Daten in Akten. Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt.

(4) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(5) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

3.3.2 § 3 [Weitere Begriffsbestimmungen]

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).

(2) Eine Datei ist

4. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
5. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, ungeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren ungeordnet und ausgewertet werden können.

(3) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) Erheben ist das Beschaffen von Daten über den Betroffenen.

(5) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise,
 - a. die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder
 - b. der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(6) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(7) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbarer natürlichen Person zugeordnet werden können.

(8) Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern lässt.

(9) Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieses Gesetzes personenbezogene Daten im Auftrag verarbeiten oder nutzen.

3.3.3 § 43 [Strafvorschriften]

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

6. speichert, verändert oder übermittelt,
7. zum Abruf mittels automatisierten Verfahrens bereithält oder
8. abrufen oder sich oder einem anderen aus Dateien verschafft,

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

(2) Ebenso wird bestraft, wer

1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,
2. entgegen § 16 Abs.4 Satz 1, § 28 Abs.4 Satz 1, auch in Verbindung mit § 29 Abs.3, § 39 Abs.1 Satz 1 oder § 40 Abs.1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
3. entgegen § 30 Abs.1 Satz 2 die in § 30 Abs.1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs.3 Satz 3 die in § 40 Abs.3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(4) Die Tat wird nur auf **Antrag** verfolgt.

3.4 UWG

3.4.1 § 17

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer als Angestellter, Arbeiter oder Lehrling eines Geschäftsbetriebs ein Geschäfts- oder Betriebsgeheimnis, das ihm vermöge des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs aus Eigennutz zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, mitteilt.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen,

1. sich ein Geschäfts- oder Betriebsgeheimnis durch

- a) Anwendung technischer Mittel,
- b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
- c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,

unbefugt verschafft oder sichert oder

2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter bei der Mitteilung weiß, daß das Geheimnis im Ausland verwertet werden soll, oder wenn er es selbst im Ausland verwertet.

3.4.2 § 18

Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer die ihm im geschäftlichen Verkehr anvertrauten Vorlagen oder Vorschriften technischer Art, insbesondere Zeichnungen, Modelle, Schablonen, Schnitte, Rezepte, zu Zwecken des Wettbewerbs oder aus Eigennutz unbefugt verwertet oder an jemand mitteilt.

3.5 TDG

3.5.1 § 5 Verantwortlichkeit

(1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern.

(3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte aufgrund Nutzerabfrage gilt als Zugangsvermittlung.

(4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

3.6 MarkenG

3.6.1 § 143 Strafbare Kennzeichenverletzung

(1) Wer im geschäftlichen Verkehr widerrechtlich

1. entgegen § 14 Abs. 2 Nr. 1 oder 2 ein Zeichen benutzt,
2. entgegen § 14 Abs. 2 Nr. 3 ein Zeichen in der Absicht benutzt, die Unterscheidungskraft oder die Wertschätzung einer bekannten Marke auszunutzen oder zu beeinträchtigen,
3. entgegen § 14 Abs. 4 Nr. 1 ein Zeichen anbringt oder entgegen § 14 Abs. 4 Nr. 2 oder 3 eine Aufmachung oder Verpackung oder ein Kennzeichnungsmittel anbietet, in den Verkehr bringt, besitzt, einführt oder ausführt, soweit Dritten die Benutzung des Zeichens

- a) nach § 14 Abs. 2 Nr. 1 oder 2 untersagt wäre oder
- b) nach § 14 Abs. 2 Nr. 3 untersagt wäre und die Handlung in der Absicht vorgenommen wird, die Ausnutzung oder Beeinträchtigung der Unterscheidungskraft oder der Wertschätzung einer bekannten Marke zu ermöglichen,
- 4. entgegen § 15 Abs. 2 eine Bezeichnung oder ein Zeichen benutzt oder
- 5. entgegen § 15 Abs. 3 eine Bezeichnung oder ein Zeichen in der Absicht benutzt, die Unterscheidungskraft oder die Wertschätzung einer bekannten geschäftlichen Bezeichnung auszunutzen oder zu beeinträchtigen,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(1a) Ebenso wird bestraft, wer die Rechte des Inhabers einer nach Rechtsvorschriften der Europäischen Gemeinschaft geschützten Marke verletzt, soweit eine Rechtsverordnung nach Absatz 7 für einen bestimmten Tatbestand auf diese Strafvorschrift verweist.

(2) Handelt der Täter gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In den Fällen des Absätze 1 und 1a wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

(5) Gegenstände, auf die sich die Straftat bezieht, können eingezogen werden. § 74a des Strafgesetzbuchs ist anzuwenden. Soweit den in § 18 bezeichneten Ansprüchen auf Vernichtung im Verfahren nach den Vorschriften der Strafprozessordnung über die Entschädigung des Verletzten (§§ 403 bis 406c der Strafprozessordnung) stattgegeben wird, sind die Vorschriften über die Einziehung nicht anzuwenden.

(6) Wird auf Strafe erkannt, so ist, wenn der Verletzte es beantragt und ein berechtigtes Interesse daran dardat, anzuordnen, dass die Verurteilung auf Verlangen öffentlich bekanntgemacht wird. Die Art der Bekanntmachung ist im Urteil zu bestimmen.

(7) Das Bundesministerium der Justiz wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrates die Tatbestände zu bezeichnen, die als Straftaten nach Absatz 1a geahndet werden können, soweit dies zur Durchsetzung des in Rechtsvorschriften der Europäischen Gemeinschaft vorgesehenen Schutzes von Marken erforderlich ist.

3.7 Strafantrag

§ 205 StGB Strafantrag

(1) In den Fällen des § 201 Abs. 1 und 2 und der §§ 202 bis 204 wird die Tat nur auf Antrag verfolgt.

(2) Stirbt der Verletzte, ...

§ 248a StGB Diebstahl und Unterschlagung geringwertiger Sachen

Der Diebstahl und die Unterschlagung geringwertiger Sachen werden in den Fällen der §§ 242 und 246 nur auf Antrag verfolgt, es sei denn, daß die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

§ 303c StGB Strafantrag

In den Fällen der §§ 303 bis 303b wird die Tat nur auf Antrag verfolgt, es sei denn, daß die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

§ 22 UWG

(1) Die Tat wird, mit Ausnahme der in den §§ 4 und 6c bezeichneten Fälle, nur auf Antrag verfolgt. Dies gilt in den Fällen der §§ 17, 18 und 20 nicht, wenn die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

§ 109 UrhG

In den Fällen der §§ 106 bis 108 wird die Tat nur auf Antrag verfolgt, es sei denn, daß die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

4. Verfahrensnormen

4.1 TKG

4.1.1 § 89 Datenschutz

(1) Die Bundesregierung erläßt für Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, durch Rechtsverordnung mit Zustimmung des Bundesrates Vorschriften zum Schutze personenbezogener Daten der an der Telekommunikation Beteiligten, welche die Erhebung, Verarbeitung und Nutzung dieser Daten regeln. Die Vorschriften haben dem Grundsatz der Verhältnismäßigkeit, insbesondere der Beschränkung der Erhebung, Verarbeitung und Nutzung auf das Erforderliche, sowie dem Grundsatz der Zweckbindung Rechnung zu tragen. Dabei sind Höchstfristen für die Speicherung festzulegen und insgesamt die berechtigten Interessen des jeweiligen Unternehmens und der Betroffenen zu berücksichtigen. Einzelangaben über juristische Personen, die dem Fernmeldegeheimnis unterliegen, stehen den personenbezogenen Daten gleich.

