Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht

Christian Schwarzenegger*

* Prof. Dr. iur., Assistenzprofessor für Strafrecht, Strafprozessrecht und Kriminologie an der Universität Zürich.

Inhaltsverzeichnis

A. Dimensionen der Cyberkriminalität

I. Die Entwicklung und Bedeutung des Internet

Die Entwicklung des Internet beruht auf mehreren Innovationsleistungen der Technik. In den 60er Jahren wurden enorme Fortschritte in der Netzwerktechnik und der paketvermittelten Übertragung von Daten erzielt, welche den Grundstein für eine effiziente und kostengünstige Übertragung von grossen Datenmengen legten. In den 70er Jahren entwarfen Informatiker ein einheitliches Datenübertragungs- und Adressierungsprotokoll. Erst der globale Durchbruch des *Transmission Control Protocol* und des *Internet Protocol* (TCP/IP) als Netzwerkprotokolle gewährleistete die Interoperabilität zwischen verschiedenen Arten von Computern unabhängig ihrer Grösse, ihres Typs, ihres Herstellers oder ihres Betriebssystems. TCP und IP steuern die Datenübertragung und Adressierung im Internet und sind heute standardmässig in die Betriebssysteme aller Computer integriert. Die 80er Jahre brachten einen Innovationsschub im Bereiche der Computertechnik. Der Heim- und später der Laptopcomputer führten zu einem Computerboom in privaten Haushalten und am Arbeitsplatz. Und schliesslich trugen die kommerzielle Öffnung des Internet,[1] die multimedialen Nutzungsmöglichkeiten des World Wide Web und die Möglichkeit zur Verknüpfung von Webdokumenten durch Hyperlinks in den frühen 90er Jahren zum enormen Wachstum des Internet bei, was diesen Dienst auch für wirtschaftliche Anwendungen attraktiv machte. Seither wächst die Zahl der Internetnutzer und der ans Internet angebundenen Rechner exponentiell.[2]

Die international vernetzte Informationsgesellschaft ist soziale Realität geworden. Seit 1997 ist die Internetnutzung in der Schweiz stark angestiegen. Nutzten im Jahr 1997 erst rund 7 Prozent der Bevölkerung das Internet regelmässig, d.h. mehrmals pro Woche, war dieser Anteil zu Beginn des Jahres 2006 schon bei 60,6 Prozent. Zählt man auch Personen hinzu, die innerhalb der letzten 6 Monate mindestens einmal auf das Internet zugegriffen haben, so ergibt sich anfangs 2006 ein Anteil von 71,8 Prozent an der gesamten Wohnbevölkerung ab 14 Jahren (1997: 15 Prozent). Nach neuesten Erhebungen benutzt jede zweite Person ab 14 Jahren das Internet täglich.[3] Die Entwicklung verläuft im Ausland ähnlich.

---

1 Zur «Netzkultur», die vor der kommerziellen Öffnung entstanden war und die von einem Klima der Kreativität und Offenheit geprägt war *(free flow of information)* siehe THOMAS BÖCKENFÖRDE, Die Ermittlung im Netz. Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Tübingen 2003, S. 5 ff. m.N.

2 JONATHAN R. OKIN, The Internet revolution. The not-for-dummies guide to the history, technology, and use of the Internet. Winter Harbor 2005, S. 22 und S. 33.

3 BUNDESAMT FÜR STATISTIK (Hrsg.), Indikatoren zur Informationsgesellschaft, Stand 2007, ‹www.bfs.admin.ch/bfs/portal/de/index/themen/16/04.html›. Vgl. zu Deutschland WERNER RÜTHER, Phänomenologie der Internetdelinquenz – Ansätze, Probleme und Erkenntnisse zu ihrer gesellschaftlichen Definition und zu ihrer quantitativen Erfassung, in: Sandro Cimichella, André

Informationstechnologie, zu der die Hardware,[4] die Software zur automatischen Datenverarbeitung[5] und die Computernetzwerke – inklusive Internet – gezählt werden,[6] ist heute allgegenwärtig *(ubiquitous computing)* und nicht mehr auf Desktop- oder Laptopcomputer beschränkt. Geräte wie Mobiltelefone, digitale TV-Festplattenrecorder, multifunktionale Musikplayer, *Personal Digital Assistants* (PDA), Bordcomputer in Autos, Mikroprozessoren in Synthesizern usw. weisen gleichwertige digitale Datenverarbeitungskapazitäten auf *(pervasive computing).* Über Computernetzwerke, insbesondere das Internet, können Texte, Bilder, Sprache, Musik, Filme und andere multimediale Inhalte zwischen solchen Geräten effizient ausgetauscht werden. Die Infrastruktur des Internet lässt sich auf vielfältige Art und Weise nutzen. Neben die «klassischen» Kommunikationsdienste wie E-Mail, Mailing Lists, World Wide Web, Internet Relay Chat, Instant Messaging, Newsgroups, Voice over IP (Internettelephonie),[7] treten heute unter dem Stichwort Web 2.0 interaktivere Nutzungsmöglichkeiten in den Vordergrund.[8] Nutzer können sowohl in der aktiven Rolle eines massenmedialen Informationsanbieters (Website, Newsgroup-Beiträge, Podcasting, Videocasting usw.) als auch der passiven Rolle des reinen Informationskonsumenten auftreten. Teilweise treten sie gleichzeitig in beiden Rollen auf, wie etwa in simulierten Erlebniswelten wie *Second Life*[9] oder beim Datenaustausch in Peer-to-Peer-Netzwerken. Die Konvergenz der Verbreitungskanäle und die multime-

---

Kuhn und Marcel Alexander Niggli (Hrsg.), Neue Technologie und Kriminalität: Neue Kriminologie?, Zürich/Chur 2006, S. 85–117, S. 91 m.N.

4 Computer, Mikroprozessoren, Peripheriegeräte (Speichermedien, Ein- und Ausgabegeräte).

5 Informatik (Computersprachen, Codierung, Datenstruktur- und -organisation, Betriebssysteme, Applikationen).

6 Der Begriff der Informationstechnologie ist alles andere als klar und wird selten näher von der Kommunikationstechnologie abgegrenzt. Siehe Europäische Kommission, Grünbuch zur Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie und ihren ordnungspolitischen Auswirkungen, Ein Schritt in Richtung Informationsgesellschaft, KOM (97) 623 endg., S. 47: «Das Internet wird eher der Informationstechnologie und Softwareindustrie als dem Telekommunikationsbereich (dessen Infrastruktur es benutzt) zugerechnet.» Nach dem Schweizer Telekommunikationsrecht fällt jede fernmeldetechnische Übertragung von Informationen für Dritte – sei dies Sprach-, Rundfunk- (hier unter Vorbehalt spezifischer Regeln im Bundesgesetz über Radio und Fernsehen, siehe Art. 51 ff. RTVG) oder Datenübertragung – unter das Fernmeldegesetz, siehe Art. 2 FMG (SR 784.10 in der Fassung vom 1.4.2007). Die Infrastruktur des Internet wäre somit eigentlich zur Kommunikationstechnologie zu zählen. Jedenfalls nicht zur Letzteren gehören auch nach Schweizer Recht die Informations- und Mediendienste wie das Bereitstellen oder Bereithalten von Inhalten im Internet oder in anderen elektronischen Netzwerken, vgl. zu diesen rechtlichen Zuordnungsfragen schon Marcel Alexander Niggli und Christian Schwarzenegger, Strafbare Handlungen im Internet, SJZ 98 (2002), S. 61–73, S. 68.

7 Eine gute Übersicht über die Kommunikationsdienste des Internet findet sich in Böckenförde (Fn. 1), S. 37 ff. m.w.N. Zu den vielfältigen Anwendungsmöglichkeiten im WWW ausführlich Jonathan R. Okin, The information revolution. The not-for-dummies guide to the history, technology, and use of the World Wide Web, Winter Harbor 2005, S. 124 ff.

8 Tom Alby, Web 2.0, Konzepte, Anwendungen, Technologien, 2. Aufl., München 2007, S. 15 ff.

9 *Second Life* ist eine virtuelle dreidimensionale digitale Onlinewelt, die von den registrierten Personen – im Juni 2007 waren es rund 7 Mio. Menschen – selbst geschaffen und weiterentwickelt

dialen Einsatzmöglichkeiten neuerer Computergenerationen eröffnen also auch privaten, nicht-kommerziellen Akteuren ein neuartiges Mittel zur Produktion und globalen Verbreitung von Informationen.

II. Cyberkriminalität als negative Folgeerscheinung der Fortschritte in der Informations- und Kommunikationstechnologie

Welche Relevanz haben die «digitale Revolution» und das Aufkommen einer international vernetzten Informationsgesellschaft für das Strafrecht?

Zunächst ist auf die Banalität hinzuweisen, dass sich die Infrastruktur der Informations- und Kommunikationstechnologie (IKT) und insbesondere die Dienste des Internet auch für illegale und kriminelle Zwecke einsetzen lassen. Es wird in diesem Zusammenhang auf die mit technischen Innovationen häufig einhergehende Möglichkeit des *dual use* hingewiesen,[10] also auf die Einsetzbarkeit der Technik für gesellschaftlich oder wirtschaftlich nützliche ebenso wie für sozialschädliche Ziele. Die Phänomene der Cyberkriminalität[11] sind aus dieser Perspektive nichts anderes als ein Ausdruck des radikal veränderten Kommunikationsverhaltens und der dadurch erweiterten Gelegenheitsstrukturen.[12] Vinton G. Cerf, der zusammen mit Robert E. Kahn das TCP/IP-Protokoll entwickelte und daher als Gründervater des Internet gilt, vergleicht die Anwendungen des Internet zu Recht mit Papier. Es seien die Nutzer, die bestimmen würden, was auf das «leere Blatt» geschrieben werde. Insofern bilde das Internet wie ein Spiegel nur die Interessen der Nutzer ab, im Guten wie im Schlechten.[13] Die vielfältigen und zum Teil komplexen Erscheinungsformen der globalen Kommunikations- und Informationssysteme erschweren die rechtliche Erfassung und Einordnung.[14] Auch im Strafrecht bleibt gelegentlich unklar, ob

---

wird. In *Second Life* können sich die Teilnehmer eine eigene Persönlichkeit schaffen und andere Atavare kennenlernen. Siehe näher unter ‹http://secondlife.com›.

10 Illustrativ Matthias Kaiserswerth, Die Technik: Eine stete Quelle der Innovation und der Veränderung der Gesellschaft, in: Sandro Cimichella, André Kuhn und Marcel Alexander Niggli (Hrsg.): Neue Technologie und Kriminalität: Neue Kriminologie?, Zürich/Chur 2006, S. 47–63, S. 51 ff.

11 Die Begriffe Internet-, Cyber- und Netzwerkkriminalität werden hier als Synonyme verwendet. Genau genommen umfasst die Netzwerkkriminalität aber ein weiteres Deliktsspektrum, da sich die Internetkriminalität auf Delikte beschränkt, die in den auf dem TCP/IP-Protokoll basierenden Kommunikationsnetzen auftreten.

12 David S. Wall, Introduction, in: David S. Wall, (ed.), Cyberspace crime, Burlington/Dartmouth 2003, S. XV–XXVI, S. XV; Rüther (Fn. 3), S. 86. Vgl. allgemein zur Veränderung der situativen Bedingungen für die Begehung von Straftaten aufgrund technischer Innovationen und die Anpassungen des Strafrechts Martin Killias, Grundriss der Kriminologie. Eine europäische Perspektive. Bern 2002, N 756 ff., N 811 m.N.

13 Vinton G. Cerf, Internet – Mirror of mankind, Speech held at the Empire Club of Canada, Toronto, 14.11.2002, ‹www.empireclubfoundation.com/details.asp?FT=yes&SpeechID=2935›.

14 Christian Tietje, Medien, Telekommunikation und Informationstechnologien, in: Eberhard Grabitz und Meinhard Hilf (Hrsg.), Das Recht der Europäischen Union, Kommentar, Teil II, München 1999 (14. Ergänzungs-Lfg.), E. 27 N 5.

das Verhalten eines Inhaltsanbieters oder eines Nutzers unter eine der bestehenden, nicht spezifisch auf die Internetkriminalität ausgerichteten Strafbestimmungen fällt. Das Strafrecht macht aber vor dem Cyberspace nicht halt und kennt grundsätzlich keinen Unterschied zwischen Online- und Offline-Straftaten. Einen rechtsfreien Raum, in welchem alles zulässig wäre und ohne jede rechtliche Konsequenzen bleiben würde, gibt es im Internet nicht.[15]

> «Ich halte die Metapher des rechtsfreien Cyberspace für irreführend: Die Infrastruktur des Netzes ist lokal. Die Menschen, die es benutzen, befinden sich ebenso klar an einem Ort und damit in einem Rechtsraum.»[16]

Wer sich mit Netzwerkkriminalität auseinandersetzt, sieht sich mit einer grossen Vielfalt von Deliktsformen konfrontiert. Das Thema ist ausserdem eine strafrechtliche Querschnittmaterie, bei der sich nicht nur Fragen der Anwendbarkeit der besonderen Bestimmungen auf netzwerkspezifische Konstellationen stellen. Es gibt zahlreiche Probleme wie die Bestimmung der Strafhoheit bei internationalen Sachverhalten, die Beteiligung verschiedener Akteure oder die Anwendbarkeit der Sonderregelungen des Medienstrafrechts, die im Allgemeinen Teil des Strafgesetzbuches zu verorten sind. Insbesondere die Strafbarkeit der verschiedenen Internet Service Provider (ISP) oder Mobilfunkbetreiber für Delikte, die mit Hilfe ihrer Infrastruktur ausgeführt werden, steht immer wieder im Zentrum intensiver Debatten.[17] Neuartige Fragestellungen treten aber auch im Strafprozessrecht,[18] bei der Rechtshilfe in Strafsachen sowie in den angren-

---

15 Marcel Alexander Niggli und Christian Schwarzenegger, Internet – ein rechtfreier Raum?, in: Ursula Cassani, Renie Maag und Marcel Alexander Niggli (Hrsg.), Medien, Kriminalität und Justiz, Zürich/Chur 2001, S. 303 ff.

16 Vinton G. Cerf und Peter Sennhauser, Interview: «Jeder kann das Internet ausbauen», Tages-Anzeiger, 3. 10. 2005, 49.

17 Etwa im Rahmen des Weltgipfels über die Informationsgesellschaft (WSIS), siehe Bundesamt für Kommunikation (Hrsg.), Zum Stand der Informationsgesellschaft in der Schweiz 2006, Biel 2007, 27; zum Stand der Diskussion in der Schweiz Bundesamt für Justiz, Frage der strafrechtlichen Verantwortlichkeit von Internet-Access-Providern gemäss Art. 27 und 322bis StGB, Gutachten vom 24. Dezember 1999, VPB 64.75; Marcel Alexander Niggli, Franz Riklin und Günter Stratenwerth, Die strafrechtliche Verantwortlichkeit von Internet-Providern, Ein Gutachten, Medialex 2000 (Sonderausgabe), S. 3 ff.; Christian Schwarzenegger, E-Commerce – Die strafrechtliche Dimension, in: Oliver Arter und Florian S. Jörg (Hrsg.), Internet-Recht und Electronic Commerce Law, Lachen/St. Gallen 2001, S. 329–375, S. 346 ff.; Eidgenössisches Justiz- und Polizeidepartement (Hrsg.), Bericht der Expertenkommission «Netzwerkkriminalität», Bern 2003, S. 61 ff. je m.w.N. Der Bundesrat hat dem Parlament anfangs 2008 empfohlen, keine Sonderregelung für die strafrechtliche Verantwortlichkeit der Provider in das StGB aufzunehmen. Die Grenzen der Strafbarkeit sollen sich nach den Allgemeinen Bestimmungen des StGB richten und durch die Rechtsprechung entwickelt werden. Siehe Bundesrat, Netzwerkkriminalität, Strafrechtliche Verantwortlichkeit der Provider und Kompetenzen des Bundes bei der Verfolgung von Netzwerkdelikten, Bericht des Bundesrates, o.O. [Bern] 2008, 7 f.; vgl. die Themenseite des Bundesamtes für Justiz: ‹www.bj.admin.ch/bj/de/home/themen/kriminalitaet/gesetzgebung/netzwerkkriminalitaet.html›.

18 Z.B. betreffend Tatortermittlung und Zuständigkeit, Internetfahndung nach unbekannten Tätern, neue Methoden der Beweissicherung (Computerforensik), Überwachung des Fernmeldeverkehrs, verdeckte Ermittlung bzw. Online-Durchsuchung von Computern u.a.

zenden Gebieten des allgemeinen Polizeirechts und im Bereich des Schutzes der inneren Sicherheit[19] auf, wo es etwa um die Gefahrenabwehr durch Sperrverfügungen gegen Fernmeldediensteanbieterinnen geht.[20]

III. Arten und Ausmass der Cyberkriminalität

Cyber-, Internet- und Netzwerkkriminalität sind keine strafrechtlichen Begriffe. Sie wurden in der öffentlichen Diskussion insbesondere durch die massenmediale Berichterstattung geprägt und bezeichnen strafbare Handlungen, die in irgendeiner Art und Weise mit vernetzten Computersystemen zusammenhängen.

1. Netzwerkunterstützte und netzwerkfokussierte Deliktsformen

In der strafrechtlichen Literatur werden meistens zwei Grunddeliktstypen unterschieden:[21] Auf der einen Seite erleichtert die IKT-Infrastruktur die Begehung «herkömmlicher» Straftaten. Es handelt sich dabei um Delikte, die auch ausserhalb von Netzwerken auftreten, bei denen aber die IKT-Infrastruktur als neues, äusserst effektives und bequemes Tatmittel zum Einsatz kommt.[22]

---

19 Eine Revisionsvorlage zur Änderung des Bundesgesetztes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) sieht neue Überwachungsmöglichkeiten und eine geheime Durchsuchung von Computern bei Gefährdungen durch Terrorismus, verbotenem politischen und militärischen Nachrichtendienst und verbotenem Handel mit Proliferationsgütern vor (Art. 18*k*–18*m* E-BWIS). In Art. 18*o* Abs. 5 E-BWIS sind Löschverfügungen gegenüber Schweizer Hostprovidern und Sperrempfehlungen gegenüber inländischen Accessprovidern vorgesehen, wenn terroristisches oder gewaltextremistisches Propagandamaterial über das Internet verbreitet wird. Siehe Botschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) (Besondere Mittel der Informationsbeschaffung) vom 15. 6. 2007, BBl. 2007, 5037.

20 Weiterführend Christian Schwarzenegger, Sperrverfügungen gegen Access-Provider – Über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Oliver Arter und Florian S. Jörg (Hrsg.), Internet-Recht und Electronic Commerce Law. 3. Tagungsband, Bern 2003, S. 249–286 m.w.N.

21 United Nations (ed.), United Nations manual on the prevention and control of computer-related crime, International review of criminal policy nos. 43 and 44, New York 1994, 4; Bundesamt für Justiz (Hrsg.): Internet, Neues Medium – neue Fragen ans Recht – Bericht einer interdepartementalen Arbeitsgruppe zur strafrechtlichen, datenschutzrechtlichen und urheberrechtlichen Fragen rund um Internet, Bern 1996, S. 5; Eric Hilgendorf, Die Neuen Medien und das Strafrecht, ZStW 113 (2001), S. 650–680, S. 653 «Datennetzkriminalität»; Böckenförde (Fn. 1), S. 8 f. Eidgenössisches Justiz und Polizeidepartement (Fn. 17), S. 24 f.; Majid Yar, The novelty of cybercrime, An assessment in light of routine activity theory, European Journal of Criminology 2005, S. 407–427, S. 409; Rüther (Fn. 3), S. 99. Siehe zu den Erscheinungsformen der Internetkriminalität auch Ursula Widmer und Konrad Bähler, Rechtsfragen beim Electronic Commerce, Sichere Geschäftstransaktionen im Internet, 2. Aufl., Zürich 2000, S. 292 ff.; Bundesamt für Polizei (Hrsg.), «Cyberkriminalität», Die dunkle Seite der Informationsrevolution, Strategischer Analysebericht, o.O. [Bern] 2001, S. 3 ff.; Schwarzenegger (Fn. 17), S. 333 ff.; Rolf H. Weber, E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zürich 2001, S. 538 ff.

22 Böckenförde (Fn. 1), S. 9 «inhaltsspezifische Netzkriminalität»; Yar (Fn. 21), S. 409 m.N. *«computer-assisted crimes»;* Rüther (Fn. 3), S. 99 m.N. «Internetdelikte im weiteren Sinne».

Texte, Bilder und Videos mit strafrechtlich relevantem Inhalt können ebenso gut im persönlichen Kontakt, in Presseerzeugnissen, im Rundfunk oder auf postalischem Wege verbreitet bzw. bezogen werden. In dem Masse, wie sich die IKT-Nutzung in der Bevölkerung ausbreitet, nehmen jedoch entsprechende Veröffentlichungen, Verbreitungs- oder Beschaffungshandlungen in den Netzwerken zu. Wegen der tiefen Kosten, der globale Reichweite, der relativen Anonymität und der Bedienungsfreundlichkeit der IKT-Mittel sind die neuen Kommunikationswege besonders für derartige Straftaten geeignet. Das Deliktsspektrum reicht sehr weit. Auch eine Anstiftung oder eine psychische Gehilfenschaft zu einem Tötungsdelikt kann beispielsweise mittels einer E-Mail begangen werden,[23] ebenso eine erpresserische Drohung in einem Chat-Room, eine arglistige Täuschung auf einer Internet-Auktionsplattform und anderes mehr. Internet, Telefonfestnetz und Mobilfunknetz sind inzwischen so wichtig wie das Strassennetz, und wie dieses ermöglichen oder begünstigen diese Kommunikationsmittel die Begehung zahlreicher Straftaten.

Häufig genannte *netzwerkunterstützte Delikte* sind:[24]

- Gewaltdarstellungen (Art. 135 StGB),
- Betrug durch Phishing (Art. 146 StGB),
- unwahre Angaben über kaufmännische Gewerbe (Art. 152 StGB),
- Kursmanipulation (Art. 161bis StGB),
- Ehrverletzungen (Art. 173 ff. StGB),
- Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte (Art. 179^{quater} StGB),
- Missbrauch einer Fernmeldeanlage (Art. 179^{septies} StGB),
- weiche und harte Pornographie (Art. 197 StGB),
- sexuelle Belästigung (Art. 198 StGB),
- Anleiten zur Herstellung von Sprengstoffen und giftigen Gasen (Art. 226 StGB),
- öffentliche Aufforderung zu Verbrechen oder zu Gewalttätigkeit (Art. 259 StGB),
- Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB),
- Rassendiskriminierung (Art. 261bis StGB),
- Veröffentlichung amtlicher geheimer Verhandlungen (Art. 293 StGB),
- Verbreitung oder Kopieren eines urheberrechtlich geschützten Werkes (Art. 67 und 69 URG),
- Widerhandlung gegen Preisbekanntgabevorschriften bei Mehrwertdiensten (Art. 10 Abs. 1 lit. q, Art. 11, Art. 21 PBV i.V.m. Art. 24 UWG).

---

23 Vgl. etwa zu Suizidforen und der Planung von Doppel- oder Gruppensuiziden via Internetdienste Tim Pfeiffer-Gerschel et al., Suizid und Internet, Verhaltenstherapie 2005, S. 20–26 m.N.

24 Vgl. Eidgenössisches Justiz und Polizeidepartement (Fn. 17), S. 60 f.

Auf der anderen Seite bieten vernetzte Computersysteme und die IKT-Infrastruktur selbst Angriffsflächen für neue Kriminalitätsformen. Solche Delikte richten sich gegen Funktionen des Netzwerks und der daran angeschlossenen Computer, oder sie beeinträchtigen die in Übermittlung stehenden bzw. abgespeicherten Daten.[25]

Netzwerkfokussierte Delikte[26] charakterisieren sich dadurch, dass sie ohne die IKT-Infrastruktur nicht durchführbar wären. Es ist vor allem auf folgende Straftatbestände hinzuweisen:

- Unbefugte Datenbeschaffung (Art. 143 StGB),
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB),
- Datenbeschädigung inklusive Herstellung und Verbreitung von Computerviren (Art. 144bis StGB),
- Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB),
- Erschleichen einer Computerleistungen («Zeitdiebstahl», Art. 150 StGB),
- Nötigung durch Denial-of-Service-Attacken (Art. 181 StGB),
- Störung von Betrieben, die der Allgemeinheit dienen, bei schweren Beeinträchtigungen der Kommunikationsnetze (Art. 239 Ziff. 1 Abs. 1 StGB),
- Fälschen oder Unterdrücken von Informationen (Art. 49 FMG),
- Stören des Fernmeldeverkehrs und des Rundfunks (Art. 51 FMG),
- Spam, d.h. elektronische Massenwerbesendungen ohne direkten Zusammenhang mit einem angeforderten Inhalt (Art. 3 lit. o UWG i.V.m. Art. 23 UWG).

2. Weitere Differenzierungen der Deliktsformen

Bühler und Kronig differenzieren zwischen Delikten, «bei deren Begehung das Internet dem (häufig zeitlich kurzfristigen) Datentransfer dient»,[27] und solchen, «bei deren Begehung das Internet über eine gewisse zeitliche Dauer benützt

25 Böckenförde (Fn. 1), S. 8 f. «technikspezifische Netzkriminalität»; Yar (Fn. 21), S. 409 m.N. *«computer-focused crimes»;* Rüther (Fn. 3), S. 99 m.N. «Internetdelikte im engeren Sinne».

26 Eine weitgehende Übereinstimmung gibt es zum Begriff der Computerkriminalität, der jedoch insofern weiter greift, als er strafbare Handlungen gegen Rechner miteinschliesst, die nicht an ein Netzwerk angeschlossen sind *(stand-alone computer)*, vgl. zu begrifflichen Abgrenzungen Jan Vetter, Gesetzeslücken bei der Internetkriminalität, Hamburg 2003, S. 3 ff. m.N.; Eric Hilgendorf, Thomas Frank und Brian Valerius, Computer- und Internetstrafrecht, Ein Grundriss, Berlin u.a. 2005, S. 2 f.; Christa Pfister, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, Berlin u.a. 2008, S. 39 f. m.N.

27 Als Beispiele nennen die Autoren neben den Computerdelikten auch Urheberrechtsverletzungen, Verstösse gegen das Lotteriegesetz, die Verletzung des Fabrikations- oder Geschäftsgeheimnisses, den verbotenen Nachrichtendienst oder die Geldwäscherei, Hans-Ulrich Bühler und Philipp Kronig, Das derzeit mögliche Vorgehen gegen die Internet-Kriminalität, NZZ, 29.5.2001, S. B 15.

wird, indem Inhalte abrufbar gehalten werden.»[28] Allerdings ist weder das Kriterium der zeitlichen Dauer noch das Element des Datentransfers geeignet, die Erscheinungsformen der Netzwerkkriminalität sauber abzugrenzen, denn Computerdelikte wie die Verbreitung von Schadsoftware können dauerhaft wirken,[29] während etwa für ein E-Mail mit ehrverletzendem Inhalt nur ein kurzer Datentransfer notwendig ist.

Eine Enquete-Kommission des deutschen Bundestages teilt die Internetdelikte in drei Kategorien ein:

1. Delikte, welche die IT-Sicherheit, d.h. die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Daten schützen, was der Gruppe der netzwerkfokussierten Delikte entspricht;
2. Delikte gegen das Urheberrecht sowie weitere Immaterialgüterrechte (Markengesetz, Gebrauchsmustergesetz, Geschmacksmustergesetz, Patentgesetz) sowie die gewerbliche oder private Softwarepiraterie, die mittels Computer begangen werden. Diese Straftatbestände hätten eine vorwiegend wirtschaftliche Zielrichtung;
3. Delikte, bei denen sich der Täter des Computers lediglich als eines Tatwerkzeugs bedient, die aber auch ausserhalb von Informations- und Kommunikationsnetzen begangen werden können. Dazu werden v.a. die Äusserungsdelikte gezählt.[30]

Die Phänomene der Cyberkriminalität können noch weiter differenziert werden in Delikte gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen,[31] traditionelle computerbezogene Delikte,[32] inhaltsbezogene Delikte,[33] Delikte in Bezug auf die Verletzung des Urheberrechts und

28 Dazu zählen Gewaltdarstellungen, der Betrug, die Pornographie, Ehrverletzungsdelikte, die Rassendiskriminierung sowie auch Urheberrechtsverletzungen, Bühler und Kronig (Fn. 27), S. B 15. Ebenso Bundespolizei, Die strafrechtliche Verantwortung von Internet Service Providern, Positionspapier der Bundespolizei, o.O. [Bern] 2000, S. 2 f.

29 Z.B. die Infiltration eines Computers mit einem trojanischen Pferd.

30 Enquete-Kommission des Deutschen Bundestages, Globalisierung der Weltwirtschaft – Herausforderungen und Antworten, Schlussbericht, Bundes-Drucksache 14/9200, 12. 6. 2002, S. 280 f.

31 Beispiele: Hacking und andere Formen unbefugter Zugriffe auf ein Computersystem, unbefugtes Abfangen von Datenübertragungen, Datenbeschädigung, Datenspionage (unbefugte Datenbeschaffung), Computersabotage und Computererpressung.

32 Beispiele: Computerbezogener Betrug, computerbezogene Urkundenfälschung, Kontaktaufnahme mit Kindern und andere Formen der Online-Opfersuche zwecks späterer Deliktsbegehung, Lebensgefährdung durch Angriffe auf Computersysteme von Krankenhäusern, Verkehrskontrollzentren und Atomkraftwerken.

33 Beispiele: Kinderpornographie, Rassendiskriminierung, Hassdelikte und Verherrlichung der Gewalt, Anstiftung, Beihilfe und Vorbereitungshandlungen zu Straftaten, Cyberstalking, Ehrverletzungen und Verbreitung falscher Informationen via Internet, Beschädigung von Websites, Internetglücksspiel.

verwandter Schutzrechte[34] sowie strafrechtlich relevante Verletzungen[35] der Privatsphäre.[36]

3. Ausmass der Cyberkriminalität

Die kriminalstatistische Erfassung der Cyberkriminalität ist mit besonderen Schwierigkeiten verbunden. Viele Delikte bleiben von den Betroffenen unbemerkt oder werden nicht als strafbar «eingestuft».[37] Dies schlägt sich in einem grossen Dunkelfeld nieder, das mit den herkömmlichen Erhebungsmethoden – zu denken ist an Opfer- oder Täterbefragungen – kaum zu erhellen ist. Cyberkriminalität ist wegen ihrer häufig grenzüberschreitenden Dimensionen sowie der Virtualität und Anonymität der Interaktionen im Cyberspace auch schwer räumlich zu verorten. Soll man beispielsweise die weltweite Verbreitung eines Computervirus nur am Ausführungsort statistisch erfassen? Oder soll das Delikt in jedem Land, wo ein Computersystem effektiv beeinträchtigt wurde, zählen?[38] Betroffene Unternehmen sind häufig zurückhaltend mit Strafanzeigen, weil sie einen Imageverlust befürchten oder kein Vertrauen in die Möglichkeiten der Strafverfolgungsbehörden haben. Zu beachten ist ausserdem, dass Anstrengungen zur Verbesserung der Strafverfolgung in der Kriminalstatistik automatisch zu mehr registrierten Delikten führen. Was als dramatischer Kriminalitätsanstieg erscheinen mag, spiegelt dann vielmehr eine Intensivierung der Strafverfolgung.

> «Die Aufgabe, einen kriminologischen Vortrag zu halten, welcher die Fragestellung nach Umfang und Entwicklung der modernen «Kriminalität begangen mittels neuer Technologien» behandeln soll, gleicht in vielerlei Hinsicht dem Ansinnen, eine Vielzahl von sich ständig bewegenden Bällen und mehr oder weniger aufgeblasenen Ballons in einem riesigen Gefäss festhalten und (be)greifen zu wollen.»[39]

34 Unbefugte Vervielfältigung und Nutzung von Computerprogrammen, Musik, Filmen, Datenbanken, Texten, Domainnamen und anderen Websites (Framing).

35 Unbefugter Zugriff auf personenbezogene Daten, unbefugte Erfassung von personenbezogenen Daten, unbefugte Verbreitung und Verknüpfung von personenbezogenen Daten.

36 So die Differenzierung mit Beispielen in Ulrich Sieber, The threat of cybercrime, in: Council of Europe (ed.), Organised crime in Europe: the threat of cybercrime. Situation report 2004, Strasbourg 2005, S. 81–240, S. 87 ff. m.w.N.

37 Pfister (Fn. 26), S. 62 f. m.N.

38 Vgl. zum berühmten I-Love-You-Virus, das sich am 4. Mai 2000 weltweit verbreitete und geschätzte Schäden von 1 Mia. $ verursacht haben soll, Schwarzenegger (Fn. 17), S. 339 f. m.N.

39 Rüther (Fn. 3), S. 99.

Tabelle 1: Polizeilich erfasste computer- und netzwerkfokussierte Delikte (Kanton Zürich, 1996–2006)[40]

Jahr	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
Art. 143, 143bis und 144bis	8	38	11	19	40	25	49	81	88	40	73
Art. 147	786	1162	1612	1673	2100	3410	6315	6247	3406	3234	4586

In der Schweiz werden nur wenige Internetdelikte polizeilich registriert, und nur vereinzelt enden sie mit einer Verurteilung (siehe Tabellen 1 und 2). Im Übrigen betreffen die Verurteilungen wegen betrügerischen Missbrauchs einer Datenverarbeitungsanlage nur zu einem geringen Teil Netzwerkdelikte. In der Mehrzahl der Fälle handelt es sich um Missbräuche von Zahlungskarten bei Bankomaten.[41]

Tabelle 2: Verurteilungen wegen computer- und netzwerkfokussierten Delikten (Schweiz, 1995–2006)[42]

Jahr	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
Art. 143	1	2	2	2	4	4	4	14	7	10	5	9
Art. 143bis	0	1	0	1	1	2	4	1	5	2	5	5
Art. 144bis	14	17	12	12	11	3	5	8	6	8	9	12
Art. 147	52	222	375	396	425	447	433	481	554	655	561	687

Aus diesen amtlichen Datenerfassungen wird ersichtlich, dass die Strafverfolgung im Bereich der Computer- und Internetkriminalität noch nicht sehr wirksam ist. Dies vor allem gemessen an den Schäden und Gefahren, die beispielsweise mit dem Hacking oder der Verbreitung von Computerviren verbunden sind.[43] Ähnliche Defizite sind auch in den Bereichen der harten und weichen Pornographie, der Rassendiskriminierung und der Musik-, Software- und Filmpiraterie zu erkennen.

Das kriminalstatistische Bild wird ergänzt durch die Fälle von Cyberkriminalität, die von der Bevölkerung an die Koordinationsstelle zur Bekämpfung

40 Quelle: KANTONSPOLIZEI ZÜRICH, KRISTA, 1997–2007. Eine gesamtschweizerische Erfassung der polizeilich bekannt gewordenen Delikte existiert noch nicht. Der Kriminalitätsanteil des Kantons Zürich macht ca. einen Drittel aller in der Schweiz registrierten Straftaten aus.

41 BUNDESAMT FÜR POLIZEI (Fn. 21), S. 12; PFISTER (Fn. 26), S. 59.

42 Quelle: BUNDESAMT FÜR STATISTIK, Strafurteilsstatistik, ‹www.bfs.admin.ch/bfs/portal/de/index/themen/19/03/03/key/straftaten/delikte_im_einzelnen.html›.

43 Vgl. die Diskrepanz zwischen diesen Daten und jenen einer Befragung von Unternehmen, in welcher 9% der Unternehmen in den letzten zwölf Monaten eine Sicherheitsverletzungen ihrer IKT-Infrastruktur festgestellt hatten. Darunter gaben 83% an, keine rechtlichen Schritte unternommen zu haben. KPMG, global e.fr@ud.survey. o.O. 2001, S. 2, ‹www.kpmg.cz/dbfetch/52616e646f6d495668cb721aa0843d2f4fe3c78eb279a1f7/global.efraud›.

der Internetkriminalität (KOBIK) gemeldet werden.[44] Von den 6329 Meldungen, die im Jahre 2006 bei KOBIK eingegangen sind, betrafen 24,3 Prozent Verdachtsmomente wegen Kinderpornographie (Art. 197 Ziff. 3 StGB). Am zweithäufigsten waren Meldungen wegen Spam-Mails mit 23,8 Prozent, an nächster Stelle folgen Hinweise auf Sachverhalte im Zusammenhang mit anderen Formen von Pornographie (9,6 Prozent). Die Prozentanteile blieben über die letzten vier Jahre ungefähr gleich. Sie reflektieren die unterschiedliche Bedeutung, welche den Internetdelikten in der Öffentlichkeit zukommt, nicht aber ihre tatsächliche Verbreitung. Als Hauptprobleme werden in der Bevölkerung die Pornographie und die Spam-Mails angesehen, während Meldungen von netzwerkfokussierten Delikten sehr selten bleiben (Hacking 0,3 Prozent; Datenbeschädigung inkl. Computerviren 0,2 Prozent).[45]

Die Lageberichte der Melde- und Analysestelle Informationssicherung (MELANI) erläutern demgegenüber die zunehmenden Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Die Formen der Cyberkriminalität passen sich sehr schnell an die Sicherungsmassnahmen der betroffenen Privaten, Behörden und Unternehmen an. So haben im ersten Halbjahr 2007 *Phishing*-Angriffe abgenommen, die mittels E-Mails und Links auf gefälschte E-Banking-Portale Passwörter und Streichlistennummern ausforschen helfen. Neu werden die Rechner der Nutzer direkt mit Schadprogrammen *(Malware)* infiziert, welche verdeckt aktiv werden, wenn der Nutzer eine Verbindung mit seinem E-Banking-Portal aufbaut. Bevor die Transaktionseingaben des Nutzers verschlüsselt über das Internet an die Bank gelangen, verändert das «trojanische Pferde» die Kontonummer, den Empfängernamen und Betrag. Die Antwort der Bank wird abgefangen und im Browser ein gefälschter Abschluss der Überweisung angezeigt. In Wahrheit erfolgt die Zahlung an einen anderen Empfänger.[46] Gemäss MELANI hat sich ein Untergrundmarkt für cyberkriminelle Dienstleistungen etabliert, der sich inzwischen in der Konsolidierungsphase befinde. Die Täter würden sich auf *Phishing*-Angriffe und Finanzdiebstähle mit *Malware* spezialisieren. Nach neuesten Schätzungen sei mit Cyberkriminalität inzwischen mehr Geld zu verdienen als im internationalen Drogengeschäft.[47]

Expertenbefragungen in der IKT-Industrie bzw. bei Systemadministratoren bestätigen diese Feststellungen. Im Januar 2006 führte IBM in 17 Ländern eine

---

44 Siehe ‹www.kobik.ch›. Weiterführend zu den Aufgaben von KOBIK Philipp Kronig und Eva Bollmann, Die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK), in: Christian Schwarzenegger, Oliver Arter und Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 19–54.

45 KOBIK, Jahresbericht 2006, o.O. [Bern] o.J. [2007], S. 4 f. Die Jahresberichte 2003–2006 sind abrufbar unter: ‹www.kobik.ch/reports.php?language=de›.

46 MELANI, Informationssicherung, Lage in der Schweiz und international, Halbjahresbericht 2007/I (Januar–Juni), o.O. [Bern] o.J. [2007], S. 6 ff. Die Lageberichte 2005–2007 sind abrufbar unter: ‹www.melani.admin.ch/dokumentation/00123/00124/index.html?lang=de›.

47 MELANI (Fn. 46), S. 11 m.N.

telephonische Befragung von leitenden IT-Mitarbeitern internationaler Unternehmen durch (N = 3002). Dabei zeigten sich 63 Prozent der IT-Verantwortlichen in deutschen Unternehmen überzeugt, die Cyberkriminalität stelle eine grössere Bedrohung für die eigene Firma dar als die herkömmlichen Delikte wie etwa Einbruch, Diebstahl, Korruption oder Betrug. Weltweit betrug dieser Anteil 40 Prozent. Die Mehrheit der Experten (58 Prozent weltweit; 74 Prozent in Deutschland) glauben, dass die Internetkriminalität ihren Unternehmen einen grösseren Schaden zufügen könne als herkömmliche Kriminalitätsformen. Die Schäden würden sich vor allem in Einnahmeverlusten, Ruf- und Markenschädigungen und dem Verlust von Kundenbeziehungen bemerkbar machen. Sowohl in Deutschland (88 Prozent) als auch in den anderen Ländern (84 Prozent) sind die IT-Verantwortungsträger der Ansicht, dass Internetdelikte kaum mehr von einzelnen Hackern verübt würden, sondern vielmehr von organisierten Gruppen mit entsprechendem technischen Know-how. Mehr als die Hälfte der Befragten (59 Prozent weltweit; 65 Prozent in Deutschland) schätzen das Schutzniveau ihrer IKT-Infrastruktur als ausreichend ein, gleichzeitig wird die ungenügende Strafverfolgung der organisierten Internetkriminalität kritisiert (60 Prozent weltweit; 48 Prozent in Deutschland). Die Studie gibt auch Aufschlüsse über die von den Unternehmen getroffenen Sicherheitsmassnahmen.[48]

Wie stark das Bild der amtlichen Statistiken vom Anzeigeverhalten der Opfer abhängt, zeigt ein Beispiel aus dem Jahr 2005. Innerhalb eines halben Jahres gingen damals rund 20 000[49] Strafanträge wegen illegaler Kopien von Musik, Software und Computerspielen bei der Karlsruher Generalstaatsanwaltschaft ein. Dahinter stand die systematische Ermittlung der IP-Adressen von Personen, die solche urheberrechtlich geschützten Werke über P2P-Netzwerke angeboten hatten, durch eine Schweizer Anti-Piraterie-Unternehmung.[50] Nur durch eine Strafanzeige können die Geschädigten an die Personendaten der Täter gelangen.[51]

> «Ergebnis: Der Tausch von Musik über Filesharing-Netzwerke ist *die größte Massenstraftat, die es je in Deutschland gegeben hat.* Die von der Musik- und der Spieleindustrie aktuell verfolgten 43 500 deutschen Tauschbörsen-Nutzer sind nur die Spitze des Eisbergs. Haupttatort für die Straftaten ist nach Angaben der Medienindustrie das

48 Eine Zusammenfassung des IBM B2B Security Surveys ist abrufbar unter: ‹www.ibm.com/news/de/de/2006/03/13.html›.

49 Die Zahlenangaben variieren zwischen 16 000 und 40 000 Strafanzeigen!

50 Siehe ‹www.logistepag.com›.

51 Die Staatsanwaltschaft eröffnet in jedem einzelnen Fall ein Ermittlungsverfahren und verlangt von den Providern Auskunft, wem in der fraglichen Zeit die genannte IP-Adresse zugewiesen war. Siehe weiterführend Ralf Dietrich, Rechtliche Bewältigung von netzbasiertem Datenaustausch und Verteidigungsstrategien – 20 000 Verfahren gegen Filesharingnutzer, NJW 2006, S. 809–811, S. 809; Rüther (Fn. 3), S. 104 f.; Simon Markus Beck und Wolfgang Kreissig, Tauschbörsen-Nutzer im Fadenkreuz der Strafverfolgungsbehörden, NStZ 2007, S. 304–309, S. 305; siehe auch Heise-Newstickers vom 26. 1. 2006 ‹www.heise.de/newsticker/Generalstaatsanwaltschaft-klagt-ueber-ungebremste-P2P-Strafanzeigen-Maschine–/meldung/68882›.

> Kinderzimmer. Auch wenn zahlreiche Rechtsfragen noch ungeklärt sind, müssen die Betroffenen voraussichtlich mit enormen straf- und zivilrechtlichen Konsequenzen rechnen. Politik und Wissenschaft sollten sich diesem Phänomen des digitalen Zeitalters stellen und über alternative Lösungsmodelle nachdenken.»[52]

Dieser Überblick über die Arten und das Ausmass der Cyberkriminalität verdeutlicht, wie breit gefächert der Untersuchungsgegenstand ist. Es würde den Rahmen der Untersuchung sprengen, alle dogmatischen Fragen – noch dazu in internationaler Perspektive – aufzuarbeiten. Nach einer Einführung in die verschiedenen Ebenen der Internationalisierung und Strafrechtsharmonisierung (Abschnitt B) werden die Auswirkungen dieser Entwicklungen auf die schweizerische Kriminalpolitik beispielhaft anhand der Delikte gegen Urheberrechte und verwandte Schutzrechte dargestellt (Abschnitt C), welche durch einen Bundesbeschluss über die Genehmigung von zwei Abkommen der Weltorganisation für geistiges Eigentum und eine Teilrevision des Urheberrechtsgesetzes (URG) dem internationalen Schutzniveau angepasst wurden. Das revidierte URG ist am 1. Juli 2008 in Kraft getreten (AS 2008, 2421 und 2497).

B. Internationale Vorgaben im Bereich der Cyberkriminalität – Konsequenzen für die schweizerische Kriminalpolitik

I. Die verschiedenen Regelungsebenen

Da das Internet grenzenlos ist, haben viele der weiter oben beschriebenen netzwerkunterstützten und -fokussierten Delikte eine internationale Dimension. In Zeiten technischer und wirtschaftlicher Globalisierung schwindet die Durchsetzungsmacht des Nationalstaates.[53] Dies wird besonders deutlich im Bereiche der Internetkriminalität. Eine klare internationale Abgrenzung der Strafhoheit im Internet, ein effizientes Auslieferungs- und Rechtshilferecht sowie eine Harmonisierung der materiellrechtlichen Strafnormen haben in den letzten 15 Jahren wesentlich an Aktualität gewonnen und stehen nunmehr auf der Agenda mehrerer internationaler Organisationen und Regierungstreffen.

1. Initiativen im Rahmen der G-8-Staaten

Bezeichnend für diese Entwicklung ist die Schlusserklärung des G-8-Gipfeltreffens in Birmingham vom 17. Mai 1998. Im Abschnitt über die Bekämpfung von Drogen und internationaler Kriminalität hielten die Staatsoberhäupter folgenden Beschluss in Bezug auf *high tech crime* fest:

---

52 Christian Solmecke, Filesharing – Straf- und zivilrechtliche Konsequenzen, MMR 2006, S. XIII–XIV, S. XIV (meine Hervorhebung).

53 Vgl. allgemein Ulrich Beck, Was ist Globalisierung? Irrtümer des Globalismus – Antworten auf Globalisierung, 3. Aufl., Frankfurt a.M. 1997.

> We agree to implement rapidly the ten principles and ten point action plan agreed by our Ministers on high tech crime. We call for close cooperation with industry to reach agreement on a legal framework for obtaining, presenting and preserving electronic data as evidence, while maintaining appropriate privacy protection, and agreements on sharing evidence of those crimes with international partners. This will help us combat a wide range of crime, including abuse of the internet and other new technologies.[54]

Die zehn Grundprinzipien der G-8 zur Bekämpfung der High-Tech-Kriminalität lauten:[55]

I. Es darf keine Zufluchtsorte für jene geben, die Informationstechnologien missbrauchen.
II. Die Ermittlung und Verfolgung internationaler High-Tech-Kriminalität muss zwischen allen betroffenen Staaten koordiniert werden, unabhängig davon, wo der Schaden eingetreten ist.
III. Das Strafverfolgungspersonal muss ausgebildet und ausgerüstet werden, um der High-Tech-Kriminalität begegnen zu können.
IV. Die Rechtssysteme müssen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen vor unbefugten Beeinträchtigungen schützen und sicherstellen, dass schwere Missbräuche bestraft werden.
V. Die Rechtssysteme sollten die [Beweis-]Sicherung von und den schnellen Zugriff auf elektronische Daten ermöglichen, welche oft von entscheidender Bedeutung für eine erfolgreiche Untersuchung sind.
VI. Gegenseitige Rechtshilfevereinbarungen müssen die rechtzeitige Erfassung und den rechtzeitigen Austausch von Beweismitteln in Fällen von internationaler High-Tech-Kriminalität sicherstellen.
VII. Der grenzüberschreitende Zugriff der Strafverfolgung auf öffentlich zugängliche (open source) Informationen erfordert keine Genehmigung durch den Staat, wo die Daten liegen.
VIII. Forensische Standards für den Abruf und die Authentifizierung elektronischer Daten für den Gebrauch in der Strafermittlung und -verfolgung müssen entwickelt und angewendet werden.
IX. Soweit machbar sollten Informationen und Telekommunikationssysteme so konzipiert werden, dass sie die Verhinderung und die Feststellung von Netzwerkmissbrauch vereinfachen. Sie sollten auch die Fahndung nach den Tätern und die Beweissammlung erleichtern.
X. Die Arbeit in diesem Gebiet sollte koordiniert werden mit der Arbeit in anderen einschlägigen internationalen Foren, um Doppelspurigkeiten zu verhindern.

---

54 G-8, The Birmingham summit: Final communique, Birmingham 17 May 1998, No. 21.

55 Justice and Interior Ministers of the Eight, Communiqué, Washington, D.C., December 9–10, 1997, Annex, ‹www.usdoj.gov/criminal/cybercrime/g82004/97Communique.pdf›.

Es handelt sich um eine gemischte Zielsetzung, die einerseits eine Harmonisierung nationaler Strafrechtsordnungen anstrebt, damit mindestens die gravierenden Formen der Cyberkriminalität angemessen sanktioniert werden können. Ebenso wichtig sind aber die schnelle, unkomplizierte Beweissicherung und Ermittlungstätigkeit durch Spezialisten, die über adäquate technische Hilfsmittel verfügen, international vernetzt sind und durch griffige Instrumente internationaler Rechts- und Amtshilfe in Strafsachen unterstützt werden.[56] Aus dem Kreis der G-8-Staaten ging beispielsweise die Initiative für ein 24/7-Kontaktnetz zur Erleichterung der internationalen Zusammenarbeit bei der Verfolgung von Internetkriminalität aus, das sich derzeit auf 50 Länder erstreckt und in der Zwischenzeit mit den Kontaktpunkten gemäss Convention on Cybercrime (Art. 35 CCC) koordiniert wurde.[57] Bei dieser grundsätzlichen Zielsetzung ist es bis heute geblieben, wobei die für eine internationale Harmonisierung bedeutsamen Deliktsbereiche in den verschiedenen internationalen Organisationen mehrere Ergänzungen erlebten.

2. Initiativen im Rahmen der Vereinten Nationen

Verschiedene Gremien der Vereinten Nationen haben sich mit Aspekten der Cyberkriminalität befasst. Die Berichte dokumentieren die Fortschritte in der Gesetzgebung und internationalen Zusammenarbeit, sind aber nicht direkt auf die Schaffung eigenständiger Harmonisierungsinstrumente ausgerichtet. Die Generalversammlung hat mehrere Resolutionen zum Thema Cyberkriminalität und -sicherheit verabschiedet:[58]

- Eine Resolution vom 4. Dezember 2000,[59] welche die Koordinations- und Kooperationsanstrengungen einiger Mitgliedstaaten begrüsst und Empfehlungen für die Verbesserung der internationalen Zusammenarbeit abgibt. Eine 15-köpfige Expertengruppe wird eingesetzt, um eine Problemanalyse vorzulegen.
- Eine Resolution vom 19. Dezember 2001,[60] welche die Mitgliedstaaten u.a. daran erinnert, Massnahmen gemäss Resolution 55/63 zu realisieren, und sie auf die Convention on Cybercrime aufmerksam macht.

---

56 Michael A. Sussmann, The critical challenges from international high-tech and computer-related crime at the millennium, Duke Journal of Comparative & International Law 1999, S. 451–489, S. 457 ff. m.w.N.

57 Council of Europe, Economic Crime Division, Project on cybercrime, Progress report, Strasbourg 2007, 24.

58 Weiterführend zu diesen und früheren UN-Resolutionen Judge Stein Schjølberg und Amanda M. Hubbard, Harmonizing national legal approaches on cybercrime, ITU Doc. CYB/04, Geneva 2005, 6.

59 United Nations, General Assembly, Resolution 55/63. Combatting the criminal misuse of information technologies, 22 January 2001, A/RES/55/63.

60 United Nations, General Assembly, Resolution 56/121. Combatting the criminal misuse of information technologies, 23 January 2002, A/RES/56/121.

- Eine Resolution vom 20. Dezember 2002,[61] welche vor allem Empfehlungen zur Verbesserung der Netzwerksicherheit enthält.
- Eine Resolution vom 23. Dezember 2003,[62] welche die Mitgliedstaaten auffordern, einen elf Punkte umfassenden Massnahmenkatalog gegen Cyberkriminalität umzusetzen. Die Liste ist in vielen Punkten mit Grundsatzprogramm der G-8 identisch.

Von Bedeutung sind ausserdem:
- Ein Bericht des Generalsekretariats über Massnahmen zur Prävention und Kontrolle von Computerkriminalität (2002),[63] welcher allgemeine Trends der internationalen Kriminalpolitik im Bereiche der Cyberkriminalität und alle Aktivitäten der UNO zusammenfasst.
- Ein Workshop über Massnahmen zur Bekämpfung von Computerdelikten anlässlich des 11th UN Congress on Crime Prevention and Criminal Justice (2005),[64] welcher in seinen Empfehlungen einen breiten Ansatz vorschlägt, der neben Strafrecht, Strafverfahren und Strafuntersuchung auch technische Aspekte der Internetsicherheit, die Beratung der Bevölkerung und den Einbezug der IKT-Industrie umfassen sollte.
- Einen Bericht einer intergouvernmentalen Expertengruppe zur Vorbereitung eine Studie über Betrug und den kriminellen Missbrauch und die Fälschung der Identität in elektronischen Netzwerken (2007).[65]

Am 19. Januar 1999 verabschiedete eine Expertenkommission der UNESCO eine Deklaration und einen Aktionsplan gegen sexuellen Missbrauch von Kindern, Kinderpornographie und Pädophilie auf dem Internet, mit welchen ein resolutes Vorgehen gegen diese Deliktsformen gefordert wurde.[66]

Im Rahmen der UN-Sonderorganisation der Internationalen Fernmeldeunion (ITU) wird derzeit an einem *ITU Toolkit for Cybercrime Legislation (Model*

61 United Nations, General Assembly, Resolution 57/239. Creation of a global culture of cybersecurity, 31 January 2003, A/RES/57/239.

62 United Nations, General Assembly, Resolution 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 30 January 2004, A/RES/58/199.

63 United Nations, Economic and Social Council, Effective measures to prevent and control computer-related crime, Report of the Secretary-General, 29 January 2002, E/CN. 15/2002/8.

64 United Nations, Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Workshop 6: Measures to combat computer-related crime, Background paper, 14 March 2005, A/CONF.203/14.

65 United Nations, Economic and Social Council, Results of the second meeting of the intergovernmental group to prepare a study on fraud and the criminal misuse and falsification of identity, Report of the secretary-general, 2 April 2007, E/CN. 15/2007/8.

66 UNESCO, Protecting children online, Final report, declaration and action plan, Paris 1999, ‹http://unesdoc.unesco.org/images/0011/001194/119432eo.pdf›.

Cybercrime Law) gearbeitet, das 2008 vorgelegt werden soll.[67] Dieses Modellgesetz will – wie schon der Entwurf eines Modellgesetzes gegen Spam[68] – eine globale Harmonisierung der Straftatbestände der Cyberkriminalität herbeiführen und in erster Linie Entwicklungsländer dabei unterstützen, einen tragfähigen Rechtsrahmen zu realisieren. Die ITU bietet ausserdem ein vollständiges Arbeitsprogramm für Cybersicherheit an und analysiert regelmässig den Stand der nationalen Gesetzgebungen im Bereich der Cyberkriminalität. Die ITU gehört heute neben dem Europarat und der Europäischen Union zu den treibenden Kräften einer internationalisierten *cybercrime policy.*

International haben aber zwei Rechtsakte einer anderen UN-Sonderorganisation die grösste Harmonisierungswirkung entfaltet. Es handelt sich dabei um die zwei schon erwähnten Abkommen der Weltorganisation für geistiges Eigentum (WIPO), einerseits um den WIPO-Urheberrechtsvertrag (WCT), andererseits um den WIPO-Vertrag über Darbietungen und Tonträger (WPPT).[69]

3. Initiativen im Rahmen des Europarates

Am 13. September 1989 legte das Ministerkomitee des Europarats eine Empfehlung über Computerdelikte vor,[70] in welcher auf die Wichtigkeit einer angemessenen und schnellen Reaktion der nationalen Gesetzgeber auf die damals neuen Herausforderungen der Computerkriminalität hingewiesen wurde. Die Empfehlung verwies auf Leitlinien betreffend die Definition bestimmter Computerstraftaten, die von einem *European Committee on Crime Problems* ausgearbeitet worden waren. Seither ergriff der Europarat mehrfach die Initiative zur Harmonisierung der strafrechtlichen Rahmenbedingungen im Bereiche der Informationstechnologie.[71] Gestützt auf die früheren Empfehlungen und weitere Untersuchungen kam der Lenkungsausschuss für Strafrechtsfragen des Europarates (CDPC) zum Schluss, dass ein verbindliches internationales Regelwerk

---

67 International Telecommunication Union, ITU cybersecurity work programme to assist developing countries, 2007–2009, Geneva 2007, 24 f. ‹http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf›.

68 Siehe dazu Derek E. Bambauer, John G. Palfrey und David E. Abrams, A comparative analysis of spam laws: The quest for a model law, Geneva 2005.

69 Dazu unten C.III.2, S. 447.

70 Council of Europe, Committee of Ministers, Recommendation No. R (89) 9 on computer-related crime, 13 September 1989.

71 Hinzuweisen ist vor allem auf Council of Europe, Committee of Ministers, Recommendation No. R (88) 2 on measures to combat piracy in the field of copyright and neighbouring rights, 18 January 1988; Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, 7 February 1995; Recommendation No. R (95) 13 concerning problems of criminal procedure law connected with information technology, 11 September 1995; Recommendation Rec (2001) 8 on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services, 5 September 2001 und ganz aktuell Recommendation CM/Rec (2008) 6 on measures to promote the respect for freedom of expression and information with regard to Internet filters, 26 March 2008.

geschaffen werden müsse und setzte Ende 1996 ein Expertenkomitee zur Ausarbeitung einer Konvention ein, die Fragen des materiellen Computer- und Internetstrafrechts, der strafprozessualen Zwangsmassnahmen im Bereiche der Telekommunikation und Dienste der Informationsgesellschaft, der Tatortbestimmung und Strafhoheit sowie der Rechtshilfe bei der Ermittlung von Cyberkriminalität regeln sollte.[72] Aus diesem Prozess gingen zwei Instrumente hervor:

- die *Convention on Cybercrime* vom 23. November 2001,[73] und
- das *Zusatzprotokoll zur Convention on Cybercrime bezüglich der Kriminalisierung von Handlungen rassistischer und fremdenfeindlicher Art begangen durch Computersysteme* vom 28. Januar 2003.[74]

Die Convention on Cybercrime verfolgt erstens das Ziel, eine Harmonisierung der materiellen Strafbestimmungen auf dem Gebiete der Computer- und Cyberkriminalität herbeizuführen.[75] Zweitens schafft sie ein einheitliches strafprozessuales Instrumentarium zur Ermittlung und Verfolgung von Computer- und Datennetzdelikten. Insbesondere soll damit die rechtzeitige Sicherung von «flüchtigen» Beweismitteln und Verbindungsdaten in elektronischer Form ermöglicht bzw. erleichtert werden.[76] Ergänzend enthält Art. 22 CCC eine Regelung über den räumlichen Geltungsbereich. Drittens versucht das Übereinkommen ein schnelleres und effizienteres Rechtshilfe- und Auslieferungssystems

---

72 Weiterführend Christian Schwarzenegger, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, Am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Fernmeldegeheimnisses, in: Andreas Donatsch, Marc Forster und Christian Schwarzenegger (Hrsg.): Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag, Zürich 2002, S. 305–324, S. 308 ff.; Christian Spannbrücker, Convention on Cybercrime (ETS 185), Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht, Regensburg 2004, S. 3 ff.; Johannes Beer, Die Convention on Cybercrime und österreichisches Strafrecht, Linz 2005, S. 95 ff.

73 CETS No. 185, Inkrafttreten 1.7.2004. Die Schweiz hat die Konvention unterzeichnet, aber noch nicht ratifiziert, siehe zum Stand der Ratifikationen, den Originaltexten und einem erläuternden Bericht ‹http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&CL=ENG›.

74 CETS No. 189, Inkrafttreten 1.3.2006, Die Schweiz hat das Zusatzprotokoll unterzeichnet, aber noch nicht ratifiziert, siehe zum Stand der Ratifikationen, den Originaltexten und einem erläuternden Bericht ‹http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&CL=ENG›.

75 Kapitel II Abschnitt 1. Die Konvention legt Mindestanforderungen für folgende Straftatbestände fest: Unrechtmässiger Zugriff (Art. 2 CCC), unrechtmässiges Abfangen (Art. 3 CCC), Eingriff in die Datenintegrität (Art. 4 CCC), den Eingriff in die Systemintegrität (Art. 5 CCC), den Missbrauch von Vorrichtungen (Art. 6 CCC), die Computerurkundenfälschung (Art. 7 CCC), den Computerbetrug (Art. 8 CCC), Straftaten in Bezug auf Kinderpornographie (Art. 9 CCC) und Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (Art. 10 CCC). Ausserdem enthält dieser Abschnitt Bestimmungen über Teilnahme und Versuch (Art. 11 CCC) sowie über die Verantwortlichkeit juristischer Personen (Art. 12 CCC).

76 Kapitel II Abschnitt 2.

bei herkömmlichen und computerbezogenen Delikten zu etablieren, das bestehende Rechtshilfeübereinkommen oder bilateralen Verträge ergänzt oder in die Lücke springt, wo solche nicht existieren.[77] Vorgesehen sind auch provisorische Massnahmen wie die beschleunigte Sicherung gespeicherter Computerdaten (Art. 29 CCC) oder die beschleunigte Weitergabe gesicherter Verbindungsdaten (Art. 30 CCC). Die Konvention ermöglicht es den Mitgliedern bezüglich zahlreicher Bestimmungen Vorbehalte anzubringen, doch müssen die Normen über die grenzüberschreitende Zusammenarbeit gewährleistet bleiben.[78]

Während die Convention on Cybercrime vor allem computer- und netzwerkfokussierte Delikte harmonisiert, konzentriert sich das Zusatzprotokoll auf netzwerkunterstützte Kommunikationsdelikte. Die Mitgliedstaaten müssen auf nationaler Ebene Strafnormen gegen folgende Verhaltensweisen einführen bzw. konventionskonform ausgestalten:[79]

- Verbreitung von rassistischem und fremdenfeindlichem Material durch Computersysteme (Art. 3 ZP-CCC)
- Rassistisch und fremdenfeindlich motivierte Drohung (Art. 4 ZP-CCC)
- Rassistisch und fremdenfeindlich motivierte Beschimpfung (Art. 5 ZP-CCC)
- Verleugnung, grobe Verharmlosung, Gutheissung oder Rechtfertigung von Völkermord oder Verbrechen gegen die Menschlichkeit (Art. 6 ZP-CCC)

Aus dem erläuternden Bericht geht hervor, dass unter Verbreitung i.S.v. Art. 3 ZP-CCC auch ein Zugänglichmachen fällt, worunter etwa die Abspeicherung auf einem öffentlich zugänglichen Web-Server oder auch das Setzen oder Zusammenstellen von Hyperlinks auf Webseiten zu subsumieren sei.[80]

Wegen der Konvergenz des Rundfunks und der Fernmeldedienste hat auch das *Europäische Übereinkommen über Rechtsschutz für Dienstleistungen mit bedingtem Zugang und der Dienstleistungen zu bedingtem Zugang*[81] Relevanz für die Cyberkriminalität. In Art. 4 des Übereinkommens werden verschiedene Handlungen definiert, mit denen ein widerrechtlicher Zugriff auf gegen Entgelt erbrachte und zugangskontrollierte Fernseh- und Radioprogramme, Dienste der

77 Kapitel III.

78 Ausführlicher Explanatory Report, CETS No. 185, N 315 ff., siehe ‹http://conventions.coe.int/Treaty/en/Reports/Html/185.htm›.

79 Weiterführend Marcel Alexander Niggli, Rassendiskriminierung und Internet, Strafrechtliche Grundlagen, Rechtsprechung und Revisionsbemühungen, in: Christian Schwarzenegger, Oliver Arter und Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 299–345, S. 323 ff. m.N.

80 Explanatory Report, CETS No. 189, N 28, siehe ‹http://conventions.coe.int/Treaty/en/Reports/Html/189.htm›.

81 CETS No. 178, Inkrafttreten 1.7.2003. Die Schweiz hat das Übereinkommen am 11.5.2005 ratifiziert. Es ist am 1.9.2005 in Kraft getreten (SR 0.784.03), siehe zum Stand der Ratifikationen, den Originaltexten und einem erläuternden Bericht ‹http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=178&CM=8&CL=GER›.

Informationsgesellschaft[82] sowie die Zugangskontrollen zu den genannten Diensten selbst ermöglicht wird. Nach Art. 5 des Übereinkommens müssen die Mitgliedstaaten Massnahmen verabschieden, damit «die Zuwiderhandlungen nach Artikel 4 durch strafrechtliche, verwaltungsrechtliche oder andere Strafen geahndet werden können.» Diese Massnahmen haben nach derselben Bestimmung «wirksam, abschreckend und verhältnismässig zu den möglichen Auswirkungen der Zuwiderhandlung» zu sein.

Eine Erweiterung erfährt der Katalog konventionalrechtlicher Vorgaben im Bereich der Cyberkriminalität durch die jüngste Konvention des Europarates, die *Konvention über den Schutz von Kindern gegen sexuelle Ausbeutung und sexuellen Missbrauch* vom 25. Oktober 2007 (CPC).[83] Nach Art. 20 CPC sind Delikte betreffend Kinderpornographie einzuführen, die zwar nicht auf Taten in Computernetzwerken beschränkt, wegen der Häufigkeit der Online-Verübung aber auf diese besonders ausgerichtet sind. Daher ist Art. 20 Abs. 1 lit. b CPC so gefasst, dass das Anbieten und Zugänglichmachen von Kinderpornographie durch Webpublikation oder Hyperlink wie schon in Art. 3 ZP-CCC unter Strafe gestellt werden muss. Art. 10 Abs. 1 lit. f CPC geht über die Anforderungen von Art. 9 CCC hinaus, indem auch die wissentliche Erlangung eines Zugriffs auf Kinderpornographie durch IKT in den Tatbestand aufzunehmen ist.[84] Allerdings ist dagegen ein Vorbehalt zulässig. Wichtig ist auch die Erhöhung der Schutzaltergrenze im Vergleich zum Schweizer Recht (Art. 197 Ziff. 3 StGB). Kinder im Sinne der Konvention sind alle Personen unter 18 Jahren (Art. 3 lit. a).

Am 7. November 2007 fasste das Ministerkomitee des Europarates seine bisherige IKT-Politik in einer Empfehlung über Massnahmen zur Förderung des Wertes des Internet als *Service Public* zusammen.[85] Das Ministerkomitee empfiehlt Massnahmen in den Politikfeldern «Menschenrechte und Demokratie»,[86]

---

82 Darunter sind Dienste zu verstehen, die durch eine elektronische Fernübertragung auf individuellen Abruf des Empfängers erbracht werden.

83 CETS No. 201, noch nicht in Kraft. Die Schweiz hat die Konvention nicht unterzeichnet, siehe zum Stand der Ratifikationen, den Originaltexten und einem erläuternden Bericht ‹http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&CL=ENG›.

84 Dieser Tatbestand soll jene Täter fassen, die kinderpornographisches Material online betrachten, indem sie auf eine kinderpornographische Website zugreifen, ohne diese Daten auf ihren Computer herunterzuladen. Es sollen allerdings nur diejenigen Personen strafbar werden, die schon vor dem Zugriff über den kinderpornographischen Inhalt Bescheid wüssten. Ein solches Wissen könne etwa daraus geschlossen werden, dass für eine Zugangsberechtigung zu einem kinderpornographischen Angebot bezahlt worden sei, siehe Explanatory Report, CETS No. 201, N 140, siehe ‹http://conventions.coe.int/Treaty/en/Reports/Html/201.htm›.

85 Council of Europe, Committee of Ministers, Recommendation CM/Rec (2007) 16 on measures to promote the public service value of the Internet, 7 November 2007.

86 Vgl. dazu auch Council of Europe, Committee of Ministers, Declaration on freedom of communication on the Internet, 28 May 2003, in der als zweites Prinzip die Priorität für Selbstregulierung und Koregulierung betreffend Inhaltsverbreitung auf dem Internet gutgeheissen wird.

«Zugang», «Offenheit», «Diversität» und «Sicherheit». Es zeigt sich betroffen über die erheblichen Schädigungsgefahren durch Inhalte und Kommunikationsprozesse im Internet und anderen IKT-Einrichtungen und erinnert die Mitgliedstaaten daran, die Convention on Cybercrime, das Zusatzprotokoll zur CCC und die Konvention zum Schutz von Kindern gegen sexuelle Ausbeutung und sexuellen Missbrauch zu ratifizieren. Auch sollen gesetzliche Regelungen und Durchsetzungsmassnahmen in den Bereichen der Spam-Mails und der Verletzung von Urheberrechten und verwandten Schutzrechten getroffen werden. Betont wird zudem, die involvierten Akteure des privaten Sektors hätten neue Formen offener Selbst- und Koregulierung zu entwickeln und ihre Zusammenarbeit mit den Behörden zu intensivieren.

4. Initiativen im Rahmen der Europäischen Union

Die Politikfelder der Europäischen Gemeinschaft und der Europäischen Union[87] werden durch den Vertrag zur Gründung der Europäischen Gemeinschaft (EGV) und den Vertrag über die Gründung der Europäischen Union (EUV) vorgegeben.[88] Eine Kompetenz zum Erlass eines supranationalen Strafgesetzbuches im Rahmen der Europäischen Gemeinschaft existiert nicht, denn es gilt das Prinzip der begrenzten Einzelermächtigung (Art. 5 Abs. 1 EGV).[89] Der Europäischen Kommission stehen zwar in bestimmten Tätigkeitsfeldern *verwaltungsrechtliche Sanktionen* zur Verfügung, wie beispielsweise im Kartellrecht,[90] wo bei Verstössen gegen verschiedene Verordnungsvorschriften Geldbussen gegen die fehlbaren Unternehmen oder Unternehmensvereinigungen vorgese-

87 I. Säule bezeichnet den Kompetenzbereich der Europäischen Gemeinschaft basierend auf dem EGV, während die III. Säule jenen der Europäischen Union gemäss EUV darstellt (hier konkret den Tätigkeitsbereich «Raum der Freiheit, der Sicherheit und des Rechts, Art. 29 ff. EUV). Nach der Ratifikation des Vertrages von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft vom 13. Dezember 2007 (ABl. C 306 vom 17.12.2007, S. 1 ff.) durch alle Mitgliedstaaten wird diese Säulenstruktur aufgegeben, siehe Art. 1 Lissabon-Vertrag: «Grundlage der Union sind dieser Vertrag und der Vertrag über die Arbeitsweise der Europäischen Union (…). Beide Verträge sind rechtlich gleichrangig. Die Union tritt an die Stelle der Europäischen Gemeinschaft, deren Rechtsnachfolgerin sie ist.» Zu den Konsequenzen aus strafrechtlicher Perspektive zusammenfassend HENNING ROSENAU, Zur Europäisierung im Strafrecht, Vom Schutz finanzieller Interessen der EG zu einem gemeineuropäischen Strafgesetzbuch?, Zeitschrift für Internationale Strafrechtsdogmatik 2008, S. 9–19, S. 15 m.N. Das weitere Schicksal des Vertrages von Lissabon ist allerdings nach der Ablehnung durch Irland (Volksabstimmung vom 12.6.2008) ungewiss.

88 Die Verträge wurden zuletzt abgeändert durch den Vertrag von Nizza, ABl. C 80 vom 10.3.2001, S. 1 ff. Vgl. konsolidierte Fassung des EGV, ABl. C 325 vom 24.12.2002, S. 33 ff.; konsolidierte Fassung des EUV, ABl. C 325 vom 24.12.2002, S. 5 ff.

89 Zur Kompetenzfrage näher VOLKER STIEBIG, Strafrechtsetzungskompetenz der Europäischen Gemeinschaft und Europäisches Strafrecht: Skylla und Charybdis einer europäischen Odyssee?, EuR 2005, S. 466–493, S. 466 ff.

90 Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln, ABl. L 1 vom 4.1.2003, S. 1 ff.

hen sind. Diesen Sanktionen soll aber kein strafrechtlicher Charakter zukommen.[91]

a. Erste Phase der Strafrechtsharmonisierung durch indirekte Angleichung mittels sekundären Gemeinschaftsrechts

Dennoch gehen heute viele nationale Strafbestimmungen auf europäische Rechtsgrundlagen zurück. Es handelt sich dabei um einen indirekten Anpassungsvorgang, der meistens durch europäische Mindestanforderungen an Straftatbestände und Sanktionsvorgaben ausgelöst wird.[92] Mehrere Richtlinien des Gemeinschaftsrechts verlangen von den Mitgliedstaaten die Einführung von «wirksamen, angemessenen und abschreckenden Sanktionen» *(Mindesttrias).*[93] Dadurch sind sie zwar nicht verpflichtet, strafrechtliche Sanktionen vorzusehen, doch zeigen mehrere Beispiele, dass eine befriedigende Lösung der Harmonisierungspflicht nur im strafrechtlichen Kontext gefunden werden kann.

Zur Illustration soll hier nur das Beispiel der *Richtlinie 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten* herausgegriffen werden.[94] Gemäss Art. 4 Richtlinie 98/84/EG haben die Mitgliedstaaten Handlungen zu verbieten, die im Zusammenhang stehen mit illegalen Vorrichtungen zur Umgehung von Zugangskontrollen für Fernseh- und Radioprogramme sowie Dienste der Informationsgesellschaft.

---

91 So explizit Art. 23 Abs. 5 Verordnung (EG) Nr. 1/2003.

92 Einen Überblick über die zahlreiche Literatur zum «Europäischen Strafrecht» bieten Kai Ambos, Internationales Strafrecht, München 2006, S. 304 ff.; Bernd Hecker, Europäisches Strafrecht, 2. Aufl., Berlin u.a. 2007; Helmut Satzger, Internationales und Europäisches Strafrecht, 2. Aufl., Baden-Baden 2008, S. 83 ff.; mit besonderem Blick auf die Informations- und Kommunikationstechnologie Christian Schwarzenegger und Sarah J. Summers, The emergence of EU criminal law, Cybercrime and the regulation of the information society, Oxford 2008, Ch. 1–3 (im Erscheinen).

93 Diese Formel wurde ursprünglich vom Europäischen Gerichtshof geprägt, European Court of Justice, Commission v. Council, C-68/88, 21 September 1989, N 23 f.: «Enthält eine gemeinschaftsrechtliche Regelung keine besondere Vorschrift, die für den Fall eines Verstosses gegen die Regelung eine Sanktion vorsieht, oder verweist sie insoweit auf die nationalen Rechts- und Verwaltungsvorschriften, so sind die Mitgliedstaaten nach Artikel 5 EWG-Vertrag verpflichtet, alle geeigneten Massnahmen zu treffen, um die Geltung und die Wirksamkeit des Gemeinschaftsrechts zu gewährleisten. Dabei müssen die Mitgliedstaaten, denen allerdings die Wahl der Sanktionen verbleibt, namentlich darauf achten, dass Verstösse gegen das Gemeinschaftsrecht nach ähnlichen sachlichen und verfahrensrechtlichen Regeln geahndet werden wie nach Art und Schwere gleichartige Verstösse gegen nationales Recht, *wobei die Sanktion jedenfalls wirksam, verhältnismässig und abschreckend sein muss.*» (meine Hervorhebungen) Indem die griechische Regierung weder straf- noch disziplinarrechtliche Schritte gegen die Hinterziehung von EG-Agrarsubventionen eingeleitet hatte, verstiess sie gegen die Verpflichtungen aus Art. 5 EWG-Vertrag. Weiterführend Hecker (Fn. 92), S. 247 ff.; Schwarzenegger und Summers (Fn. 92), Ch. 2 (im Erscheinen).

94 Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, ABl. L 320 vom 28.11.1998, S. 54 ff.; vgl. Abbildung 1, mit weiteren Beispielen von Richtlinien des Gemeinschaftsrechts (1. Säule), die für das Internetstrafrecht von Relevanz sind.

Bezüglich der Sanktionen sieht Art. 5 Abs. 1 Richtlinie 98/84/EG vor, diese müssten «wirksam, abschreckend und der potentiellen Wirkung der Zuwiderhandlung angemessen sein.» Erwägungsgrund 23 ergänzt dies mit dem Hinweis, die Mitgliedstaaten seien nicht verpflichtet, strafrechtliche Sanktionen für die Zuwiderhandlungen im Sinne der Richtlinie 98/84/EG vorzusehen. In ihrem ersten Bericht zur Umsetzung der Richtlinie[95] stellt die Kommission fest, dass sie in sehr unterschiedlicher Weise in nationale Rechtsvorschriften umgesetzt worden sei. Weiters führt sie aus:

> «Die Richtlinie verpflichtet die Mitgliedstaaten nicht zu strafrechtlichen *Sanktionen,* aber alle Mitgliedstaaten ausser zwei (Italien und Portugal) sehen Sanktionen in Form von Freiheitsstrafe und/oder Geldstrafe für die von ihnen als wesentlich betrachteten Zuwiderhandlungen (Herstellung und Vertrieb) vor. Es bestehen offensichtliche nationale Unterschiede in der Bewertung der Zuwiderhandlungen und der notwendigen Abschreckung.
>
> Einige Mitgliedstaaten haben ein System abgestufter Sanktionen eingeführt. Durch die Einbeziehung von Verboten und Sanktionen im Strafrecht sind auch die klassischen Bereiche mittelbarer Straftaten (Mittäterschaft, Anstiftung, Beihilfe) erfasst und Strafverfahren (Durchsuchung und Beschlagnahme, Geldstrafe) verfügbar.
>
> In einigen Mitgliedstaaten (Österreich, Deutschland, Italien), in denen bereits bestehende Rechtsvorschriften für die Verfolgung bestimmter Formen der Piraterie angewandt werden konnten, führte die Einführung spezifischer aber weniger schwerer Sanktionen für die in der Richtlinie aufgeführten Zuwiderhandlungen *de facto* zu einer Verringerung des rechtlichen Schutzes in diesen Mitgliedstaaten.»[96]

Ähnliche Vorgaben enthält beispielsweise die *Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG* in Art. 5 Abs. 1, nach welchem das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer zu untersagen ist, und Art. 13 Abs. 1 und Abs. 4, in welchen festgehalten wird, dass unerbetene Spam-Mails zu verbieten sind.[97] Diese Rechtsgüter lassen sich praktisch nur mit strafrechtlichen Sanktionen effektiv sichern.

Die Kommission war in dieser ersten Phase der Strafrechtsharmonisierung durch Gemeinschaftsrecht bemüht, dem Problem der fehlenden Regelungskompetenz im Strafrecht dadurch auszuweichen, dass die vorgeschlagenen Instru-

---

95 Europäische Kommission, Rechtlicher Schutz elektronischer Bezahldienste, Bericht der Kommission an den Rat, das Europäische Parlament und den Europäischen Wirtschafts- und Sozialausschuss über die Umsetzung der Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, KOM(2003) 198 endg.

96 Europäische Kommission (Fn. 95), S. 13 (Hervorhebungen im Original).

97 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37 ff.

mente «bloss» die Einführung von Sanktionen und wirksamen Rechtsbehelfen verlangen, ohne direkt eine Verankerung im Strafrecht vorzuschreiben. *De facto* handelte es sich jedoch – mangels ausreichender Äquivalente im Zivil- und Verwaltungsrecht – fast immer um Kriminalisierungsvorschriften.