(2) Nach Maßgabe der Rechtsverordnung dürfen Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, die Daten natürlicher und juristischer Personen erheben, verarbeiten und nutzen, soweit dies erforderlich ist

1. zur betrieblichen Abwicklung ihrer jeweiligen geschäftsmäßigen Telekommunikationsdienste, nämlich für

- a) das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses,
- b) das Herstellen und Aufrechterhalten einer Telekommunikationsverbindung,
- c) das ordnungsgemäße Ermitteln und den Nachweis der Entgelte für geschäftsmäßige Telekommunikationsdienste einschließlich der auf andere Netzbetreiber und Anbieter von geschäftsmäßigen Telekommunikationsdiensten entfallenden Leistungsanteile; für den Nachweis ist dem Nutzer eine Wahlmöglichkeit hinsichtlich Speicherdauer und Speicherumfang einzuräumen,
- d) das Erkennen und Beseitigen von Störungen an Telekommunikationsanlagen,
- e) das Aufklären sowie das Unterbinden von Leistungerschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie der geschäftsmäßigen Telekommunikationsdienste, sofern tatsächliche Anhaltspunkte vorliegen; nach näherer Bestimmung in der Rechtsverordnung dürfen aus den Gesamtdatenbeständen die Daten ermittelt werden, die konkrete Indizien für eine mißbräuchliche Inanspruchnahme von geschäftsmäßigen Telekommunikationsdiensten enthalten,

2. für das bedarfsgerechte Gestalten von geschäftsmäßigen Telekommunikationsdiensten; dabei dürfen Daten in bezug auf den Anschluß, von dem der Anruf ausgeht, nur mit Einwilligung des Anschlußinhabers verwendet und müssen Daten in bezug auf den angerufenen Anschluß unverzüglich anonymisiert werden,

3. auf schriftlichen Antrag eines Nutzers zum Zwecke

- a) der Darstellung der Leistungsmerkmale; hierzu dürfen insbesondere Datum, Uhrzeit, Dauer und Rufnummern der von seinem Anschluß hergestellten Verbindungen unter Wahrung des in der Rechtsverordnung zu regelnden Schutzes von Mitbenutzern und Anrufen bei Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die gemäß ihrer von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannten Aufgabenbestimmung grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, mitgeteilt werden,
- b) des Identifizierens von Anschlüssen, wenn er in einem zu dokumentierenden Verfahren schlüssig vorgetragen hat, das Ziel bedrohender oder belästigender Anrufe zu sein; dem Nutzer werden die Rufnummern der Anschlüsse sowie die von diesen ausgehenden Verbindungen und Verbindungsversuche einschließlich Name und Anschrift des Anschlußinhabers nur bekanntgegeben, wenn er zuvor die Anrufe nach Datum und Uhrzeit eingrenzt, soweit ein Mißbrauch der Überwachungsmöglichkeit nicht auf andere Weise ausgeschlossen werden kann; grundsätzlich wird der Anschlußinhaber über die Auskunftserteilung nachträglich informiert.

(3) Es dürfen nur die näheren Umstände der Telekommunikation erhoben, verarbeitet und genutzt werden. Soweit es für Maßnahmen nach Absatz 2 Nr. 1 Buchstabe e unerlässlich ist, dürfen im Einzelfall Steuersignale maschinell erhoben, verarbeitet und genutzt werden; die Regulierungsbehörde ist hierüber in Kenntnis zu setzen. Der Betroffene ist zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahmen möglich ist. Die Erhebung, Verarbeitung und Nutzung anderer Nachrichteninhalte ist unzulässig, es sei denn, daß sie nach Absatz 4 notwendig oder im Einzelfall für Maßnahmen nach Absatz 5 unerlässlich ist.

(4) Beim geschäftsmäßigen Erbringen von Telekommunikationsdiensten dürfen Nachrichteninhalte nur aufgezeichnet, Dritten zugänglich gemacht oder sonst verarbeitet werden, soweit dies Gegenstand oder aus verarbeitungstechnischen Gründen Bestandteil des Dienstes ist. § 85 Abs. 3 Satz 3 bleibt unberührt.

(5) Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber der Telekommunikationsanlage oder seinem Beauftragten das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist. Das Aufschalten muß den betroffenen Gesprächsteilnehmern durch ein akustisches Signal angezeigt und ausdrücklich mitgeteilt werden.

(6) Ferner haben die in Absatz 2 genannten Unternehmen und Personen personenbezogene Daten, die sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben, im Einzelfall auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist. Auskünfte an die genannten Stellen dürfen Kunden oder Dritten nicht mitgeteilt werden.

(7) Die in Absatz 2 genannten Unternehmen und Personen dürfen die personenbezogenen Daten, die sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben, verarbeiten und nutzen, soweit dies für Zwecke der Werbung, Kundenberatung oder Marktforschung für die in Absatz 2 genannten Unternehmen und Personen erforderlich ist und der Kunde eingewilligt hat. Personenbezogene Daten von Kunden, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes von den in Absatz 2 genannten Unternehmen und Personen bereits erhoben waren, dürfen für die in Satz 1 genannten Zwecke verarbeitet und genutzt werden, wenn der Kunde nicht widerspricht. Sein Einverständnis gilt als erteilt, wenn er in angemessener Weise über sein Widerspruchsrecht informiert worden ist und von seinem Widerspruchsrecht keinen Gebrauch gemacht hat.

(8) Diensteanbieter können Kunden mit ihrem Namen, ihrer Anschrift und zusätzlichen Angaben, wie Beruf, Branche, Art des Anschlusses und Mitbenutzer, in öffentliche gedruckte oder elektronische Verzeichnisse eintragen, soweit der Kunde dies beantragt hat. Dabei kann der Kunde bestimmen, welche Angaben in den Kundenverzeichnissen veröffentlicht werden sollen, daß die Eintragung nur in gedruckten oder elektronischen Verzeichnissen erfolgt oder daß jegliche Eintragung unterbleibt. Mitbenutzer dürfen eingetragen werden, soweit sie damit einverstanden sind. Sind Kunden beim Inkrafttreten dieses Gesetzes in ein Kundenverzeichnis eingetragen, so muß die Eintragung künftig unterbleiben, wenn der Kunde widerspricht. Absatz 7 Satz 3 gilt entsprechend.

(9) Nach Maßgabe der entsprechenden Rechtsverordnung dürfen Unternehmen und Personen im Sinne des Absatzes 2 im Einzelfall Auskunft über in öffentlichen Verzeichnissen enthaltene Daten der Nutzer von geschäftsmäßigen Telekommunikationsdiensten erteilen oder durch Dritte erteilen lassen. Die Auskunft darf nur über Daten von Kunden erteilt werden, die in angemessener Weise darüber informiert worden sind, daß sie der Weitergabe ihrer Daten widersprechen können, und die von ihrem Widerspruchsrecht keinen Gebrauch gemacht haben. Ein Widerspruch ist in den Verzeichnissen des Diensteanbieters unverzüglich zu vermerken. Er ist auch von anderen Diensteanbietern zu beachten, sobald er in dem öffentlichen Verzeichnis des Diensteanbieters vermerkt ist.

(10) Die geschäftsmäßige Erbringung von Telekommunikationsdiensten und deren Entgeltfestlegung darf nicht von der Angabe personenbezogener Daten abhängig gemacht werden, die für die Erbringung oder Entgeltfestlegung dieser Dienste nicht erforderlich sind. Soweit die in Absatz 2 genannten Unternehmen die Verarbeitung oder Nutzung personenbezogener Daten eines Kunden von seiner Einwilligung abhängig machen, haben sie ihn in sachgerechter Weise über Inhalt und Reichweite der Einwilligung zu informieren. Dabei sind die vorgesehenen Zwecke und Nutzungszeiten zu nennen. Die Einwilligung muß ausdrücklich und in der Regel schriftlich erfolgen. Soll sie im elektronischen Verfahren erfolgen, ist dabei für einen angemessenen Zeitraum eine Rücknahmemöglichkeit vorzusehen.

• Inhalt Auskunft

§ 89 Abs. 6 TKG Kundenbestandsdatenerfassung

Subscriber Management Systems (SMS)

- Name, Vorname, Rufnummern, Kundennummern
- Adresse, ggf. abweichende Rechnungsadresse
- ggf. Lage der Wohnung (zB für Netz-Entstörung)
- Geburtsdatum
- Art der Dienstleistungen (zB IDSN, AktivPlus, Wartungsverträge)
- „TDSV-Optionen (zB EVN, Kein Eintrag in TK-Verzeichnisse, Keine Werbung, Rufnummernanzeige aktiv usw.)
- Zahlungsweise (zB Lastschrift)
- Bankverbindung, Konto-Nr.
- ggf. Bonitätsbewertungen (zB seit 2 Monaten Zahlungsrückstand)

4.1.2 § 90 Auskunftersuchen der Sicherheitsbehörden

(1) Wer geschäftsmäßig Telekommunikationsdienste anbietet, ist verpflichtet, Kundendateien zu führen, in die unverzüglich die Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere vergeben werden, sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingenten aufzunehmen sind, auch soweit diese nicht in öffentliche Verzeichnisse eingetragen sind.

(2) Die aktuellen Kundendateien sind von dem Verpflichteten nach Absatz 1 verfügbar zu halten, so daß die Regulierungsbehörde einzelne Daten oder Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann. Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, daß ihm Abrufe nicht zur Kenntnis gelangen können.

(3) Auskünfte aus den Kundendateien nach Absatz 1 werden

1. den Gerichten, Staatsanwaltschaften und anderen Justizbehörden sowie sonstigen Strafverfolgungsbehörden,
2. den Polizeien des Bundes und der Länder für Zwecke der Gefahrenabwehr,
3. den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes und
4. den Verfassungsschutzbehörden des Bundes und der Länder, dem militärischen Abschirmdienst und dem Bundesnachrichtendienst

jederzeit unentgeltlich erteilt, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.

(4) Die Regulierungsbehörde hat die Daten, die in den Kundendateien der Verpflichteten nach Absatz 1 gespeichert sind, auf Ersuchen der in Absatz 3 genannten Stellen im automatisierten Verfahren abzurufen und an die ersuchende Stelle weiter zu übermitteln. Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlaß besteht. Die Verantwortung für die Zulässigkeit der Übermittlung tragen die in Absatz 3 genannten Behörden. Die Regulierungsbehörde protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, die die Daten abrufende Person sowie die ersuchende Stelle und deren Aktenzeichen. Eine Verwendung der Protokoll Daten für andere Zwecke ist unzulässig. Die Protokoll Daten sind nach zwölf Monaten zu löschen.

(5) Absatz 1 gilt entsprechend für Dritte, die geschäftsmäßig Rufnummern aus einem Rufnummernkontingent vergeben, ohne Verpflichteter im Sinne von Absatz 1 zu sein, mit der Maßgabe, daß es dem Dritten überlassen bleibt, in welcher Form er die in Absatz 1 genannten Daten zur Auskunftserteilung vorhält. Er hat die Auskünfte aus den Kundendateien den in Absatz 3 genannten Behörden auf deren Ersuchen zu erteilen. Über die Tatsache einer Abfrage und die erteilten Auskünfte sowie über deren nähere Umstände hat der Auskunftspflichtige Stillschweigen, insbesondere gegenüber dem Betroffenen, zu wahren.

(6) Der Verpflichtete nach Absatz 1 hat alle Vorkehrungen in seinem Verantwortungsbereich auf seine Kosten zu treffen, die für den automatisierten Abruf gemäß Absatz 2 erforderlich sind.

(7) In den Fällen der Auskunftserteilung nach Absatz 5, in denen das Gesetz über die Entschädigung von Zeugen und Sachverständigen nicht gilt, sind die Vorschriften des genannten Gesetzes über die Höhe der Entschädigung entsprechend anzuwenden.

(8) Bei wiederholten Verstößen gegen die Absätze 1 und 2 kann die geschäftliche Tätigkeit des Verpflichteten durch Anordnung der Regulierungsbehörde dahingehend eingeschränkt werden, daß der Kundenstamm bis zur Erfüllung der sich aus diesen Vorschriften ergebenden Verpflichtungen außer durch Vertragsablauf oder Kündigung nicht verändert werden darf.

4.2 Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz -TDDSG)

§ 1 Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für den Schutz personenbezogener Daten bei Telediensten im Sinne des Teledienstegesetzes.

(2) Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. "Diensteanbieter" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln,
2. "Nutzer" natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste nachfragen.

§ 3 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Durchführung von Telediensten erhobene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.

- (3) Der Diensteanbieter darf die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in nicht zumutbarer Weise möglich ist.
- (4) Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.
- (5) Der Nutzer ist vor der Erhebung über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer vor Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muß für den Nutzer jederzeit abrufbar sein. Der Nutzer kann auf die Unterrichtung verzichten. Die Unterrichtung und der Verzicht sind zu protokollieren. Der Verzicht gilt nicht als Einwilligung im Sinne der Absätze 1 und 2.
- (6) Der Nutzer ist vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen. Absatz 5 Satz 3 gilt entsprechend.
- (7) Die Einwilligung kann auch elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, daß
1. sie nur durch eine eindeutige und bewußte Handlung des Nutzers erfolgen kann,
 2. sie nicht unerkennbar verändert werden kann,
 3. ihr Urheber erkannt werden kann,
 4. die Einwilligung protokolliert wird und
 5. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann.

§ 4 Datenschutzrechtliche Pflichten des Diensteanbieters

- (1) Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.
- (2) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, daß
1. der Nutzer seine Verbindung mit dem Diensteanbieter jederzeit abbrechen kann,
 2. **die anfallenden personenbezogenen Daten über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht werden**, soweit nicht eine längere Speicherung für Abrechnungszwecke erforderlich ist,
 3. der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
 4. die personenbezogenen Daten über die Inanspruchnahme verschiedener Teledienste durch einen Nutzer getrennt verarbeitet werden; eine Zusammenführung dieser Daten ist unzulässig, soweit dies nicht für Abrechnungszwecke erforderlich ist.
- (3) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.
- (4) Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig. Unter einem Pseudonym erfaßte Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

§ 5 Bestandsdaten

- (1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich sind (Bestandsdaten).
- (2) Eine Verarbeitung und Nutzung der Bestandsdaten für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste ist nur zulässig, soweit der Nutzer in diese ausdrücklich eingewilligt hat.