Wenn es um die Gewährleistung des Binnenmarktes und der vier Grundfreiheiten der EG geht, kann das Gemeinschaftsrecht auch entkriminalisierende oder strafrechtsbegrenzende Wirkung entfalten. So schränkt die *Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr*[98] unter anderem die Strafbarkeit der verschiedenen Internetprovider ein, die sich allenfalls nach den allgemeinen Regeln der nationalen Strafgesetzbücher ergeben würde. Aufgrund der unpräzisen und widersprüchlichen Vorgaben der Richtlinie 2000/31/EG ist allerdings strittig, ob Art. 2 lit. h, der den koordinierter Bereich für Dienste der Informationsgesellschaft definiert, und Art. 3, der für diese einen freien Binnenmarkt einrichtet, auch für das Strafrecht die zwingende Einführung des *Herkunftslandprinzips* verlangen.[99]

Neben den genannten Rechtsangleichungsinstrumenten müssen die nationalen Gesetzgeber, Gerichte und Behörden der Mitgliedstaaten auch dem sogenannten *Anwendungsvorrang* des Gemeinschaftsrechts im Bereich des Strafrechts Rechnung tragen. Bei Kollisionen zwischen nationalen Strafnormen und unmittelbar anwendbarem Gemeinschaftsrecht geht letzteres vor, was ebenfalls entkriminalisierend wirken kann.[100]

So stellt beispielsweise ein Straftatbestand, der die Ausübung von Tätigkeiten des Sammelns, der Annahme, der Bestellung und der Übertragung von Wetten, insbesondere über Sportereignisse, ohne eine von dem betreffenden Mitgliedstaat erteilte Konzession oder polizeiliche Genehmigung verbietet, eine Beschränkung der Niederlassungsfreiheit und des freien Dienstleistungsverkehrs nach den Art. 43 und 49 EGV dar. Diese Bestimmungen des EGV sind dahin auszulegen, dass sie einer nationalen Regelung, die für Personen eine strafrechtliche Sanktion wegen Sammelns von Wetten ohne die nach dem nationalen Recht erforderliche Konzession oder polizeiliche Genehmigung vorsieht, dann entgegenstehen, wenn sich diese Personen diese Konzessionen oder Genehmigungen deshalb nicht beschaffen konnten, weil der betreffende Mitglied-

98 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt («Richtlinie über den elektronischen Geschäftsverkehr»), ABl. L 178 vom 17.7.2000, S. 1 ff.

99 Für Deutschland eher ablehnend Hans Kudlich, Herkunftslandprinzip und Internationales Strafrecht, HRR Strafrecht 2004, S. 278–284 m.N.; aus österreichischer Perspektive ablehnend Christian Schwarzenegger, Hyperlinks und Suchmaschinen aus strafrechtlicher Sicht, in: Oliver Plöckinger, Dieter Duursma und Michael Mayrhofer (Hrsg.), Internet-Recht, Beiträge zum Zivil- und Wirtschaftsprivatrecht, Öffentlichen Recht, Strafrecht, Wien 2004, S. 395–434, S. 422 ff.

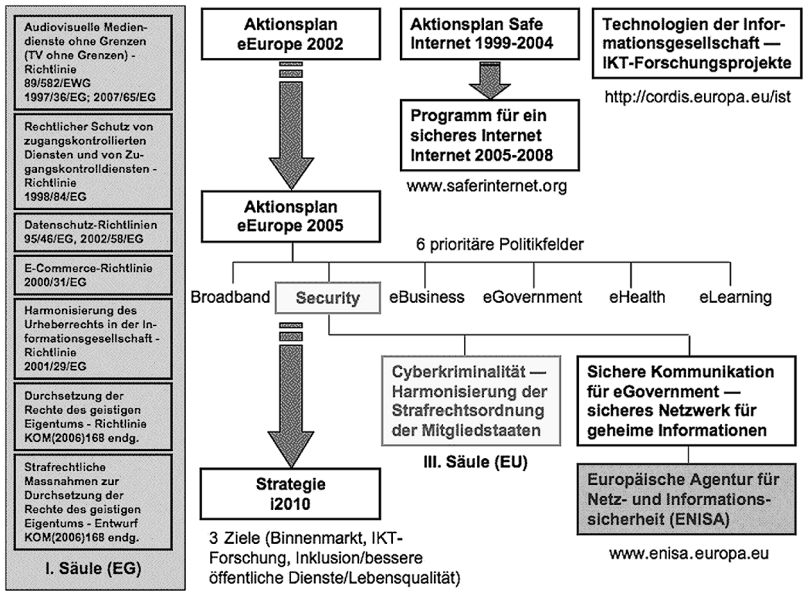
100 Ausführlich zum Anwendungsvorrang des Gemeinschaftsrechts Hecker (Fn. 92), S. 321 ff. m.w.N.

staat es unter Verstoss gegen das Gemeinschaftsrecht abgelehnt hatte, sie ihnen zu erteilen.[101]

b. Zweite Phase der Strafrechtsharmonisierung durch Instrumente der dritten Säule der EU

Im Rahmen der Europäischen Union können die Mitgliedstaaten einerseits mittels völkerrechtlicher Übereinkommen eine Angleichung der nationalen Strafgesetze erwirken, andererseits steht ihnen innerhalb des Rates der Europäischen Union ein Vorschlagsrecht für Rahmenbeschlüsse (Art. 34 Abs. 2 lit. b EUV) zur Verfügung, die gestützt auf Art. 29 Abs. 2 i.V.m. Art. 31 Abs. 1 lit. e EUV auch eine Annäherung der Strafvorschriften der Mitgliedstaaten beschlagen können.[102] Es handelt sich dabei um eine *Angleichungskompetenz*.[103]

Abbildung 1: Aktionsfelder der EU-Kriminalpolitik im Bereich der Cyberkriminalität



101 European Court of Justice, Gambelli et al., C-243/01, 6 November 2003, N 76; European Court of Justice, Placanica, Palazzese and Sorricchio, C-338/04, C-359/04, C-360/04, 6 March 2007, N 72; vgl. zu den Konsequenzen aus deutscher Sicht Sebastian Meyer, Sportwetten als illegales Glücksspiel? – Zur Anwendung des § 284 StGB auf Sportwetten, JR 2004, S. 447–453.

102 Nach dem Wortlaut handelt es sich um «Mindestvorschriften über die Tatbestandsmerkmale strafbarer Handlungen und die Strafen in den Bereichen organisierte Kriminalität, Terrorismus und illegaler Drogenhandel.»

103 Vgl. den aktuellen Überblick bei Hecker (Fn. 92), § 11 mit zahlreichen Nachweisen.

Mit Blick auf die Cyberkriminalität sind folgende Instrumente zu nennen, in denen verschiedene Teilbereiche harmonisiert werden:[104]

- Beschluss 2000/375/JI zur Bekämpfung der Kinderpornographie im Internet,[105]
- Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln,[106]
- Rahmenbeschluss 2002/475/JI zur Terrorismusbekämpfung,[107]
- Rahmenbeschluss 2004/68/JI zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie,[108]
- Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme,[109]
- Vorschlag für einen Rahmenbeschluss des Rates zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit,[110]

Wie aus Abbildung 1 hervorgeht, gehören diese Harmonisierungsinstrumente zu einem die verschiedenen Aktionsfelder integrierenden kriminalpolitischen Ansatz der Europäischen Kommission, in dem die Sicherung der IKT-Infrastruktur durch das Strafrecht nur einen Teilaspekt ausmacht (Aktionsplan eEurope 2005 – Security).

c. Dritte Phase der Strafrechtsharmonisierung durch direkte Anweisungen im sekundären Gemeinschaftsrecht

Gestützt auf Art. 5 Abs. 2 EGV in Verbindung mit verschiedenen Kompetenznormen in den Politikbereichen der EG sieht sich die Europäische Kommission selbst ermächtigt, die Strafrechtsangleichung voranzubringen. Sie hat dabei Rechtsgebiete im Auge, in denen die auf der nationalstaatlichen Ebene in Be-

---

104 Siehe auch Eric Hilgendorf, Tendenzen und Probleme einer Harmonisierung des Internetstrafrechts auf Europäischer Ebene, in: Christian Schwarzenegger, Oliver Arter und Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 257–298.

105 Beschluss des Rates vom 29. Mai 2000 zur Bekämpfung der Kinderpornographie im Internet (2000/375/JI), ABl. L 138 vom 9.6.2000, S. 1 ff.

106 Rahmenbeschluss des Rates vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (2001/413/JI), ABl. L 149 vom 2.6.2001, S. 1 ff.

107 Rahmenbeschluss des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (2002/475/JI), ABl. L 164 vom 22.6.2002, S. 3 ff.

108 Rahmenbeschluss 2004/68/JI des Rates vom 22. Dezember 2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie, ABl. L 13 vom 20.1.2004, S. 44 ff.

109 Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl. L 69 vom 16.3.2005, S. 67 ff.

110 Europäische Kommission, Vorschlag für einen Rahmenbeschluss des Rates zur Bekämpfung von Rassismus und Fremdenfeindlichkeit, KOM(2001) 664 endg. An der Tagung des Europäischen Rates vom 20. April 2007 wurde dieser Rahmenbeschluss unter Vorbehalt einiger parlamentarischer Prüfungsvorbehalte angenommen. Am 29.11.2007 erfolgte die legislative Entschliessung des Europäischen Parlaments zu dem Vorschlag für einen Rahmenbeschluss des Rates zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit (11522/2007 – C6–0246/2007 – 2001/0270 (CNS)).

tracht gezogenen Massnahmen nicht ausreichend erscheinen. Dabei will sie mittels Richtlinien direkter und verbindlicher zum Ziel der Strafrechtsharmonisierung kommen.[111]

Um den Kompetenzkonflikt zu lösen, der aufgrund dieser Auffassung mit dem Rat der Europäischen Union entstanden war und sich in parallelen Gesetzgebungsverfahren für Richtlinien und Rahmenbeschlüsse im Bereich des Umweltschutzes und der Meeresverschmutzung durch Schiffe bemerkbar gemacht hatte, klagte die Kommission vor dem Europäischen Gerichtshof gegen den Rat auf Aufhebung der diesbezüglichen Rahmenbeschlüsse. Der Europäische Gerichthof kam in beiden Urteilen[112] zum Schluss, dass die Kommission gestützt auf den EGV eine «implizite Kompetenz» habe, die Mitgliedstaaten zu verpflichten, strafrechtliche Sanktionen in die nationalen Strafgesetze aufzunehmen, wenn dies zur Erreichung der Gemeinschaftsziele notwendig und eine spezifische Rechtsgrundlage im EGV gegeben sei. Für die Umwelt- und Verkehrspolitik sei dies offensichtlich. Obschon also weder das materielle noch das formelle Strafrecht im allgemeinen zu den Kompetenzen der Gemeinschaft zähle, könne eine solche in Fällen bejaht werden, in welchen die Einführung wirksamer, angemessener und abschreckender Strafen auf nationaler Ebene erforderlich sei, um schwerwiegende Umweltstraftaten zu bekämpfen.[113] Der Europäische Gerichthof hob daher die beiden Rahmenbeschlüsse auf. Allerdings begrenzt er im zweiten Urteil diese Kompetenz der Gemeinschaft entscheidend:

> «By contrast, and contrary to the submission of the Commission, the determination of the type and level of the criminal penalties to be applied does not fall within the Community's sphere of competence.»[114]

Damit ist nunmehr klar, dass EG-Richtlinien nur Anweisungen an die nationalen Strafgesetzgeber enthalten dürfen, sie hätten ein bestimmtes Verhalten unter Androhung von Kriminalstrafe zu verbieten. Die Art und das Mass der Sankt-

---

111 Der wichtigste Unterschied zwischen Rahmenbeschlüssen der dritten Säule und Richtlinien des sekundären Gemeinschaftsrechts besteht im Gesetzgebungsverfahren. Erstere können nur einstimmig beschlossen werden, letztere wie auch Verordnungen werden in der Regel in einem Mitentscheidungsverfahren zusammen mit dem Europäischen Parlament und mit qualifizierter Mehrheit erlassen. Zu den weiteren Vorteilen siehe JOHN A. E. VERVAELE, The European Community and harmonization of the criminal law enforcement of community policy, Eucrim 2006, S. 87–93, S. 90 f.

112 EUROPEAN COURT OF JUSTICE, Commission v. Council, C-176/03, 13 September 2005, vgl. hierzu EUROPÄISCHE KOMMISSION, Mitteilung der Kommission an das Europäische Parlament und den Rat über die Folgen des Urteils des Gerichtshofs vom 13. September 2005 (Rs. C-176/03, Kommission gegen Rat), KOM(2005) 583 endg.; SIMONE WHITE, Case C-176/03 and options for the development of a community criminal law, Eucrim 2006, S. 93–99, S. 94 f.; kritisch ROLAND HEFENDEHL, Europäischer Umweltschutz: Demokratiespritze für Europa oder Brüsseler Putsch? Zeitschrift für Internationale Strafrechtsdogmatik 2006, S. 161–167, S. 164 f.; EUROPEAN COURT OF JUSTICE, Commission v. Council, C-440/05, 23 October 2007.

113 EUROPEAN COURT OF JUSTICE, Commission v. Council, C-440/05, 23 October 2007, N 66 m.N.

114 EUROPEAN COURT OF JUSTICE, Commission v. Council, C-440/05, 23 October 2007, N 70 m.N.

ionsfolgen können dagegen nicht über das Gemeinschaftsrecht harmonisiert werden.

Die Auslegung des EGV durch den Europäischen Gerichthof überzeugt allerdings kaum,[115] denn sie bricht vollständig mit dem verfassungsrechtlichen Grundsatz, dass das Strafrecht ein eigener Regelungs- bzw. Politikbereich ist, für den es eine selbständige Kompetenznorm braucht. So enthalten Art. 123 BV für die Schweiz, Art. 74 Nr. 1 GG[116] für Deutschland und Art. 10 Abs. 1 Ziff. 6 B-VG für Österreich explizite Bundeskompetenzen für das «Strafrecht» bzw. das «Strafrechtswesen». Es käme in der Schweiz niemandem in den Sinn, aus Art. 74 BV, der eine Bundeskompetenz im Bereiche des Umweltschutzes statuiert, eine implizite Kompetenz für ein Umweltstrafrecht abzuleiten.

Es ist damit zu rechnen, dass die Kommission nach diesen Grundsatzentscheidungen des Europäischen Gerichtshofes die bestehenden Rahmenbeschlüsse unberührt lassen und die strafrechtliche Harmonisierung in wichtigen Politikbereichen mittels Richtlinien befördern wird.[117] Rahmenbeschlüssen der dritten Säule sind aber bis zum Inkrafttreten des Vertrages von Lissabon unabdinglich für die genauere Ausgestaltung der Sanktionsfolgen und weiterer strafrechtlicher Rahmenbedingungen.

d. Kriminalpolitische Ziele im Bereich der Cyberkriminalität

Gestützt auf eine umfassende Lageanalyse[118] legte die Kommission 2001 ein kriminalpolitisches Konzept gegen Cyberkriminalität vor, das mehrere Stossrichtungen aufzeigte (siehe Abbildung 1). Die Analyse des rechtlichen Rahmens endet mit der Schlussfolgerung, dass die Kommission eine legislative Massnahme in der dritten Säule zur Annäherung der Strafvorschriften der Mitgliedstaaten in Bezug auf Angriffe auf Computersysteme, einschliesslich Hacking und der gezielten Überlastung von Servern vorschlagen würde.[119]

2007 folgte eine Überprüfung der erreichten Fortschritte und ein Entwurf für eine Initiative zur Bekämpfung der Internetkriminalität. In dieser Mitteilung beschreibt die Kommission ihren dreigleisigen Ansatz, um gegen die Bedrohungen für die Sicherheit der Informationsgesellschaft vorzugehen. Dieser setzt sich aus spezifischen Massnahmen zur Stärkung der Netz- und Informationssi-

---

115 Siehe nochmals ROLAND HEFENDEHL, Der EuGH stellt die strafrechtliche Kompetenzordnung auf den Kopf – und wundert sich über Kritik, in: Jan C. Joerden und Andrzeij J. Szwarc (Hrsg.), Europäisierung des Strafrechts in Polen und Deutschland – rechtsstaatliche Grundlagen, Berlin 2007, S. 41–58 m.N.

116 Konkurrierende Gesetzgebung, d.h. wo der Bund von seiner Gesetzgebungskompetenz Gebrauch macht, können die Länder grundsätzlich keine Gesetze mehr erlassen (Art. 72 GG).

117 Zu den verschiedenen Optionen näher WHITE (Fn. 112), S. 96 ff.

118 EUROPÄISCHE KOMMISSION, eEurope 2002, Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, Mitteilung, KOM(2000) 890 endg.

119 EUROPÄISCHE KOMMISSION, Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz, Mitteilung, KOM(2001) 298 endg., S. 29.

cherheit, der Schaffung eines rechtlichen Rahmens für die elektronische Kommunikation und der Bekämpfung der Internetkriminalität zusammen.[120] Zum aktuellen Regelungsbedarf schreibt die Kommission:

> «Eine allgemeine Angleichung der Straftatbestände und der nationalen Strafrechtsvorschriften auf dem Gebiet der Internetkriminalität ist noch nicht angebracht, da mit diesem Begriff zurzeit noch zu viele unterschiedliche Delikte abgedeckt werden … Ein wichtiger Fortschritt auf dem Wege zur Angleichung bestimmter zentraler Tatbestände wurde bereits in Form des Rahmenbeschlusses über Angriffe auf Informationssysteme aus dem Jahr 2005 erzielt … Ein besonderer Punkt, der eine gesetzliche Regelung erforderlich machen könnte, ist die in Verbindung mit *Identitätsdiebstahl* begangene Internetkriminalität.»[121]

Der Rat der Europäischen Union hat Ende 2007 unter anderem folgende Leitlinien für die «Bekämpfung der Cyberkriminalität» beschlossen:[122]

- Die Mitteilung der Kommission vom 22. Mai 2007, welche einen weiteren Schritt zu einer kohärenten EU-Politik zur Prävention und Bekämpfung der Cyberkriminalität darstellt, wird begrüsst und ihre Bedeutung hervorgestrichen.
- Die Bedeutung einer verstärkten EU-weiten Kooperation bei der Ausbildung von Mitgliedern der Strafverfolgungsbehörden in den Bereichen der Cyberkriminalität wird betont.
- Die Initiative der Kommission, zwischen dem öffentlichen und dem privaten Sektor einen Dialog aufzubauen, um die Prävention und die Erfassung von Computerkriminalität zu erleichtern, wird begrüsst. Der Rat weist darauf hin, dass die meisten Kommunikationsdienstleister heute private Unternehmen sind und auch die Entwicklung von Sicherheitstechnologie mehrheitlich durch Private vorangebracht wird. Angriffen auf die Informationssysteme und rechtswidrige Inhalte werden in erster Linie von den betroffenen Privaten festgestellt. Deshalb sind Polizei und Untersuchungsbehörden auf die Unterstützung des privaten Sektors angewiesen, um effektiv gegen Täter vorgehen zu können.
- Es wird hervorgehoben, dass die Convention on Cybercrime ein wichtiges Instrument darstellt, das von möglichst allen Staaten umgesetzt werden sollte.
- Besondere Anstrengungen sind notwendig, um die internationale Koordination der Strafverfolgung zu verbessern. Genannt werden die zwischenstaatliche Zusammenarbeit, aber auch der Informationsaustausch über Europol, Eurojust und Interpol sowie das 24/7-Netzwerk.

---

120 Europäische Kommission, Eine allgemeine Politik zur Bekämpfung der Internetkriminalität, Mitteilung, KOM(2007) 267 endg., S. 5.

121 Europäische Kommission (Fn. 120), S. 9.

122 2827th Council Meeting, Justice and Home Affairs, Brussels, 8–9 November 2007, Doc. 14617/07, S. 18 ff.

5. Initiativen im Rahmen anderer internationaler Organisationen

Die OECD hat 1992 *Guidelines for the security of information systems and networks* erlassen, die im Jahre 2002 revidiert wurden.[123] Mit diesen Richtlinien will die Organisation auf die Risiken der Informationsgesellschaft und -netzwerke aufmerksam machen und ein international koordiniertes Sicherheitskonzept fördern. Eine Spam-Task-Force der OECD hat ein *Anti-spam toolkit* entwickelt und spezifische Massnahmen und Empfehlungen vorgelegt.[124]

II. Konsequenzen für die schweizerische Kriminalpolitik

Der Überblick über die internationalen Standards und Vorgaben im Bereich der Cyberkriminalität hat gezeigt, dass ein immer engmaschigeres Netz an mehr oder weniger verbindlichen Normen entstanden ist, das die nationale Kriminalpolitik in harmonisierte Bahnen lenken will. Zur Unterzeichnung und Ratifikation völkerrechtlicher Verträge kann sich die Schweiz grundsätzlich frei entscheiden. Wo diese aber – wie im Beispiel des TRIPS-Abkommens – mit anderen für die Schweizer Interessen wichtigen Regelungsbereichen verknüpft sind, entsteht ein stärkerer Anpassungsdruck. Da die Schweiz nicht Mitgliedstaat der Europäischen Union ist, sind die detaillierteren Vorgaben des EG- und EU-Rechts mit den verbindlichen Umsetzungsfristen hierzulande nicht verbindlich. Es zeigt sich jedoch eine starke Parallelität zwischen den Konventionen des Europarates und den Richtlinien bzw. Rahmenbeschlüssen der EU. So sind das Europäische Übereinkommen über den rechtlichen Schutz von zugangskontrollierten Diensten und Zugangskontrolldiensten[125] und die Richtlinie 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten beinahe identisch. Hier wird auf dem Umweg über die Harmonisierungsinstrumente des Europarates eine EU-kompatible Rechtslage herbeigeführt.

Die Unabhängigkeit der schweizerischen Kriminalpolitik im Bereich der Cyberkriminalität wird relativiert durch das Bedürfnis nach einem schnellen Informationsaustauch und der funktionierenden Rechtshilfe in Strafsachen. Es ist vor diesem Hintergrund im Interesse der Schweiz, dem international harmonisierten Standard des Internet- und Computerstrafrechts zu entsprechen.

Aufgrund der schnellen technischen Innovation im IKT-Sektor wird international und national zunehmend eine Ergänzung des klassischen Strafrechts um

123 Organisation for Economic Co-operation and Development, OECD guidelines for the security of information systems and networks, Toward a culture of security, Paris 2002, ‹www.oecd.org/dataoecd/16/22/15582260.pdf›.

124 Organisation for Economic Co-operation and Development, Task Force on Spam, Report on the OECD task force on spam: Anti-spam toolkit of recommended policies and measures, Paris 2006, ‹www.oecd.org/dataoecd/63/28/36494147.pdf›.

125 SR 0.784.03.

Formen der Selbst- und Koregulierung diskutiert. So haben beispielsweise im Februar 2007 die an mobilen Mehrwertdiensten beteiligten Provider und die Europäische Kommission eine Vereinbarung geschlossen,[126] mit welcher sich die Provider verpflichten, innerhalb eines Jahres ein effektives Selbstregulierungssystem aufzubauen, dass eine wirksame Separierung von schädlichen Inhalten bei unter 18-jährigen Handynutzern gewährleisten soll. Die Fortschritte werden von der Kommission im Frühjahr 2008 evaluiert. Sollten gesetzgeberische Schritte notwendig erscheinen, erwägt die Kommission die Einführung eines Koregulierungsrahmens.[127]

C. Internationale Harmonisierung des Urheberstrafrechts in der Informationsgesellschaft

I. Problembeschreibung – Mangelhafte Durchsetzbarkeit der urheberrechtlichen Ausschliesslichkeitsrechte im Cyberspace und digitalen Umfeld

Die im Oktober 2007 abgeschlossene Revision des schweizerischen Urheberrechtsgesetzes (URG) folgte unter anderem dem Ziel, die WIPO-Staatsverträge (WCT, WPPT) für die Schweiz zu ratifizieren und deren Vorgaben in nationales Recht umzusetzen.[128] Gleichzeitig sollte damit dem Bedürfnis Rechnung getragen werden, den Rechtsschutz des Urheberrechts im digitalen Umfeld zu stärken; dies insbesondere mit Blick auf das Internet und den Bereich der Mobilkommunikation, welche neue Nutzungshandlungen ermöglichen und die bisherige Limitiertheit der physischen Vervielfältigung oder Verbreitung beseitigt haben. Die Errungenschaften der Informations- und Kommunikationstechnologie eröffnen den Rechteinhabern attraktive neue Geschäftsmodelle für Audio- und audiovisuelle Produkte.[129] Sie bergen aber auch die Gefahr eines massenhaften Missbrauchs, wie der rechtswidrige Up- und Download urheberrechtlich geschützter Musik, Filme und Computerspiele in P2P-Netzwerken

126 European Framework for Safer Mobile Use by Younger Teenagers and Children, February 2007.

127 European Commission, Summary of the results of the public consultation ‹Child safety and mobile phone services›, S. 7 und S. 11, ‹http://ec.europa.eu/information_society/activities/sip/docs/public_consultation_mobile/public_consultation_rsults_en.pdf›. Im Auftrag der Europäischen Kommission führte das Hans-Bredow-Institut eine grosse international vergleichende Studie über Koregulierungsmassnahme im Bereich Medien und Jugendschutz durch, siehe Hans-Bredow Institut, Endbericht, Studie über Co-Regulierungsmassnahmen im Medienbereich, Hamburg 2006.

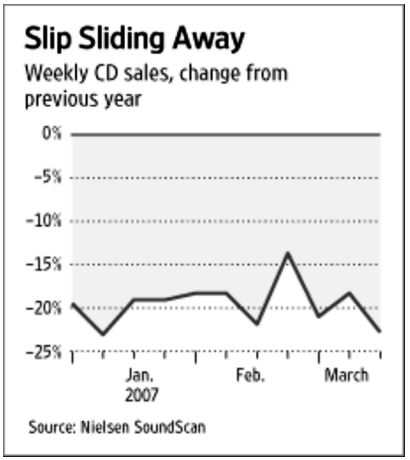
128 Vgl. Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG), Änderung vom 5. Oktober 2007, BBl. 2007, 7149; Bundesbeschluss über die Genehmigung von zwei Abkommen der Weltorganisation für geistiges Eigentum und über die Änderung des Urheberrechtsgesetzes vom 5. Oktober 2007, BBl. 2007, 7201.

129 Beispielhaft sind zu nennen: virtuelle Nutzung auf Zeit, Auswahldienste, Abonnemente.

zeigt. Weiter oben wurde darüber berichtet, dass es sich dabei möglicherweise um die statistisch bedeutsamste Massenstraftat handelt.

Nach neueren Erhebungen hat sich im Bereich der Musikindustrie die Erosion des CD-Verkaufs fortgesetzt. In den ersten drei Monaten des Jahres 2007 wurden in den USA noch einmal 20 Prozent weniger CDs verkauft als vor einem Jahr (siehe Abbildung 2). Der Anstieg digitaler Downloads im Internet (54 Prozent innerhalb eines Jahres) reicht nicht aus, um die Verluste im CD-Geschäft zu decken. In der Schweiz ist 2007 im Vergleich zum Vorjahr ein Rückgang der CD-Verkäufe von 9 Prozent zu verzeichnen.[130] Insgesamt ist der Verkauf von Musik um 10 Prozent gesunken. Obschon das Ausmass des Zusammenhangs strittig ist, muss als eine Hauptursache dieser negativen Entwicklung die illegale Verbreitung von Musikdateien in P2P-Netzwerken angesehen werden. Amerikanischen Schätzungen zufolge sollen pro Monat eine Milliarde Musikstücke illegal angeboten und vervielfältigt werden.[131]

Abbildung 2: Wöchentliche CD-Verkäufe, Veränderung im Vergleich zum Vorjahr[132]



Mit zunehmender Bandbreite der privaten Internetverbindungen und verbesserten dezentralen Filesharing-Systemen hat sich diese negative Entwicklung

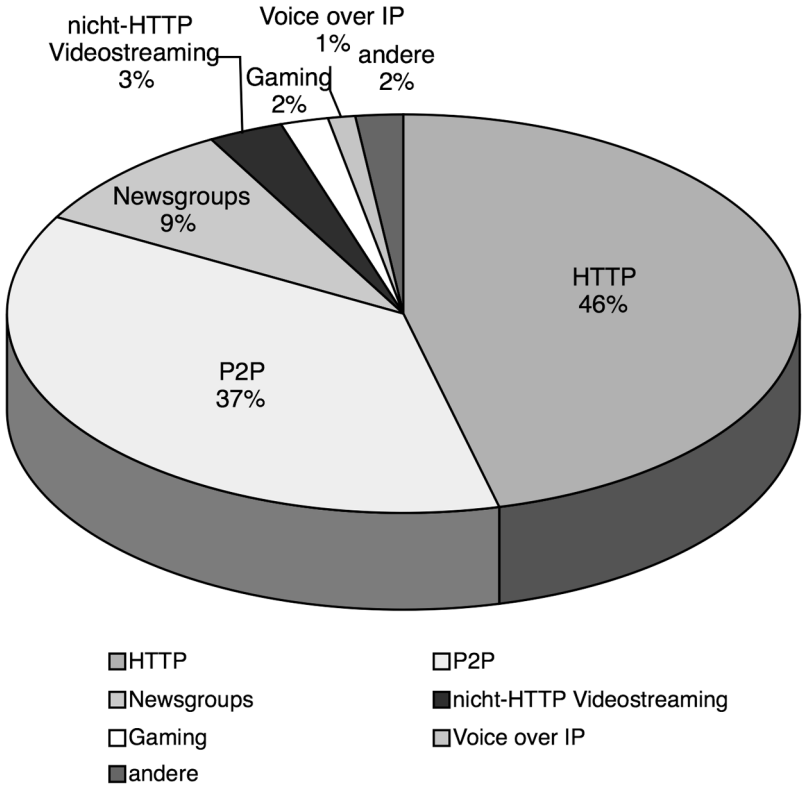
130 Quelle: Ifpi Schweiz, zit. in Eric Baumann, Downloads machen den Einbruch bei CDs nicht wett, Tages-Anzeiger 26.3.2008, S. 29.

131 Ethan Smith, Sales of music, long decline, plunge sharply, Wall Street Journal, 21 March 2007, S. A1; siehe zum Ausmass des P2P-Datenverkehrs auch Christian Schwarzenegger, Urheberstrafrecht und Filesharing in P2P-Netzwerken – Die Strafbarkeit der Anbieter, Downloader, Verbreiter von Filesharing-Software und Hash-Link-Setzer, in: Christian Schwarzenegger, Oliver Arter und Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 205–255, S. 207 ff. m.N.

132 Quelle: Nielsen SoundScan, zit. in Smith (Fn. 131), S. A1.

schon auf den audiovisuellen Sektor übertragen. Eine statistische Erfassung der Datenpakete, die im Internet zirkulieren, zeigte während der letzten Jahre, dass das P2P-Filesharing gemessen an der übertragenen Datenmenge eine grössere Bedeutung hatte als alle anderen Internetanwendungen. Innerhalb der Filesharing-Protokolle lagen die BitTorrent- und eDonkey-Netzwerke an der Spitze.[133] 2007 scheint der Anteil des Abrufvolumens für Webdaten (HTTP) erstmals wieder über dem Anteil an Datentransfers in P2P-Netzwerken (P2P) zu liegen (siehe Abbildung 3).

Abbildung 3: Datenverkehr im Internet nach Anwendungsprotokollen (USA, 2007)[134]



133 Quelle: Andrew Parker, The True Picture of Peer-to-Peer-Filesharing, July 2004, Daten wiedergegeben in Schwarzenegger (Fn. 131), S. 209.

134 Quelle: Ellacoya Networks, zit. in: Nate Anderson, The YouTube effect: HTTP traffic now eclipses P2P, 19 June 2007, ‹http://arstechnica.com/news.ars/post/20070619-the-youtube-effect-http-traffic-now-eclipses-p2 p.html›.

Der Zuwachs des Datenverkehrs im WWW ist auf den Popularitätszuwachs von Streaming-Diensten zurückzuführen, darunter insbesondere der Videoplattformen wie YouTube, MySpace TV-Video, Yahoo! Video und Veoh. Gemäss der zitierten Erhebung machen traditionelle Webseiten nur 45 Prozent der abgerufenen HTTP-Daten aus. 36 Prozent der HTTP-Datenpakete enthalten Videostreams, 5 Prozent sind Audiostreams.[135]

Der Up- und Download von urheberrechtlich geschützten Daten in P2P-Netzwerken, aber auch mittels anderer Dienste des Internet (E-Mail, Web, FTP, Chat) ist an keine Landesgrenzen gebunden. Die tiefen Kosten der Computerinfrastruktur, der Internetanbindung und der Speichermedien machen es selbst Laien möglich, sich praktisch kostenlos mit den neuesten Medieninhalten «einzudecken». Die Internationalität der Vorgänge, die Flüchtigkeit der Datenspuren und ein gut ausgebauter Schutz des Fernmeldegeheimnisses erschweren den Nachweis der Urheberrechtsverletzung oder der Verletzung verwandter Schutzrechte. Es ist ausserdem nicht zu verkennen, dass die funktionale Arbeitsteilung in P2P-Netzwerken[136] nicht zuletzt deshalb geschaffen wurde, um eine mögliche zivilrechtliche Haftung bzw. Strafbarkeit durch die Fragmentierung in viele Teilverantwortlichkeiten auszuschalten oder zumindest zu minimieren. Die P2P-Nutzer, der Filesharing-Software-Hersteller und der Informationsportal-Betreiber tragen je ein kleines Stück zum Funktionieren einer gigantischen «P2P-Kopiermaschine» bei, die nach gesichertem Wissensstand vornehmlich für unrechtmässige Musik-, Film- und Software-Up- und Downloads eingesetzt wird.[137]

> «Die Freiheit und Perfektion der digitalen (Kopier-)Technik haben das Internet zum kostenlosen Selbstbedienungsladen werden lassen.»[138]

Die zivilrechtlichen Instrumente[139] zum Schutz vor Urheberrechtsverletzungen und Verletzungen von verwandten Schutzrechten sind dem Verletzungspotential der weltweiten digitalen Verbreitung nicht mehr gewachsen, insbesondere wenn man an deren prozessuale Durchsetzung denkt. Soll der Rechtsschutz des Urheberrechts im digitalen Umfeld auf internationaler wie nationaler Ebene verbessert werden, sind zwei Schlussfolgerungen zu ziehen:

1. Ähnlich wie das Vermögensstrafrecht einen subsidiären Schutz gegen gravierende Verletzungen des Eigentums und der Vermögensrechte statuiert,[140] muss das Urheberstrafrecht in Zeiten der Informationsgesellschaft und der zu-

135 Anderson (Fn. 134).
136 Filesharing-Software, dezentrale Server-Funktion auf privaten Computern, Fragmentierung der Up- und Download-Daten, Zugangsinformationen über Hash-Link-Portale oder Webforen.
137 Schwarzenegger (Fn. 131), S. 245 f.
138 Hannes Rösler, Pauschalvergütungen für digitale Medieninhalte – Reflexionen der U.S.-amerikanischen Rechtswissenschaft zum Urheberrecht im digitalen Zeitalter, GRUR Int. 2005, S. 991–997, S. 997.
139 Feststellungs-, Leistungs- oder Schadenersatzklagen, siehe Art. 61 ff. URG.
140 Siehe für die Schweiz Art. 137 ff. StGB.

nehmenden Bedeutung immaterieller Rechtsgüter aufgewertet werden.[141] Nur im strafrechtlichen Kontext bestehen ausreichend effektive Mittel zur schnellen grenzüberschreitenden Ermittlung der Täterschaft und zur Sicherung der Beweise.[142] Die grenzenlosen, auf Tausende von Teilnehmern verteilten P2P-Netzwerke haben eine Zustand geschaffen, in welchem sich die massenhafte Missachtung von Urheberrechten und verwandten Schutzrechten lohnt. Nur mit strafrechtlichen Sanktionen – so scheint es zumindest aus heutiger Sicht – kann das Unrechtsbewusstsein für den «Diebstahl» immaterieller Rechtsgüter gestärkt werden, wobei auch dies nur im Zusammenspiel mit präventiven Massnahmen und einer aktiven Informationspolitik gelingen kann. Die urheberstrafrechtlichen Bestimmungen müssen daher sorgfältig mit den gesetzlich garantierten Urheberrechten und verwandten Schutzrechten koordiniert werden. Eine Aufwertung des strafrechtlichen Instrumentariums ist dort angezeigt, wo der zivilrechtliche Schutz durch globale Filesharingsysteme und andere Kommunikationskanäle geschwächt bzw. wirkungslos ist.

2. Der zivil- und strafrechtliche Schutz der Urheberrechte und verwandten Schutzrechte beschränkte sich bisher auf Verletzungshandlungen. Digitale Daten sind aber beliebig und auf einfachste Weise vervielfältig- und übertragbar, so dass Verletzungshandlungen mittlerweile weiter verbreitet sind als die legale Nutzung und folglich die Verfolgung der Rechtsverletzung im Kontext moderner Kommunikationsnetzwerke einer Sisyphusarbeit gleichkommt. Soll dieser Zustand nicht einfach hingenommen werden, muss der Schutz von Urheberrechten und verwandten Schutzrechten in das Vorfeld der Verletzung verlagert werden. Kriminalpolitisch kann dieses Ziel auf unterschiedliche Weise umgesetzt werden: So kann der Gesetzgeber beispielsweise im Vorfeld die Distribution von Filesharing-Software unterbinden,[143] die Einrichtung von Hash- oder Direct-Links auf urheberrechtlich geschützte Daten kriminalisieren[144] oder das Herstellen einer Kopie von einer offen-

141 Skeptisch Lucas David, in: Barbara K. Müller und Reinhard Oertli (Hrsg.), Stämpflis Handkommentar, Urheberrechtsgesetz (URG), Bern 2006, Art. 69 mit Rev. Art. 69a (neu) N 3: «Aus schweizerischer Sicht stellen die strafrechtlichen Sanktionen einen wichtigen Bestandteil des urheberrechtlichen Schutzes dar, auch wenn ihre praktische Bedeutung aufgrund der zeitlichen Überforderung und fachlichen Unvertrautheit der kantonalen Untersuchungsbehörden mit der Materie und deren technischen Sachverhalten erfahrungsgemäss nicht allzu gross ist».

142 Vgl. Art. 14 ff. CCC (Verfahrensrecht), Art. 23 ff. CCC (Internationale Zusammenarbeit), hierzu unten C.III.3.c, S. 452.

143 Etwa durch einen verwaltungsrechtlichen Erlass, der für den Erwerb, Handel etc. ein Zulassungsverfahren vorsehen könnte, oder durch eine Verbotsnorm im StGB, vgl. Art. 179sexies (Inverkehrbringen und Anpreisen von Abhör-, Ton- und Bildaufnahmegeräten).

144 Bisher kann eine Strafbarkeit von Filesharing-Software- und Hash-Link-Anbietern nur qua Gehilfenschaft zu einem unrechtmässigen Angebot oder zu einer unrechtmässigen Vervielfältigung eines Users entstehen, siehe Schwarzenegger (Fn. 131), S. 240 ff.; ebenso KGer GR, 27.7.2006, PS 06 6, Erw. 3; BezGer Frauenfeld, 11.2.2008, S.2006.42.

sichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage strafrechtlich verfolgen.[145] Charakteristisch für diesen Ansatz ist die Intervention gegen wichtige Schaltstellen *vor* dem massenhaften Download durch einzelne Nutzer. Im Bereich digitaler Information eignen sich auch technische Schutzmassnahmen zur Sicherung vor unrechtmässiger Vervielfältigung.[146] Die internationalen Harmonisierungsinstrumente haben die technischen Schutzmassnahmen in den Vordergrund gerückt, weshalb sie von den Mitgliedstaaten zivil- und strafrechtlich abgesichert werden müssen. Es wurde in der Debatte um die Erweiterung des urheberrechtlichen Schutzes zunächst kaum beachtet, dass damit eine Verlagerung des Rechtsgüterschutzes in das Vorfeld einer Verletzung verbunden ist, der notwendigerweise mit einer Akzentverschiebung *weg vom zivilrechtlichen hin zum strafrechtlichen Schutz* verbunden ist. Aus urheberstrafrechtlicher Sicht wird dadurch der Deliktstypus gewechselt. Urheberstrafrechtliche Bestimmungen waren bisher ausschliesslich als Verletzungsdelikte gefasst. Bei den neuen Strafnormen handelt es sich entweder um *konkrete Gefährdungsdelikte* (rechtliche Sicherung der technischen Schutzvorkehrung) oder um *abstrakte Gefährdungsdelikte* (Vorbereitungshandlungen im Hinblick auf Umgehungshandlungen). In letzterem Fall existiert eigentlich kein zivilrechtlicher Schutzbereich mehr. Die Norm schützt dann vielmehr ein gesellschaftliches Interesse. Zu den Konsequenzen später.