§ 6 Nutzungs- und Abrechnungsdaten

- (1) Der Diensteanbieter darf personenbezogene Daten über die Inanspruchnahme von Telediensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist,
1. um dem Nutzer die Inanspruchnahme von Telediensten zu ermöglichen (Nutzungsdaten) oder
 2. um die Nutzung von Telediensten abzurechnen (Abrechnungsdaten).
- (2) Zu löschen hat der Diensteanbieter
1. Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung, soweit es sich nicht um Abrechnungsdaten handelt,
 2. Abrechnungsdaten, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind; nutzerbezogene Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers gemäß Absatz 4 gespeichert werden, sind **spätestens 80 Tage nach Versendung des Einzelnachweises zu löschen**, es sei denn, die Entgeltforderung wird innerhalb dieser Frist bestritten oder trotz Zahlungsaufforderung nicht beglichen.
- (3) Die Übermittlung von Nutzungs- oder Abrechnungsdaten an andere Diensteanbieter oder Dritte ist unzulässig. Die Befugnisse der Strafverfolgungsbehörden bleiben unberührt. Der Diensteanbieter, der den Zugang zur Nutzung von Telediensten vermittelt, darf anderen Diensteanbietern, deren Teledienste der Nutzer in Anspruch genommen hat, lediglich übermitteln
1. anonymisierte Nutzungsdaten zu Zwecken deren Marktforschung,
 2. Abrechnungsdaten, soweit diese zum Zwecke der Einziehung einer Forderung erforderlich sind.

(4) Hat der Diensteanbieter mit einem Dritten einen Vertrag über die Abrechnung des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Der Dritte ist zur Wahrung des Fernmeldegeheimnisses zu verpflichten.

(5) Die Abrechnung über die Inanspruchnahme von Telediensten darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Teledienste nicht erkennen lassen, es sei denn, der Nutzer verlangt einen Einzelnachweis.

§ 7 Auskunftsrecht des Nutzers

Der Nutzer ist berechtigt, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Diensteanbieter einzusehen. Die Auskunft ist auf Verlangen des Nutzers auch elektronisch zu erteilen. Das Auskunftsrecht ist im Falle einer kurzfristigen Speicherung im Sinne des § 33 Abs. 2 Nr. 5 des Bundesdatenschutzgesetzes nicht nach § 34 Abs. 4 des Bundesdatenschutzgesetzes ausgeschlossen.

§ 8 Datenschutzkontrolle

(1) § 38 des Bundesdatenschutzgesetzes findet mit der Maßgabe Anwendung, daß die Überprüfung auch vorgenommen werden darf, wenn Anhaltspunkte für eine Verletzung von Datenschutzvorschriften nicht vorliegen.

(2) Der Bundesbeauftragte für den Datenschutz beobachtet die Entwicklung des Datenschutzes bei Telediensten und nimmt dazu im Rahmen seines Tätigkeitsberichtes nach § 26 Abs. 1 des Bundesdatenschutzgesetzes Stellung.

4.2.1 Datenschutz

6.2 Datenschutzgerechte Protokollierung der Abrufe

Wer eigene Angebote ins Internet einstellt, will in aller Regel wissen, wie oft welche Angebotsseiten abgerufen wurden. Mitunter protokollieren die Betreiber der WWW-Server hierzu nicht nur, wann welche Angebotsseite abgerufen wurde, sondern registrieren auch die Netzadresse des abrufenden Computers, die sog. IP-Adresse.

Bei dieser Vorgehensweise ist folgendes zu bedenken:

Der numerischen IP-Adresse eines am Internet angeschlossenen Computers läßt sich mit Hilfe des DNS-Dienstes ein Name zuweisen. Daraus geht häufig hervor, in welchem Land der Rechner installiert ist. Zudem gibt der Rechnername oft auch Aufschluß über die Stelle, die den Rechner betreibt, beispielsweise ein Universitätsinstitut. Schon allein dies läßt einen Rückschluß auf den Kreis derjenigen zu, die mit diesem Rechner arbeiten. Vollends zu einem persönlichen Merkmal werden Rechnername und Netzadresse, wenn der Internet-Nutzer immer mit demselben Computer arbeitet, diesen Rechner allein nutzt und die Adresse dieses Computers im Internet verwendet wird. Mit anderen Worten: IP-Adressen können personenbezogen sein. Für die Anbieter von WWW-Angeboten hat dies folgende Konsequenz: Da sie mit ihrem Angebot in der Regel einen Tele- oder Mediendienst anbieten, müssen sie die Datenschutzregelungen des Teledienste-Datenschutzgesetzes oder des Mediendienste-Staatsvertrags der Länder beachten. In beiden heißt es klipp und klar, daß der Diensteanbieter per-

sonenbezogene Daten über die näheren Umstände des einzelnen Abrufs spätestens mit dem Beenden der Verbindung löschen muß, es sei denn, er benötigt die Daten noch für Zwecke der Abrechnung. Da die IP-Adressen je nach konkretem Einsatz personenbezogen sein können, dürfen IP-Adressen nach erfolgtem Webseiten-Zugriff allenfalls für Abrechnungs- nicht aber für andere Zwecke gespeichert werden.

Quelle: Datenschutzbeauftragter Baden-Württemberg

4.2.2 Verbotene Protokolle

(...) Grob vereinfacht verbietet das Teledienstedatenschutzgesetz (TDDSG) zunächst einmal jegliches Erheben von personenbezogenen Daten im Zusammenhang mit Diensten nach dem Teledienstegesetz (TDG), es sei denn, der Betroffene (Dienste-Nutzer) willigt ein oder einer der wenigen Ausnahmetatbestände des TDDSG greift. Erlaubt wird - ebenfalls auf einen schlichten Nenner gebracht - nur das Nötigste, um überhaupt einen Teledienst anbieten zu können. Analoges gilt für Dienste nach dem Mediendienstestaatsvertrag (MDStV).

(...) Es ist nachvollziehbar und verständlich, dass der Gesetzgeber sich seinerzeit dazu entschlossen hat, durch das TDDSG solche Datensammlungen zu verbieten. Umso erstaunlicher ist es immer wieder, dass in den Medien Berichte auftauchen, nach denen Online-Straftaten durch Zurückverfolgung der Zugriffswege auch im Nachhinein aufgeklärt werden konnten. Eine solche Aufklärung müsste bei konsequenter Anwendung des TDDSG eigentlich ausgeschlossen sein.

So hat das auch der Bundesbeauftragte für den Datenschutz, Dr. Joachim Jacob, gegenüber der Zeitschrift c't bestätigt: "Ein Provider [darf] in keinem Fall mit Blick auf eine eventuell mögliche Strafverfolgung vorsorglich speichern, wann welche IP-Nummer hatte." Nur wenn bereits während der Nutzung "vorausgesehen ist, dass gerade diese Daten für die Strafverfolgung erforderlich sind", käme die Ausnahme in § 6 (3) TDDSG zum Zuge, dass "die Befugnisse der Strafverfolgungsbehörden unberührt bleiben"

(...) Das TDDSG erlaubt die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten - ohne die vorherige Einwilligung des Betroffenen - nur

dann, wenn es sich um Bestands-, Nutzungs- oder Abrechnungsdaten handelt; und in den beiden letzten Fällen auch nur für eine bestimmte Zeit.

Bestandsdaten definiert § 5 TDDSG als die Daten, die "für die Begründung, die inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses ... notwendig sind". Es handelt sich also regelmäßig um die Vertragsdaten, die mit der Nutzung des Dienstes selbst nicht zusammenhängen. Die Verarbeitung dieser Daten unterliegt keiner zeitlichen Beschränkung.