II. P2P-Filesharing-Netzwerke und technische Schutzmassnahmen

1. Funktionsweise der Internetkommunikation

Wer auf dem World Wide Web die Nachrichten des Tages abrufen will, gibt die Webadresse[147] (= URL) eines Informationsportals – z.B. http://news.bbc.co.uk – in die Adresszeile des Browsers ein und betätigt die Eingabetaste. Vorausgesetzt der Computer ist mit dem Internet verbunden, löst dieser Eingabevorgang eine elektronische Datenabfrage beim Web-Server der BBC aus. Die unter der URL-Adresse bereitgestellten Dateien werden dann von diesem *Server* – in Datenpakete unterteilt – zum Computer des Abfragenden übertragen. Der *Client,* wie der Rechner des Internetnutzers genannt wird, speichert die eintreffenden Datenpakete in seinem RAM-Speicher und stellt sie im Browser dar. Clients

145 So der deutsche Lösungsansatz, siehe §§ 53 Abs. 1 Satz 1, 106 Abs. 1 dUrhG. Dazu Michael Heghmanns, Musiktauschbörsen im Internet aus strafrechtlicher Sicht, MMR 2004, S. 14–18, S. 15 f.; Hilgendorf, Frank und Valerius, (Fn. 26), S. 166 f. m.w.N.; Thomas Dreier und Gernot Schulze, Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz, Kommentar, München 2006, § 53 N 11 und § 106 N 6.

146 Siehe dazu unten C.II.4, S. 444.

147 Uniform Resource Locator (URL), siehe Andrew S. Tanenbaum, Computer networks, 4. ed., Upper Saddle River 2003, S. 622 ff.; Douglas E. Comer, Computer networks and Internet with internet applications, 4. ed., Upper Saddle River 2004, S. 535, 679.

dienen somit zum Abruf und Empfang von digitalisierter Information sowie zu deren Darstellung.[148] Die Daten können danach auf einem permanenten Datenträger (Festplatte, CD, DVD usw.) abgespeichert werden. Ein Charakteristikum der Client-Server-Architektur des Internet ist darin zu sehen, dass auf den Computern der User, also den Clients, keine Daten zum Download bereitgehalten werden. Diese Funktion ist den Servern vorbehalten, die in der Regel nicht von Internetnutzern, sondern von kommerziellen Host-Providern betrieben werden.[149]

In *Peer-to-Peer-Netzwerken* wird die Arbeitsteilung des Client-Server-Modells aufgegeben.[150] Technisch basieren diese Netzwerke auf einem simplen Konzept: aus jedem Client – also Computer eines Internetnutzers – wird gleichzeitig ein Server gemacht. In P2P-Netzwerken ist es daher möglich, Daten direkt vom Computer eines Peers, d.h. eines anderen ans P2P-Netzwerk angeschlossenen Internetnutzers, herunterzuladen. Ein zentraler Host-Server wird hierzu nicht mehr benötigt. Die meisten der heute gebräuchlichen P2P-Netzwerke ermöglichen nicht nur die Suche und Datenübertragung von Musiktiteln im MP3-Format, sondern von Musik, Filmen, Software, Texten und Bildern in den verschiedensten Datenformaten. Mit zunehmender Rechnerleistung moderner Computer und den erhöhten Datenübertragungsvolumina (Bandbreite) der Netzwerke steigt auch die Leistungsfähigkeit eines solchen P2P-Netzwerks, denn in diesem müssen die Computer der Nutzer gleichzeitig die lokale Datenverarbeitung und die Server-Funktion übernehmen.[151]

---

148 Die Darstellung erfolgt auf dem Bildschirm des Computers.

149 Unrechtmässige Angebote und Downloads können selbstverständlich auch in der Client-Server-Architektur realisiert werden, insbesondere mittels passwortgeschützter FTP-Server, Newsgroup-Postings, IRC oder E-Mail-Attachments. Urheberstrafrechtlich sind solche Angebote und Downloads gleich zu behandeln, wie entsprechende Handlungen in P2P-Netzwerken. Am 21. Februar 2007 wurden die Verantwortlichen des weltweit wohl grössten Falles illegaler Downloads vom Landgericht Mühlhausen wegen gewerblicher Verletzung von Urheberrechten zu Bewährungsstrafen verurteilt. Auf der Internet-Site www.ftp-welt.com konnten sich Interessenten über ein Flat-Rate-Abo von 135 € pro Monat unbegrenzt Software-Pakete oder Filme von FTP-Servern herunterkopieren, die im Ausland standen. Seit Juni 2003 registrierten sich dort 45 000 Personen. Die Betreiber haben Einkünfte von über 600 000 € erzielt und einen Schaden in zweistelliger Millionenhöhe verursacht. Die Staatsanwaltschaft wollte ursprünglich nicht nur gegen die Betreiber von www.ftp-welt.com, sondern gegen alle 45 000 Abonnenten Strafverfahren einleiten. Siehe zum Urteil die Meldung des Heise-Newstickers vom 21.2.2007 ‹www.heise.de/newsticker/Bewaehrungsstrafen-fuer-FTPWelt-Betreiber–/meldung/85675›.

150 Gewisse Server-Funktionen (Verzeichnisse, Rooting) bleiben in einigen P2P-Netzwerken erhalten, doch erfolgt der Datenabruf und die entsprechende Übertragung immer zwischen den Peers.

151 Zu technischen Aspekten siehe die Website der Peer-to-Peer Research Group, Computer Science Department, Stanford University: ‹http://infolab.stanford.edu/peers›; aus der juristischen Literatur Till Kreutzer, Napster, Gnutella & Co.: Rechtsfragen zu Filesharing-Netzen aus der Sicht des deutschen Urheberrechts de lege lata und de lege ferenda, GRUR 2001, 193 ff.; Andreas Glarner, Musikpiraterie im Internet. Urheberstrafrechtliche Betrachtungen, Bern 2002, S. 20 ff. m.N.; Heghmanns (Fn. 145), S. 14 f.; Philippe Gilliéron, Propriété intellectuelle et Internet, Lausanne 2003, S. 304 f.; Sven Freiwald, Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing, Baden-Baden 2004.

2. *Zentralisierte und dezentralisierte P2P-Filesharing-Netzwerke*

P2P-Netzwerke basieren einerseits auf einer geeigneten Hardware[152] und andererseits auf einer P2P-Filesharing-Software, die auf den ans Netzwerk angebundenen Computern installiert sein muss.[153] Es gibt zahlreiche Softwareangebote, die jeweils auf unterschiedlichen Datenübertragungsprotokollen aufbauen und im aktivierten Zustand im Zusammenwirken mit anderen Rechnern eine bestimmte Netzwerktopologie bilden. Der Aufbau der Netzwerke kann zentralisiert oder dezentralisiert, hierarchisch oder als Ring gleichwertiger Peer-Rechner konzipiert sein. Es existieren auch hybride Mischformen.

Für die normative Einordnung ist wichtig, welche Akteure an einem unrechtmässigen Angebot oder Download unmittelbar und in unterstützender Funktion beteiligt sind. In *zentralisierten P2P-Netzwerken* der ersten Generation (Napster, Aimster) wurden zentrale Server eingesetzt, welche durchsuchbare Listen der angeschlossenen Peers und der Dateien, die dort zum Download angeboten wurden, speicherten. Jede im Napster-Programm ausgeführte Suche nach einer Datei griff auf diesen zentralen Server zu, der eine Mittlerfunktion übernahm. Erst der Download der ausgewählten Datei wurde direkt zwischen den Peers abgewickelt.

Bei der zweiten Generation von P2P-Netzwerken werden keine Datei-Listen mehr auf zentralen Servern abgespeichert. Je nach Netzwerktopologie benötigen diese Systeme allerdings doch noch einen oder mehrere Server, so etwa in zentralisierten-dezentralisierten Netzwerken, in denen sogenannte Super Peers eine Liste von Rechnern bereithalten, die im Moment im Netzwerk aktiv sind (eDonkey). Komplett *dezentralisierte P2P-Netzwerke* brauchen nicht einmal mehr diese Server (EarthStation5, KaZaA, Overnet).

BitTorrent,[154] eines der populärsten P2P-Systeme, unterscheidet sich wesentlich von den anderen P2P-Netzwerken KaZaA, eDonkey und Gnutella, bei denen ein Kontakt zu allen aktiven Peers und allen dort angebotenen Dateien gewährleistet ist. Bei BitTorrent geht es um eine möglichst schnelle Verteilung einer bestimmten Datei an möglichst viele Personen, wobei ein BitTorrent-Client[155] bei jedem Download gleichzeitig immer – vom P2P-User nicht verhin-

---

152 Computer und das elektronische Kommunikationsnetz (Internet), über welches die Daten übertragen werden.

153 Diese übernimmt die Bearbeitung von externen Datenabfragen, die Datenübertragung, die Zwischenspeicherung von eintreffenden Datenübertragungen, das Routing von Daten zwischen Peers und die eigentlichen Funktionen des Filesharings (Nutzeroberfläche, Dateiverwaltung, Suchfunktionen usw.).

154 Siehe hierzu die Website von BitTorrent, ‹www.bittorrent.com›, und den entsprechenden Eintrag in Wikipedia, ‹http://de.wikipedia.org/wiki/BitTorrent›.

155 P2P-Filesharing-Programme werden im Fachjargon vereinfachend als Clients bezeichnet, obschon sie gerade keine Clients im Sinne des Client-Server-Modells sind. Ein Client wird also von P2P-Usern zum Download von Dateien sowie zum Upload eigener Dateien verwendet und dient als Peer im Netzwerk. BitTorrent-Clients sind Programme, welche das BitTorrent-Protokoll unterstützen.

derbar – den Upload zulässt *(swarming)*. Hierzu werden die Hash-Werte[156] für alle Datenblöcke der Datei in der Form eines BitTorrent-Files angelegt.[157] Dieses File lässt sich in der Folge bequem via E-Mail, Webseite oder andere Dienste verbreiten. Für einen Download der Datei muss der Empfänger nur noch auf das BitTorrent-File klicken, was bei installiertem BitTorrent-Client sofort den Datentransfer auslöst. Seit 2005 funktioniert das BitTorrent-System ohne zentralen Server (Tracker-Server). Die Koordination der Downloads der verschiedenen Datenblöcke wird nun direkt von der Clientsoftware vorgenommen. Damit wird es schwieriger, die Verbreitung der Dateien zu blockieren und die beteiligten User zu ermitteln.

Das *eDonkey-Netzwerk*[158], welches durch mehrere Filesharing-Programme unterstützt wird (eDonkey2000, MLDonkey, eMule, Shareaza), basiert auf dem Multisource File Transfer Protokoll (MFTP). Es ermöglicht das gleichzeitige Herunterladen von Fragmenten einer Datei von unterschiedlichen Quellen und sorgt auch dafür, dass fragmentarisch vorhandene Dateien automatisch freigegeben und anderen Benutzern zum Download bereitgestellt werden. eDonkey ermöglicht die Suche von Dateien mit deren Hash-Codes, d.h. einem elektronischen Wasserzeichen. Diese Funktion ermöglicht die Identifikation von identischen Dateien auch bei abweichendem Dateinamen. Hash-Code-Suchen können direkt aus Webpages oder E-Mails mittels Hash-Links übernommen und ausgeführt werden.[159] eDonkey ist wie BitTorrent so konfiguriert, dass die Datenblöcke, die heruntergeladen wurden, gleichzeitig für Dritte abrufbar sind. Zum Netzwerk gehören neben dem Filesharing-Programm auch Server. Die eDonkey-Clients der P2P-User wählen zunächst diese Server an, von wo sie eine Liste der aktiven P2P-Netzwerkrechner abrufen. Alle weiteren Kommunikationsprozesse, insbesondere der Download, laufen danach immer von Peer zu Peer.

Eine *dritte Generation* von P2P-Netzwerken versucht, die Anonymität der Produzenten und Konsumenten von Informationen in der Datenübertragung durch Verschlüsselung der Dateien zu gewährleisten (Freenet,[160] Invisible Internet Project [I2P],[161] GNUnet[162]). Damit hätten die Nutzer keine Kontrolle und

156 Ein Hash-Wert bildet eine umfangreiche Datei eindeutig in einer kleineren Zeichenmenge ab. Dieser Wert ist wie ein elektronisches Wasserzeichen der Datei und dient zu ihrer Auffindung http://de.wikipedia.org/wiki/Datenbank für http://de.wikipedia.org/wiki/Digitale_Signatur.

157 Dateiendung: ~.torrent.

158 Am 12. September 2006 wurde der Vertrieb des eDonkey-Clients eingestellt und die entsprechenden Webseiten ‹www.edonkey2000.com› und ‹www.overnet.com› abgeschaltet. De facto ist jetzt der eMule-Client das Standardprogramm für dieses Protokoll, siehe hierzu den Eintrag in Wikipedia: ‹http://de.wikipedia.org/wiki/Edonkey›.

159 Schwarzenegger (Fn. 131), S. 237 ff.

160 Siehe hierzu ‹http://freenetproject.org›. Erklärtes Ziel dieses kooperativen verteilten Filesharingsystem ist es, Besitzer und Vermittler der gespeicherten und übertragenen Informationen «unangreifbar» zu machen, siehe ‹http://archiv.tu-chemnitz.de/pub/2002/0050/data/vortrag.html›.

161 Siehe hierzu ‹www.i2p2.de›.

162 Siehe hierzu ‹http://gnunet.org›.

auch kein Wissen über die Übertragungsvorgänge, in denen sie als Knotenpunkte des Netzwerks fungieren.

3. Viele Beteiligte an der Kommunikationskette

Die Frage, wer für die Verletzung von Urheberrechten und verwandten Schutzrechten bei der Übertragung digitaler Dateien in P2P-Netzwerken verantwortlich sei, lässt sich nicht leicht beantworten, weil die oben beschriebenen Kommunikationsprozesse von der Mitwirkung zahlreicher Personen bzw. der von ihnen betriebenen Rechner und Programme abhängen. Am Beginn der Distributionskette sind Personen angesiedelt, die Dateien urheberrechtlich geschützter Werke – oder Fragmente davon – zum Download via P2P-Netzwerk bereitstellen («Anbieter»). Am anderen Ende der Kette agieren Personen, die solche Werkdateien – oder wiederum Teile davon – via P2P-Netzwerk herunterladen («Downloader»). Als Bindeglied zwischen Anbietern und Downloadern steht die P2P-Filesharing-Software, mit deren Aktivierung durch unzählige User sich das P2P-Netzwerk erst konfiguriert. Es stellt sich die komplizierte Frage, wie der Beitrag der Software-Hersteller und -anbieter an späteren Urheberrechtsverletzungen im P2P-Netzwerk (straf)rechtlich zu würdigen ist. Ist das P2P-Netzwerk auf Supernodes angewiesen, d.h. zentrale Server mit Adressierungsinformationen wie zum Beispiel im eDonkey-Netzwerk, sind auch die Betreiber dieser Server involviert. Schliesslich kann auch die Informationsvermittlung durch Hash-Link-Webdirectories oder Torrent-File-Directories eine kausale Förderung dieser Urheberrechtsverletzungen darstellen.

4. Technische Schutzmassnahmen

Der rechtliche Schutz technischer Schutzmassnahmen[163] gilt im Offline- wie im Online-Bereich. Der Schutz der Urheberrechte und Leistungsschutzrechte vor unerlaubter Nutzung greift folglich nicht nur im Internet und sonstigen elektronischen Netzwerken. Dennoch ist die Einführung entsprechender Normen durch internationale Harmonisierungsinstrumente vor allem vor dem Hintergrund des digitalen und vernetzten Umfeldes zu erklären. Weiter gefasst ist der Begriff der Digital Rights Management (DRM)-Systeme, die neben den technischen Schutzfunktionen auch Mechanismen zur Feststellung und Abrechnung des konkreten Umfangs der Nutzung von Werkdaten umfassen.[164] Damit steht den Urhebern oder den Verwertern als derivativen Berechtigten ein Mittel zur

163 Der rechtliche Schutz wird beschränkt auf «wirksame technische Massnahmen», vgl. Art. 6 Abs. 3 Richtlinie 2001/29/EG, Art. 39a Abs. 2 URG, § 95a Abs. 2 Satz 2 dUrhG, 90c Abs. 2 öUrhG. Unter wirksamen technischen Massnahmen sind alle Technologien, Vorrichtungen und Bestandteile zu verstehen, die im normalen Betrieb dazu bestimmt sind, Rechtsverletzungen zu verhindern oder einzuschränken, und die die Erreichung dieses Schutzziels sicherstellen.

164 Tobias Baumgartner, Privatvervielfältigung im digitalen Umfeld, Zürich 2006, S. 17 m.N.

Verfügung, dass den Verkauf von Informationen vom «Informationsprodukt» im gegenständlichen Sinn loslöst und über definierte Lizenzvereinbarungen eine massgeschneiderte Nutzung in der Form technisch gesicherter Werkdaten ermöglicht.

Zu den technischen Massnahmen werden alle Hardware- oder Software-Lösungen gezählt, die beim Abruf oder bei der Nutzung eines geschützten Werkes oder anderer Schutzgegenstände dafür sorgen, dass nicht genehmigte Handlungen verhindert werden. Es werden zwei Ansätze unterschieden: Zugangskontrollen und Nutzungskontrollen.[165] Zugangskontrollen werden beispielsweise durch die programmgesteuerte Kontrolle von Passwörtern bzw. Login-Daten oder die Entschlüsselung von kryptographisch gespeicherten Daten erzielt. Eine Nutzungskontrolle kann demgegenüber in einer technischen Beschränkung der Nutzungshäufigkeit, -dauer bzw. -disponibilität (Beschränkung auf Lesefunktion) bestehen oder sich auf die Lesbarkeit nur durch bestimmte Lesegeräte beziehen. Eine nachträgliche Erkennbarkeit der Nutzung kann durch hardware- oder softwarebasierte Kennzeichnung der Werkdaten bzw. des Datenträgers, z.B. durch digitale Wasserzeichen oder Koppelung mit persönlichen Daten des Konsumenten, gewährleistet werden.

III. Konventionsrechtliche Vorgaben und internationaler Schutzstandard

Der Rechtsschutz im digitalen Umfeld wird für das Urheberrecht zunehmend von internationalen, konventionsrechtlichen Vorgaben vorgezeichnet und geprägt. Für die Schweiz standen im Rahmen der letzten Revision des URG zwei internationale Urheberrechtsabkommen im Vordergrund: Der WIPO-Urheberrechtsvertrag (WCT) und der WIPO-Vertrag über Darbietungen und Tonträger (WPPT). Indessen beschränkt sich der konventionsrechtliche Rahmen der Urheberrechtsgesetzgebung nicht auf diese Abkommen. Der internationale Schutzstandard – insbesondere der strafrechtliche – wird durch weitere völkerrechtliche Instrumentarien definiert. Schliesslich ist auch der Vergleich mit der Gesetzgebung der wichtigsten Industrieländer von Bedeutung, wenn man an die internationale Rechtshilfe in Strafsachen und insbesondere die grenzüberschreitende Beweissicherung denkt.

165 Ausführlich am Beispiel der DVD und von Handy-Inhalten Volker Grassmuck, Wissenskontrolle durch DRM: von Überfluss zu Mangel, in: Jeanette Hofmann (Hrsg.), Wissen und Eigentum, Geschichte, Recht und Ökonomie stoffloser Güter, Bonn 2006, S. 164–186; Vgl. Enquete-Kommission des Deutschen Bundestages (Fn. 30), S. 296 f.; Baumgartner (Fn. 88), S. 17 ff.

1. TRIPS-Abkommen

Bereits das Abkommen über handelsbezogene Aspekte der Rechte an geistigem Eigentum (TRIPS, Annex 1C zum WTO-Vertrag von 1994)[166] verpflichtet die WTO-Mitgliedstaaten, anknüpfend an den bestehenden internationalen Abkommen (wie der revidierten Berner Übereinkunft[167] und dem Rom-Abkommen[168]) auf internationale Mindeststandards im Rechtsschutz des geistigen Eigentums (vgl. Art. 1 Ziff. 1). Das Abkommen fordert wirksame Verfahren für den Rechtsschutz des geistigen Eigentums und «Abhilfemassnahmen zur Abschreckung von weiteren Verletzungen» (Art. 41 Ziff. 1). Dass sich die Pflichten auch auf den *strafrechtlichen Schutz* gegen gewerbsmässige «Piraterie» erstrecken, geht aus Art. 61 TRIPS hervor:[169]

> Die Mitglieder sehen Strafverfahren und Strafen vor, die zumindest bei gewerbsmässiger vorsätzlicher Nachahmung von Markenwaren und bei gewerbsmässiger vorsätzlicher unerlaubter Herstellung urheberrechtlich geschützter Waren Anwendung finden. Die vorzusehenden Rechtsfolgen umfassen Freiheits- und/oder Geldstrafen, die ausreichen, um abschreckend zu wirken, und dem Strafmass entsprechen, das bei entsprechend schweren Straftaten angewandt wird. Gegebenenfalls umfassen die vorzusehenden Rechtsfolgen auch die Beschlagnahmung, die Einziehung und die Vernichtung oder Zerstörung der rechtsverletzenden Waren und der Materialien und Werkzeuge, die vorwiegend zur Begehung der Straftat verwendet wurden. Die Mitglieder können Strafverfahren und Strafen für andere Fälle der Verletzung von Rechten an geistigem Eigentum vorsehen, insbesondere wenn die Handlungen vorsätzlich und gewerbsmässig begangen werden.

Mit dem TRIPS-Abkommen wurde der Urheberrechtsschutz in den regulatorischen Rahmen des internationalen Freihandels aufgenommen und damit die Rolle der Urheber- und Leistungsschutzrechte als Wirtschaftsgut in einem globalen Markt hervorgehoben. Bei Art. 61 TRIPS handelt es sich um die erste Norm des internationalen Immaterialgüterrechts, welche den Mitgliedstaaten eine Pflicht auferlegt, unter anderem auch wirksame strafrechtliche Rechtsbehelfe und Sanktionen gegen gravierende Urheberrechtsverletzungen einzuführen. Teil III des Abkommens («Durchsetzung der Rechte an geistigem Eigentum») legt gleichzeitig einen Minimalstandard fest, den sich Staaten im Rahmen bilateraler Handelsabkommen gegenseitig garantieren.[170] Dadurch ent-

---

166 Abkommen vom 15. April 1994 zur Errichtung der Welthandelsorganisation, für die Schweiz in Kraft getreten am 1. Juli 1995 (SR 0.632.20).

167 SR 0.231.15.

168 SR 0.231.171.

169 Ausführlich zur Entstehungsgeschichte Thomas Dreier, TRIPS und die Durchsetzung von Rechten des geistigen Eigentums, GRUR Int. 1996, S. 205–218, S. 210 ff.; siehe auch Alesch Staehelin, Das TRIPs-Abkommen, Immaterialgüterrecht im Licht der globalisierten Handelspolitik, 2. Aufl., Bern 1999, S. 188.

170 Siehe beispielhaft Abkommen über Handel und wirtschaftliche Zusammenarbeit zwischen der Schweizerischen Eidgenossenschaft und der Bundesrepublik Jugoslawien vom 21. November 2001 (Inkrafttreten: 1.6.2002, SR 0.946.298.184), Anhang zu Art. 13 «Schutz des geistigen Eigentums», Art. 6: «Die Vertragsparteien treffen Durchsetzungsbestimmungen, welche einem

steht ein engmaschiges Netz gegenseitiger Verpflichtungen, die auch den strafrechtlichen Schutz international festigen.[171]

Auch bezüglich der Strafandrohungen enthält Art. 61 TRIPS eine Vorgabe: sie sollen jenen anderer Straftaten entsprechender Schwere gleichstehen. Zu denken ist etwa an den Diebstahl und Betrug.[172] Eine Nichtbefolgung der Vorgaben des TRIPS-Abkommens kann im Rahmen der WTO zu Sanktionen gegen den fehlbaren Staat führen.[173] Die Internationale Vereinigung für den Schutz des Geistigen Eigentums (AIPPI) hat 2002 Länderberichte und einen zusammenfassenden Gesamtbericht zur Umsetzung von Art. 61 TRIPS vorgelegt. Die Länder bzw. Ländergruppen, deren AIPPI-Gruppe einen Bericht vorgelegt hatte, gingen alle mit dem TRIPS-Abkommen konform,[174] doch bemängelt die Europäische Kommission in einem Richtlinienentwurf von 2003, dass u.a. bezüglich der Umsetzung der im TRIPS-Abkommen vorgesehenen strafrechtlichen Sanktionen weiterhin grosse Unterschiede in den Mitgliedstaaten bestünden.[175]

2. WIPO-Abkommen (WCT, WPPT)

Im Rahmen der Weltorganisation für geistiges Eigentum (WIPO) wurden 1996 ein WIPO-Urheberrechtsvertrag (WCT[176]) und ein WIPO-Vertrag über Darbietungen und Tonträger (WPPT[177]) abgeschlossen und von der Schweiz unterzeichnet. Darin verpflichten sich die Unterzeichnerstaaten, im Wesentlichen in-

---

dem TRIPS-Abkommen, insbesondere den Artikeln 41–61, vergleichbaren Niveau entsprechen.»

171 Die USA nutzen vor allem bilaterale Freihandelsabkommen dazu, die TRIPS-, WCT- und WPPT-Standards international durchzusetzen, siehe S. Haochen Sun, Copyright law under siege: An inquiry into the legitimacy of copyright protection in the context of the global divide, Journal of Intellectual Property and Competition Law 2005, S. 199 m.N.

172 Auf diese Straftatbestände weist David Vaver, Some aspects of the TRIPS agreement: Copyright enforcement and dispute settlement, Oxford 2000, S. 6, hin. Diese Vorgabe wurde allerdings von der Schweiz nicht umgesetzt. Die Strafdrohungen von Art. 67 Abs. 2 und Art. 69 Abs. 2 URG lauten in den revidierten Fassungen (BBl. 2007, 7204 f.): «Die Strafe ist Freiheitsstrafe bis zu *fünf Jahren* oder Geldstrafe. Mit der Freiheitsstrafe ist eine Geldstrafe zu verbinden.» Auf gewerbsmässigen Diebstahl (Art. 139 Ziff. 2 StGB) oder gewerbsmässigen Betrug (Art. 146 Abs. 2 StGB) steht dagegen eine Strafdrohung von «Freiheitsstrafe bis zu *zehn Jahren* oder Geldstrafe nicht unter 90 Tagessätzen» (meine Hervorhebungen).

173 So können die durch das WTO-Abkommen gewährten Vorzüge im Rahmen eines Streitschlichtungsverfahrens gemindert oder im Extremfall sogar die WTO-Mitgliedschaft entzogen werden, siehe zusammenfassend Till Kreutzer, Die Entwicklung des Urheberrechts in Bezug auf Multimedia der Jahre 1994–1998, Hamburg 1999, S. 74 f. m.N.

174 AIPPI, Executive Committee Meeting, Lisbon, June 16–22, 2002, Question Q 169, Criminal law sanctions with regard to the infringement of intellectual property rights, ‹www.aippi.org/reports/q169/gr_q169_index.htm›.

175 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Massnahmen und Verfahren zum Schutz der Rechte an geistigem Eigentum, KOM(2003) 46 endg., S. 14 ff.

176 Genf (1996), deutsche Version in ABl. L 89 vom 11.4.2000, S. 8 ff. und BBl. 2006, 3453 ff.

177 Genf (1996), deutsche Version in ABl. L 89 vom 11.4.2000, S. 15 ff. und BBl. 2006, 3463 ff.

haltsgleich für das Urheberrecht und bestimmte Nachbarrechte zur Einführung:[178]

1. des Ausschliesslichkeitsrechts, Werke bzw. Leistungsschutzgegenstände in der Weise drahtlos oder -gebunden *öffentlich zugänglich zu machen,* dass sie Mitgliedern der Öffentlichkeit an Orten und zu Zeiten ihrer Wahl zugänglich sind (Art. 8 WCT; Art. 10 und Art 14 WPPT);
2. eines hinreichenden *Schutzes* und wirksamer *Rechtsbehelfe gegen die Umgehung wirksamer technischer Vorkehrungen,* von denen Urheber bzw. Nachbarrechteinhaber in Ausübung ihrer Rechte Gebrauch machen und die Handlungen in Bezug auf die Werke bzw. Schutzgegenstände einschränken, die sie nicht erlaubt haben bzw. die gesetzlich nicht zulässig sind (Art. 11 WCT; Art. 18 WPPT);
3. eines entsprechenden *Schutzes* der am Exemplar des Werks oder Schutzgegenstands angebrachten *elektronischen Information zur Wahrung der Schutzrechte* (Art. 12 Abs. 1 lit. i und Abs. 2 WCT; Art. 19 Abs. 1 lit. i und Abs. 2 WPPT);
4. sowie dazu, in Übereinstimmung mit ihren Rechtsordnungen die notwendigen Massnahmen zu ergreifen, um die Anwendung der Abkommen sicherzustellen, und sicherzustellen, dass in ihren Rechtsordnungen Verfahren zur Rechtsdurchsetzung verfügbar sind, um ein *wirksames Vorgehen gegen jede Verletzung* von unter die Abkommen fallenden Rechten zu ermöglichen, einschliesslich beschleunigte Verfahren zur Verhinderung von Verletzungshandlungen und Rechtsbehelfen zur Abschreckung von weiteren Verletzungshandlungen (Art. 14 WCT; Art. 23 WPPT).

Die WIPO-Abkommen verlangen einen angemessenen Rechtsschutz durch sachgerechte materielle Sanktionen. Eine strafrechtliche Umsetzung ist nicht zwingend vorgesehen.[179]

3. Convention on Cybercrime

a. Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (Art. 10 CCC)

Die Convention on Cybercrime (CCC) des Europarats[180] auferlegt ihren Unterzeichnerstaaten – darunter der Schweiz – in Art. 10 CCC folgende Vorgaben für den strafrechtlichen Schutz spezifisch des Urheber- und Nachbarschutzrechts,

178 Genauer zu den Vorgaben von WCT und WPPT Botschaft, BBl. 2006, 3397 ff.; Cyrill P. Rigamonti, Schutz gegen Umgehung technischer Massnahmen im Urheberrecht aus internationaler und rechtsvergleichender Perspektive, GRUR Int. 2005, S. 1–14, S. 3 ff. m.w.N.

179 Ausführlich Michael Girsberger, Schutz von technischen Massnahmen im Urheberrecht, Die WIPO-Internetabkommen und deren Umsetzung in den Vereinigten Staaten, der Europäischen Union und der Schweiz, Bern 2007, S. 117 ff. m.w.N.

180 Siehe dazu oben B.I.3, S. 422 f.

darunter ausdrücklich auch der durch die WIPO-Abkommen aufgestellten Schutzstandards:

> **Artikel 10 – Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte[181]**
>
> (1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um Urheberrechtsverletzungen, wie sie im Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach der Pariser Fassung der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst vom 24. Juli 1971, dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Urheberrechtsvertrag festgelegt sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte, wenn diese Handlungen vorsätzlich, in gewerbsmässigem Umfang und mittels eines Computersystems begangen werden, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben.
>
> (2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Verletzungen verwandter Schutzrechte, wie sie im Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach dem Internationalen Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen (Abkommen von Rom), dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Vertrag über Darbietungen und Tonträger festgelegt sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte, wenn diese Handlungen vorsätzlich, in gewerbsmässigem Umfang und mittels eines Computersystems begangen werden, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben.
>
> (3) Eine Vertragspartei kann sich das Recht vorbehalten, eine strafrechtliche Verantwortlichkeit nach den Absätzen 1 und 2 unter einer begrenzten Zahl von Umständen nicht vorzusehen, sofern andere wirksame Abhilfen zur Verfügung stehen und dieser Vorbehalt die internationalen Verpflichtungen dieser Vertragspartei aus den in den Absätzen 1 und 2 genannten völkerrechtlichen Übereinkünften nicht beeinträchtigt.

Nach den Erläuterungen des Expertenkomitees wurde Art. 10 CCC mit Blick darauf eingeführt, dass strafbare Handlungen gegen das Urheberrecht eine der häufigsten Arten von Computer- oder Internetkriminalität darstellten. Das Ausmass dieser Kriminalität löse international unter den Rechteinhabern und jenen, die professionell mit Computernetzwerken befasst seien, Besorgnis aus und mache es notwendig, strafrechtliche Sanktionen in die Konvention aufzunehmen und die internationale Zusammenarbeit in diesem Feld zu verbessern.[182]

Die von der Convention on Cybercrime vorgegebene Kriminalisierungspflicht beschränkt sich auf ein Handeln *«by means of a computer system»* und *«on a commercial scale»*. Urheberrechtsverletzungen und Verletzungen ver-

181 Zitiert nach der bereinigten Übersetzung zwischen Deutschland, Österreich und der Schweiz abgestimmte Fassung, ‹http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm›, abgedruckt in Christian Schwarzenegger, Oliver Arter und Florian S. Jörg (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 372 f., dort auch zu den weitergehenden Vorschlägen, die im Entstehungsprozess gemacht wurden.

182 Explanatory Report, CETS No. 185, N 35 und N 107.

wandter Schutzrechte sind nach dieser Vorgabe zumindest dann unter Strafe zu stellen, wenn sich der Täter einen wirtschaftlichen Vorteil verschaffen will und die Tat «kommerziell, d.h. im Rahmen einer gewissen, auf kommerzielle Bereicherung gerichteten Mindestorganisation» vornimmt.[183] Im deutschsprachigen Raum wird dies – wie die unter Deutschland, Österreich und der Schweiz abgestimmte Übersetzung zeigt – mit «Gewerbsmässigkeit» gleichgesetzt. Der einzelne Up- und Download in einem P2P-Netzwerk würde diesem Kriterium jedenfalls nicht genügen.

Art. 10 Abs. 1 CCC definiert keine weiteren Elemente des Tatbestandes, sondern begnügt sich mit einer Verweisung auf andere Abkommen. Damit sind gemeint:

- die Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst revidiert in Paris am 24. Juli 1971[184]
- das TRIPS-Abkommen[185]
- der WIPO-Urheberrechtsvertrag (WCT)[186]

Art. 10 Abs. 2 CCC ist inhaltlich zu ergänzen durch die Vorgaben aus:

- dem Internationalen Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen vom 26. Oktober 1961 (Rom-Abkommen)[187]
- dem TRIPS-Abkommen
- dem WIPO-Vertrag über Darbietungen und Tonträger (WPPT)[188]

Während also die WIPO-Abkommen den Mitgliedstaaten die Wahl überlassen, ob sie die Schutzverpflichtungen in einem zivil-, straf- oder öffentlich-rechtlichen Rechtsrahmen gewährleisten wollen, verlangt die Convention on Cybercrime eine Überführung der Materie in den Bereich des Strafrechts, zumindest bei schwerwiegenden Verletzungen des Urheberrechts bzw. der verwandten Schutzrechte.[189] Als Minimalanforderung an die urheberstrafrechtlichen Tatbestände seien die Vorgaben von Art. 61 TRIPS-Abkommen zu beachten.[190]

Abgeschwächt wird die konventionalrechtliche Vorgabe durch Art. 10 Abs. 3 CCC, wonach unter «einer begrenzten Zahl von Umständen» auf eine strafrechtliche Verantwortlichkeit verzichtet werden kann, wenn Verletzungen des Urheberrechts und verwandter Schutzrechte durch andere wirksame Mittel

183 Beer (Fn. 72), S. 207.
184 In Kraft getreten für die Schweiz am 25.9.2003 (SR 0.231.15).
185 Siehe oben C.III.1, S. 446 f.
186 Siehe oben C.III.2, S. 447 f.
187 In Kraft getreten für die Schweiz am 24.9.1993 (SR 0.231.171).
188 Siehe oben C.III.2, S. 447 f.
189 Der erläuternde Bericht erwähnt explizit die Bedeutung der WIPO-Abkommen für den internationalen Schutz von Urheberrechten und verwandten Schutzrechten, Explanatory Report, CETS No. 185, N 111.
190 Explanatory Report, CETS No. 185, N 116.

unterbunden werden. Gedacht wurde dabei an Parallelimporte oder Mietrechte. Hier lässt die Konvention den Mitgliedstaaten einen gesetzgeberischen Spielraum offen.[191] Die Pflichten aus Art. 10 CCC entstehen erst, nachdem ein Mitgliedstaat die erwähnten Abkommen zum Schutze der Urheberrechte und verwandten Schutzrechte ratifiziert hat. Ist also ein Staat beispielsweise Mitglied der Convention on Cybercrime, nicht aber des TRIPS-Abkommens oder der WIPO-Abkommen, so trifft ihn keine Umsetzungspflicht aus Art. 10 CCC.[192]

Nach Art. 11 Abs. 1 CCC sind vorsätzlich begangene Anstiftungs- und Gehilfenhandlungen zu einer der Straftaten gemäss Art. 2–10 CCC ebenfalls unter Strafe zu stellen. Dies gilt somit auch für die gewerbsmässige Verletzung von Urheberrechten und verwandter Schutzrechte. Die Strafbarkeit des Versuches einer Straftat nach Art. 10 CCC gehört nicht zu den Vorgaben der Konvention (vgl. Art. 11 Abs. 2 CCC).

Art. 13 CCC verlangt, dass die in den Art. 2–11 CCC definierten Straftaten mit «wirksamen, angemessenen und abschreckenden Sanktionen bedroht» werden müssen, die Freiheitsentzug einschliessen. Eine Strafbarkeit der juristischen Person für solche Delikte ist vorgesehen, aber nicht zwingend vorgeschrieben (Art. 12 CCC).

b. Missbrauch von Vorrichtungen (Art. 6 CCC)

Ohne direkten Bezug zum Urheberrechtsschutz, allerdings in auffallender Parallelität zu den praktisch zeitgleichen EU-Bestimmungen über den Verkehr mit Umgehungstechnologien, gibt Art. 6 CCC zudem vor, dass gesetzgeberische Massnahmen zum Schutz gegenüber Technologien für illegalen Zugang zu und illegales Abfangen von Daten sowie die Beeinträchtigung von Daten und Computersystemen zu treffen sind:[193]

> **Artikel 6 – Missbrauch von Vorrichtungen**
>
> (1) Jede Partei trifft die gesetzgeberischen und anderen Massnahmen, die notwendig sind, um nach ihrem innerstaatlichen Recht unter Strafe zu stellen, falls vorsätzlich und unrechtmässig begangen:
> a) das Herstellen, Verkaufen, Beschaffen zum Gebrauch, Einführen, Verbreiten oder sonstwie Zugänglichmachen:
> i) einer Vorrichtung, einschliesslich eines Computerprogramms, die hauptsächlich zum Zwecke der Begehung einer der nach den oben erwähnten Artikeln 2 bis 5 geschaffenen Straftaten entworfen oder angepasst wurde;
> ii) eines Computerpasswortes, eines Zugriffscodes oder ähnlicher Daten, durch welche auf das Ganze oder einen Teil eines Computersystems zugegriffen werden kann;

191 Marco Gercke, Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 1: Umsetzung im Bereich des materiellen Strafrechts, MMR 2004, S. 728–735, S. 733 f.

192 Spannbrucker (Fn. 72), S. 114.

193 Übersetzung des Autors: ‹www.rwi.uzh.ch/lehreforschung/alphabetisch/schwarzenegger/links/CCCDeutsch.pdf›.

mit der Absicht, sie zum Zwecke der Begehung einer der Straftaten zu verwenden, auf welche die Artikel 2 bis 5 abzielen; und

b) den Besitz eines oben in den lit. a.i) oder ii) genannten Mittels mit der Absicht, es zum Zwecke der Begehung einer der Straftaten zu verwenden, auf welche die Artikel 2 bis 5 abzielen. Eine Partei kann nach dem innerstaatlichen Recht den Besitz einer bestimmten Anzahl dieser Mittel verlangen, um die strafrechtliche Verantwortlichkeit zu begründen.

(2) Dieser Artikel darf nicht so ausgelegt werden, als schreibe er eine strafrechtliche Verantwortlichkeit vor, wenn das in Absatz 1 dieses Artikels genannte Herstellen, Verkaufen, Beschaffen zum Gebrauch, Einführen, Verbreiten oder sonstwie Zugänglichmachen oder Besitzen[194] nicht zum Zwecke der Begehung einer nach den oben erwähnten Artikeln 2 bis 5 dieses Übereinkommens geschaffenen Straftat erfolgt, wie im Fall des genehmigten Tests oder des Schutzes eines Computersystems.

(3) Jede Partei kann sich das Recht vorbehalten, Absatz 1 dieses Artikels nicht anzuwenden, soweit der Vorbehalt nicht das Verkaufen, Verbreiten oder sonstwie Zugänglichmachen der in Absatz 1 lit. a.ii) dieses Artikels genannten Mittel betrifft.

Die verschiedenen Missbrauchsformen nach Art. 6 CCC werden vom geltenden Schweizer Strafrecht nur partiell abgedeckt.

c. Bedeutung der strafprozessualen Harmonisierungsvorgaben (Art. 14–21 CCC)

Von besonderer Bedeutung ist der erweiterte Geltungsbereich der strafprozessualen Vorgaben der Konvention. Sie sind auf alle mittels Computersystemen begangenen Straftaten und alle Massnahmen zur Sicherung elektronischer Beweismittel anwendbar, nicht nur auf die in den Art. 1–11 CCC definierten Computer- und Internetdelikte (Art. 14 Abs. 2 lit. b und c CCC). Somit müssen die in der Convention on Cybercrime vorgesehenen Zwangsmassnahmen auch in allen urheberstrafrechtlichen Verfahren zur Disposition stehen, soweit es um strafbares Verhalten im digitalen Umfeld geht. Diese Verpflichtung wurde im Hinblick auf die Rechtshilfe in Strafsachen eingeführt.[195]

4. EFTA-Übereinkommen

Das Übereinkommen zur Errichtung der Europäischen Freihandelsassoziation (EFTA) von 1960 in der Fassung des Vaduzer Abkommens von 2001[196] enthält unter Art. 2 lit. g die Zielsetzung, in *Übereinstimmung mit den höchsten internationalen Standards* einen angemessenen Schutz der geistigen Eigentumsrechte sicherzustellen. Sie wird konkretisiert durch die Pflicht der Mitgliedstaaten, einen angemessenen und wirksamen Schutz der Rechte an geistigem Eigentum zu erteilen und zu gewährleisten (Art. 19 Abs. 1). In einem Anhang J

194 Fehlt in der französischen Fassung.
195 SCHWARZENEGGER (Fn. 72), S. 310.
196 Für die Schweiz in Kraft am 1.6.2002 (SR 0.632.31).

zu Art. 19 des Übereinkommens bestätigen die Mitgliedstaaten ihre Verpflichtungen aus den internationalen Abkommen, insbesondere auch aus dem hier interessierenden TRIPS-Abkommen (Anhang J, Art. 2 Ziff. 1), und verpflichten sich explizit, vor dem 1. Januar 2005 dem WCT und WPPT beizutreten (Anhang J, Art. 2 Ziff. 2). In Art. 7, Anhang J, wird bezüglich der Durchsetzung von Rechten des geistigen Eigentums auf die Standards des TRIPS-Abkommens (Art. 41–61) verwiesen.

5. Der internationale Schutzstandard aus strafrechtlicher Perspektive

a. Urheberstrafrecht in den USA

Die Strafbestimmungen des US-amerikanischen Urheberrechts finden sich verstreut auf das 17.[197] und 18. Buch des U.S. Code.[198]

> **§ 506(a)(1). Criminal offenses**
>
> In general.– Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed–
>
> (A) for purposes of commercial advantage or private financial gain;
>
> (B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $ 1,000; or
>
> (C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

Wie aus § 506(a)(1) hervorgeht, ist nicht nur das Handeln in der Absicht, einen wirtschaftlichen Vorteil oder privaten finanziellen Gewinn zu erzielen (lit. A), strafrechtlich erfasst, sondern alle vorsätzlichen Urheberrechtsverletzungen über einer bestimmten Erheblichkeitsschwelle. Nach § 506(a)(1)(B) ist zu bestrafen, wer innerhalb einer Frist von 180 Tagen eine Kopie oder mehrere Kopien von Werkexemplaren im Gesamtverkaufswert von 1000 $ herstellt oder ein Werkexemplar oder mehrere Werkexemplare im gleichen Gesamtwert verbreitet. Beträgt der finanzielle Gewinn mehr als 2500 $ droht dem Täter eine Geldstrafe oder Freiheitsstrafe von bis zu fünf Jahren.[199] Ein gleichartiger Rückfall ist strafschärfend zu berücksichtigen und führt zu einer Geldstrafe oder Freiheitsstrafe bis zu 10 Jahren.[200] Zu beachten sind die allgemeinen Grenzen der

197 17 USC § 506(a) (in der Fassung des No Electronic Theft (NET) Act, Pub. L. 105–147, Dec. 16, 1997, 111 Stat. 2678).
198 18 USC § 2319, Strafandrohungen.
199 18 USC § 2319(b)(1).
200 18 USC § 2319(b)(2).

Verantwortlichkeit, die sich insbesondere aus der *«fair use»*-Doktrin ableiten.[201]

Durch den Digital Millennium Copyright Act (DMCA)[202] wurde das US-amerikanische Urheberrecht bereits 1998 an die WIPO-Abkommen angepasst. Dabei wurde insbesondere auch ein Rechtsschutz gegen die Umgehung technischer Massnahmen und für Massnahmen zur Zugangskontrolle – in Abgrenzung zur Nutzungskontrolle – auch gegen Vorbereitungshandlungen einführt.[203] Die Strafnorm lautet:

> **§ 1204. Criminal offenses and penalties**
>
> (a) IN GENERAL. – Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain –
>
> (1) shall be fined not more than $ 500,000 or imprisoned for not more than 5 years, or both, for the first offense; and
> (2) shall be fined not more than $ 1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.
>
> (b) LIMITATION FOR NON PROFIT LIBRARY, ARCHIVES, OR EDUCATIONAL INSTITUTION.–Subsection (a) shall not apply to a nonprofit library, archives, or educational institution.
>
> (c) STATUTE OF LIMITATIONS.–No criminal proceeding shall be brought under this section unless such proceeding is commenced within 5 years after the cause of action arose.

Zu beachten ist der Unterschied zwischen dem Begriff der «Gewerbsmässigkeit», das im schweizerischen URG und häufig auch in anderen europäischen Urheberrechtsgesetzen als Qualifikationsmerkmal vorgesehen ist, und jenem der *«purposes of commercial advantage or private financial gain»*. Während die Gewerbsmässigkeit neben einer objektiven Vielzahl an Begehungen auch eine Erwerbsabsicht sowie Wiederholungsbereitschaft verlangt,[204] sind die Absichten des wirtschaftlichen Vorteils oder des privaten finanziellen Gewinns nach US-amerikanischer Lesart breiter aufzufassen. Dies setzt nur voraus, dass eine Handlung zu einem direkten oder indirekten wirtschaftlichen Vorteil führen muss, was schon bei einem einzigen unbefugten «kostensparenden» Download der Fall sein kann.[205]

---

201 Weiterführend Eckart Gottschalk, Digitale Musik und Urheberrecht aus US-amerikanischer Sicht, GRUR Int. 2002, S. 95–105, S. 97 f.

202 17 USC §§ 101 ff. (in der Fassung gemäss Pub. L. 105–304, Oct. 28, 1998, 112 Stat. 2860).

203 17 USC § 1201, Circumvention of copyright protection systems. Siehe zusammenfassend Eckart Gottschalk, Das Ende von «fair use»? Technische Schutzmassnahmen im Urheberrecht der USA, MMR 2003, S. 148–152, S. 149 f.

204 Jürg-Beat Ackermann, in: Marcel Alexander Niggli und Hans Wiprächtiger (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–110, Jugendstrafgesetz, 2. Aufl., Basel 2007, Art. 49 N 14 m.N.

205 17 USC § 101 «The term ‹financial gain› includes receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works.» Vgl. § 1204(a)(1) «for the first offense»; siehe Gottschalk (Fn. 201), S. 99; Marybeth Peters, Piracy of intellectual property,

b. Angleichung der Schutzstandards in der Europäische Union

aa. Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (Urheberrechtsrichtlinie)

Die Europäische Gemeinschaft, selbst Unterzeichnerin der WIPO-Abkommen (Art. 17 Abs. 3 WCT; Art. 26 Abs. 3 WPPT), hat mit der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft[206] die WIPO-Abkommen in für alle Mitgliedstaaten bindendes Gemeinschaftsrecht umgesetzt. Teilweise hat sie dabei die Vorgaben der Abkommen weiter konkretisiert, und teilweise ist sie über deren Schutzstandards hinausgegangen.[207]

Sowohl für Urheber von Werken (Art. 3 Abs. 1) als auch für die genannten Schutzgegenstände der Leistungsschutzberechtigten (Art. 3 Abs. 2) sieht die Richtlinie 2001/29/EG vor, dass ein Recht der öffentlichen Zugänglichmachung in die Urhebergesetze der Mitgliedstaaten aufzunehmen ist. Das Verbreitungsrecht (Art. 4) bezieht sich im Gegensatz zur Zugänglichmachung nur auf die körperliche Verbreitung von Werken und ist daher im Kontext der Cyberkriminalität nicht bedeutsam.

Im Besonderen hat die Richtlinie 2001/29/EG den Schutz technischer Massnahmen zur Wahrung der Urheber- und Nachbarrechte auf zwei Schutzbereiche erstreckt: Neben den Rechtsschutz gegen Handlungen zur Umgehung solcher technischer Massnahmen (Art. 6 Abs. 1 und 4) steckt sie auch den Rechtsschutz gegen den Verkehr mit Umgehungsmitteln und -dienstleistungen ab, ohne dabei nach Zugangs- oder Nutzungskontrolle zu unterscheiden (Art. 6 Abs. 2). Der entsprechende Absatz lautet:

> Die Mitgliedsstaaten sehen einen angemessenen Rechtsschutz gegen die Herstellung, die Einfuhr, die Verbreitung, den Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und den Besitz zu kommerziellen Zwecken von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen vor,
>
> a) die Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Massnahmen sind oder
> b) die, abgesehen von der Umgehung wirksamer technischer Massnahmen nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben oder
> c) die hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Massnahmen zu ermöglichen oder zu erleichtern.

Statement before the Subcommittee on Intellectual Property, Committee on the Judiciary, U.S. Senate, 109th Congress, 1st Session, May 25, 2005.

206 ABl. L 167 vom 22.6.2001, S. 10 ff.

207 Vgl. weiterführend Richard Brunner, Urheber- und leistungsschutzrechtliche Probleme der Musikdistribution im Internet – unter besonderer Berücksichtigung der Richtlinie 2001/29/EG und ihrer Umsetzung in deutsches Recht, Berlin 2004, 92 ff. m.w.N.

Bezüglich der Sanktionen und Rechtsbehelfe hält Art. 8 Abs. 1 Richtlinie 2001/29/EG im Stile des indirekt strafrechtsharmonisierenden sekundären Gemeinschaftsrechts fest:

> «Die Mitgliedstaaten sehen bei Verletzungen der in dieser Richtlinie festgelegten Rechte und Pflichten angemessene Sanktionen und Rechtsbehelfe vor und treffen alle notwendigen Massnahmen, um deren Anwendung sicherzustellen. Die betreffenden Sanktionen müssen wirksam, verhältnismässig und abschreckend sein.»[208]

bb. Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums und Entwurf einer Richtlinie über strafrechtliche Massnahmen zur Durchsetzung der Rechte des geistigen Eigentums

Schon im Januar 2003 legte die Europäische Kommission einen weiteren Richtlinienentwurf zur Durchsetzung der Rechte des geistigen Eigentums vor.[209] Mit einer stark auf den Binnenmarkt ausgerichteten Optik wird das unterschiedliche Schutzniveau hinsichtlich der Rechte an geistigem Eigentum in den Mitgliedstaaten kritisiert und zur Gewährleistung eines fairen und gleichberechtigten Wettbewerbs – aber auch mit Blick auf den Konsumentenschutz und die Aufrechterhaltung der öffentlichen Ordnung[210] – eine Richtlinie vorgeschlagen, die erstmals auch explizit die Einführung strafrechtlicher Normen vorschreibt. Etwas zweideutig hält die Kommission fest, man strebe mit dieser Richtlinie nicht direkt eine Harmonisierung der strafrechtlichen Sanktionen an, doch werde sich «die Verhängung wirklich abschreckender Strafen in allen Mitgliedstaaten positiv auf die Bekämpfung von Nachahmung und Produktpiraterie auswirken.»[211]

Art. 20 des Entwurfs von 2003 lautete:

> 1. Die Mitgliedstaaten achten darauf, dass jede schwerwiegende oder versuchte schwerwiegende Verletzung eines Rechts an geistigem Eigentum sowie Beihilfe und Anstiftung dazu als strafbare Handlungen gilt. Eine schwerwiegende Verletzung liegt vor, wenn sie vorsätzlich und zu gewerblichen Zwecken erfolgt ist.
> 2. Bei natürlichen Personen sehen die Mitgliedstaaten strafrechtliche Sanktionen einschliesslich Freiheitsstrafen vor.
> 3. Bei juristischen Personen sehen die Mitgliedstaaten die folgenden Sanktionen vor:
>   a) Geldstrafen;
>   b) die Beschlagnahme der Ware, Instrumente und Erzeugnisse aus der in Absatz 1 genannten strafbaren Handlung, oder von Vermögenswerten, die im Wert diesen Erzeugnissen entsprechen.
>
> In geeigneten Fällen sehen die Mitgliedstaaten ferner folgende Sanktionen vor:
> a) Vernichtung der Ware, die Rechte an geistigem Eigentum verletzt;

208 Auch Erwägungsgrund 58 der Richtlinie spricht von wirksamen, verhältnismässigen und abschreckenden Sanktionen.

209 Europäische Kommission (Fn. 175).

210 Europäische Kommission (Fn. 175), S. 11 f.

211 Europäische Kommission (Fn. 175), S. 17.

b) völlige oder teilweise, endgültige oder vorübergehende Schliessung der Betriebsstätte, die vorwiegend zur Begehung der Rechtsverletzung gedient hat;
c) dauerhaftes oder zeitweiliges Verbot der gewerblichen Betätigung;
d) Anordnung richterlicher Aufsicht;
e) gerichtliche Auflösung;
f) Ausschluss von öffentlichen Zuwendungen und Beihilfen;
g) Veröffentlichung von Gerichtsentscheidungen.

4. Im Sinne dieses Kapitels bedeutet «juristische Person» eine Rechtspersönlichkeit, die diesen Status nach dem einzelstaatlichen Recht hat, ausgenommen Staaten und andere Körperschaften des öffentlichen Rechts, die in Ausübung ihrer hoheitlichen Befugnisse handeln, und internationale Organisationen des öffentlichen Rechts.

Aufbauend auf Art. 61 TRIPS-Abkommen werden auch die Beihilfe und Anstiftung zu vollendeten oder versuchten schwerwiegenden Verletzungen von Rechten an geistigem Eigentum in die Kriminalisierungsvorgabe aufgenommen. Gemeint sind nicht nur Urheberrechte, sondern generell alle Rechte an geistigem Eigentum (vgl. Art. 2 Abs. 1 Richtlinienentwurf). Als Kriterium der Deliktsschwere wird wie in anderen Harmonisierungsinstrumenten auf das Handeln «zu gewerblichen Zwecken» abgestellt. Um wirksam und abschreckend zu sein, müssen die Straftatbestände für natürliche Personen mindestens auch Freiheitsstrafen androhen. Nach französischem und spanischem Vorbild werden auch zahlreiche Vorgaben aufgeführt bezüglich Einziehung und Vernichtung, Berufsverbot und verschiedene Sanktionen gegen juristische Personen. Die vorgesehene Veröffentlichung gerichtlicher Entscheidungen ist ein zusätzliches Element der Abschreckung.[212]

Der Entwurf konnte sich in dieser Form jedoch nicht durchsetzen. Die Richtlinie wurde vielmehr beschränkt auf die Regelung der zivilrechtlichen Durchsetzung der Rechte des geistigen Eigentums. Die strafrechtliche Ahndung von Produktpiraterie soll sich nach wie vor nach dem TRIPS-Übereinkommen bzw. dem Recht der Mitgliedstaaten richten (Artikel 2 Abs. 3 Buchstabe b und c). In Erwägungsgrund 28 wird zu dieser Frage ausgeführt, dass zusätzlich zu den zivil- und verwaltungsrechtlichen Massnahmen, Verfahren und Rechtsbehelfen, die in dieser Richtlinie vorgesehen sind, in geeigneten Fällen auch strafrechtliche Sanktionen ein Mittel zur Durchsetzung der Rechte des geistigen Eigentums darstellen.

cc. Vorschlag für eine Richtlinie über strafrechtliche Massnahmen zur Durchsetzung der Rechtes des geistigen Eigentums

Im Moment steht eine *Richtlinie über strafrechtliche Massnahmen zur Durchsetzung der Rechte des geistigen Eigentums* kurz vor der endgültigen Verab-

212 Vgl. Europäische Kommission (Fn. 175), S. 26.

schiedung durch den Rat der Europäischen Union.[213] Die Richtlinie wurde in zwei Etappen vorbereitet, wobei der zweite Vorschlag schon die neue Rechtsprechung des Europäischen Gerichtshofs über die Kompetenzausscheidung betreffend strafrechtliche Rechtsangleichung berücksichtigt und Elemente eines zuvor separat vorgeschlagenen Rahmenbeschlusses aufnahm.[214] Erstmals werden im Rahmen des sekundären Gemeinschaftsrechts explizit strafrechtliche Sanktionen für Verletzungen der Rechte des geistigen Eigentums vorgeschlagen. Der Entwurf sieht eine Kriminalisierungsverpflichtung für vorsätzliche, in gewerblichem Umfang begangene Rechtsverletzungen (Art. 3) und Sanktionen für natürliche und juristische Personen vor (Art. 4: Freiheitsstrafe, Geldstrafe, Vernichtung der schutzverletzenden Gegenstände, Schliessung der Betriebsstätte, Gewerbeuntersagung, richterliche Aufsicht, gerichtliche Auflösung, Ausschluss von Zuwendungen und Beihilfen, Veröffentlichung von Gerichtsentscheidungen). Art. 5 des Vorschlags setzt Strafrahmen fest (Mindesthöchststrafen von 4 Jahren bzw. 300 000 € bzw. 100 000 € für alle Fälle ausser den besonders schweren). Art. 6 des Vorschlags sieht erweiterte Einziehungsbefugnisse vor, Art. 7 Regeln für gemeinsame Ermittlungsgruppen und Art. 8 Regeln für die Einleitung der Strafverfolgung (Abgehen vom Antragserfordernis im Immaterialgüterrecht). Das Europäische Parlament hat den Richtlinienvorschlag am 25. April 2007 mit einigen Einschränkungen angenommen. Der parlamentarische Berichterstatter strich die Bedeutung dieser Richtlinie besonders hervor:

> «We are turning a new page: this is the first directive where criminal law is included. […] To harmonise criminal codes will be a radical new thing.»[215]

213 Zuletzt Europäisches Parlament, Legislative Entschliessung des Europäischen Parlaments vom 25. April 2007 zu dem geänderten Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Massnahmen zur Durchsetzung der Rechte des geistigen Eigentums, P6_TA(2007)0145.

214 Vgl. Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Massnahmen zur Durchsetzung der Rechte des geistigen Eigentums, Vorschlag für einen Rahmenbeschluss des Rates zur Verstärkung des strafrechtlichen Rahmens zur Ahndung der Verletzung geistigen Eigentums, KOM(2005) 276 endg.; Europäische Kommission, Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Massnahmen zur Durchsetzung der Rechte des geistigen Eigentums, KOM(2006) 168 endg.

215 Nicola Zingaretti, ‹www.ip-watch.org/weblog/index.php?p=573›. Vgl. die kritische Stellungnahme von Reto Hilty, Annette Kur und Alexander Peukert, Stellungnahme des Max-Planck-Instituts für Geistiges Eigentum, Wettbewerbs- und Steuerrecht zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über strafrechtliche Massnahmen zur Durchsetzung des Rechts des geistigen Eigentums, KOM(2006) 168 endg., ‹www.ip.mpg.de/shared/data/pdf/strafrecht_stellungnahme_final.pdf›.

c. Stand der Umsetzung der völker- und europarechtlichen Vorgaben in Deutschland und Österreich mit Blick auf den Schutz technischer Massnahmen und das Verbot von Vorbereitungshandlungen

Die Richtlinie 2001/29/EG ist inzwischen von den Mitgliedstaaten weitestgehend in nationales Recht umgesetzt worden.[216]

In *Deutschland* erfolgte 2003 die Anpassung des nationalen Rechts durch das (erste) Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft. Hier wurde die deutsche Fassung von Art. 6 Abs. 2 der Richtlinie fast wörtlich in § 95a Abs. 3 dUrhG übernommen. Dieser lautet:

> Verboten sind die Herstellung, die Einfuhr, die Verbreitung, der Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und der gewerblichen Zwecken dienende Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen, die
> 1. Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Massnahmen sind oder
> 2. abgesehen von der Umgehung wirksamer technischer Massnahmen nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben oder
> 3. hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Massnahmen zu ermöglichen oder zu erleichtern.

Neben den Strafnormen gegen das Vervielfältigen und Verbreiten von Werken (§ 106 dUrhG)[217] ergibt sich die strafrechtliche Absicherung der technischen Schutzmassnahmen aus § 108b dUrhG:[218]

> Unerlaubte Eingriffe in technische Schutzmassnahmen und zur Rechtewahrnehmung erforderliche Informationen
>
> (1) Wer
>
> 1. in der Absicht, sich oder einem Dritten den Zugang zu einem nach diesem Gesetz geschützten Werk oder einem anderen nach diesem Gesetz geschützten Schutzgegenstand oder deren Nutzung zu ermöglichen, eine wirksame technische Massnahme ohne Zustimmung des Rechtsinhabers umgeht oder

---

216 Siehe JAN ROSÉN, Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft – Zur Umsetzung der EG-Richtlinie 2001/29/EG in den nordischen Ländern, GRUR Int. 2002, S. 195–206; TH. STEINHAUS, Spanien – Strafrechtlicher Schutz gegen Umgehung von technischen Schutzmassnahmen und Zugangskontrollen, GRUR Int. 2004, S. 531–532, alle Urheberrechtsdelikte (Art. 270, 271 CP) wurden zu Offizialdelikten umgestaltet und zählen zu den Deliktsformen, die unter den Tatbestand der Organisierten Kriminalität fallen können.

217 Siehe dazu MICHAEL HEGHMANNS, Straftaten gegen die betriebliche Datenverarbeitung, in: Hans Achenbach und Andreas Ransiek (Hrsg.), Handbuch Wirtschaftsrecht (HWSt), Heidelberg 2004, S. 405–460, S. 428 ff. m.w.N.

218 ULRICH HILDEBRANDT, in: Artur-Axel Wandtke und Winfried Bullinger (Hrsg.), Praxiskommentar zum Urheberrecht (UrhR), 2. Aufl., München 2006, Art. 108b N 1 ff.; GERD KAISER, in: Georg Erbs und Max Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze, Kurzkommentar, München 2007 (168. Ergänzungslieferung), Art. 108b N 1 ff. beide m.w.N.

2. wissentlich unbefugt
   a) eine von Rechtsinhabern stammende Information für die Rechtewahrnehmung entfernt oder verändert, wenn irgendeine der betreffenden Informationen an einem Vervielfältigungsstück eines Werkes oder eines sonstigen Schutzgegenstandes angebracht ist oder im Zusammenhang mit der öffentlichen Wiedergabe eines solchen Werkes oder Schutzgegenstandes erscheint, oder
   b) ein Werk oder einen sonstigen Schutzgegenstand, bei dem eine Information für die Rechtewahrnehmung unbefugt entfernt oder geändert wurde, verbreitet, zur Verbreitung einführt, sendet, öffentlich wiedergibt oder öffentlich zugänglich macht und dadurch wenigstens leichtfertig die Verletzung von Urheberrechten oder verwandten Schutzrechten veranlasst, ermöglicht, erleichtert oder verschleiert,

   wird, wenn die Tat nicht ausschliesslich zum eigenen privaten Gebrauch des Täters oder mit dem Täter persönlich verbundener Personen erfolgt oder sich auf einen derartigen Gebrauch bezieht, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer entgegen § 95a Abs. 3 eine Vorrichtung, ein Erzeugnis oder einen Bestandteil zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet.

(3) Handelt der Täter in den Fällen des Absatzes 1 gewerbsmässig, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

§ 111a Abs. 1 Ziff. 1 Bst. a und b dUrhG

(1) Ordnungswidrig handelt, wer

1. entgegen § 95a Abs. 3
   a. eine Vorrichtung, ein Erzeugnis oder einen Bestandteil verkauft, vermietet oder über den Kreis der mit dem Täter persönlich verbundenen Personen hinaus verbreitet oder
   b. zu gewerblichen Zwecken eine Vorrichtung, ein Erzeugnis oder einen Bestandteil besitzt, für deren Verkauf oder Vermietung wirbt oder eine Dienstleistung erbringt,

   […].

Im *österreichischen* Urheberrechtsgesetz wurde – ebenfalls 2003 – die Bestimmung in § 90c öUrhG redaktionell anders gefasst, ohne aber in der Reichweite der Tathandlungen von der Richtlinie abzuweichen:

Schutz technischer Massnahmen

(1) Der Inhaber eines auf dieses Gesetz gegründeten Ausschliessungsrechts, der sich wirksamer technischer Massnahmen bedient, um eine Verletzung dieses Rechts zu verhindern oder einzuschränken, kann auf Unterlassung und Beseitigung des dem Gesetz widerstreitenden Zustandes klagen,

1. wenn diese Massnahmen durch eine Person umgangen werden, der bekannt ist oder den Umständen nach bekannt sein muss, dass sie dieses Ziel verfolgt,
2. wenn Umgehungsmittel hergestellt, eingeführt, verbreitet, verkauft, vermietet und zu kommerziellen Zwecken besessen werden,

3. wenn für den Verkauf oder die Vermietung von Umgehungsmitteln geworben wird oder
4. wenn Umgehungsdienstleistungen erbracht werden.

(2) Unter wirksamen technischen Massnahmen sind alle Technologien, Vorrichtungen und Bestandteile zu verstehen, die im normalen Betrieb dazu bestimmt sind, die in Abs. 1 bezeichneten Rechtsverletzungen zu verhindern oder einzuschränken, und die die Erreichung dieses Schutzziels sicherstellen. Diese Voraussetzungen sind nur erfüllt, soweit die Nutzung eines Werks oder sonstigen Schutzgegenstandes kontrolliert wird

1. durch eine Zugangskontrolle,
2. einen Schutzmechanismus wie Verschlüsselung, Verzerrung oder sonstige Umwandlung des Werks oder sonstigen Schutzgegenstands oder
3. durch einen Mechanismus zur Kontrolle der Vervielfältigung.

(3) Unter Umgehungsmitteln beziehungsweise Umgehungsdienstleistungen sind Vorrichtungen, Erzeugnisse oder Bestandteile beziehungsweise Dienstleistungen zu verstehen,

1. die Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Massnahmen sind,
2. die, abgesehen von der Umgehung wirksamer technischer Massnahmen, nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben oder
3. die hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Massnahmen zu ermöglichen oder zu erleichtern.

[…].

Damit sind die folgenden Strafdrohungen verbunden*:*

§ 91 Abs. 1 und 2a öUrhG

(1) Wer einen Eingriff der im § 86 Abs. 1, § 90b, § 90c Abs. 1 oder § 90d Abs. 1 bezeichneten Art begeht, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen. Der Eingriff ist jedoch dann nicht strafbar, wenn es sich nur um eine unbefugte Vervielfältigung oder um ein unbefugtes Festhalten eines Vortrags oder einer Aufführung jeweils zum eigenen Gebrauch oder unentgeltlich auf Bestellung zum eigenen Gebrauch eines anderen handelt.

(1a) *aufgehoben*

(2) Ebenso ist zu bestrafen, wer als Inhaber oder Leiter eines Unternehmens einen im Betrieb des Unternehmens von einem Bediensteten oder Beauftragten begangenen Eingriff dieser Art (Abs. 1 und 1a) nicht verhindert.

(2a) Wer eine nach den Abs. 1, 1a oder 2 strafbare Handlung gewerbsmäßig begeht, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

[…].

Der *französische* Code de la propriété intellectuelle[219] schützt gegen den Verkehr mit Umgehungstechnologien unmittelbar durch die Strafnorm des Art. L. 335-3-1 Abs. 2 und auch im *italienischen* Gesetz über das Urheberrechtsgesetz findet sich der von der Richtlinie vorgegebene Schutz gegen den Verkehr mit Umgehungstechnologien direkt in der Strafnorm des Art. 171-ter Abs. 1 lit. f-bis.

IV. P2P-Filesharing und die Umgehung technischer Schutzmassnahmen nach dem neuen schweizerischen Urheberstrafrecht

1. Anwendbarkeit der Allgemeinen Bestimmungen des Strafgesetzbuches auf das Urheberstrafrecht

Die Allgemeinen Bestimmungen des StGB gelten auch für das Nebenstrafrecht, soweit dieses nichts Abweichendes regelt (Art. 333 Abs. 1 StGB). Das URG enthält keine Sondernormen bezüglich des materiellen Legalitätsprinzips (Art. 1 StGB), des Strafanwendungsrechts (Art. 3 ff. StGB), der Teilnahme (Art. 24–26 StGB), der persönlichen Verhältnisse (Art. 27 StGB), des Strafantrages (Art. 30–33 StGB[220]), der Einziehung (Art. 69 StGB[221]) sowie des Gerichtsstandes (Art. 340 ff. StGB). Die allgemeinen Regeln des StGB sind somit immer zu beachten. Für Widerhandlungen in Geschäftsbetrieben, durch Beauftragte und dergleichen gelten gemäss Art. 71 URG die Sonderbestimmungen des Verwaltungsstrafgesetztes (Art. 6–7 VStrG).[222]

2. Deliktstypen und Konsequenzen

a. Verletzung von Urheberrechten und verwandten Schutzrechten (Art. 67, 69 URG)

Das geschützte Rechtsgut der urheberrechtlichen Strafnormen nach Art. 67 URG besteht im freien Verfügungsrecht des Urhebers über sein Werk,[223] soweit dieses Recht nicht durch gesetzliche Schranken eingeschränkt ist.[224] Aufgrund der ausschliesslichen Verfügungsmacht kann der Urheber allein darüber entscheiden, ob, wann und wie sein Werk oder Teile davon verwendet werden (Nutzungsrechte).[225] Wird eine Tathandlung nach Art. 67 StGB ausgeführt, etwa

219 Der strafrechtliche und technische Schutz wird derzeit verstärkt, siehe zusammenfassend Sébastien Fanti, Cybercriminalité, droit d'auteur et protection des données, Panorama législatif et jurisprudentiel en Europe et en Suisse, Jusletter, 31.3.2008, Rz. 1 ff. m.N.

220 Vgl. Christof Riedo, Zur Strafantragsberechtigung bei Eingriffen in Immaterialgüterrechte, insbesondere bei Patentrechtsverletzungen, sic! 2004, S. 549–552.

221 Die Sonderbestimmung von Art. 72 URG ist bezüglich des P2P-Filesharings irrelevant.

222 SR 313.0.

223 Schwarzenegger (Fn. 17), S. 342.

224 Siehe Art. 19 ff. URG.

225 Manfred Rehbinder, Schweizerisches Urheberrecht, 3. Aufl., Bern 2000, N 21 und N 117 «Werkherrschaft»; Schwarzenegger (Fn. 17), S. 342; Glarner (Fn. 151), S. 42 m.w.N.

ohne Einverständnis des Urhebers eine Kopie eines Werkexemplares hergestellt (Art. 67 Abs. 1 lit. e URG), wird das strafrechtlich gesicherte Schutzrecht des Urhebers verletzt. Es handelt sich bei den verschiedenen Tathandlungsvarianten von Art. 67 URG daher um *Verletzungsdelikte,* die mit Ausführung der Handlung vollendet sind *(schlichte Tätigkeitsdelikte)*. Parallel dazu wird durch Art. 69 URG das Rechtsgut des Verfügungsrechts der Leistungsschutzberechtigten strafrechtlich gesichert. Auch ihre Freiheit, über das Wie, Wann und Wo der Auswertung von Werkdarbietungen, Ton- und Tonbildträgern sowie Sendungen zu bestimmen, wird durch die Ausführung tatbestandsmässiger Handlungen verletzt, z.B. wenn die Aufnahme einer Werkdarbietung im P2P-Netzwerk Dritten zum Download angeboten wird (Art. 69 Abs. 1 lit. c URG).[226]

b. Verletzung des Schutzes durch technische Massnahmen (Art. 69a Abs. 1 lit. a URG)

Art. 69a Abs. 1 lit. a URG führt eine Strafbestimmungen gegen die Umgehung wirksamer technischer Massnahmen nach Art. 39a Abs. 1–2 URG ein. Da sich der strafrechtliche Schutz im Urheberrecht wie im Bereich des Vermögensstrafrechts akzessorisch zur zivilrechtlichen Ausgestaltung des Rechtsschutzes verhält, ist es für die Bestimmung des Deliktstypus massgebend, wie der zivilrechtliche Schutz konzipiert ist. Es stellt sich daher die Frage, ob mit Art. 69a Abs. 1 lit. a URG ein subjektives Recht der Inhaber von Urheber- und verwandten Schutzrechten am Umgehungsschutz gesichert wird.[227] Da ein solches subjektives Recht bisher nicht existierte, hätte es mit dieser URG-Revision eingeführt werden müssen. Eine systematische Auslegung des Gesetzes lässt den Schluss zu, dass kein verselbständigter, individueller Rechtsschutz für technische Massnahmen geschaffen wurde. Der Anspruch ist vielmehr als Reflexwirkung des Urheber- oder verwandten Schutzrechts zu verstehen, weil Art. 62 Abs. 1bis URG eine zivilrechtliche Aktivlegitimation zur individuellen Abwehr solcher Handlungen gewährt. Verstösse gegen Art. 39a Abs. 1 URG werden explizit als Gefährdungen des individuellen Schutzrechts bezeichnet.

Die Ausgestaltung von Art. 69a Abs. 1 URG als Antragsdelikt weist ebenfalls darauf hin, das ein subjektives Recht geschützt wird und folglich die Möglichkeit eines tatbestandsausschliessenden Einverständnisses besteht.[228] Dass das Umgehungsverbot in Art. 39a Abs. 1 URG als abstrakt-hoheitliche Verbots-

226 Es handelt sich ebenfalls um Verletzungsdelikte, die als schlichte Tätigkeitsdelikte konzipiert sind, siehe SCHWARZENEGGER (Fn. 17), S. 342.

227 Anknüpfend an Art. 6 Abs. 3 Satz 1 der Richtlinie 2001/29/EG wird der Rechtsschutz technischer Massnahmen in Deutschland als individueller Rechtsschutz der Inhaber der Urheber- und Leistungsschutzrechte verstanden, siehe § 95a Abs. 1 dUrhG. Vgl. dazu HORST-PETER GÖTTING in: Gerhard Schricker (Hrsg.), Urheberrecht, Kommentar, 3. Aufl., München 2006, § 95 N 7. So auch § 90 Abs. 1 öUrhG.

228 Ungenau ist der Gesetzestext, wenn er von einer «in ihrem Schutz *verletzten* Person», statt von einer «in ihren Rechten *gefährdeten* Person» spricht.

norm formuliert und nicht vom Fehlen einer Zustimmung des Rechteinhabers abhängig gemacht wird,[229] schadet insofern nichts, als die zivilrechtliche Aktivlegitimation und strafrechtliche Antragsbefugnis aus Art. 62 Abs. 1bis URG und Art. 69a Abs. 1 URG deutlich hervorgehen. Damit handelt es sich bei Art. 69a Abs. 1 lit. a URG um ein *konkretes Gefährdungsdelikt,*[230] weil mit Umgehungshandlungen an wirksam gesicherten Werkdaten gleichzeitig eine konkrete Gefahr für bestimmte Urheber- und verwandte Schutzrechte entstehen muss *(Erfolgsdelikt)*. Verletzt werden diese Rechte aber erst mit einer weiteren Handlung wie z.B. dem Kopieren ausserhalb der Schutzschranken oder der öffentlichen Zugänglichmachung. Auch aus der Botschaft[231] geht hervor, dass «technische Massnahmen nicht generell geschützt [werden], sondern nur insofern, als sie sich auf urheberrechtlich geschützte Werke oder Leistungen beziehen.» Ein Verletzungsdelikt, bei welchem die Umgehung der technischen Massnahme als Verletzung eines geschützten Rechts[232] an der Massnahme selbst anzusehen wäre, fällt somit ausser Betracht.

c. Vorbereitungshandlungen zur Umgehung technischer Massnahmen (Art. 69a Abs. 1 lit. b URG)

Art. 69a Abs. 1 lit. b URG statuiert ein Verbot verschiedener Vorbereitungshandlungen, welche sich alle auf Vorrichtungen, Erzeugnisse, Bestandteile oder Dienstleistungen beziehen, die hauptsächlich zur Umgehung technischer Massnahmen dienen. Solche Handlungen richten sich nicht gegen ein konkretes Angriffsobjekt, d.h. gegen ein durch technische Massnahmen gesichertes Werkexemplar bzw. gegen einen entsprechend gesicherten Datenträger. Demzufolge sind auch die Verfügungsrechte konkreter Schutzrechtsinhaber noch nicht betroffen. Der Deliktstypus ist eindeutig ein *abstraktes Gefährdungsdelikt.*[233] Folglich lässt sich gar nicht sagen, welcher Rechteinhaber von der Vorbereitungshandlung betroffen ist. Die strafrechtliche Doktrin ist sich einig, dass

---

229 Das Fehlen einer Zustimmung des Rechteinhabers wird in § 95a dUrhG explizit vorausgesetzt.

230 Insofern ungenau Andreas Glarner, Werknutzung im digitalen Zeitalter: Strafrechtliche Betrachtungen zu Art. 19 Abs. 1 lit. a URG und zum Schutz technischer Massnahmen, sic! 2006, S. 641–651, S. 648, der Art. 69a URG generell den abstrakten Gefährdungsdelikten zuordnet.

231 Botschaft, BBl. 2006, 3424.

232 Sei es des Herstellers dieser Schutzmassnahmen, sei es des Nutzers derselben.

233 Ebenso David (Fn. 141), Art. 69 mit Rev. Art. 69a (neu) N 9; Glarner (Fn. 230), S. 648. Der Begriff des «abstrakten» Gefährdungsdelikts ist widersprüchlich. Mit abstrakter, potenzieller und konkreter Gefahr sind unterschiedliche Grade der Verletzungswahrscheinlichkeit gemeint, die fliessend ineinander übergehen, je näher ein Angriffsobjekt dieser Gefahr ausgesetzt ist. Die h.L. verlangt bei abstrakten Gefährdungsdelikten nur den Nachweis der Tathandlung (schlichtes Tätigkeitsdelikt, Verhaltensdelikt). Weiterführend zum Charakter des abstrakten Gefährdungsdelikts, Christian Schwarzenegger, Abstrakte Gefahr als Erfolg im Strafanwendungsrecht – ein leading case zu grenzüberschreitenden Internetdelikten, sic! 2001, S. 240–250, S. 247 mit zahlreichen Nachweisen.

es sich bei solchen Strafnormen um eine Vorfeldkriminalisierung im Interesse der Öffentlichkeit handelt.[234]

d. Verletzung des Schutzes von Informationen für die Wahrnehmung von Rechten (Art. 69a Abs. 1 lit. c URG)

Art. 39c i.V.m. Art. 69a Abs. 1 lit. c URG dient der Umsetzung von Art. 12 WCT und Art. 19 WPPT. Schutzobjekt sind dabei die elektronischen Informationen, mit welchen Werke und andere Schutzobjekte markiert werden. Zweck dieser Kennzeichnung, Zahlen oder Codes ist die jederzeitige Identifizierung der Werke, des Urhebers, der Berechtigten und allenfalls der Modalitäten und Bedingungen der Nutzung. Die strafrechtliche Absicherung wird davon abhängig gemacht, ob dem Täter bekannt ist oder den Umständen nach bekannt sein muss, dass mit der Entfernung oder Änderung derartiger Informationen die Verletzung eines Urheber- oder verwandten Schutzrechts veranlasst, ermöglicht, erleichtert oder verschleiert wird (Art. 69a Abs. 3 URG).