Nutzungsdaten darf der Diensteanbieter nach § 6 (1) Nr. 1 TDDSG zwar erheben, verarbeiten und nutzen, aber nur soweit dies zur Inanspruchnahme des Teledienstes notwendig ist und *nur solange die Nutzung andauert*; danach sind die Daten sofort zu löschen (§ 6 (2) Nr. 1 TDDSG). Zu den Nutzungsdaten zählen diejenigen, die beschreiben, welcher Nutzer gerade welche Internetseite abrufen, welche IP-Nummer er verwendet und die IP-Nummer des Ziels.

Quelle: RA Stefan Jaeger, Wiesbaden

4.3 StPO

§ 94

- (1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.
- (2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.
- (3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen.

§ 95

- (1) Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.
- (2) Im Falle der Weigerung können gegen ihn die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. Das gilt nicht bei Personen, die zur Verweigerung des Zeugnisses berechtigt sind.

§ 102

Bei dem, welcher als Täter oder Teilnehmer einer Straftat oder der Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist, kann eine Durchsuchung der Wohnung und anderer Räume sowie seiner Person und der ihm gehörenden Sachen sowohl zum Zweck seiner Ergreifung als auch dann vorgenommen werden, wenn zu vermuten ist, daß die Durchsuchung zur Auffindung von Beweismitteln führen werde.

§ 103

- (1) Bei anderen Personen sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder zur Verfolgung von Spuren einer Straftat oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet. Zum Zwecke der Ergreifung eines Beschuldigten, der dringend verdächtig ist, eine Straftat nach § 129a des Strafgesetzbuches oder eine der in dieser Vorschrift bezeichneten Straftaten begangen zu haben, ist eine Durchsuchung von Wohnungen und anderen Räumen auch zulässig, wenn diese sich in einem Gebäude befinden, von dem auf Grund von Tatsachen anzunehmen ist, daß sich der Beschuldigte in ihm aufhält.
- (2) Die Beschränkungen des Absatzes 1 Satz 1 gelten nicht für Räume, in denen der Beschuldigte ergriffen worden ist oder die er während der Verfolgung betreten hat.

§ 160

- (1) Sobald die Staatsanwaltschaft durch eine Anzeige oder auf anderem Wege von dem Verdacht einer Straftat Kenntnis erhält, hat sie zu ihrer Entschließung darüber, ob die öffentliche Klage zu erheben ist, den Sachverhalt zu erforschen.
- (2) Die Staatsanwaltschaft hat nicht nur die zur Belastung, sondern auch die zur Entlastung dienenden Umstände zu ermitteln und für die Erhebung der Beweise Sorge zu tragen, deren Verlust zu besorgen ist.

(3) Die Ermittlungen der Staatsanwaltschaft sollen sich auch auf die Umstände erstrecken, die für die Bestimmung der Rechtsfolgen der Tat von Bedeutung sind. Dazu kann sie sich der Gerichtshilfe bedienen.

§ 161

Zu dem im vorstehenden Paragraphen bezeichneten Zweck kann die Staatsanwaltschaft von allen öffentlichen Behörden Auskunft verlangen und Ermittlungen jeder Art entweder selbst vornehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen lassen. Die Behörden und Beamten des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen.

§ 161a

(1) Zeugen und Sachverständige sind verpflichtet, auf Ladung vor der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen oder ihr Gutachten zu erstatten. Soweit nichts anderes bestimmt ist, gelten die Vorschriften des sechsten und siebensten Abschnitts des ersten Buches über Zeugen und Sachverständige entsprechend. Die eidliche Vernehmung bleibt dem Richter vorbehalten.

(2) Bei unberechtigtem Ausbleiben oder unberechtigter Weigerung eines Zeugen oder Sachverständigen steht die Befugnis zu den in den §§ 51, 70 und 77 vorgesehenen Maßregeln der Staatsanwaltschaft zu. Jedoch bleibt die Festsetzung der Haft dem Richter vorbehalten; zuständig ist das Amtsgericht, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat, welche die Festsetzung beantragt.

(3) Gegen die Entscheidung der Staatsanwaltschaft nach Absatz 2 Satz 1 kann gerichtliche Entscheidung beantragt werden. Über den Antrag entscheidet, soweit nicht in § 120 Abs. 3 Satz 1 und § 135 Abs. 2 des Gerichtsverfassungsgesetzes etwas anderes bestimmt ist, das Landgericht, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat. Die §§ 297 bis 300, 302, 306 bis 309, 311a sowie die Vorschriften über die Auferlegung der Kosten des Beschwerdeverfahrens gelten entsprechend. Die Entscheidung des Gerichts ist nicht anfechtbar.

(4) Ersucht eine Staatsanwaltschaft eine andere Staatsanwaltschaft um die Vernehmung eines Zeugen oder Sachverständigen, so stehen die Befugnisse nach Absatz 2 Satz 1 auch der ersuchten Staatsanwaltschaft zu.

4.4 § 12 FAG

(1) In strafgerichtlichen Untersuchungen kann der Richter und bei Gefahr im Verzuge auch die Staatsanwaltschaft Auskunft über die Telekommunikation verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und daß die Auskunft für die Untersuchung Bedeutung hat. Das Grundrecht des Art. 10 des Grundgesetzes wird insoweit eingeschränkt.

(2) § 100 b Abs. 6 und § 101 Abs. 1 Satz 1 der Strafprozessordnung gelten entsprechend.

4.4.1 Inhalt Auskunft

§ 12 FAG Verbindungsdatenerfassung Kommunikationsdatensatz (KDS)

- Rufnummer des anrufenden Anschlusses
- Rufnummer des angerufenen Anschlusses
- Datum der Verbindung
- Beginn der Verbindung
- Ende der Verbindung
- ggf. Dienstleistungsmerkmale (zB Faxnachricht)
- ggf. Standortkennungen (Mobilfunk)

02241926692 ...02281817409020.08.00 ...14.33 ... 14.42 ...

| | | | | |
|---|---|----|------|------|
| A | B | Dt | Beg. | End. |
|---|---|----|------|------|

- Jeder KDS wird zunächst in der jeweiligen Ortsvermittlungsstelle (Computer) des A-Teilnehmers erzeugt und zwischengespeichert.
- Arbeitstäglich werden die Datenspeicher der OVSt ausgelesen; die Daten werden elektronisch zu Fakturierungssystemen überspielt und dort - nach (entgeltpflichtigen) A-Teilnehmern und chronologisch geordnet - bis zur Rechnungserstellung zwischengespeichert.

- In der Regel werden die KDS nach Rechnungsversand mit um 3 Stellen verkürzter Zielrufnummer 80 Tage weitergespeichert und danach endgültig gelöscht.

4.5 TDSV

„Das Bundeskabinett hat (...) den geänderten Entwurf einer Telekommunikations-Datenschutzverordnung (TDSV) auf der Grundlage von § 89 Abs. 1 Telekommunikationsgesetz (TKG) beschlossen. (...)

Die Verordnung regelt den Schutz personenbezogener Daten der an der Telekommunikation Beteiligten bei der Verarbeitung durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken.

Die Novellierung berücksichtigt insbesondere den durch die Marktliberalisierung erweiterten Kreis der Diensteanbieter und den technischen Fortschritt im Bereich der Telekommunikation. Die Verordnung enthält u. a. eine Reihe von Verfahrensvereinfachungen und eine Ordnungswidrigkeitenvorschrift, die die Durchsetzung einzelner Datenschutzregelungen sicherstellt.“ (BGBI. I 2000, 1740).

5. Ermittlungen

Hoeren/**Sieber**, a.a.O., RN 686 ff.

Bei luK-Ermittlungen ist stets daran zu denken, dass Daten „verderbliche Waren“ sind, dass mit dem Verlust der beweisrelevanten Tatsachen aufgrund Zeitablaufs zu rechnen ist.