3. Das unrechtmässige Zugänglichmachen von Werkdaten in P2P-Netzwerken (Art. 67 Abs. 1 lit. g^{bis} URG)

Die vorliegende Analyse beschränkt sich auf die Darstellung des strafrechtlichen Schutzes der Urheberrechte gemäss Art. 67 URG. Zu beachten ist jedoch, dass eine Verletzung von verwandten Schutzrechten in P2P-Netzwerken nach Art. 69 URG ebenfalls möglich ist und die einzelnen Straftatbestände der Art. 67 URG und Art. 69 URG zueinander in echter Konkurrenz stehen.[235]

Die Einführung der Tathandlungsvariante des Zugänglichmachens in Art. 67 Abs. 1 lit. g^{bis} URG schützt das ausschliessliche Nutzungsrecht von Art. 10 Abs. 2 lit. c URG,[236] das bisweilen als «On-Demand-Recht» bezeichnet wird.[237] Die Bestimmungen gehen auf Art. 8 WCT zurück und garantieren dem Rechteinhaber das exklusive Recht, seine Werke in drahtgebundener oder drahtloser Form abrufbar zu machen. Damit wurde der Meinungsstreit, ob es sich beim Bereitstellen digitaler Werkdateien in einem P2P-Netzwerk um ein Anbieten eines Werkexemplares (Art. 67 Abs. 1 lit. f URG) oder um ein Wahrnehmbarmachen eines Werkes (Art. 67 Abs. 1 lit. g URG) handle, entschärft und einer klaren Lösung zugeführt.[238]

---

234 Dies wird in Botschaft, BBl. 2006, 3428, nicht beachtet.

235 Glarner (Fn. 151), S. 90 m.N., vgl. dort auch S. 99 f., S. 107 f.

236 Vgl. Art. 69 Abs. 1 lit. e^{ter} URG, der das Nutzungsrecht des Zugänglichmachens von Werkdarbietungen, Ton- oder Tonbildträgern oder Sendungen unter strafrechtlichen Schutz stellt. Er geht auf Art. 10 und Art 14 WPPT zurück.

237 AB 2007 N 1201 (Votum J. Alexander Baumann).

238 Siehe pro Anbieten: Denis Barrelet und Willi Egloff, Das neue Urheberrecht, Kommentar zum Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, 3. Aufl., Bern 2008, Art. 10 N 16 «Vertrieb via Internet»; Glarner (Fn. 151), S. 103 ff.; Schwarzenegger (Fn. 131), S. 216 ff. je m.N. Pro Wahrnehmbarmachen: Rolf H. Weber, E-Commerce und Recht,

a. Objektiver Tatbestand

Werke sind gemäss Art. 2 Abs. 1 URG geistige Schöpfungen der Literatur und Kunst mit individuellem Charakter. Abs. 2 der Vorschrift enthält eine beispielhafte Aufzählung von geistigen Schöpfungen, die als Werke im Sinne dieser Vorschrift zu behandeln sind. Nach Art. 2 Abs. 2 lit. b URG stellen Musikstücke Werke dar. Nach Art. 2 Abs. 2 lit. g URG gilt dies auch für «fotografische, filmische und andere visuelle oder audiovisuelle» Kreationen. Aus Abs. 3 des Art. 2 URG geht hervor, dass Computerprogramme eine eigenständige Werkkategorie darstellen.[239] Bei den in P2P-Netzwerken bereitgestellten Werkdaten handelt es sich – soweit sie aufgrund eines individuellen Charakters überhaupt urheberrechtlich geschützt sind – mehrheitlich um Werkexemplare, d.h. um eine codierte Form der unkörperlichen Text-, Musik-, Filmwerke oder Computerprogramme, die auf einem Speichermedium (vorübergehend) fixiert werden.[240]

Für die Vollendung der Tatbestandsvariante des Zugänglichmachens genügt es schon, wenn der Täter einem anderen – z.B. durch Abspeicherung auf einem öffentlich zugänglichen Webserver oder auf einem an ein P2P-Netzwerk angeschlossenen Computer – die Möglichkeit eröffnet, einen Download durchzuführen. Zu einem effektiven Download muss es nicht kommen.[241] Es genügt, wenn Fragmente von Werkdaten abrufbar sind.

Das Zugänglichmachen von Dateien in P2P-Netzwerken erfolgt in der Regel durch eine Konfiguration des P2P-Filesharing-Programms, die einen Ordner, d.h. ein Unterverzeichnis der Festplatte mit den darin abgespeicherten Dateien, für den Fernzugriff durch Dritte freischaltet. Bei fast allen File-Sharing-Programmen ist die Konfiguration schon von vornherein, zum Teil sogar unveränderlich[242] so eingerichtet. Falls sich im Sharing-Ordner Kopien von urheberrechtlich geschützten Werkdaten befinden und der Rechner ans P2P-Netz angeschlossen ist, kann von einem Zugänglichmachen im zuvor definierten Sinne ausgegangen werden. Falls der Sharing-Ordner noch leer ist, kann erst von einem Zugänglichmachen gesprochen werden, wenn durch einen eigenen

---

Rechtliche Rahmenbedingungen elektronischer Geschäftsplattformen, Zürich 2001, S. 223 m. N.; ROLF H. WEBER und ROLAND UNTERNÄHRER, Online-Tauschbörsen, AJP 2004, S. 1372–1392, S. 1375 f.; BERNHARD WITTWEILER, Produktion von Multimedia und Urheberrecht aus schweizerischer Sicht, UFITA 1995, S. 5–30, S. 11 f., zusammenfassend BAUMGARTNER (Fn. 164), S. 198 f. m.w.N.

239 Dazu näher URSULA WIDMER, Der urheberrechtliche Schutz von Computerprogrammen, ZSR I 1993, S. 247–268.

240 LUKAS BÜHLER, Schweizerisches und internationales Urheberrecht im Internet, Freiburg 1999, S. 156; EMIL F. NEFF und MATTHIAS ARN, Urheberrechtlicher Schutz der Software, in: ROLAND VON BÜREN und DAVID LUCAS (Hrsg.): Schweizerisches Immaterialgüter- und Wettbewerbsrecht, Band II/2, Basel 1998, S. 110; REHBINDER (Fn. 221), N 1 und zum Werkcharakter allgemein N 71 ff.

241 SCHWARZENEGGER (Fn. 17), S. 360 ff. am Beispiel von Hyperlinks.

242 Z.B. bei BitTorrent. Bei anderen P2P-Clients ist das Upload-Download-Verhältnis so konfiguriert, dass erst ab 20KB/s Upload ein unbegrenzter Download möglich ist.

Download oder auf andere Weise eine Datei in den Sharing-Ordner hineinkopiert wird, womit die Datei unmittelbar auch zum Download durch Dritte verfügbar wird. Hinzu kommt, dass das Anbieten häufig temporär unterbrochen wird. Dies ist der Fall, wenn die Verbindung des Rechners zum P2P-Netzwerk beendet wird, z.B. beim Abschalten des Computers oder bei Deaktivierung des Sharing-Programms. Bei jeder erneuten Netzverbindung bei gleichzeitig aktivierter Sharing-Software sind die Dateien im Sharing-Ordner wieder für Dritte abrufbar und somit im Sinne von Art. 67 Abs. 1 g^{bis} URG zugänglich gemacht. Mit anderen Worten: Immer wenn ein P2P-User die Kopie eines Werkexemplares im Sharing-Bereich seines Rechners ablegt oder belässt, erfüllt er die objektive Tathandlung des Zugänglichmachens eines Werkes, sobald der Computer an das P2P-Netzwerk angeschlossen und die Sharing-Software aktiviert ist.

b. Unrechtmässigkeit als objektives Tatbestandsmerkmal

Richtigerweise ist die Unrechtmässigkeit in von Art. 67 Abs. 1 URG als objektives Tatbestandsmerkmal anzusehen, weil hier die Rechtswidrigkeit konstitutives Element schon der generell-abstrakten Unrechtsdefinition ist. Die schlichte Tatsache, dass eine Werkdatei in einem Netzwerk zum öffentlichen Abruf eingestellt wird, kann für sich noch nicht unrechtsbegründend sein. Es könnte sein, dass der Rechteinhaber selbst oder ein sonstiger Berechtigter die Datei öffentlich zur Verfügung stellt. Die Unrechtmässigkeit ist deshalb Teil des objektiven Tatbestandes, auf welchen sich der Vorsatz ebenfalls beziehen muss. Der Vorsatz muss bei Art. 67 Abs. 1 URG folglich auch die Rechtswidrigkeit erfassen. Liegt ein Einverständnis des Berechtigten bezüglich des Zugänglichmachens vor, schliesst das die Tatbestandsmässigkeit nach Art. 67 Abs. 1 lit. g^{bis} URG aus.[243] Das Einverständnis der Rechteinhaber liegt beim Filesharing in P2P-Netzwerken aber nur in vereinzelten Ausnahmefällen vor.

c. Rechtmässiger Eigengebrauch beim Zugänglichmachen in P2P-Netzwerken?

Ein rechtmässiger *Eigengebrauch* ist bei Computerspielen *unmöglich* (Art. 19 Abs. 4 URG).

Bezüglich der Musik- und Filmdateien ist fraglich, ob ihr Anbieten im P2P-Netzwerk für jedermann überhaupt eine Verwendung im persönlichen Bereich oder im Kreis von eng verbundenen Personen darstellt. Bei einer Verwendung im persönlichen Bereich wird auf den Zweck der Nutzung abgestellt.[244] Es wird lediglich die höchstpersönliche Werkverwendung von dieser Variante erfasst. Beim Kreis eng verbundener Personen handelt es sich um einen privaten

243 Gl.M. Glarner (Fn. 151), S. 75 f.; Cyrill P. Rigamonti, Eigengebrauch oder Hehlerei? – Zum Herunterladen von Musik- und Filmdateien aus dem Internet, GRUR Int. 2004, S. 278–289, S. 281; Schwarzenegger (Fn. 131), S. 429.

244 Barrelet und Egloff (Fn. 238), Art. 19 N 10.

Kreis und damit eine begrenzte Anzahl von Personen.[245] Das Zugänglichmachen von Dateien im Internet zum Abruf für jedermann geht klar darüber hinaus und ist nicht durch den Eigengebrauch gedeckt. Ausnahmsweise kann ein rechtmässiger Eigengebrauch bejaht werden, wenn sich die P2P-Software derart konfigurieren lässt, dass nur einzelne eng verbundene Freunde zum Fernabruf der Dateien zugelassen sind.

d. Subjektiver Tatbestand

Wie bei allen Urheberstrafnormen reicht auch bei Art. 67 Abs. 1 lit. g^{bis} URG ein *Eventualvorsatz.*[246] Ein Eventualvorsatz ist gegeben, wenn der Täter die Tatbestandsverwirklichung für möglich hält, aber dennoch handelt, weil er diese Verwirklichung in Kauf nimmt oder sich auch bloss damit abfindet, selbst wenn ihm das grundsätzlich als unerwünscht erscheint. Der eventualvorsätzlich handelnde Täter weiss also um das Risiko der Tatbestandsverwirklichung. Im Unterschied zur bewussten Fahrlässigkeit, die vorliegend nicht strafbar wäre, vertraut der Täter nicht auf das Ausbleiben der Tatbestandsverwirklichung, sondern er handelt, komme, was wolle. Eine solche Inkaufnahme genügt nach der expliziten Regelung in Art. 12 Abs. 2 Satz 2 StGB. Eine besondere Billigung der Tatbestandsverwirklichung ist dagegen nicht erforderlich.[247]

Was derjenige, der Werkdaten auf seinem Computer zugänglich macht, wusste, wollte und in Kauf nahm, betrifft die Innenseite der Tat und ist damit eine Tatfrage, die durch die Untersuchungsbehörde abzuklären und nachzuweisen ist. Üblicherweise wird in der Einvernahme gefragt, ob der Angeschuldigte darüber Bescheid wusste, wie das P2P-Filesharing funktioniert. Fehlt ein diesbezügliches Geständnis, muss aus den äusseren Umständen auf die inneren Tatsachen zum Tatzeitpunkt geschlossen werden. Man kann jedoch davon ausgehen, dass ein P2P-User, der Dateien von urheberrechtlich geschützten Werken in seinem Sharing-Ordner belässt oder sie dorthin kopiert, regelmässig über sein unrechtmässiges Zugänglichmachen der Werkdaten Bescheid weiss. Unternimmt er nichts dagegen, nimmt er die Tatbestandsverwirklichung in Kauf.[248] Auf den Websites der Sharing-Software-Anbieter, aber auch in den Diskussionsforen des Webs wird immer wieder darauf hingewiesen, dass keine urheberrechtlich geschützten Werke wie Musik, Film, Computerspiele oder andere Software via P2P-Netzwerk angeboten werden dürfen. In der Regel hat der Nutzer daher auch mindestens eine laienhafte Kenntnis von der Unrechtmässigkeit seines Tuns.

---

245 Barrelet und Egloff (Fn. 238), Art. 19 N 8.
246 Vgl. Glarner (Fn. 151), S. 87 m.N.
247 Siehe nur BGE 125 IV 251 m.N.
248 So auch zum in dieser Frage identischen deutschen Recht: AG Cottbus, Urteil vom 6.5.2004, Az. 95 Ds 1653 Js 15556/04 (57/04), Erw. II.

e. Rechtswidrigkeit und Schuld

Anwendungsfälle der gesetzlichen oder übergesetzlichen *Rechtfertigungsgründe* sind kaum denkbar. Auch ein rechtlich beachtlicher Rechtsirrtum gemäss Art. 21 StGB lässt sich kaum annehmen.

4. Rechtmässiger und strafbarer Download von Werkdaten in P2P-Netzwerken

a. Objektiver Tatbestand

Als Täter einer unrechtmässigen Herstellung eines Werkexemplares kommt jeder in Frage, der einen Download urheberrechtlich geschützter Werkdaten via P2P-Netzwerk auf seinen Computer durchführt (Art. 67 Abs. 1 lit. e, Art. 10 Abs. 2 lit. a URG). Art. 67 Abs. 1 lit. e URG stellt das Vervielfältigungsrecht unter den strafrechtlichen Schutz.[249] In Frage stehen zumeist mehrfache Widerhandlungen gegen diese Strafnorm, weil P2P-User gewöhnlich wiederholt Dateien «downloaden» und häufig ganze Sammlungen anlegen.

Auch beim Download von Werkdaten sind Werke im Sinne von Art. 2 URG betroffen. *Herstellen* bedeutet im digitalen Umfeld die programmtechnisch ausgeführte Duplizierung der Werkdaten, die durch einen Speicherungsvorgang dauerhaft auf ein Medium fixiert werden. Zu den Vervielfältigungsarten gehört auch der Download im Internet.[250] Wer also eine urheberrechtlich geschützte Datei via P2P-Netzwerk auf seine Festplatte herunterlädt und dort speichert, stellt eine identische Kopie dieser Datei und somit ein Werkexemplar her. Daran ändert sich auch nichts, wenn die Kopie – wie beim P2P-Filesharing via eDonkey-Netzwerk beispielsweise – aus mehreren Teilen zusammengesetzt und von verschiedenen Quellen heruntergeladen wird.[251]

Wie schon beim Zugänglichmachen würde ein Einverständnis des Rechteinhabers in den Download den objektiven Tatbestand ausschliessen, doch liegt ein solches beim Filesharing in P2P-Netzwerken praktisch nie vor.

b. Rechtmässiger Eigengebrauch auch bei rechtswidriger Kopiervorlage?

Eine Streitfrage der URG-Revision betraf das Herstellen von Werkkopien ab rechtswidriger Kopiervorlage, was vor allem im digitalen Umfeld von Bedeutung ist. Ausser bei Computerprogrammen, bei welchen ein rechtmässiger Eigengebrauch gemäss ausdrücklicher gesetzlicher Grundlage nicht möglich ist

249 Vgl. Art. 69 Abs. 1 lit. f und lit. i URG, die analog das Nutzungsrecht der Vervielfältigung von Ton- oder Tonbildträgern bzw. von auf Ton-, Tonbild- oder Datenträgern festgelegten Sendungen unter strafrechtlichen Schutz stellt.

250 Barrelet und Egloff (Fn. 238), Art. 10 N 12 m.N. So auch KGer GR, Strafmandat vom 27.7.2006, PS 06 5, E. 3.a.aa, sic! 2008, S. 205.

251 Schwarzenegger (Fn. 131), S. 225.

(Art. 19 Abs. 4 URG),[252] stellte die «Privatkopie» ab rechtswidriger Kopiervorlage nach bisherigem Urheberstrafrecht *einen erlaubten Eigengebrauch* nach Art. 19 Abs. 1 lit. a URG dar.[253]

Der Schweizer Gesetzgeber hat sich mit dieser Frage auseinandergesetzt und bewusst auf eine Einschränkung der Vervielfältigung zum Eigengebrauch verzichtet.[254] Damit weicht die schweizerische Lösung wesentlich von derjenigen in Deutschland ab, wo § 53 Abs. 1 Satz 1 dUrhG n.F. die Voraussetzungen des rechtmässigen Eigengebrauchs explizit und eng regelt. Die seit dem 1. Januar 2008 geltende Fassung dieses Paragraphen bestimmt, dass sich nicht auf die Schranke zum Eigengebrauch berufen kann, wer eine «offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage» zum privaten Gebrauch vervielfältigt.[255] Ein offensichtlich rechtswidriges öffentliches Zugänglichmachen wird nach dem revidierten dUrhG bei Werkdateien in P2P-Netzwerken immer dann anzunehmen sein, wenn sie bekanntermassen im kom-

252 Der Download von Computerspielen ohne Einverständnis des Rechteinhabers erfüllt somit immer den objektiven Tatbestand von Art. 67 Abs. 1 lit. e i.V.m. Art. 10 Abs. 2 lit. a URG.

253 Im zivilrechtlichen Kontext wurde teilweise der Standpunkt vertreten, der Eigengebrauch i.S.v. Art. 19 Abs. 1 lit. a URG sei nur dann rechtmässig, wenn die Kopiervorlage selbst rechtmässig angeboten bzw. verbreitet werde, Reto Hilty, § 52 Schweiz, in: Ulrich Loewenheim (Hrsg.): Handbuch des Urheberrechts, München 2003, S. 841 N 42; Weber und Unternährer (Fn. 238), S. 1382; Christoph Gasser, in: Barbara K. Müller und Reinhard Oertli (Hrsg.), Stämpflis Handkommentar, Urheberrechtsgesetz (URG), Bern 2006, Art. 19 mit Rev. Art. 19 Abs. 2 und 3 N 10 m.N. Generell gegen ein ungeschriebenes Tatbestandsmerkmal der «Rechtmässigkeit» der Kopiervorlage Rigamonti (Fn. 243), S. 282 und 286. Im Strafrecht ist eine Analogie zu Lasten des Angeschuldigten jedenfalls nicht zulässig (Art. 1 StGB), siehe zum Meinungsstand vor der Revision 2007 Schwarzenegger (Fn. 131), S. 226 m.w.N. Der Eigengebrauch war nach der bisherigen Rechtsprechung und Lehre aber unzulässig, wenn kein rechtmässiger tatsächlicher Zugang zum vervielfältigten Werkexemplar bestand (z.B. Ausdrucken eines Werkes aus einer Datenbank, zu welcher die betreffende Person keinen rechtmässigen Zugang hatte), BGE 128 IV 201, E. 3.5; Christoph Gasser, Der Eigengebrauch im Urheberrecht, Bern 1997, S. 61; Barrelet und Egloff (Fn. 238), Art. 19 N 7b, siehe hierzu auch unten C. IV.7.b, S. 480 ff.

254 Botschaft, BBl. 2006, 3430; Baumgartner (Fn. 164), S. 200 f.; Pascal Fehlbaum, Lutte contre l'échange illicite de musique sur Internet: une autre approche?, sic! 2007, S. 855–861, S. 856. Ein Antrag auf Ergänzung von Art. 19 URG durch folgenden Absatz wurde klar abgelehnt: «Vervielfältigungen von Werken nach den Bestimmungen zum Eigengebrauch dürfen nicht unter Verwendung offensichtlich unerlaubt hergestellter oder zugänglich gemachter Werkexemplare vorgenommen werden.» Vgl. dazu die Stellungnahme von Bundesrat Christoph Blocher: «Aber wir bitten Sie dringend, diesen Antrag abzulehnen. Wir sollten aufhören, Gesetzesbestimmungen zu erlassen, die man gar nicht durchsetzen kann! Ich bitte Sie, zu überlegen: Wenn Sie für den privaten Gebrauch zu Hause etwas auf eine leere Kassette aufnehmen würden, aus dem Internet beispielsweise, dann müsste die Polizei in Ihre Wohnung kommen, um das zu überprüfen.» AB 2007 N 1204.

255 Fassung gemäss dem Zweiten Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 26. Oktober 2007, Bundesgesetzblatt 2007 I Nr. 54, S. 2513 ff. (Inkrafttreten am 1.1.2008). Bis zum 31.12.2007 lautete dieser Passus «offensichtlich rechtswidrige hergestellte Vorlage» siehe zu den diesbezüglichen Auslegungsproblemen ausführlich Freiwald (Fn. 151), passim; Heghmanns (Fn. 145), S. 15 f.; Dreier und Schulze (Fn. 145), § 53 N 11 m.w.N.

merziellen Handel erhältlich sind.[256] In Österreich geht die Lehre überwiegend davon aus, dass die Zulassung der Vervielfältigung eines urheberrechtswidrig hergestellten Werkexemplars zum privaten Gebrauch den gesetzlichen Interessenausgleich derart zu Lasten der Urheber aus dem Gleichgewicht brächte, «dass sowohl der dem Urheberrecht zugrunde liegende Schutzgedanke als auch internationale Vorgaben zwingend gebieten, die Vervielfältigungsfreiheit entsprechend teleologisch zu reduzieren bzw. gesetzlich zu beschränken.»[257] Gemäss § 91 Abs. 1 öUrhG ist eine Vervielfältigung zum eigenen Gebrauch bzw. zum eigenen Gebrauch eines anderen ausdrücklich von der Strafbarkeit ausgenommen. Daher kommt der Fassung des § 42 Abs. 4 öUrhG, der die Vervielfältigungsfreiheit zum privaten Gebrauch regelt, als negatives Tatbestandsmerkmal des § 91 Abs. 1 öUrhG eine wesentliche Bedeutung zu. Wie in der Schweiz lässt der Wortlaut von § 42 Abs. 4 öUrhG offen, ob die Schrankenfreiheit auch zum Tragen komme, wenn die Kopiervorlage aus «trüber Quelle» stammt. Interessanterweise wird aber auch im Strafrecht eine Auslegung nach dem international- und EG-rechtlich vorgegebenen «Drei-Stufen-Test» vorgenommen,[258] weil er als Rechtsakt der Europäischen Gemeinschaften *unbedingten Anwendungsvorrang vor nationalem Recht* geniesst.

> «Anders formuliert: Eine Beschränkung des Vervielfältigungsrechts durch den nationalen Gesetzgeber oder nationale Behörden und Gerichte ist nur in einem solchen Umfang zulässig, als damit nicht gegen die Grenzen von Art. 5 Abs. 5 Info-RL verstossen wird.»[259]

Der Drei-Stufen-Test führt zum Resultat, dass eine Ausdehnung der Vervielfältigungsfreiheit zum privaten Gebrauch urheberrechtswidrig hergestellter Kopiervorlagen die normale Auswertung des urheberrechtlich geschützten Werks beeinträchtigt und auch die materiellen Interessen der Urheber ungebührlich verletzen. Daraus folgt: Das negative Tatbestandsmerkmal des § 91 Abs. 1 öUrhG ist bei rechtswidriger Kopiervorlage nicht erfüllt. Wer in P2P-Netzwer-

---

256 Da der Rechteinhaber nach § 19a dUrhG das ausschliessliche Recht der öffentlichen Zugänglichmachung innehat, wird das Fehlen eines Einverständnisses des Rechteinhabers leichter erkennbar, vgl. Baumgartner (Fn. 164), S. 198.

257 Florian Philapitsch, Die digitale Privatkopie, Eine Untersuchung der Freiheit der Vervielfältigung zum eigenen und privaten Gebrauch im internationalen, europäischen und nationalen Recht im digitalen Umfeld, Wien und Graz 2007, S. 206 und zum Ganzen S. 182 ff. So auch Sabine Plöckinger und Oliver Plöckinger, Das Urheberstrafrecht – Eine wirksame Waffe im Kampf gegen Film- und Musikpiraterie?, in: Oliver Plöckinger, Dieter Duursma und Michael Mayrhofer (Hrsg.), Internet-Recht, Beiträge zum Zivil- und Wirtschaftsprivatrecht, Öffentlichen Recht, Strafrecht, Wien 2004, S. 375–393, S. 382 ff.

258 Gemäss Art. 5 Abs. 5 Richtlinie 2001/29/EG dürfen nationale Schrankenbestimmungen nur in bestimmten Sonderfällen angewendet werden, in denen die normale Verwertung des Werkes oder des sonstigen Schutzgegenstandes nicht beeinträchtigt wird und die berechtigten Interessen des Rechteinhabers nicht ungebührlich verletzt werden. Dieser Drei-Stufen-Test ist auch nach Art. 9 Abs. 2 RBÜ, Art. 13 TRIPS, Art. 10 WCT und Art. 16 WPPT einzuhalten.

259 Oliver Plöckinger, Kunstfälschung und Raubkopie, Eine strafrechtliche Untersuchung, Wien 2006, S. 54 m.N.

ken Downloads ab solchen Quellen ausführt, macht sich nach dem geltenden österreichischen Urheberstrafrecht strafbar.[260]

Der Download von urheberrechtlich geschützten Werkdateien fällt in der Schweiz aber *nur dann* unter den *rechtmässigen Eigengebrauch* gemäss Art. 19 Abs. 1 lit. a URG, wenn der P2P-Nutzer seine Sharing-Software so konfiguriert, dass ein gleichzeitiges Weitergeben der Datei bzw. Datenpakete an weitere P2P-Nutzer unmöglich ist.[261] Dies ist aber ein Ausnahmefall. Auf dem Markt existieren verschiedene P2P-Netzwerke und Filesharing-Programme. Normalerweise ist bei diesen Programmen in der Grundkonfiguration mindestens der Upload der gerade heruntergeladenen Dateien freigeschaltet. Teilweise kann der Nutzer diese Sharing-Funktion gar nicht blockieren.[262] Die Filesharing-Programme sind ausserdem so angelegt, dass eine Sperrung der Sharing-Funktion den Download verlangsamt oder erschwert, schliesslich würde ein System mit lauter «Freeridern» (Trittbrettfahrern) gar nicht funktionieren. Das bedeutet, dass derjenige, der gerade Dateien aus dem Internet herunterlädt oder schon heruntergeladen hat, alle bei ihm im Sharing-Ordner abgespeicherten Datenpakete anderen P2P-Nutzern zur Verfügung stellt, solange sein Rechner mit dem P2P-Netzwerk verbunden ist.[263] Das hat zur Folge, dass der Downloader gleichzeitig zum Anbieter wird. Ist das Filesharing-Programm derartig eingestellt, so verwendet der Downloader die heruntergeladenen Dateien jedenfalls nicht nur für sich privat oder im engsten Kreis, sondern stellt sie unzähligen, ihm unbekannten Personen zur Verfügung. Daher stellt der Download von Werkdaten mit Hilfe derartig konfigurierter Programme keinen von Art. 19 Abs. 1 lit. a URG gedeckten Eigengebrauch dar und erfüllt somit den objektiven Tatbestand des Art. 67 Abs. 1 lit. e i.V.m. Art. 10 Abs. 2 lit. a URG.

Nur wenn die Upload-Funktion des P2P-Sharing-Programms völlig blockiert ist, kann der Download einer Datei als zustimmungsfreier rechtmässiger Eigengebrauch nach Art. 19 Abs. 1 lit. a URG angesehen werden.

---

260 Vgl. zum Ganzen Plöckinger (Fn. 259), S. 48 ff.; Philapitsch, (Fn. 257), S. 222 ff. je m.w.N.

261 Gl.M. KGer GR, Strafmandat vom 27.7.2006, PS 06 5, E. 3.b, sic! 2008, S. 206; Weber und Unternährer (Fn. 238), S. 1382; Heghmanns (Fn. 145), S. 16, zum deutschen Recht; wohl auch Fehlbaum (Fn. 250), S. 856. Abweichend Marcel Küchler, Anmerkung zu KGer GR, Strafmandat vom 27.7.2006, PS 06 5, sic! 2008, S. 208, der den Download bei offener Upload-Funktion des P2P-Clients gleichwohl als eine durch den Eigengebrauch gedeckten Herstellung eines Werkexemplars ansieht. Dem ist entgegenzuhalten, dass der Täter die Werkdaten objektiv in einem *öffentlichen Bereich* verwendet, wenn die heruntergeladenen Dateifragmente via P2P-Netzwerk unmittelbar nach ihrer lokalen Abspeicherung wieder beliebigen Dritten zugänglich sind.

262 So insbesondere bei den BitTorrent-, BearShare-, eDonkey2000- und Overnet-Clients. Vgl. die Übersicht der University of Chicago mit genauen Angaben über die Möglichkeiten zur Sperrung der Sharing-Funktion: ‹http://security.uchicago.edu/guidelines/peer-to-peer›.

263 Sandrine Rohmer und Joëlle Sambuc Bloise, Le mp3 face au droit d'auteur du point de vue des utilisateurs, AJP 2003, S. 51–57, S. 55; Fehlbaum (Fn. 250), S. 856.

c. Subjektiver Tatbestand

Der Downloader muss bezüglich aller objektiven Tatbestandsmerkmale mit Vorsatz handeln, wobei bei Art. 67 Abs. 1 lit. e URG der Eventualvorsatz genügt.[264]

Wie schon beim Anbieter ist die Ermittlung des Tätervorsatzes beim Downloader eine Tatfrage, die jeweils durch die Untersuchungsbehörde abzuklären und nachzuweisen ist. Es ist allgemein und insbesondere in der P2P-Community bekannt, dass neueste Musikstücke, Filme und Spielsoftware, die üblicherweise für 30 bis 200 Fr. pro Werkexemplar im Handel sind oder zum Teil erst im Kino gegen Entrichtung eines Eintrittspreises angeschaut werden können, nicht rechtmässig in einem P2P-Netzwerk zum Abruf bereitgehalten werden können und dass ihr Download eine Herstellung eines Werkexemplares darstellt. Eine laienhafte Vorstellung darüber dürfte regelmässig gegeben sein. P2P-User, die ein Computerspiel oder bei offener Sharing-Funktion Musik oder Filme herunterladen, handeln daher in aller Regel mindestens mit Eventualvorsatz bezüglich aller objektiven Tatbestandsmerkmale.[265] Meistens wird es sich sogar um einen direkten Vorsatz handeln, weil die Downloader diese Dateien gerade deshalb vom P2P-Netzwerk runterladen, weil sie dadurch die Kosten für einen rechtmässigen Erwerb einsparen können. Diese Downloader dürften auch alle den erforderlichen (Eventual-)Vorsatz bezüglich der Unrechtmässigkeit ihres Tuns haben, ist es doch aus Medienberichten und Onlinequellen allgemein bekannt, dass die Hersteller bzw. Rechteinhaber dieser Werke das Einverständnis zum File-Sharing in P2P-Netzwerken nicht abgegeben haben. Schliesslich müssen Downloader – falls sie es nicht wissen – mindestens mit der Möglichkeit rechnen, dass ein rechtmässiger Eigengebrauch bei Computerspielen unmöglich und bei Musik und Filmen – im Falle offener Sharing-Funktion – ausgeschlossen ist. Wer trotzdem die Dateien herunterlädt, hat keinen «Vorsatz» auf einen rechtmässigen Eigengebrauch, sondern nimmt in Kauf, objektiv tatbestandsmässig zu handeln.[266]

d. Rechtswidrigkeit und Schuld

Das Einverständnis des Rechteinhabers und der rechtmässige Eigengebrauch sind tatbestandsausschliessend; Anwendungsfälle der gesetzlichen oder überge-

---

264 Glarner (Fn. 151), S. 87 m.N. Siehe zur Definition des Eventualvorsatzes Art. 12 Abs. 2 Satz 2 StGB.

265 So auch Rohmer und Sambuc Bloise (Fn. 263), 56.

266 Informativ hierzu aus einer deutschen Beschuldigtenvernehmungen: «Ich muss ehrlich sagen, ich habe schon davon gehört, dass es nicht ganz legal ist. Allerdings war es immer etwas unklar, teilweise wurde auch gesagt, dass man doch was herunterladen darf. Ich war auf jeden Fall nicht ganz sicher. Hinzu kommt noch, dass in meinem Bekanntenkreis sehr viel aus dem Internet heruntergeladen wird und es hat sich eigentlich niemand Gedanken darüber gemacht. Das hat mich eben auch dazu veranlasst, diese Filme herunterzuladen», siehe Polizeikommissariat Einbeck, 31.10.2007, abrufbar unter: ‹www.logistepag.com/de/urteile.php›.

setzlichen Rechtfertigungsgründe sind kaum denkbar. Ein *Irrtum über die Rechtswidrigkeit* nach Art. 21 StGB fällt ebenfalls ausser Betracht, weil das Bewusstsein über die Rechtswidrigkeit schon zum subjektiven Tatbestand gehört.[267]

5. *Strafbare Teilnahme durch Zurverfügungstellen der P2P-Filesharing-Software?*

Mit dem Zurverfügungstellen von Filesharing-Software werden weder technische Massnahmen umgangen (Art. 69a Abs. 1 lit. a URG) noch handelt es sich um Vorrichtungen, Erzeugnisse oder Bestandteile i.S.v. Art. 69a Abs. 1 lit. b URG. Da aber der Up- und Download von urheberrechtlich geschützten Werkdaten gar nicht möglich wäre, wenn keine Filesharing-Software zur Verfügung stünde, wird die Frage aufgeworfen, ob nicht die Programmierer, Anbieter und Verbreiter der Filesharing-Software als Gehilfen zur Verantwortung zu ziehen sind (Art. 25 StGB).[268] Richtet man das Augenmerk auf dezentralisierte P2P-Netzwerke,[269] fällt auf, dass die Strafbarkeit an das Verbreiten der Filesharing-Software anknüpfen müsste, weil die Verantwortlichen danach keinerlei Kontrolle über das Funktionieren des Netzwerkes und die Handlungen der P2P-User mehr ausüben können.

a. *Harmlose Alltagshandlungen*

Programmierer, Anbieter und Verbreiter von Filesharing-Software sind mit Herstellern und Anbietern von Waffen oder Abhörgeräten vergleichbar. Sie legen den Grundstein für rechtmässige wie strafbare Handlungen, in der Regel ohne genauere Kenntnis über nachmalige Täter und Taten zu haben. Allerdings besteht gerade im Kreise einiger P2P-Software-Entwickler eine offenkundige Doppelmoral, nach welcher man gegen aussen jeglicher illegaler Nutzung der Programme absagt, während man indirekt über Werbebanner in der Software wirtschaftlich Profit schlägt,[270] obwohl bekannt ist, dass die P2P-User die Programme überwiegend zu unrechtmässigen Zwecken einsetzen.

Gemäss bundesgerichtlicher Rechtsprechung gilt als Hilfeleistung jeder kausale Beitrag, der die Tat fördert, so dass sich diese ohne Mitwirkung des Gehilfen anders abgespielt hätte. Nicht erforderlich ist, dass es ohne die Gehilfen-

---

267 Siehe dazu den voranstehenden Abschnitt.

268 Haupttäterschaft oder Mittäterschaft kommt mangels Tatherrschaft über die inkriminierten Handlungen nicht in Betracht.

269 Die Frage nach der Gehilfenstrafbarkeit für das Anbieten eines zentralen Dateiverzeichnisses mit Suchfunktion, wie sie im Zusammenhang mit zentralisierten P2P-Netzwerken à la Napster aufgetreten war, kann an dieser Stelle ausgeklammert werden, weil sie wegen des technischen Wandels der P2P-Netzwerke kaum mehr von praktischer Relevanz ist (vgl. GLARNER (Fn. 151), S. 126 ff. m.N., aber ohne eigene Stellungnahme; HEGHMANNS (Fn. 145), S. 15 f., der eine Beihilfestrafbarkeit nach deutschem Recht für klar gegeben erachtet).

270 JACQUES DE WERRA, L'évolution du droit d'auteur à l'épreuve d'internet, in: Alan Raguenau (éd.), Internet 2003, Lausanne 2004, S. 15 f. m.N.

handlung nicht zur Tat gekommen wäre. Strafbare Beihilfe liegt also grundsätzlich z.B. auch dann vor, wenn der Haupttäter sich die vom Gehilfen erhaltenen Tatwerkzeuge auch anderswo hätte beschaffen können.[271] Weiter ist nicht vorausgesetzt, dass der Täter vom Verhalten des Gehilfen Kenntnis hat.

Eine Gehilfenschaft der Programmverbreiter kommt sowohl hinsichtlich der unrechtmässigen Downloads wie auch des Uploads in Betracht, weil beides ohne die Software nicht möglich wäre. Sie setzt in objektiver Hinsicht eine tatbestandsmässige, rechtswidrige Haupttat eines anderen sowie eine diese Haupttat fördernde Gehilfenhandlung voraus. In subjektiver Hinsicht muss sich der (Eventual-)Vorsatz des Gehilfen sowohl auf die Haupttat wie auch auf die eigene Beihilfehandlung beziehen.

An einem objektiv kausalen Förderungsbeitrag ist kaum zu zweifeln. Zahlreiche P2P-User begehen die strafbaren Urheberrechtsverletzungen mittels der zur Verfügung gestellten Filesharing-Software. Dass sie auch ein alternatives Programm hätten einsetzen können, ändert nichts an diesem konkreten objektiven Kausalzusammenhang. Hier setzt nun die Diskussion darüber an, ob und unter welchen Voraussetzungen sogenannte «neutrale» Handlungen oder «Alltagshandlungen» straflos sein sollen, selbst wenn dies in Kenntnis möglicherweise strafbarer Nutzung durch Dritte geschieht.[272]

Im Antilopenfleisch-Fall[273] hat das Bundesgericht erste Kriterien entwickelt, die eine Eingrenzung des Tatbestandes der Gehilfenschaft bei «Alltagshandlun-

---

271 BGE 121 IV 109, E. 3.a; 120 IV 265, E. 2.c; 119 IV 289, E. 2.c je m.w.N.

272 Zum Stand der Diskussion in der Schweiz siehe BGE 120 IV 265, E. 2.c; 119 IV 289, E. 2.c; Peter Albrecht: Kommentar zum schweizerischen Strafrecht, Sonderband Betäubungsmittelstrafrecht, Art. 19–28 BetmG, Bern 1995, Art. 19 N 94 f.; Marc Forster: Der Wirtschaftsalltag als strafrechtsdogmatischer «Hort des Verbrechens», Zum «zielobjektivierten Beihilfetatbestand» bei sogenannten Alltagsgeschäften und berufstypischen Dienstleistungen, in: Jürg-Beat Ackermann, Andreas Donatsch und Jörg Rehberg (Hrsg.), Wirtschaft und Strafrecht, Festschrift für Niklaus Schmid, Zürich 2001, S. 127–142; Marcel Alexander Niggli, Klassische Teilnahme (Gehilfenschaft), in: Marcel Alexander Niggli, Franz Riklin und Günter Stratenwerth, Die strafrechtliche Verantwortlichkeit von Providern, Medialex Sonderausgabe 2000, S. 22–29, S. 25 ff.; Wolfgang Wohlers, Gehilfenschaft durch «neutrale» Handlungen – Ausschluss strafrechtlicher Verantwortlichkeit bei alltäglichem bzw. berufstypischem Verhalten?, ZStrR 117 (1999), S. 425–438; Günter Stratenwerth, Schweizerisches Strafrecht, Allgemeiner Teil I: Die Straftat, 3. Aufl., Bern 2005, § 13 N 120; Andreas Donatsch und Brigitte Tag, Strafrecht I, Verbrechenslehre, 8. Aufl., Zürich 2006, S. 159 ff. alle m.N. Spezifisch zur Bereitstellung von P2P-Software aus deutscher Sicht Heghmanns (Fn. 145), S. 17 f. m.w.H. zur deutschen Lehre. Nach Heghmanns soll es schon genügen, wenn der Programmverbreiter die besonderen Qualitäten des Programms gerade zum Musikdatentausch und die schützende Anonymität des dezentralen Netzes hervorhebe, selbst wenn dies mit dem Hinweis verbunden werde, die Nutzer sollten damit keine Urheberrechtsverletzungen begehen. Denn darin sei eine Bestärkung des Täterwillens zu sehen, womit das Handeln des Programmverbreiters nicht mehr als sozialadäquate Alltagshandlung gewürdigt werden könne. Das Verbreiten derartiger Programme ohne die erwähnten Hervorhebungen falle dagegen unter die straflosen normalen Alltagshandlungen.

273 BGE 119 IV 289. Siehe auch BGE vom 18.8.2001, 6S.656/2000, Erw. 3 (Gehilfenschaft zur mehrfachen teilweise versuchten Widerhandlung gegen Art. 105 Abs. 1 AVIG i.V.m. Art. 25 StGB durch unrichtige Arbeitszeiterfassungen).

gen» erlauben. Bei objektiv rechtmässigem Verhalten, wie dem Verkauf eines Produkts unter richtiger Bezeichnung,[274] darf der Verkäufer prinzipiell darauf vertrauen, dass die Käufer die gekaufte Ware legal verwenden. Wenn aber eine mögliche legale Verwendung des Produkts faktisch ausser Betracht fällt und der Verkäufer weiss, dass der Abnehmer die bezogene Ware praktisch nur illegal verwenden kann, sei ein deliktischer Sinnbezug und darüber hinaus auch eine Solidarisierung des Verkäufers mit dem Haupttäter gegeben. Aus diesen Erwägungen ist zu entnehmen, dass die Einschränkung einerseits über eine normative Wertung («deliktischer Sinnbezug»), andererseits über ein subjektives Element («Solidarisierung mit dem Verkäufer») eröffnet wird. In der Rechtsprechung und Lehre wird teilweise völlig auf die subjektive Seite abgestellt.[275] Andere Meinungen wollen das Problem im Anschluss an die deutsche Lehre unter dem Aspekt der «objektiven Zurechnung» strafrechtlicher Verantwortlichkeit aus dem objektiven Tatbestand herausschälen.[276]

Der Ansatz, schon auf Stufe der objektiven Unrechtsdefinition zu einer Einschränkung zu gelangen, ist richtig. Er ergibt sich letztlich aus verfassungsrechtlichen Grundsätzen und sollte auch vermehrt darauf abgestützt werden. Die Grundrechte sind nicht nur für den Gesetzgeber, sondern auch für die Strafgerichte bei der Auslegung der Strafbestimmungen Vorgabe und Grenze zugleich.[277] Werden durch Strafbestimmungen Grundrechte eingeschränkt, muss das den Voraussetzungen von Art. 36 BV genügen und kann zu einem Korrektiv «überschiessender Tendenzen» schon auf Stufe des objektiven Tatbestandes führen.[278] Jedenfalls sind im Bereiche der Äusserungsdelikte konventional- und verfassungsrechtliche Schranken anerkannt, die trotz Vorliegens der konsti-

274 Wie beim (kostenlosen) Anbieten von Filesharing-Software.

275 Albrecht (Fn. 272), Art. 19 N 95, der bei normalen Alltagshandlungen einen direkten Vorsatz ersten Grades fordert (bezüglich Art. 19 Ziff. 1 BetmG, der bestimmte Gehilfenhandlungen als eigenständige Haupttaten definiert); vgl. Stratenwerth (Fn. 272), § 13 N 120 m.N.

276 Wohlers (Fn. 272), S. 427 ff. Ähnlich die Ansätze, welche die Strafbarkeit nur dann annehmen, wenn eine bestimmte Gehilfenhandlung unter den gegebenen Umständen allein den Sinn haben kann, zur Begehung eines Delikts beizutragen, siehe Stratenwerth (Fn. 272), § 13 N 120 a.E.

277 EGMR, Lingens vs. Austria (Appl. no. 9815/82), 8. Juli 1986, § 39: «The Contracting States have a certain margin of appreciation in assessing whether such a need [«restrictions or penalties necessary in a democratic society», Art. 10 Abs. 2 EMRK] exists …, but it goes hand in hand with a European supervision, embracing both the legislation and the decisions applying it, even those given by an independent court.»

278 Siehe Andreas Auer, Les médias dans la nouvelle Constitution fédérale, in: Ursula Cassani, Renie Maag, Marcel Alexander Niggli (Hrsg.), Medien, Kriminalität und Justiz, Chur/Zürich 2001, S. 13–34, S. 28 ff. m.N., am Beispiel der Berücksichtigung der Medien- (Art. 17 Abs. 1 BV) und Informationsfreiheit (Art. 16 Abs. 1 BV) bzw. Meinungsäusserungsfreiheit (Art. 10 EMRK) bei der Anwendung von Art. 3 lit. a i.V.m. Art. 23 UWG (unrichtige, irreführende oder unnötig verletzende Äusserungen über Waren etc.). Eine Interessenabwägung zwischen den genannten Freiheitsrechten und der Wirtschaftsfreiheit müsste zur Straflosigkeit von vergleichenden Medienberichten über Produkte führen (entgegen BGE 117 IV 193).

tutiven Strafbarkeitsvoraussetzungen keine Strafbarkeit zur Folge haben dürfen[279].

Im schweizerischen Verfassungsrecht ergeben sich vor allem in Bezug auf eine genügend präzise gesetzliche Umschreibung der Eingriffsnorm (Bestimmtheitsgebot, vgl. Art. 1 StGB) und die Verhältnismässigkeit des Eingriffs (Art. 36 Abs. 3 BV)[280] Anhaltspunkte, die für die Limitierung der objektiven Tatbestandsmerkmale herangezogen werden können und müssen. Unter dem Aspekt des Verhältnismässigkeitsgrundsatzes wird vorausgesetzt, dass die konkret gewählte Strafnorm zur Verwirklichung des im öffentlichen Interesse liegenden Ziels geeignet und notwendig ist. Ausserdem muss der angestrebte Zweck in einem vernünftigen Verhältnis zu den eingesetzten Mitteln bzw. den zu seiner Erreichung notwendigen Grundrechtsbeschränkungen stehen.[281]

Am Beispiel der Filesharing-Programmverbreiter: Anstatt darauf abzustellen, ab wann sie «ein über das zulässige Mass hinausgehendes, unerlaubtes Risiko» schaffen,[282] müsste die grundrechtsorientierte Frage lauten: Ab wann ist die Beschränkung ihrer Wirtschafts- (Art. 27 BV), Meinungs- (Art. 16 BV) und allenfalls Wissenschaftsfreiheit (Art. 20 BV) durch die Strafnormen nicht mehr verfassungskonform. Dies führt zu einer auf Verhaltenstypen bezogenen Interessenabwägung. Zu beachten ist bei Filesharing-Software, dass ihre Entwicklung und Verbreitung auch anderen, sozial erwünschten Zwecken dient.[283]

---

279 Wie mehrere Verfahren vor dem EGMR zeigen. Siehe Jersild v. Denmark (EGMR, Urteil Nr. 36/1993/431/510 vom 23. September 1994, ÖJZ 1995, 227 ff.); Lingens v. Austria (Appl. no. 9815/82), 8. Juli 1986 (= EuGRZ 1986, 424 ff.); Oberschlick v. Austria (Appl. no. 1662/851), 23. Mai 1991 (= EuGRZ 1991, 216 ff.); Kürkçü v. Turkey (Appl. no. 43996/98), 27. Juli 2004. In diesen Entscheidungen hat der EGMR sowohl bezüglich Ehrverletzungen und Gehilfenschaft zu rassendiskriminierenden Äusserungen in konkreten Einzelfällen die strafrechtliche Sanktionierung als Verletzung von Art. 10 EMRK angesehen. Zwar äussert sich der EGMR nicht über die dogmatische Eingliederung dieser Begrenzung (Tatbestand, Rechtfertigung, Schuld), doch dürfte es einem Mitgliedsstaat der EMRK schon gar nicht zustehen, ein Unrecht jenseits der Grenzen dessen zu definieren, was «in einer demokratischen Gesellschaft im Interesse namentlich der Aufrechterhaltung der Ordnung und der Verbrechensverhütung, des Schutzes der Gesundheit und der Moral, des Schutzes des guten Rufs oder der Rechte anderer notwendig» ist (so Art. 10 Abs. 2 EMRK). Folglich muss diese Schranke schon auf der objektiven Tatbestandsebene beachtet werden, zumindest wenn sie sich infolge der grundrechtlichen Interessenabwägung für bestimmte Verhaltenstypen generalisieren lässt. Mangels verfassungsgerichtlicher Kompetenz (Art. 191 BV) kann das BGer diese Einschränkung nur unter dem Titel einer verfassungs- und EMRK-konformen Auslegung vornehmen (BGE 128 IV 204 f. m.N.; BGE vom 22.1.2003, 6S.698/2001, Erw. 5). Auch diese erfolgt auf der Stufe des objektiven Tatbestandes.

280 Vgl. EGMR, Lingens v. Austria (Appl. no. 9815/82), 8. Juli 1986, § 40.

281 Siehe allgemein BGE 113 Ia 126; 128 I 3 m.w.N.

282 Stratenwerth (Fn. 272), § 13 N 120.

283 Zum Beispiel als kostengünstige und leistungsfähige Distributionsform für Softwareentwickler oder unabhängige Musiker; als Archiv für Musiktitel, Filme und andere Werke, die nicht mehr dem urheberrechtlichen Schutz unterstehen (vgl. Art. 29–31 URG, Erlöschen des Urheberrechts 70 Jahre nach dem Tod des Urhebers bei den erwähnten Werkkategorien); als Alternative zu zentralisierten Netzwerken in einem Unternehmen usw. P2P-Filesharing ist auch aus wissenschaftlicher Sicht von grosser Bedeutung. Zum *chilling effect* durch Verbote, bestimmte Techniken zu entwickeln, vgl. Werra (Fn. 270), S. 16 m.N.

Diese legitimen Zwecke müssen bei der Begrenzung des objektiven Tatbestandes der Gehilfenschaft (Art. 25 StGB) angemessen berücksichtigt werden, denn ohne Limitierung wirkt die Strafnorm wie ein *Verbot* derartiger Software-Entwicklungen und der damit zusammenhängenden Handlungen.

Hier setzt ein weiteres verfassungsrechtlich verankertes Kriterium zur Beschränkung des objektiven Tatbestandes ein: das Bestimmtheitsgebot (Art. 5 Abs. 1, Art. 31 Abs. 1, Art. 36 Abs. 1 BV, Art. 1 StGB). Der objektive Beihilfetatbestand – «Hilfe leisten» zu einem beliebigen Verbrechen oder Vergehen – ist unpräzis und konturenlos. Das Kriterium der Voraussehbarkeit als Bestandteil der genügend präzisierten Gesetzesgrundlage (Art. 36 Abs. 1 BV) wird faktisch ausgehöhlt, falls bei technischen Innovationen (Programmentwicklung und -verbreitung), denen aus grundrechtlicher Sicht ein relativ hoher Stellenwert beizumessen ist, eine Gehilfenstrafbarkeit bejaht wird, weil ein Dritter das daraus entstandene Produkt (Filesharing-Software) zu kriminellen Zwecken missbraucht und der Vertreiber des Produkts damit rechnen müsste. Selbst wenn er die Missbrauchsmöglichkeiten beschreibt und in allgemeiner Form darauf hinweist, sollte dies bei Dual-Use-Produkten noch nicht für eine Gehilfenstrafbarkeit reichen.[284]

Nach dem Bestimmtheitsgebot und dem Verhältnismässigkeitsgrundsatz wären minder eingriffsintensive Mittel und eine gesetzliche Regelung anzustreben. So könnte die Gefahrenabwehr im Bereich des P2P-Filesharings mit einer bundesgesetzlichen Kontrolle der Programmverbreitung konkretisiert werden oder aber im strafrechtlichen Kontext mit der Einführung eines abstrakten Gefährdungsdeliktes, das die Verbreitung von Filesharing-Programmen einschränkt, wie dies bei Waffen (Art. 260^{quater} StGB) und Abhörgeräten (Art. 179^{sexies} StGB) tatsächlich geschehen ist. Der objektive Tatbestand von Art. 179^{sexies} StGB erfasst bezeichnenderweise nur «Geräte, die *insbesondere* dem widerrechtlichen Abhören usw. dienen.»[285] Aus dieser Überlegung ist in der Regel schon der objektive Beihilfetatbestand bei Filesharing-Softwarevertreibern nicht erfüllt. Ein anderes Resultat ergibt die Interessenabwägung aber dann, wenn ein Produkt praktisch nur zu illegalen Zwecken eingesetzt werden kann.[286] Die tangierten Freiheitsrechte des Herstellers und Vertreibers sind dann wesentlich weniger gewichtig zu veranschlagen.

284 Insofern a.M. HEGHMANNS (Fn. 145), S. 17 f. für Deutschland.

285 Meine Hervorhebung. Für eine gesetzliche Regelung auch DE WERRA (Fn. 270), S. 12 ff.

286 So im älteren Fall der Sperrkreisfilter, die nur als Decodiergeräte für den unrechtmässigen Empfang eines Pay-TV-Angebots eingesetzt werden konnten, BGE 114 IV 112 E. 2.c.bb (Gehilfenschaft zum Versuch der Leistungserschleichung durch den Verkäufer, heute eigenständige Haupttäterschaft nach Art. 150bis StGB).

b. Straflosigkeit mangels genügend konkretisierten Vorsatzes

Auch auf der subjektiven Tatbestandsebene ist ein Ausschluss der Strafbarkeit möglich, wenn man die Kenntnisse der objektiven und subjektiven Merkmale der von allfälligen Haupttätern zu begehenden Delikte im Zeitpunkt der «Gehilfenhandlung» des Filesharing-Software-Anbieters noch als zu unspezifisch ansieht bzw. eine Gehilfenschaft ablehnt, wenn keiner der Haupttäter zum Zeitpunkt der Gehilfenhandlung einen Tatentschluss gefasst hat.[287]

6. Strafbare Teilnahme durch Webportale und Hash-Link-Verweisungen auf urheberrechtlich geschützte Werkdaten?

In den letzten Jahren wurden Webportale mit Informationen zur Verfügbarkeit von urheberrechtlich geschützten Werkdaten in P2P-Netzwerken sehr populär. Dabei ermöglichen direkte Hash-Links den unmittelbaren Zugriff auf solche Daten, falls ein funktionstüchtiges P2P-Filesharing-Programm auf dem Computer des Nutzer installiert ist und dieser einen Anschluss an das Internet hat.[288] Die Rechtsprechung sieht in solchen Angeboten eine Hilfestellung zum unrechtmässigen Zugänglichmachen und gleichzeitig zum unrechtmässigen Herstellen von Werkdaten.[289]

7. Der strafrechtliche Schutz gegen die Umgehung von technischen Schutzmassnahmen und Vorbereitungshandlungen

a. Das Merkmal der Unrechtmässigkeit im objektiven Tatbestand von Art. 69a Abs. 1 URG

Art. 69a Abs. 1 URG knüpft die Strafbarkeit aller nachfolgenden Tatbestandsvarianten an das Merkmal der Unrechtmässigkeit der Tathandlung.[290] Verboten und damit unrechtmässig sind die unter Strafe gestellten Handlungen bereits nach Art. 39a Abs. 1 und 3 URG. Bei den Straftatbeständen, welche die Verletzung von Urheber- und Nachbarrechten erfassen (vgl. Art. 67 Abs. 1, 69 Abs. 1, 69a Abs. 1 lit. d URG), macht die besondere Hervorhebung der Unrechtmässigkeit als objektives Tatbestandsmerkmal Sinn, weil keine strafbare Urheber- und Nachbarrechtsverletzungen vorliegen kann, wenn der Rechteinhaber vorher sein *Einverständnis* zur Nutzungshandlung abgegeben hat.[291]

---

287 Mit dieser Begründung gegen eine Strafbarkeit GLARNER (Fn. 151), S. 129. Eingehend zur Frage, ob ein Tatentschluss beim Haupttäter schon zum Zeitpunkt der Gehilfenhandlung gefasst sein muss, SCHWARZENEGGER (Fn. 131), S. 242 ff. m.w.N.

288 Siehe für eine genauere Beschreibung und ausführliche Analyse der möglichen Gehilfenstrafbarkeit SCHWARZENEGGER (Fn. 131), S. 237 ff.

289 KGer GR, 27.7.2006, PS 06 5 und PS 06 6; BezGer Frauenfeld, 11.2.2008, S.2006.42.

290 Art. 69a Abs. 1 URG: «… wer vorsätzlich und unrechtmässig …».

291 Zur tatbestandsausschliessenden Wirkung eines Einverständnisses (teilweise auch tatbestandsausschliessende Einwilligung genannt) siehe allgemein DONATSCH und TAG (Fn. 272), S. 248;

Weil der strafrechtliche Schutz gegen Umgehungshandlungen mittelbar ebenfalls auf die Urheber- und verwandten Schutzrechte zurückgeht,[292] ist es plausibel, auch bei Art. 69a Abs. 1 lit. a URG bei Vorliegen eines zuvor erteilten Einverständnisses den Tatbestand entfallen zu lassen. Falsch ist dies aber bei den Tatbestandsvarianten der Vorbereitungshandlungen zur Umgehung (Art. 69a Abs. 1 lit. b URG), weil bei der Begehung dieser abstrakten Gefährdungsdelikte noch gar nicht erkennbar ist, welches Angriffsobjekt und welcher Rechtsgutsträger betroffen sein könnte. Einverständnis oder Einwilligung sind aber nur denkbar, wenn der Straftatbestand ein individuelles Rechtsgut schützt. Und: Nur wenn ein Tatbestand ausdrücklich oder nach seinem Normzweck eine Handlung voraussetzt, welche gegen den Willen des individuellen Rechtsgutsträgers erfolgen muss, kann die Unrechtmässigkeit Teil des objektiven Tatbestandes sein. Bei Art. 69a Abs. 1 lit. b URG existiert die erforderliche individuelle Rechtsposition der Urheber und Leistungsschutzberechtigten aber nicht.

De lege ferenda ist zu empfehlen, Art. 69a Abs. 1 lit. a und lit. c URG und Art. 69a Abs. 1 lit. b URG auf zwei separate Straftatbestände aufzuteilen, wobei bei den Vorbereitungshandlungen die Unrechtmässigkeit aus dem Tatbestand zu streichen wäre.

b. Die Bedeutung der Schutzschranken, insbesondere des Eigengebrauchs (Art. 19 Abs. 1 URG), für die Strafbarkeit nach Art. 69a Abs. 1 URG

Nach einer wechselhaften historischen Entwicklung wurde am 9. Oktober 1992 die noch heute bestehende Regelung zum Eigengebrauch verabschiedet.[293] Zur Funktion dieser Schrankenregelung schreiben auf der Maur und Keller:[294]

> «Die bisherige Entwicklung zeigt, dass im Urheberrecht das Prinzip verankert ist, den Urheber möglichst umfassend an der wirtschaftlichen Werkverwertung teilhaben zu lassen. Gleichzeitig war das Urheberrecht immer einer Interessenabwägung zwischen den Urheberinteressen und den Interessen der Allgemeinheit unterworfen. Es kann dem Urheberrecht jedoch kein Prinzip entnommen werden, wonach dem Nutzer ein absolutes Recht auf Pivatkopie zustünde. Vielmehr zeigt die Entstehungsgeschichte der Schrankenbestimmungen zum Privatgebrauch, dass sich das Urheberrecht immer aufgrund einer Abwägung der wirtschaftlichen und technischen Gegebenheiten an die sich wandelnden Interessen anpassen musste. Das Recht auf Privatkopie, wie es im heutigen URG verankert ist, wurde seit der Einführung und Weiterentwicklung dieser Schrankenbestimmung als behelfsmässige Lösung für ein juristisch und technisch an-

---

Vera Delnon und Bernhard Rüdy, in: Marcel Alexander Niggli und Hans Wiprächtiger (Hrsg.), Basler Kommentar, Strafrecht II, Art. 111–392, 2. Aufl., Basel 2007, Art. 186 N 34, und spezifisch zum Urheberstrafrecht Glarner (Fn. 151), S. 76 f.; Schwarzenegger (Fn. 131), 218 f.; Barrelet/Egloff (Fn. 253), Art. 67 N 6a je m.w.N.

292 Siehe oben C.IV.1.b, S. 463 f.

293 Siehe zusammenfassend Botschaft, BBl. 1989 III 537 ff.; Inkrafttreten am 1.7.1993 (AS 1993, 1820).

294 Rolf auf der Maur und Claudia Keller, Privatkopie: Ein wohlerworbenes Recht? Eine Schrankenbestimmung als Spielball sich wandelnder Interessen, sic! 2004, S. 79–89, S. 86.

derweitig nicht lösbares Problem verstanden. Die Schutzschranke zugunsten des Privatgebrauchs kann daher nicht als «wohlerworbenes Recht» interpretiert werden, das es in der bisherigen umfangreichen Form ins digitale Zeitalter hinüber zu retten gilt.»

Aus strafrechtlicher Sicht stellt sich die Frage, welchen Einfluss Art. 19 Abs. 1 URG[295] auf die strafrechtliche Würdigung der verschiedenen Tatbestandsvarianten von Art. 67 ff. URG hat. Im Zusammenhang mit der Verletzung des Urheberrechts und der verwandten Schutzrechte (Art. 67, 69 URG) sind die genehmigungsfreien Nutzungsarten gemäss Art. 19 URG *tatbestandsausschliessende Merkmale.*[296] Hier verhält sich das Strafrecht zivilrechtsakzessorisch. Die Verwendung veröffentlichter Werke zum Eigengebrauch wird als «gesetzliche Lizenz» bezeichnet.[297] Sie ist ohne Zustimmung des Rechteinhabers zulässig, im Gegenzug sieht das Gesetz ein System indirekter Vergütungen vor. Somit handelt es sich bei Nutzungsformen innerhalb der Schutzschranken um rechtmässiges Verhalten. Dieses lässt aufgrund der expliziten negativen Tatbestandsvoraussetzung der Unrechtmässigkeit in den Art. 67 ff. URG schon die Tatbestandsmässigkeit dahinfallen.

Ob die Schrankenbestimmung des Eigengebrauchs (Art. 19 URG) durch die Einführung zivil- und strafrechtlicher Schutznormen betreffend technische Massnahmen limitiert werden sollte, war eine der strittigen Kernfragen der URG-Revision,[298] die letztlich durch den Gesetzgeber zugunsten des Vorrangs des Eigengebrauchs entschieden wurde.

«Der Schutz technischer Massnahmen besteht aus *zwei Komponenten:* erstens aus einem *Umgehungsverbot* und zweitens aus dem *Verbot, Vorbereitungshandlungen vorzunehmen.* … Absatz 4 enthält einen Vorbehalt gegenüber dem Umgehungsverbot, der sich auf alle Schutzmassnahmen [recte: Schutzschranken], nicht nur auf den in Artikel 19 geregelten Eigengebrauch bezieht. Diese Bestimmung schützt die Nutzer und Konsumenten vor einer missbräuchlichen Anwendung des Umgehungsverbotes – das

295 Die Bestimmungen über die Schranken des Urheberrechts finden auch auf die verwandten Schutzrechte Anwendung, siehe Art. 38 URG.

296 Siehe auch oben C.IV.4.d, S. 473 f.

297 Siehe statt aller Rehbinder (Fn. 221), N 142; Gasser (Fn. 253), Art. 19 mit Rev. Art. 19 Abs. 2 und 3 N 3; siehe auch Barrelet/Egloff (Fn. 238), Art. 19 N 2, die beim Eigengebrauch nach Art. 19 Abs. 1 lit. a URG von einer «materiellen Schranke des Urheberrechts» sprechen.

298 Zur Diskussion im Vorfeld der Revision siehe auf der Maur/Keller (Fn. 294), S. 87 ff.; Reto M. Hilty, Urheberrecht in der Informationsgesellschaft – Schweizer Modell vs. Europäische Vorgaben, sic! 2004, S. 966–980, S. 978 ff.; Cyrill P. Rigamonti, Angriff auf die digitale Privatkopie, NZZ 21.6.2004, S. 16; Jacqueline Schwerzmann, Kartellrechtlicher Schutz vor technischen Schutzmassnahmen?, sic! 2004, S. 148–155, S. 148 ff.; Thomas Dreier, Schöne neue Welt? Technische Schutzmassnahmen, digitales Rechtemanagement und ihr rechtlicher Schutz gegen unerlaubte Umgehung im Recht der EU und ihrer Mitgliedstaaten, EuZ 2005, S. 46–53, S. 46 ff. (mit internationalem Vergleich); Brigitte Lindner, Fehlende Bekenntnis zum Urheberschutz, Gefährlicher Alleingang der Schweiz, NZZ 11.9.2006, S. 14; Sandrine Rohmer und Joëlle Sambuc Bloise, Le nouveau droit d'auteur en Suisse: un équilibre délicat entre la lutte contre la piraterie en ligne et le respect des droits fondamentaux, AJP 2007, S. 831–838.

gibt es nämlich auch. Sie verhindert, dass jemand, der eine gesetzlich erlaubte Werkverwendung vornimmt, indem er z.B. eine Kopiersperre umgeht, um eine Privatkopie herzustellen, für diese Umgehung belangt werden kann. Im Falle der beantragten Streichung von Absatz 4 würde das *Umgehungsverbot die Schutzausnahmen aushebeln,* die der Gesetzgeber im Interesse der Allgemeinheit vorgesehen hat.»[299]

Der Nationalrat folgte mit deutlichem Mehr der Bitte des Bundesrates, Art. 39 Abs. 4 URG nicht zu streichen, was deutlich werden lässt, dass die Schutzschranken gegenüber dem Umgehungsschutz Vorrang behalten sollten. Über die Vorbereitungshandlungen wurde nichts gesagt. Es ist jedoch aufgrund des gesetzessystematischen Zusammenhanges anzunehmen, dass sowohl für das Umgehungsverbot wie auch für das Verbot der Vorbereitungshandlungen eine Koppelung oder Bindung an das materielle Urheberrecht gelten sollte.[300]

299 Bundesrat Christoph Blocher, AB 2007 N 1353 (meine Hervorhebungen).

300 Wie hier Barrelet und Egloff (Fn. 253), Art. 69a N 5 «Nicht unrechtmässig sind danach Umgehungshandlungen, die ausschliesslich für eine erlaubte Verwendung [i.S.v. Art. 39a Abs. 4 URG] vorgenommen werden.» Auch im Zivilrecht entfällt die Widerrechtlichkeit der unerlaubten Handlung (Art. 41 OR), wenn eine gesetzlich erlaubte Verwendung vorgenommen wird, Barrelet und Egloff (Fn. 253), Art. 39a N 6 und N 12. Vgl. auch Rigamonti (Fn. 178), S. 4 ff., der sogar die Meinung vertritt, dass Koppelungsprinzip ergebe sich zwingend aus Art. 11 WCT und Art. 18 WPPT; Baumgartner (Fn. 164), S. 194. Aus strafrechtlicher Sicht unhaltbar ist die Ansicht von Dominik P. Rubli, Das Verbot der Umgehung technischer Massnahmen zum Schutz digitaler Datenangebote, Diss. Zürich 2008, N 47 und N 452 ff. (im Erscheinen), der den Schrankenbestimmungen im Zusammenhang mit der Verletzung des Umgehungsverbotes bloss die Funktion einer «negativen objektiven Strafbarkeitsbedingung» einräumen will. Hier wird die Bedeutung objektiver Strafbarkeitsbedingungen im Strafrecht verkannt. Diese dienen als Strafausschlussgründe, die für den Unrechts- und Schuldgehalt eines Tatbestandes ohne Bedeutung sein müssen. Charakteristikum der objektiven Strafbarkeitsbedingungen ist insbesondere, dass sie vom Vorsatz nicht erfasst werden. Aus Art. 69a Abs. 1 und Abs. 3 URG geht aber deutlich hervor, dass der Gesetzgeber die unerlaubte Verwendung als Tatbestandsmerkmal dem Unrecht der Umgehungshandlungen zuordnet. In Art. 69a Abs. 1 lit. a URG ist sogar eine diesbezügliche Absicht gefordert. Rublis Ansicht hätte weiter zur Folge, dass gegen Umgehungshandlungen innerhalb der Schutzschranken Notwehr- und Notstandshandlungen möglich wären (etwa durch programmgesteuerte Zerstörmechanismen bei versuchter Umgehung). Auch den aus dieser Ansicht abgeleiteten Schlussfolgerungen hinsichtlich des Ausschlusses einer Rechtfertigung im Rahmen der Computerdelikte kann daher nicht gefolgt werden.

Tabelle 3: Reichweite des rechtmässigen Eigengebrauchs in der Schweiz im Vergleich zu Deutschland und Österreich

Reichweite des rechtmässigen Eigengebrauchs	Verletzungen von Urheberrechten	Verletzung von verwandten Schutzrechten	Umgehung von technischen Massnahmen	Vorbereitungshandlungen
Schweiz	Tatbestandsausschluss bei unrechtmässiger und rechtmässiger Kopiervorlage	Tatbestandsausschluss bei unrechtmässiger und rechtmässiger Kopiervorlage	Tatbestandsausschluss	Tatbestandsausschluss
Deutschland	Rechtfertigung *nur* bei rechtmässiger Kopiervorlage	Rechtfertigung *nur* bei rechtmässiger Kopiervorlage	rechtswidrig, aber nicht strafbar[301]	strafbar
Österreich	Rechtfertigung *nur* bei rechtmässiger Kopiervorlage	Rechtfertigung *nur* bei rechtmässiger Kopiervorlage	rechtswidrig, aber nicht strafbar[302]	strafbar

Haben jedoch die Schutzschranken auch bei den Strafnormen betreffend Umgehungsverbot und Vorbereitungshandlungen (Art. 69a Abs. 1 URG) eine tatbestandsausschliessende Wirkung, was Art. 39a Abs. 4 URG und das Merkmal der Unrechtmässigkeit in Art. 69a Abs. 1 URG nahelegen, wird die Strafnorm *keine praktische Bedeutung erlangen.*[303]

Ausser bei Computerprogrammen[304] und (noch) nicht veröffentlichten Werken[305] sind kaum Anwendungsbeispiele vorstellbar, in welchen die Strafverfolgungsbehörden nach- und beweisen könnten, dass die Umgehungs- oder die Vorbereitungshandlung im Hinblick auf eine unrechtmässige Nutzung er-

301 § 108b Abs. 1 dUrhG. Die Privatkopie darf aber zivilrechtlich gegenüber technischen Schutzmechanismen nicht durchgesetzt werden, § 95b Abs. 1 Satz 1 Nr. 6 dUrhG e contrario, siehe Thomas Dreier und Astrid Buhrow, Für die digitale Verwertung erforderliche Nutzungsrechte, in: Hans-Werner Moritz und Thomas Dreier (Hrsg.), Rechts-Handbuch zum E-Commerce, 2. Aufl., Köln 2005, S. 306; Baumgartner (Fn. 164), S. 192 f., der auf die Rechtmässigkeit der analogen Signalabnahme hinweist; Dreier und Schulze (Fn. 145), § 95b N 12 und § 108b N 6 m.w.N.

302 § 91 Abs. 1 Satz 2 öUrhG, strittig. Plöckinger (Fn. 259), S. 59 ff. m.N., hält die Vervielfältigung unter Umgehung technischer Schutzmassnahmen de lege lata für strafbar (§ 90c öUrhG), selbst bei Handlungen innerhalb der Schrankenbestimmung des § 42 Abs. 4 öUrhG, tritt aber de lege ferenda für eine Entkriminalisierung ein; de lege lata für Straflosigkeit Philapitsch (Fn. 257), S. 218 m.N.

303 Dies wurde in der parlamentarischen Beratung durchaus gesehen: «Mit dieser Bestimmung [Art. 39a Abs. 4 URG] wird klar, dass man den Rechtsschutz der elektronischen Werkverbreitung, dass man Digital Rights Management (DRM) und damit letztlich die Wipo-Regelungen überhaupt nicht will.» (Votum J. Alexander Baumann, AB 2007 N 1351).

304 Die Verwendung zum Eigengebrauch ist hier ausgeschlossen (Art. 19 Abs. 4 URG).

305 Die Schutzschranken sind diesbezüglich nicht anwendbar, vgl. Art. 19 Abs. 1 URG.

folgte.[306] Jede Person, die eine tatbestandsmässige Handlung nach Art. 69a Abs. 1 URG ausführt, beispielsweise zu Hause eine Zugangssperre aushebelt, wird sich darauf berufen, sie habe dies zum Zwecke des rechtmässigen Eigengebrauch getan. Die Beweislast für das Gegenteil liegt bei der zuständigen Strafverfolgungsbehörde. Stellt die gleiche Person die Werkdatei später in einem P2P-Netzwerk zum Download bereit, ist keine Strafbarkeit nach Art. 69a Abs. 1 lit. a URG mehr möglich, weil die Umgehungshandlung schon zuvor vollendet wurde, als sie nicht tatbestandsmässig war. Ein *dolus superveniens* ist mit anderen Worten irrelevant. Das Zugänglichmachen wird durch die neuen Straftatbestände in Art. 67 Abs. 1 lit. g^{bis} und Art. 69 Abs. 1 lit. e^{ter} URG erfasst, doch wird dabei mit der strafrechtlichen Verfolgung wieder bis zur Verletzung des Urheberrechts bzw. des verwandten Schutzrechts zugewartet und der Rechtsschutz der Rechteinhaber nicht verbessert. Damit eine Umgehungshandlung überhaupt bestraft werden kann, müsste wohl schon aus den objektiven Umständen erkennbar sein, dass sie ein Täter nicht zum Eigengebrauch ausführt, was nur dann der Fall sein dürfte, wenn sie etwa in den Räumlichkeiten eines illegalen Kopierstudios stattfindet.

Die Auswirkungen auf Art. 69a Abs. 1 lit. b URG sind noch abstruser. Ist eine Vorbereitungshandlung, mit der eine Person explizit nur Umgehungshandlungen zum rechtmässigen Eigengebrauch ermöglichen will, nicht auch vom Tatbestand ausgenommen (Art. 39a Abs. 4 URG)? Zu dieser Schlussfolgerung muss man nach dem Wortlaut dieser Bestimmung i.V.m. Art. 69 Abs. 1 URG, dem Willen des Gesetzgebers und der Systematik des Gesetzes kommen, doch erscheint das Resultat vor dem Hintergrund der Motive für die URG-Revision unverständlich.[307]

c. Das Merkmal der Absicht im subjektiven Tatbestand von Art. 69a Abs. 1 lit. a URG

Erforderlich ist zunächst der Vorsatz, wobei Eventualvorsatz genügt. Für Art. 69a Abs. 1 lit. a URG wurde ein weiteres subjektiven Tatbestandsmerkmals eingeführt: die Absicht, eine gesetzlich unerlaubte Verwendung von Werken oder anderen Schutzobjekten vorzunehmen.

Das revidierte URG lässt den Schutzschranken wie erläutert[308] tatbestandsausschliessende Wirkung zukommen. Dies hat zur Folge, dass *ihr Fehlen* als negatives Tatbestandsmerkmal vom (Eventual-)Vorsatz mitumfasst sein muss. Damit ist aber das zusätzliche subjektive Tatbestandsmerkmal der Absicht

306 Die Botschaft, BBl. 2006, 3428, schweigt hierzu völlig.

307 Für Rigamonti (Fn. 178), S. 7, «mag zwar sein, dass ein derart beschränktes Verbot weniger effektiv ist als ein pauschales Verbot sämtlicher Umgehungsmittel, doch ist dies als Folge der von den WIPO Abkommen getroffenen Interessenabwägung hinzunehmen.»

308 Siehe Tabelle 3, S. 483.

überflüssig, weil schon der Vorsatz des Täters auf eine unrechtmässige Handlung zielen muss.

Dementsprechend muss die Strafverfolgungsbehörde nicht nur nachweisen, dass eine Umgehungshandlung begangen wurde, sondern darüber hinaus, dass der Täter mindestens mit einem bedingten Vorsatz handelte, eine unerlaubte Verwendung vorzunehmen oder allenfalls einen anderen eine solche Verwendung vornehmen zu lassen.

d. Das Verhältnis von Art. 69a Abs. 1 lit. d URG zu den Art. 67 und 69 URG

Die Strafbestimmung des Art. 69a Abs. 1 lit. d URG soll das Verbot aus Art. 39c Abs. 3 URG strafrechtlich absichern. Die Botschaft schreibt zur Begründung der Norm:

> «In den *Buchstaben d* und *e*[309] werden die Handlungen unter Strafe gestellt, die den Schutz von elektronischen Informationen für die Rechtewahrnehmung verletzen».[310]

Art. 39c Abs. 3 URG lautet:

> [3] Werke oder andere Schutzobjekte, an denen Informationen für die Wahrnehmung von Urheber- und verwandten Schutzrechten entfernt oder geändert wurden, dürfen in dieser Form weder vervielfältigt, eingeführt, angeboten, veräussert oder sonst wie verbreitet noch gesendet, wahrnehmbar oder zugänglich gemacht werden.

Die Umsetzung der Zielvorgabe ist missglückt. Es stellt sich insbesondere die Frage, worin überhaupt der Unterschied zwischen den Tatbestandsvarianten des Art. 69a Abs. 1 lit. d URG und denjenigen der Art. 67 und 69 URG bestehen soll.[311]

Aus der nachfolgenden Tabelle wird ersichtlich, dass beinahe alle Tatbestandsvarianten des Art. 69a Abs. 1 lit. d URG eine Entsprechung in den Art. 67 und 69 URG haben. *Der einzige Unterschied* besteht in allen Varianten darin, dass bei Art. 69a Abs. 1 lit. d URG jeweils ein *spezifisches Angriffsobjekt erforderlich* ist, nämlich ein Werk oder anderes Schutzobjekt, an welchem zuvor Informationen über die Wahrnehmung von Rechten nach Art. 39c Abs. 2 URG entfernt oder geändert wurden.

309 In der endgültigen Fassung Buchstaben c und d.

310 Botschaft, BBl. 2006, 3428.

311 Darauf wurde schon im Gesetzgebungsprozess hingewiesen Christian Schwarzenegger, Stellungnahme betreffend strafrechtliche Aspekte der laufenden URG-Revision, Zürich 2007, S. 28 ff.