5.1 Erstzugriff

Nach Eingang einer Anzeige oder eines Ermittlungsauftrages sollten die offenen Erkenntnisquellen sofort genutzt werden, um einen Überblick über die beteiligten Personen oder Unternehmungen zu erlangen. Bei Internet-bezogenen Taten sind nützlich:

DENIC, internic : Zur Identifikation der Beteiligten zu einer "Second-Level-Domain" (<http://www.denic.de> - <http://www.internic.net>).

RIPE : Zur Auflösung einer IP-Nummer (<http://www.ripe.net> - <http://www.apnic.net> - <http://www.arin.net>).

Neben der Anzeige des Geschädigten als Erkenntnisquelle dürfen die üblichen Beweismittel (z. B. Fingerabdrücke auf einer CD-R oder Hülle) nicht außer Acht gelassen werden.

Weitere Informationen ergeben sich aus den Auskünften der Provider oder der RegTP (nach §§ 89, 90 TKG).

Verbindungsdaten sind grundsätzlich im Beschlussverfahren nach § 12 FAG zu erheben, wobei hier der Zeitfaktor eine besondere Rolle spielt.

5.2 Durchsuchung

Durchsuchungen bei Beschuldigten (§ 102 StPO) oder Dritten (§ 103 StPO) bedürfen grundsätzlich eines richterlichen Beschlusses (vgl. BVerfG, B. v. 20.2.2001, 2 BvR 1444/00: Anforderungen an Durchsuchungsmaßnahme (in Wohnraum) und zu Gefahr im Verzuge, Konkretisierung des Durchsuchungsprogrammes (wo / was)).

Bei der Sicherstellung der Computer als Tatwerkzeuge ist an eine spätere Einziehung zu denken. In geeigneten Fällen (insb. Urheberrechtsverletzungen) sollte an die Rückgewinnhilfe zugunsten des Geschädigten gedacht werden.

Zu beachten ist, dass bei Durchsuchungen bestimmter Räumlichkeiten ein Online-Zugriff auf Daten außerhalb der im Beschluss bezeichneten Örtlichkeit nicht zulässig ist. Eine Anordnung der „Online-Durchsuchung“ wegen Gefahr im Verzug (s.o.) dürfte aber angezeigt sein.

Zulässig ist die Inbetriebnahme einer Computeranlage vor Ort. Unzulässig ist eine "Durchsuchung" im Ausland durch Online-Zugriff - auch mit Einwilligung des Beschuldigten oder Betroffenen (Hoeren/**Sieber**, a.a.O., RN 735 ff.).²

Eine Postbeschlagnahme ist in geeigneten Fällen zweckmäßig (z. B. Zahlungsverkehr und Versand von Raubkopien per Post).

5.3 Auswertung

Die Durchsicht gespeicherter Daten ("Papiere") erfolgt gem. § 100 StPO.

² Neben praktisch allen Providern, die Raum für eigene Internetseiten zur Verfügung stellen, wird „Webspace“ insbesondere von den Anbietern *my-files.de* und *xdrive.com* vorgehalten. Der passwortgeschützte Speicherplatz kann online wie ein Netzwerkverzeichnis genutzt werden und ist praktisch nicht ohne Hinweise aufzufinden. Speicherplatz für Internetseiten kann zusätzlich als „Versteck“ genutzt werden, indem beliebige Dateien, auf die nicht „verlinkt“ wird, hochgeladen werden. Ohne Kenntnis der genauen URL oder des FTP-Verzeichnisses sind diese Dateien praktisch unauffindbar.

Bei der Sicherstellung und Auswertung von Datenträgern (vgl. dazu BKA-Mitteilungsblatt 1/2000, S. 63/64) sind die allgemein gültigen Regelungen zu beachten. Sofern keine Originale sichergestellt werden, muss eine „Spiegelung“ des Datenträgers und nicht nur eine Sicherung der Daten vorgenommen werden, um auch „gelöschte“ Dateien o.ä. auffinden zu können.³

Eine Dokumentation der Arbeitsschritte ist erforderlich.

5.4 Täter

Die Praxis zeigt, dass Täter im IuK-Bereich oft sog. Mehrfach-Täter sind, d.h. sie schädigen in einem bestimmten Zeitraum durch Verwendung falscher Einwahldaten mehrere Provider. Problematisch ist dies dann, wenn die Taten mit einem relativ geringen Betrag zuerst bekannt oder ermittelt werden und nach § 153 (a) StPO entschieden wird („Strafklageverbrauch“?). Zudem besteht die Gefahr, dass bei relativ geringen beträgen eine Durchsuchung aus Verhältnismäßigkeitsgründen unterbleibt und der Täter so in die Lage versetzt wird, Beweismittel für – die ihm bekannten – weiteren Taten zu beseitigen.

Zudem zeigt die Praxis, dass sog. Hacker auch Urheberrechtsverletzungen – wie möglicherweise *alle* Computernutzer – begehen und Raubkopien mit kommerziellen Erwägungen vertreiben. Daneben ist der Missbrauch von Pay-TV-Karten zu beobachten.

Problematisch ist die Zuordnung von Taten dann, wenn ein Computer von mehreren Personen (Familienmitgliedern, Arbeitskollegen, Freunde) genutzt werden kann bzw. zur Tatzeit genutzt wurde. Die Auswertung des Emailverkehrs mag da, soweit noch vorhanden, Hinweise auf die tatsächliche Nutzung geben.

Erfahrungsgemäß kommen bei Familien (nur) die jugendlichen oder heranwachsenden Söhne als Täter in Betracht.⁴

5.5 Probleme

- Für die Auskunft über Bestandsdaten nach § 89 VI TKG soll richterlicher Beschluss (entspr. § 12 FAG) erforderlich sein (Beck'scher TKG-Komm., § 89 RN 45).

Diese Ansicht findet im Gesetz keine Stütze. Die Gesamtschau mit den für die Strafverfolgungsbehörden relevanten Normen der StPO erlaubt es, die Auskünfte auch mit

³ Der überwiegend genutzte Internet Explorer zeichnet in bestimmten Umfang die Internetnutzung mit. Die Daten aus „Verlauf“ und „Favoriten“ sowie alle temporären Dateien sollten daher auch gesichert werden einschließlich der Ordner „Recycled“. Zu beachten ist, dass auch in der Registry zumindest die letzten fünf aufgerufenen URL's vermerkt sind.

⁴ Bei den von mir in den Jahren 2000 und 2001 bearbeiteten ca. 175 Verfahren des Computerbetrugs (Einwahl mit fremden Zugangsdaten) wurde keine Frau als Täterin ermittelt.

staatsanwaltschaftlichen Auskunftersuchen einzufordern (vgl. die Praxis bei Abankauskunftersuchen). Ggf. können Zeugen zur Vernehmung durch die Staatsanwaltschaft geladen werden. Im Weigerungsfall sind Zwangsmittel zulässig. Notfalls ist ein Durchsuchungsbeschluss (§ 103 StPO) zur Sicherstellung der Datenträger angezeigt. Vor bzw. bei Vollziehung wird i. d. R. mit der Erfüllung des Auskunftsanspruchs zu rechnen sein.⁵

- Verbindungsdaten werden von Free-Mail-Providern im Hinblick auf die Datenschutzbestimmungen nicht mehr (max.) 80 Tage aufgezeichnet, da sie keine Abrechnung vornehmen und daher keine Verbindungsdaten brauchen. Es wird allenfalls die IP-Nummer des letzten Log-Ins aufgezeichnet.

Diese zunehmend übliche Vorgehensweise der Provider steht mit dem Gesetzeswortlaut bzw. einer engen Auslegung⁶ der Bestimmungen im Einklang.

- Die Bestandsdaten (Adressen) werden von Free-Mail-Providern (GMX u.a.) nicht überprüft und können daher falsch sein.

⁵ Es erscheint m. E. nicht zweckmäßig, bei Weigerung des Providers, die Auskunft zu erteilen, aus Gründen der „Einfachheit“ einen Beschluss nach § 12 FAG einzuholen.

⁶ Vgl. die entsprechende Beurteilung des Datenschutz-Beauftragten in Baden-Württemberg: <http://www.baden-wuerttemberg.datenschutz.de/material-afd/internet-merkblatt.html>

6. Rechtliche Einordnung einzelner Fallbeispiele

6.1 Raubkopien

Software ist grundsätzlich urheberrechtlich geschützt.⁷ Jedenfalls bei in Deutschland nur kommerziell erhältlicher Anwendungssoftware bekannter Firmen (z. B. Microsoft, Adobe) oder bei Spielprogrammen, die in aktuellen Hitlisten vertreten sind, ist auch den (jugendlichen) Tätern bekannt, dass es sich um geschützte Software handelt.⁸

Die Herstellung von „Raubkopien“ (Vervielfältigungsstücke) stellt bei Software stets ein Vergehen dar, sofern die Vervielfältigung nicht durch den „bestimmungsgemäßen Gebrauch“ abgedeckt ist. Bei der Herstellung **einer** Sicherungskopie auch bei CD-ROM ist i. d. R. von bestimmungsgemäßer Nutzung auszugehen.⁹ Unzulässig ist allerdings, eine als Sicherungskopie bezeichnete Vervielfältigung zur Nutzung an Dritte weiterzugeben oder diese selbst – auf einem zweiten Rechner – zu installieren.¹⁰

Das Zur-Verfügung-Stellen von Software zum „Herunterladen“ auf eigenen Rechnern bzw. auf „Webspace“, der dem Täter zugewiesen ist, stellt ein Verbreiten dar (§ 69c Nr. 3 UrhG).

Das Setzen von Links kann als Beihilfehandlung gewertet werden. Hierzu ist aber eine genaue Erfassung und Beschreibung der umgebenden Texte¹¹ erforderlich, um die subjektive Seite darlegen zu können.¹² Auf § 5 TDG wird hingewiesen.

6.2 Computerbetrug

Unter diese Strafnorm fallen die Mehrzahl der statistisch erfassten Computer- oder IuK-Delikte. Dazu zählen die in den Beispielen genannten Fälle

⁷ Dazu im einzelnen Gruhl in Müller-Gugenberger/Bieneck, a.a.O., § 55 RN 94 ff.

⁸ Begriffe wie „warez“ deuten stets auf illegale Quellen hin.

⁹ Gruhl in Müller-Gugenberger/Bieneck, a.a.O., § 55 RN 95

¹⁰ Allerdings gestattet(e) z. B. Microsoft die zusätzliche Installation eines Anwendungsprogrammes auf einem transportablen PC (Notebook) des Nutzers, wenn eine Parallelbenutzung nicht stattfindet. Bei Betriebssystemen ist dies grundsätzlich unzulässig. Besonderheiten bestehen bei Freeware oder Public-Domain-Software. Beim Vertreib von Shareware können ggf. Vorsatzprobleme auftreten.

¹¹ Einfacher Link als Hypertextverknüpfung auf fremde Seite; Link auf eigene Seite; Inline-Link auf fremde Seite, so dass Text im eigenen Frame erscheint; bloße textliche Wiedergabe der URL ohne Hypertext-Funktion; textliche Beschreibung des fremden Angebots mit der Notwendigkeit der eigenen Recherche. Vorhandensein von distanzierendem (ernstgemeintem) Disclaimer.

¹² Vgl. Hoffmann, NJW 14/2001, S. 29*, 31*

- des Missbrauchs fremder Zugangsdaten zum Internet oder anderen Telekommunikationsleistungen,
- des Missbrauchs der EC-Karte.

Kein Computerbetrug liegt vor, wenn der Täter über das Internet Waren unter Verwendung fremder Daten bestellt und die Entscheidung über die Belieferung durch Mitarbeiter des Unternehmens erfolgt.¹³

6.3 Pay-TV

Der Missbrauch von Pay-TV-Karten ist ein „Paradebeispiel“ für die Schwierigkeiten der rechtlichen Beurteilung neuer Lebenssachverhalte. Wirtschaftlich wird die Tat dadurch gekennzeichnet, dass der Täter (selbst oder für Dritte) den unentgeltlichen Empfang von (digital oder analog ausgestrahlten) Fernsehsendungen ermöglicht und nutzt. Technisch steht im Vordergrund, dass ein Schutzmechanismus, nämlich die Verschlüsselung¹⁴ der gesendeten Daten, „geknackt“ wird.

Die nachfolgende Übersicht zeigt die denkbaren Zuordnungen der Tatbeiträge der Beteiligten.

Die Anwendung der Strafnormen zur Leistungerschleichung beim Kunden¹⁵ einerseits und des Ausspähens von Daten beim Hersteller andererseits erscheint am sinnvollsten.

¹³ Das Beispiel 2.3.2 Kreditkarte scheint nach der Presseberichterstattung eher ein Fall des klassischen Betrugs zu sein. Das im Vorfeld des Betrugs unternommene Sammeln von Daten könnte im Einzelfall ein Ausspähen von Daten darstellen.

¹⁴ Offen ist derzeit, ob die Entschlüsselung der auf DVD kodiert vorliegenden Informationen (Film) und die Speicherung auf anderen Datenträgern, z. B. CD-R, per se strafrechtlich relevant ist. Davon ist die Nutzung illegal erworbener Software zu trennen.

¹⁵ Praktisch erhält der Kunde – wie beim Kabelversehen – die Sendeleistung des Unternehmers ohne Zahlung des Entgelts. Jedenfalls bei permanenter Ausstrahlung sind Kabelfernsehen und Pay-TV-Fernsehen gleichwertig. Anders mag die Beurteilung bei „TV on demand“ ausfallen.

| Norm (StGB) | Hersteller | Händler | Nutzer | Bemerkung |
|---|--|------------------------|---|---|
| § 202a: Ausspähen von Daten | Ja (beim Auslesen der Berechtigungsinformationen aus der Smart-Card) | Nein | Nein | Strafantrag erforderlich, § 205 |
| §§ 259 ff.: Hehlerei | Nein | Nein | Nein | |
| § 261: Geldwäsche | Ja (Abs. 1 S. 2 Nr. 4a) | Ja | Ja | Vortat § 269 |
| § 263a: Computerbetrug | Nein (keine mittelbare Täterschaft oder Anstiftung; Beihilfe nur, wenn Haupttat hinreichend bestimmt und zumindest versucht) | Nein (vgl. Hersteller) | Fraglich (vgl. Tröndle/Fischer, StGB, 49 Aufl., § 263a RN 8b) | Unmittelbare Vermögensschädigung idR nicht gegeben; zu Gehilfenvorsatz vgl. „Sachverständigen-Entscheidung“ (Tröndle/Fischer, § 263 RN 46 a.E.); bejahend Scheffler, Das Strafrecht der Kryptographie (...), in Kilian/Heussen, Computerrechts-Handbuch |
| § 265a: Leistungserschleichung | Nein (vgl. § 263a) | Nein | Ja (vgl. Tröndle/Fischer, § 265a RN 1a, § 263a RN 8b) | S.a. Krause/Wuermeling, Mißbrauch von Kabelfernsehanschlüssen, NStZ 1990, 526 |
| § 267: Urkundenfälschung | Nein | Nein | Nein | Keine visuell sichtbare Erklärung |
| § 268: Fälschung technischer Aufzeichnungen | Nein | Nein | Nein | Input-, nicht Programmmanipulation (vgl. Tröndle/Fischer, § 268 RN 13b, Müller-Gugenberger/Richter, WiStrR, 3. Aufl., § 42 RN 57) |
| § 269: Fälschung beweisrelevanter Daten | Ja | Nein | Ja | |

| Norm (StGB) | Hersteller | Händler | Nutzer | Bemerkung |
|--|---|------------------------------|--------|---|
| cher Daten | | | | |
| § 17 II UWG: Verrat von Geschäfts- und Betriebsgeheimnissen | Ja (nein bei bloßer 1:1-Kopie; Becher/ Engels, CR 1999, 101, 102) | Ja (Nein, vg. Hersteller) | Nein | |
| § 108 I Nr. 8 UrhG: Unerlaubter Eingriff in verwandte Schutzrechte | Nein | Nein | Nein | Fraglich, ob Informationen auf der Smart-Card als Datenbank Schutz genießen |
| § 43 BDSG | Nein | Nein | Nein | |
| § 15 FAG (Betreiben einer Fernmeldeanlage) | Nein | Nein | Nein | OWi nach §§ 19 I Nr. 1, 26 FAG, sofern (private) WWW-Präsenz als meldepflichtige Telekommunikationsdienstleistung (§ 1 FAG) gewertet wird |

6.4 Markenrechtsverstöße

Das sog. Domain-Grabbing stellt eine Kennzeichenverletzung und (ggf.) versuchte Erpressung dar (LG München II, W 5 KLS 70 Js 12730/99).

6.4 Computersabotage

Der Einsatz von Viren o. ä. zur Durchsetzung finanzieller Interessen kann neben der Verwirklichung der Tatbestände nach §§ 303a, b StGB auch Nötigung oder Erpressung darstellen.

Die verstärkt auftretenden Fälle des Portscan sind dagegen strafrechtlich ohne Relevanz, da § 202a StGB eine Versuchsstrafbarkeit nicht vorsieht. Ein unmittelbares Ansetzen zu sonstigen IuK-bezogenen Taten liegt grundsätzlich beim einfachen Portscan nicht vor.

7. Ausland, Rechtshilfe

Es gelten die allgemeinen Kriterien - auch bei Online-Daten bzw. -Taten:

- Tatort in Deutschland
- Täter ist Deutscher
- Opfer ist Deutscher
- Weltrechtsprinzip

(vgl. BGH, NJW 2001, 624; Sieber, ZRP 2001, 97).

Insoweit sind Ermittlungen angezeigt. Zur Rechtshilfe und zu Ermittlungen im Ausland gelten die allgemeinen Regelungen. „Erleichterungen“ für IuK-Ermittlungen bestehen nicht.

Beim BKA ist der deutsche Kontaktbeamte für eilige Internet-Ermittlungen gemäß Vereinbarung G7/P8 angesiedelt. Er kann eingeschaltet werden im Vorfeld von Rechtshilfeersuchen, die folgen müssen. Über die deutsche Kontaktperson können Datensicherungen im Ausland

veranlasst werden, die bei dem Zeitbedarf einer üblichen Rechtshilfe vor Ort möglicherweise gelöscht worden sind.

8. Zuständigkeiten

Es gelten die Bestimmungen der §§ 158, 160, 161, 163 StPO. Danach ist jedes Strafverfolgungsorgan (Polizei / Staatsanwaltschaft) bei (dienstlicher) Kenntnis von Straftaten zu Ermittlungen berufen. Eine Konzentration bestimmter Ermittlungen am Sitz eines Providers im Falle des Missbrauchs von Zugangsdaten ist angezeigt (vgl. RiStBV: Sammelverfahren). Die örtliche Zuständigkeit richtet sich vorrangig nach dem Tatort, wobei bei IuK-Taten der Wohnort oftmals auch Tatort ist.

Verwiesen wird auf die Zuständigkeitsvereinbarung der Generalstaatsanwälte vom 22./23.11.2000, Nr. 12: **Ermittlungsverfahren wegen Missbrauchs der Zugangsdaten zum Internet** werden grundsätzlich von der Staatsanwaltschaft geführt, für deren Bezirk der Festnetztelefonanschluss, von dem aus die Einwahl erfolgte, erfolgte, registriert ist bzw. in deren Bezirk der Mobilfunkanschlussinhaber seinen Wohnsitz hat.

Bei Jugendlichen oder Heranwachsenden ist § 42 JGG einschlägig.

Soweit eine Anklage zum Landgericht erhoben werden soll, ist bei Computerbetrug nach § 74c GVG die Wirtschaftsstrafkammer zuständig, *sofern für die Beurteilung des Falles besondere Kenntnisse des Wirtschaftslebens erforderlich sind.*

9. Literatur

- **Allmendinger**, Probleme bei der Umsetzung namens- und markenrechtlicher Unterlassungsverpflichtungen im Internet, GRUR 2000, 966
- **Büchner** u.a. (Hg.), Beck'scher TKG Kommentar, 2. Aufl. 2000
- **Eißmann**, Sicherheit im Internet, Wikri-Info/09 LKA, 01/2001 (*Viren/Trojaner*)
- **Gora/Mann**, Handbuch Electronic Commerce, 2. Aufl. 2001
- **Haft/Eisele**, Zur Einführung: Rechtsfragen des Datenverkehrs im Internet, JuS 2001, 112 (*Entstehung des Internets; luKDG; TDDSG, SigG; TDG; Beispiele*)
- **Härting**, Internetrecht, 1999
- **Hoeren/Sieber**, Handbuch Multimedia-Recht, 1999
- **Hoffmann**, Entwicklung des Internet-Rechts, NJW, Beilage 14/2001
- **Kurtz/McClure/Scambray**, Das Anti-Hacker-Buch, 2000
- **Müller-Gugenberger/Bieneck**, Wirtschaftsstrafrecht, 3. Aufl. 2000
- **Satzger**, Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, CR 2001, 109 (*zu § 5 TDG, § 5 MDStV*)
- **Schmidt-Bogatzky**, Zeichenrechtliche Fragen im Internet, GRUR 2000, 959
- **Schneider**, Urheberrechtsverletzungen im Internet bei Anwendung des § 5 TDG, GRUR 2000, 969
- **BKA**, Internet-Kriminalität und elementare Internet-Ermittlungen, luK-Mitteilungsblatt 1/2000, Mai 1999
- **BKA**, Handbuch für Internet-Ermittlungen, luK-Mitteilungsblatt 1/01, Januar 2001; auch unter www.interpol.int
- Online-Informationen der Uni Saarbrücken: <http://www.jura.uni-sb.de/projekte/online/>

10. Autor

Staatsanwalt -GL- Jens Gruhl

Email: jens.gruhl@epost.de

Internet: <http://www.gruhl.de>

Konzept und HTML-Seiten erstellt mit *MindManager 4* - <http://www.mindjet.de>

Folien und Text-Dokument erstellt mit *MS Office 2000 (Word, PowerPoint)*