Tabelle 4: Gegenüberstellung der Tatbestandsvarianten von Art. 69a Abs. 1 lit. d URG und Art. 67 bzw. 69 URG

Tatbestandsvarianten des Art. 69a Abs. 1 lit. d URG[312]	**Deckungsgleiche Tatbestandsvarianten der Art. 67 und 69 URG (Angriffsobjekt: Werk oder andere Schutzobjekte)**
Vervielfältigung	Herstellung von Werkexemplaren (Art. 67 Abs. 1 lit. e URG) Vervielfältigung eines Ton- oder Tonbildträgers (Art. 69 Abs. 1 lit. f URG) Vervielfältigung einer auf Ton-, Tonbild- oder Datenträger festgelegten Sendung (Art. 69 Abs. 1 lit. i URG)
Einführen	Keine Entsprechung (ev. als Verbreitungshandlung erfasst)
Anbieten	Anbieten von Werkexemplaren (Art. 67 Abs. 1 lit. f URG) Anbieten der Vervielfältigungsexemplare eines Ton- oder Tonbildträgers (Art. 69 Abs. 1 lit. f URG)
Veräusserung	Veräusserung von Werkexemplaren (Art. 67 Abs. 1 lit. f URG) Veräusserung der Vervielfältigungsexemplare eines Ton- oder Tonbildträgers (Art. 69 Abs. 1 lit. f URG)
Verbreitung	Verbreitung von Werkexemplaren (Art. 67 Abs. 1 lit. f URG) Verbreitung der Vervielfältigungsexemplare eines Ton- oder Tonbildträgers (Art. 69 Abs. 1 lit. f URG) Verbreitung der Vervielfältigungsexemplare einer auf Ton-, Tonbild- oder Datenträger festgelegten Sendung (Art. 69 Abs. 1 lit. i URG)
Sendung	Sendung eines Werks (Art. 67 Abs. 1 lit. h URG) Sendung einer Werkdarbietung durch Radio, Fernsehen oder ähnliche Verfahren, auch über Leitungen (Art. 69 Abs. 1 lit. a URG) Ev. auch die Weitersendung einer gesendeten Werkdarbietung mittels technischer Einrichtungen, deren Träger nicht das ursprüngliche Sendeunternehmen ist (Art. 69 Abs. 1 lit. d URG) Ev. auch die Weitersendung einer Sendung (Art. 69 Abs. 1 lit. g URG)
Wahrnehmbarmachung	Wahrnehmbarmachung eines Werks (Art. 67 Abs. 1 lit. g und lit. i URG) Wahrnehmbarmachung einer gesendeten oder weitergesendeten Werkdarbietung (Art. 69 Abs. 1 lit. e URG)
Zugänglichmachung	Zugänglichmachung eines Werks (Art. 67 Abs. 1 lit. g^{bis} URG) Zugänglichmachung einer Werkdarbietung, eines Ton- oder Tonbildträgers oder einer Sendung mit irgendwelchen Mitteln (Art. 69 Abs. 1 lit. e^{ter} URG)

312 Angriffsobjekt: Werk oder andere Schutzobjekte, an denen Informationen über die Wahrnehmung von Rechten nach Artikel 39c Absatz 2 entfernt oder geändert wurden.

Weshalb diese Kongruenzen eingeführt wurden, ist aus den Gesetzgebungsmaterialien nicht ersichtlich. Nach den allgemeinen Rechtsauslegungsgrundsätzen müsste den verschiedenen Varianten von Art. 69a Abs. 1 lit. d URG im Verhältnis zu den älteren und weniger spezifischen Varianten der Art. 67 und 69 URG *lex specialis-Charakter* zukommen. Das heisst, wenn an einem Werk oder anderen Schutzobjekt Informationen über die Wahrnehmung von Rechten nach Art. 39c Abs. 2 URG entfernt oder geändert wurden und anschliessend eine Tathandlung nach Art. 69a Abs. 1 lit. d URG ausgeführt wird, wäre nur diese Bestimmung anwendbar. Die Strafbarkeit nach den einschlägigen Varianten der Art. 67 und 69 URG entfiele.

Weil Art. 69a Abs. 1 lit. d URG nur Busse androht, handelt es sich um eine *Übertretung* – mit allen negativen Konsequenzen,[313] die für die Strafverfolgung damit verbunden sind – und somit um einen *privilegierten Tatbestand gegenüber den Art. 67 und 69 URG.* Es ist erstaunlich, dass diese Schwächung des strafrechtlichen Schutzes der Urheber und Inhaber verwandter Schutzrechte nicht beachtet wurde.[314]

Hätte man im Gegenzug den Schutz dieser Rechtspositionen durch Art. 39c Abs. 3 i.V.m. Art. 69a Abs. 1 lit. d URG durch ein absolutes Verbot der Tathandlungen nach Art. 69a Abs. 1 lit. d URG verstärkt, also auch den Schutzschranken, insbesondere dem Eigengebrauch, keine tatbestandsausschliessende Wirkung zugebilligt, wäre die Privilegierung allenfalls noch nachvollziehbar gewesen.[315] Allein, die Ausführungen der Botschaft zu Art. 39c Abs. 3 URG zeigen die genau gegenteilige Intention. Das Verbot, Informationen für die Wahrnehmung von Urheberrechten und verwandten Schutzrechten zu entfernen oder zu ändern, könne dann nicht geltend gemacht werden, heisst es da,[316] wenn diese Handlungen ausschliesslich zum Zweck einer erlaubten Verwendung im Rahmen der Schutzschranken ausgeführt würden. Das blieb in der parlamentarischen Beratung unwidersprochen.

Am Beispiel: Wenn eine Person den Identifikationscode[317] an einer über den iTunes Store erworbenen, mit beschränkten Abspielrechten versehenen Musikwerkdatei entfernt, um danach eine Vervielfältigung für den Eigengebrauch anzufertigen, verletzt sie weder Art. 39c Abs. 3 URG noch kann sie nach Art. 69a Abs. 1 lit. d URG bestraft werden. Nur: Dazu braucht es keinen neuen Straftatbestand, denn genau das Gleiche galt schon nach Art. 67 und 69 URG.

Als Fazit kann festgehalten werden, dass Art. 69a Abs. 1 lit. d URG den strafrechtlichen Schutz von Art. 67 und 69 URG verdrängt, sobald an einem Werk oder anderen Schutzobjekt Informationen über die Wahrnehmung von

313 Siehe sogleich unter C.IV.7.e, S. 488.

314 In der Botschaft, BBl. 2006, 2428, findet sich nichts zum Verhältnis zwischen diesen Strafnormen.

315 Vgl. auch David (Fn. 141), Art. 69 mit Rev. Art. 69a (neu) N 18.

316 Botschaft, BBl. 2006, 3427.

317 Dieser wurde zur Wahrnehmung des Urheberrechts und verwandten Schutzrechts angebracht.

Rechten nach Art. 39c Abs. 2 URG entfernt oder geändert werden (lex specialis). Er schwächt diesen Rechtsschutz, weil die Strafnorm zu einer Übertretung herabgestuft wird. Handlungen im Rahmen der Schutzschranken sollen nach der Intention der Botschaftverfasser vom Verbot nicht erfasst werden, d.h. tatbestandsausschliessend wirken. Die aktuelle Fassung von Art. 69a Abs. 1 lit. d URG steht damit in einem deutlichen Widerspruch zum deklarierten Ziel der URG-Revision, eine Stärkung des Rechtsschutzes für Urheber und Leistungsschutzberechtigte im digitalen Umfeld zu implementieren. Wurde diese Entscheidung bewusst gefällt, handelt sich um ein Beispiel symbolischer Gesetzgebung. Für einen effektiven Rechtsschutz hätte die tatbestandsausschliessende Wirkung der Schutzschranken aufgegeben und die Strafdrohung für Handlungen nach Art. 69a Abs. 1 lit. d URG zumindest an jene der Art. 67 und 69 URG (Vergehen, maximal 1 Jahr Freiheitsstrafe) angepasst werden müssen.

e. Die Strafdrohung von Art. 69a Abs. 1 URG und ihre Konsequenzen

Art. 69a Abs. 1 URG sieht als Strafdrohung für alle Tatbestandsvarianten Busse vor. Sie werden folglich den *Übertretungen* zugeordnet (vgl. Art. 103, Art. 333 Abs. 3 StGB).[318] Urheberrechtsverletzungen nach Art. 67 URG und Verletzungen von verwandten Schutzrechten (Art. 69 URG) sind dagegen Vergehen, weil die maximale Strafdrohung «Freiheitsstrafe bis zu einem Jahr» lautet (vgl. Art. 10 Abs. 3 StGB). Die Botschaft[319] verweist zur Begründung des tieferen Strafrahmens in Art. 69a Abs. 1 URG auf den Strafrahmen der parallelen Bestimmung zum Schutz des elektronischen Geschäftsverkehrs (Art. 150bis StGB). Allerdings ist eine Parallelität nur zu den Vorbereitungshandlungen des Technologieverkehrs (Art. 69a Abs. 1 lit. b URG) erkennbar, nicht jedoch zum Umgehungstatbestand selbst (Art. 69a Abs. 1 lit. a URG), ebensowenig zur Entfernung oder Veränderung von elektronischen Informationen zur Wahrnehmung der Urheber- und verwandten Schutzrechte (Art. 69a Abs. 1 lit. c URG) und zu Verletzungshandlungen nach Art. 69a Abs. 1 lit. d URG. Der Unrechtsgehalt einer konkreten Rechtsgutsgefährdung (Umgehung, Informationsentfernung) oder sogar -verletzung (Vervielfältigung usw.) wird in der Regel höher veranschlagt als derjenige von Vorbereitungshandlungen hierzu, die noch im Bereich einer abstrakten Gefährdung liegen.

Die Konsequenzen der Einstufung als Übertretung für die Strafverfolgung wurden im Gesetzgebungsprozess nicht beachtet. In der jetzigen Form ist der strafrechtliche Schutz wenig effektiv, weil *strafprozessuale Zwangsmittel,* wie sie z.B. im Bereich der Internetkriminalität für die Ermittlung praktisch unentbehrlich sind, bei Übertretungen nur beschränkt zulässig sind und die Verfolgung in die *Zuständigkeit von Verwaltungsbehörden* im Übertretungsstrafver-

318 Nur die qualifizierte Variante der gewerbsmässigen Tatbegehung gehört zu den Vergehen (vgl. Art. 10 Abs. 3 StGB).

319 BOTSCHAFT, BBl. 2006, 3428.

fahren fällt.[320] Ausserdem können die Vorgaben der Convention on Cybercrime in Bezug auf strafprozessuale Zwangsmassnahmen auf diese Weise nicht gewährleistet werden.[321] Übertretungen sind auch *keine Auslieferungsdelikte* (Art. 35 Abs. 1 lit. a IRSG) und nur dann internationale Rechtshilfedelikte, wenn die doppelte Strafbarkeit gegeben ist.

Der *Versuch* ist *nicht strafbar;* ebensowenig die *Gehilfenschaft* (Art. 105 Abs. 2 StGB). Gerade im Bereich der Internetkriminalität – man denke an die für den Datenaustausch zentralen P2P-Netzwerke – spielen aber Gehilfen eine wichtige Rolle. Strafverfolgungsbehörden müssen hier häufig zunächst gegen eine Person ermitteln, die eine unüberblickbare Vielzahl von Haupttätern durch untergeordnete Tatbeiträge unterstützt,[322] welche die Haupttaten aber erst möglich machen. Der illegale Verkehr mit Umgehungstechnologien ist wie die massenhafte Verletzung der Urheber- und Nachbarrechte bei der Verbreitung in P2P-Netzwerken ganz wesentlich auf diese Schnittstellen angewiesen, auch wenn die Betreiber dieser Dienste nach der strafrechtlichen Verantwortlichkeitsregelung «nur» Gehilfenhandlungen ausführen.

Zur Illustration ein Beispiel: Im Juli 2006 konnte das Kantonsgericht Graubünden den Betreiber einer Website (Swissmule), welche über sog. Hash-Links einer grossen Zahl von Nutzern den direkten Zugriff auf illegal im Internet angebotene Werkdaten ermöglichte, nur als Gehilfen eines Täters einzelner Urheberrechtsverletzungen verurteilen.[323] Es ist absehbar, dass diese Probleme bei der Strafverfolgung von Umgehungen technischer Massnahmen und mehr noch der Verbreitung der Umgehungstechnologie gehäuft auftreten werden. Ist die Verfolgung von Gehilfen ausgeschlossen, wird der strafrechtliche Schutz erheblich geschwächt, wenn nicht sogar gänzlich ausgehöhlt. Schliesslich ist auch keine Strafbarkeit des Unternehmens nach Art. 102 StGB möglich.[324]

Immerhin werden die Vorgaben der Convention on Cybercrime für «Handlungen in gewerbsmässigem Umfang» erfüllt, weil Art. 69a Abs. 2 URG für diese eine Strafdrohung von maximal einem Jahr Freiheitsstrafe androht, womit

320 Die Strafverfolgung ist mit Ausnahme von Delikten nach Art. 70 URG Sache der Kantone (Art. 73 Abs. 1 URG). Diese wird folglich im herkömmlichen kantonalen Übertretungsstrafverfahren durchzuführen sein. Zwangsmassnahmen sind dabei nur unter einschränkenden Bedingungen zulässig, vgl. nur NIKLAUS SCHMID, Strafprozessrecht, Eine Einführung auf der Grundlage des Strafprozessrechtes des Kantons Zürich und des Bundes, 4. Aufl., Zürich 1994, N 925.

321 Siehe oben C.III.3.c, S. 452.

322 Denkbar sind das Betreiben eines Host-Servers, eines Internetauktionsportals, eines Super-Peer-Servers, einer Informationswebsite mit Hash-Links usw.

323 KGer GR, 27.7.2006, PS 06 6.

324 Zu beachten sind die Art. 6–7 VStrR. Bei Übertretungen ist Art. 7 VStrR allein anwendbar. Bei Vergehen wurde die Frage einer ausschliesslichen oder alternativen Anwendbarkeit von Art. 102 StGB bisher offengelassen. Gemäss neuerer Rechtsprechung kann Art. 7 VStrR diesfalls nur in Betracht gezogen werden, wenn die Ermittlung der individuellen Verantwortlichkeiten gemäss Art. 6 VStrR angesichts der verwirkten Strafe unverhältnismässige Untersuchungsmassnahmen erfordern würde, siehe BGE vom 15.10.2007, 6B_256/2007, E. 3–4 = forumpoenale 2008, Nr. 29 mit Anm. von ALAIN MACALUSO.

das gewerbsmässige Delikt zu einem Vergehen hinaufgestuft wird, gegen welches die erforderlichen prozessualen Zwangsmassnahmen auch rechtshilfeweise durchgeführt werden können.

Mit der Einstufung von Art. 69a Abs. 1 URG als Übertretung – so kann zusammenfassend festgehalten werden – hat der Gesetzgeber einen Fehlgriff begangen. Auf dieser Rechtsgrundlage kann ein effektiver strafrechtlicher Schutz von technischen Massnahmen nicht gewährleistet werden. Es drängt sich *de lege ferenda* auf, die Strafdrohung an diejenige von Art. 67 und 69 StGB anzupassen.[325] Möglich wäre auch eine Differenzierung zwischen Art. 69a Abs. 1 lit. a (Vergehen) und lit. b–d URG (Übertretung), doch müssten dann bei letzteren mindestens der Versuch und die Gehilfenschaft explizit strafbar erklärt werden, wie dies auch in Art. 150bis Abs. 2 StGB vorgesehen ist. Die Nachteile des Übertretungsstrafverfahrens würden in diesem Fall aber nicht ausgeräumt.

8. Das Antragserfordernis als Prozessvoraussetzung in Art. 69a URG

Art. 69a Abs. 1 URG stellt sämtliche Straftatbestände betreffend technische Massnahmen unter das Erfordernis des Strafantrags. Antragsberechtigt ist die «in ihrem Schutz verletzte Person».

Zu beachten ist hierbei, dass sich die Antragsberechtigung nicht nach privat-, sondern nach strafrechtlichen Grundsätzen richtet. Zum Strafantrag berechtigt ist jeder durch die Tat Verletzte (Art. 30 Abs. 1 StGB). Gemäss bundesgerichtlicher Rechtsprechung gelten nur jene Personen als Verletzte, welche «materiellrechtlich Träger des verletzten Rechtsgutes» sind.[326] Der Gebrauchsberechtigte gehört beispielsweise nicht zu diesem Personenkreis.[327] Im Kontext des Patentrechts gilt der einfache Lizenznehmer im Gegensatz zum Inhaber ausschliesslicher oder qualifizierter Lizenzen nicht als antragsberechtigt, weil er kein rechtlich geschütztes Interesse daran hat, dass Dritte das Patent nicht nutzen.[328]

Im revidierten URG lässt sich eine indirekte individualschutzrechtliche Konzeption für den Umgehungsschutz aus Art. 39a Abs. 1 i.V.m. Art. 62 Abs. 1bis URG ableiten,[329] da eine konkrete Gefährdung des Urheberrechts bzw. der ver-

---

325 D.h. eine maximale Strafdrohung von mindestens einem Jahr Freiheitsstrafe.

326 BGE 128 IV 84 «Le lésé au sens de l'art. 28 CP [jetzt Art. 30 StGB] est celui dont le *bien juridique est directement atteint* par l'infraction» (meine Hervorhebung). Erweitert wird die Antragsberechtigung neben dem Rechtsgutsträger auch auf Personen, die an der Erhaltung des Rechtsgutes ein gleichartiges rechtlich geschütztes Interesse haben, vgl. Christof Riedo, in: Marcel Alexander Niggli und Hans Wiprächtiger (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–110, Jugendstrafgesetz, 2. Aufl., Basel 2007, Art. 28 N 10 m.N.

327 Günter Stratenwerth und Wolfgang Wohlers, Schweizerisches Strafgesetzbuch, Handkommentar, Bern 2007, Art. 30 N 1.

328 Riedo (Fn. 220), S. 551.

329 Deutschland und Österreich folgen einem individualschutzrechtlichen Konzept und sehen deshalb ein Antragserfordernis vor (Deutschland: §§ 109 i.V.m. 108b dUrhG, bei besonderem öffentlichen Interesse an der Strafverfolgung wird die Tat zum Offizialdelikt; Österreich: § 91 Abs. 1 i.V.m. Abs. 3 öUrhG).

wandten Schutzrechte anzunehmen ist.[330] Bei den Vorbereitungshandlungen gibt es nach strafrechtlichen Kriterien keine in ihrem Schutz verletzte Person. Daran kann auch der Hinweis auf eine Gefährdung in Art. 62 Abs. 1bis URG nichts ändern.

Da die Vorbereitungshandlungen nach Art. 69a Abs. 1 lit. b URG *abstrakte Gefährdungsdelikte* sind,[331] haben Existenz und Identität eines Gefährdeten keine Relevanz und hätten diese Tatbestandsvarianten folglich als Offizialdelikte definiert werden müssen.[332]

Dies würde bedeuten, dass *kein Antragsberechtigter* i.S. von Art. 30 Abs. 1 StGB[333] und ausserdem *kein Verletzter* existiert,[334] der die Verfahrensrechte eines Geschädigten[335] wahrnehmen oder im Rahmen eines Strafverfahrens adhäsionsweise[336] allenfalls Zivilforderungen geltend machen könnte. Die Klagebefugnisse aus Art. 62 URG auch mit der Ergänzung durch Art. 62 Abs. 1bis URG, die von den soeben aufgezeigten straf- und strafprozessrechtlichen Regelungen abweichen, vermögen an diesen Konsequenzen nichts zu ändern. Insbesondere werden dadurch keine Antragsberechtigung im Strafrecht und keine Geschädigtenstellung im Strafverfahren begründet.

Zu Recht wird allerdings im Zusammenhang mit Art. 150bis StGB vorgebracht, der Gesetzgeber habe schwerlich wollen können,[337] dass dieses als Antragsdelikt ausgestaltete abstakte Gefährdungsdelikt gar nie angewandt werden könne.[338] Als antragsberechtigt wird man deshalb – wohl oder übel bzw. mehr Übel als Wohl – jeden *potentiell betroffenen* Urheber oder sonstigen Leistungsschutzberechtigten ansehen müssen. Ob es aufgrund dieser weitgefassten Antragsberechtigung zu «Sammelklagen» kommen wird, bleibt abzuwarten.

---

330 Siehe oben C.IV.2.b. S. 463.

331 Siehe oben C.IV.2.c. S. 464.

332 Man vergleiche nur mit dem ähnlich gelagerten Art. 144bis Ziff. 2 StGB («Computervirentatbestand»), wo richtigerweise kein Antragserfordernis vorgesehen ist.

333 Siehe zur Nichtanerkennung von Verletzten bei Leugnung von Völkermord oder andern Verbrechen gegen die Menschlichkeit (Art. 261bis Abs. 4 zweiter Satzteil StGB) BGE 129 IV 95, E. 3.5–3.6, «Individuelle Rechtsgüter werden nur mittelbar geschützt.»; vgl. Niklaus Schmid, Computer- sowie Check- und Kreditkarten-Kriminalität, Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994, § 5 N 11 m.N.

334 Siehe z.B. § 395 Abs. 1 Ziff. 2 ZH-StPO: Person, welche durch das Delikt «unmittelbar ein Schaden zugefügt wurde oder zu erwachsen drohte»; zur Unterscheidung zwischen unmittelbarer und mittelbarer Beeinträchtigung privater Interessen Schmid (Fn. 320), N 509.

335 Teilnahme an Untersuchungshandlungen, Beweisanträge, Akteneinsicht, Ergreifen von Rechtsmitteln usw., vgl. Schmid (Fn. 320), N 515 ff.

336 Zum Adhäsionsprozess Schmid (Fn. 320), N 511.

337 Art. 150bis StGB ist als Nebenprodukt der FMG-Revision von 1997 ohne Beizug strafrechtlichen Sachverstandes eingeführt worden, vgl. BBl. 1996 III 1452. Es ist deshalb anzunehmen, dass der Gesetzgeber diesbezüglich überhaupt keinen Willen gebildet hat.

338 Gerhard Fiolka, in: Marcel Alexander Niggli und Hans Wiprächtiger (Hrsg.), Basler Kommentar, Strafrecht II, Art. 111–392, 2. Aufl., Basel 2007, Art. 150bis N 39 m.N.

9. *Wirksamkeit des strafrechtlichen Rechtsgüterschutzes im Verhältnis Urheber- und Computerstrafrecht?*

Das Verhältnis der Strafnormen des URG zu jenen des Computerstrafrechts (Art. 143, 143bis, 144bis, 147, 150, 150bis StGB) ist bisher dogmatisch wenig ausgeleuchtet worden. Auch die URG-Revision hat das Thema fast vollständig ausgeblendet. Es stellen sich aber zahlreiche neuartige Abgrenzungsfragen, weil Werke und andere Schutzobjekte im digitalen Umfeld als Daten gespeichert oder übermittelt werden. Die Nutzungshandlung des Vervielfältigens, Verbreitens, Zugänglichmachens geschehen heute überwiegend durch elektronische Datenverarbeitungsprozesse und Datenspeichermedien.

Angriffsobjekte oder Tatmittel der Computerdelikte sind ebenfalls *Daten,* die im Zusammenhang mit den Computerstrafnormen als Informationen definiert werden, die in codierter Form von einer Datenverarbeitungsanlage verarbeitet, gespeichert oder übermittelt werden können. Dazu werden nach neuerer Lehre auch Ton- und Tonbilddaten sowie die Programme gezählt.[339] Digitalisierte Werkdaten sind folglich immer auch Computerdaten im Sinne der Art. 143 ff. StGB. Es entsteht damit eine Überschneidung zwischen den Tatbeständen des Urheber- und des Computerstrafrechts.

Herausgegriffen wird hier vor allem die Frage, wie sich das Verhältnis zwischen Art. 69a Abs. 1 lit. a i.V.m. Art. 39a Abs. 1 und Abs. 4 URG einerseits und den Computerdelikten des StGB andererseits bei der Umgehung von technischen Schutzmassnahmen präsentiert. Der Umgehungsschutz wird durch zwei grundsätzlich verschiedene Mechanismen gewährleistet:[340] Einerseits kann schon der Zugriff auf die urheberrechtlich geschützten Daten technisch kontrolliert werden *(Zugangskontrolle)*; anderseits kann die Verwendung einer bereits im Verfügungsbereich des Nutzers befindlichen Werkdatei technisch eingeschränkt oder verhindert werden *(Nutzungskontrolle)*.[341]

Je nach Geschäftsmodell kommt der eine oder andere Mechanismus zum Einsatz, wobei auch eine Kombination aus Zugriffskontrolle auf die Daten mit einem in der Datei eingebauten Nutzungsbeschränkungsmechanismus möglich ist. Als Beispiel einer Kombination aus Zugangs- und Nutzungskontrolle lassen sich die Musikdateien des iTunes Store von Apple aufführen. Dieses Musik- und Multimediaportal ermöglicht eingetragenen Nutzern oder Prepaid-Karteninhabern unter anderem den kostenpflichtigen Download von Musikdateien aus einem umfangreichen digitalen Katalog (Datenbank). Der Zugriff auf die vollständigen Werkdaten ist durch eine Benutzer-ID und ein Passwort geschützt. Die Musikdateien selbst sind mit einer programmtechnischen Nutzungskontrolle versehen, die ein Wahrnehmbarmachen nur mit einem proprietären Player und ausserdem nur auf 5 Computern zulässt.

---

339 Weiterführend zum Datenbegriff SCHWARZENEGGER (Fn. 72), S. 313 ff. m.w.N.
340 Gemäss Legaldefinition in Art. 39a Abs. 2 URG, siehe auch oben C.II.4. S. 444.
341 Siehe auch GLARNER (Fn. 230), S. 648.

Tabelle 5: Vergleich zwischen dem urheberstrafrechtlichen Umgehungsschutz (Art. 69a Abs. 1 lit. a URG) und den wichtigsten Computer- und Vermögensstrafnormen (Art. 143, 143bis, 150, 150bis StGB)

	Art. 69a Abs. 1 lit. a URG	**Art. 143 Abs. 1 StGB**	**Art. 143bis StGB**	**Art. 150 StGB**	**Art. 150bis StGB**
geschütztes Rechtsgut	unbeeinträchtigte Verfügung über Werkdaten	unbeeinträchtigte Verfügung über Daten	unbeeinträchtigte Verfügung über Datenverarbeitungsanlage («Computerfrieden»)	Vermögen des Leistungsanbieters	Vermögen des Rundfunkprogramm- oder Fernmeldedienstanbieters (indirekt)
Deliktstypus	konkretes Gefährdungsdelikt, Erfolgsdelikt	Verletzungsdelikt, Erfolgsdelikt	Verletzungsdelikt, Erfolgsdelikt	Verletzungsdelikt, Erfolgsdelikt	abstraktes Gefährdungsdelikt, schlichtes Tätigkeitsdelikt
Angriffsobjekt	technische Schutzmassnahme	Daten	Datenverarbeitungsanlage	Dienstleistung (die eine Vermögensposition des Verletzten darstellt)	noch nicht konkretisierte *codierte* Rundfunkprogramme oder *codierte* Fernmeldedienste
Tatmittel	beliebig	Umgehung einer besonderen Sicherung	Umgehung einer besonderen Sicherung, auf dem Wege von Datenübertragungseinrichtungen	durch Täuschung, List, unlauteres Verhalten	Geräte zur Entschlüsselung
Tathandlung	Umgehen	Beschaffen	Eindringen	unentgeltliche Inanspruchnahme der Dienstleistung	Herstellen, Einführen, Ausführen, Durchführen, In-Verkehr-Bringen, Installieren
Erfolg	Überwindung der Schutzmassnahme	Verfügungsgewalt über die Daten	«Präsenz» im geschützten Bereich der Datenverarbeitungsanlage	Vermögensschaden	nicht erforderlich
subjektiver Tatbestand	Eventualvorsatz, Absicht einer unrechtmässigen Werk- oder Schutzobjektsverwendung	Eventualvorsatz, Bereicherungsabsicht	Eventualvorsatz, *keine* Bereicherungsabsicht	Eventualvorsatz, aber direkter Vorsatz betreffend Entgeltlichkeit der Leistung	Eventualvorsatz
Antragserfordernis	ja	nein	ja	ja	ja
Strafrahmen	Übertretung, Busse	Verbrechen, bis zu 5 Jahre Freiheitsstrafe oder Geldstrafe	Vergehen, bis zu 3 Jahre Freiheitsstrafe oder Geldstrafe	Vergehen, bis zu 3 Jahre Freiheitsstrafe oder Geldstrafe	Übertretung, Busse

a. Umgehung einer Zugangskontrolle

Anhand eines konkreten Beispiels einer Umgehung der Zugangkontrolle sollen das Verhältnis zwischen urheberstrafrechtlicher Regelung und den Strafnormen des Computerstrafrechts aufgezeigt werden.

> Beispiel: Urheberrechtlich geschützte Textdateien werden auf einer Web-Datenbank – wie z.B. swisslex.ch – zum Abruf über das Internet bereitgehalten. Um auf die Datenbank zugreifen zu können, muss der Nutzer eine Zugangskontrolle mit Benutzer-ID und Passwort passieren. Die Textdateien selbst werden technisch nicht in der Nutzung beschränkt. Das heisst, nach dem erfolgreichen Zugriff können sie beliebig kopiert und sonstwie genutzt werden. Einer Person gelingt es, durch ein nicht näher zu spezifizierendes Vorgehen die genannte Zugangskontrolle zu umgehen. Der Zugriff erfolgt in der Absicht, allenfalls interessierende Textdateien zum Eigengebrauch herunterzuladen.

Wie ist in einer solchen Konstellation die Umgehung der Zugangskontrolle aus strafrechtlicher Sicht zu würdigen?

aa. Urheberstrafrechtliche Aspekte

Die urheberstrafrechtliche Betrachtung beginnt mit der Bestimmung des Rechtsgutsträgers. Falls der Urheber dem Verlag eine Lizenz zur Online-Verbreitung seiner Texte eingeräumt hat, darf letzterer Textdateien erstellen und diese in der Online-Datenbank zum Abruf durch zahlende Nutzer bereitstellen. Der Schutz der Nutzungsrechte vor Umgehungshandlungen steht grundsätzlich dem Urheber zu. Der Verlag als Betreiber der Datenbank lässt sich aber von diesem in der Regel einzelne oder alle Nutzungsrechte am Text übertragen. Dabei handelt es sich üblicherweise um eine gegenständlich wirkende Lizenzierung, die auch Abwehrrechte gegenüber Dritten gewährleistet.[342] Im Beispielfall ist deshalb davon auszugehen, dass der Verlag die urheberrechtlichen Abwehrrechte geltendmachen kann. Bei einer ausschliesslichen Lizenz wäre auch von einer Antragsberechtigung des Verlags nach Art. 69a Abs. 1 URG i.V.m. Art. 30 Abs. 1 StGB auszugehen.

Da aber der Eigengebrauch auch hinsichtlich der Umgehungsstrafnorm tatbestandsausschliessende Wirkung hat (Art. 19 Abs. 1, Art. 39a Abs. 4 URG), sind die Nutzungsrechte des Verlags *urheberstrafrechtlich nicht* durch Art. 69a Abs. 1 lit. a URG *geschützt.* Ebenso entfällt eine Strafbarkeit gemäss Art. 67 Abs. 1 lit. e URG wegen einer rechtmässigen Handlung innerhalb der Schutzschranke, falls der Täter nach der Umgehung der Zugangskontrolle tatsächlich Textdateien aus der Datenbank abruft. Zu beachten ist dabei, dass das bewusste Auswählen einer Textdatei zur Einsichtnahme auf dem eigenen Rechner immer

342 Möglich ist allerdings auch eine nur schuldrechtlich wirkende Lizenz, wobei hier die Abwehrrechte gegenüber Dritten fehlen, vgl. weiterführend REHBINDER (Fn. 221), N 155 ff. m.N.

einen Datentransfer über das Web voraussetzt. Dabei löst der Täter einen digitalen Kopiervorgang aus, der je nach Konfiguration des Browsers zu einer identischen Kopie der Datei im Cache-Speicher oder direkt auf der Festplatte des Computers führt.[343] Damit ist aber schon eine digitale Kopie der Werkdaten hergestellt, die von Art. 67 Abs. 1 lit. e URG erfasst wird. Diese Datenübertragungs- und -kopierprozesse schliessen es im Übrigen aus, Angebote von kostenpflichtigen Web-Datenbanken oder Content-Plattformen der geschilderten Art[344] als Dienstleistungen i.S.v. Art. 150 StGB anzusehen.[345]

bb. Computerstrafrechtliche Aspekte

Das Verfügungsrecht über die auf einem Webserver abrufbare Datenbank und die darin abgespeicherten Textdateien liegt in computerstrafrechtlicher Hinsicht ebenfalls beim Verlag bzw. seinen Organen.[346] Bezüglich der Umgehung der Zugangskontrolle kommt eine *Strafbarkeit nach der «Hacking»-Strafnorm* (Art. 143bis StGB) in Frage. Mit diesem Straftatbestand soll das Rechtsgut der unbeeinträchtigten Verfügungsmacht und Kontrolle der natürlichen oder juristischen Personen über ihre Computersysteme geschützt werden, ohne dass damit deren Vermögen angegriffen werden müsste.[347] Zu Recht hält daher Trechsel die Einordnung bei den Vermögensdelikten für ungerechtfertigt. Das Delikt sei eher vergleichbar mit einer Verletzung des Schriftgeheimnisses (Art. 179 StGB) und schütze die «Privatsphäre des gegen Zutritt von Unbekannten geschützten Datenverarbeitungssystems».[348] Die Tathandlung besteht in einem unbefugten Zugriff auf ein besonders gesichertes Computersystem, d.h. der Täter gelangt via öffentliche Telekommunikationsnetze in ein lokales Netzwerk. Dabei genügt es, wenn der Zugriff auf einen Teil des Systems erfolgt, z.B. auf die Ebene des Betriebssystems, auf Dateiverzeichnisse oder angeschlossene externe Speichermedien. Nicht notwendig ist dagegen, dass der Täter weitere Programmfunktionen in Gang setzt oder dass er Daten einsehen, verändern oder kopieren

343 Dabei handelt sich nicht um eine vorübergehende Vervielfältigung i.S.v. Art. 24a URG, weil sie nicht «begleitend» und blosse Übertragung zwischen Dritten ist. Diese Bestimmung will bloss die vorübergehende Vervielfältigung auf den Übertragungswegen des Internet (Router, Cache-Server) vom Schutzbereich ausnehmen.

344 Bsp.: www.zeitschriften.recht.ch, Beck-Online-Datenbank, www.ciando eBooks, iTunes Store u.a.

345 Anders Glarner (Fn. 230), S. 649. Zu den Schwierigkeiten, Plattformen mit gemischten Angeboten und vertikaler Integration (Carrier, Content, Service) überhaupt rechtlich einzuordnen, siehe aktuell Paul Leo Giani, «Plattformen» – Rundfunkveranstalter oder «nur» Dienstleister? Medialex 2007, S. 168–170.

346 Glarner (Fn. 230), S. 649, meint allgemein, es würde mit Zugriffskontrollsystemen primär die Leistung des Datenbankbetreibers bzw. das Vermögen der Online-Anbieter geschützt.

347 Schwarzenegger (Fn. 72), S. 315 f.; Pfister (Fn. 26), S. 99 f. m.w.N.

348 Stefan Trechsel, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Aufl., Zürich 1997, Art. 143bis N 2.

kann.[349] Im Beispielfall ist der Täter nicht befugt, auf den geschützten Teil des Computersystems zuzugreifen. Indem er eindringt, erfüllt er den objektiven Tatbestand von Art. 143bis StGB. Subjektiv ist neben einem Eventualvorsatz das *Fehlen einer Bereicherungsabsicht* erforderlich. Die missglückte Fassung der Hacking-Strafnorm hat zur Folge, dass ein technisch interessierter Täter, welcher aus reiner Neugierde in ein System eindringt, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft werden kann, während ein mit Bereicherungsabsicht Eindringender nur sanktioniert wird, wenn er einen anderen Straftatbestand erfüllt.[350] Wer – wie im Beispiel – in ein Computersystem eindringt, um sich eine urheberrechtlich geschützte Textdatei zu beschaffen, handelt in Bereicherungsabsicht und erfüllt somit den subjektiven Tatbestand von Art. 143bis StGB nicht![351]

In Frage kommt noch eine Strafbarkeit wegen *versuchter unbefugter Datenbeschaffung* (Art. 143 Abs. 1 StGB).[352] Die Strafnorm der unbefugten Datenbeschaffung schützt das Rechtsgut des freien oder ungestörten *Verfügungsmacht über Daten* i.S. der weiter oben aufgeführten Definition.[353]

Ungleich des Eigentums an Sachen (Art. 641 ZGB) existiert im Zivilrecht keine lückenlose Regelung der «Berechtigung an immateriellen Daten». Informationen in der Form von personenbezogenen Daten (Datenschutzrecht), Geheimnissen (Persönlichkeitsrecht, Firmenrecht, Bankenrecht) oder Werken, Marken usw. (Immaterialgüterrecht) werden partikulär geschützt. Soweit Daten nicht in diese Kategorien fallen, besteht an ihnen zwar ein ungeschriebenes persönliches Recht. Dieses ist aber mangels Schutzrechtscharakters gegenüber Dritten nicht durchsetzbar.[354]

---

349 Solche Handlungen werden von anderen Tatbeständen erfasst (Art. 143, Art. 144bis StGB, Art. 67 Abs. 1 lit. e, Art. 69 Abs. 1 lit. f URG), vgl. weiterführend Pfister (Fn. 26), S. 115 ff. mit zahlreichen Nachweisen.

350 Zu denken ist an einen Versuch der unbefugten Datenbeschaffung (Art. 143 i.V.m. Art. 22 StGB) oder den Versuch eines urheberstrafrechtlichen Delikts (Art. 67, Art. 69 URG i.V.m. Art. 22 StGB).

351 Ähnlich Glarner (Fn. 151), S. 175; a.M. aber Glarner (Fn. 230), S. 649. Daher sieht Pfister (Fn. 26), S. 139, keine Konkurrenzkonstellationen zwischen Art. 143bis StGB und den Straftatbeständen des URG.

352 Eine Strafbarkeit nach Art. 147 Abs. 1 StGB fällt ausser Betracht, weil mit der Überwindung der Zugangskontrolle durch eine unrichtige, unvollständige oder unbefugte Verwendung von Daten nicht direkt der Datentransfer (= Vermögensverschiebung) herbeigeführt wird. Der Täter muss noch weitere Programmschritte veranlassen, die selbst nicht mehr als missbräuchliche Verwendung von Daten erscheinen.

353 Schwarzenegger (Fn. 72), S. 320; Günter Stratenwerth und Guido Jenny, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 6. Aufl., Bern 2003, § 14 N 22; Stratenwerth und Wohlers (Fn. 327), Art. 143 N 1; Philippe Weissenberger, in: Marcel Alexander Niggli und Hans Wiprächtiger (Hrsg.), Basler Kommentar, Strafrecht II, Art. 111–392, 2. Aufl., Basel 2007, Art. 143 N 4.

354 Schwarzenegger (Fn. 72), S. 320, Fn. 70. Ähnlich aus zivilrechtlicher Sicht Urs Hess-Odoni, Die Herrschaftsrechte an Daten, Jusletter, 17.5.2004, Rz. 16 ff.

Bezüglich des Versuchs einer unbefugten Datenbeschaffung hat der Täter im Beispielsfall einen Vorsatz auf Verwirklichung aller objektiven Tatbestandsmerkmale. Es handelt sich um codierte Daten, die nicht für den Täter bestimmt sind, weil er weder nach Zivil- noch nach öffentlichem Recht darüber verfügen darf.[355] Der Täter will sie sich unter Umgehung einer besonderen Sicherung gegen den unbefugten Zugriff beschaffen.[356] Allerdings wird zum Teil behauptet, Daten, die für jedermann zugänglich seien, seien «für den Täter bestimmt».[357] Es finde daher keine «unbefugte» Datenbeschaffung statt, wenn jemand auf diese Daten zugreife, ohne die Nutzungsbedingungen einzuhalten (z.B. finanzielle Entschädigung). Dies sei vielmehr eine Erschleichung einer Leistung.[358] Diese Auffassungen sind abzulehnen,[359] weil sie verkennen, dass bei diesen Handlungen keine Dienstleistungen erbracht, sondern Daten unbefugt übertragen werden, über die der Täter in der Folge frei verfügen kann. Der Täter überschreitet mit dem Überwinden der Zugangssicherung auch die Schwelle zum Versuch. In subjektiver Hinsicht ist neben dem Eventualvorsatz ausserdem eine Absicht an einer unrechtmässigen Bereichung erforderlich. Diese ist gegeben, wenn die Daten einen vermögensrelevanten Gebrauchswert haben[360] und der Täter auf das Kopieren der Textdateien keinen Anspruch hat. Beides ist im Beispielfall zu bejahen.

Dagegen ist im Beispielsfall eine Subsumtion unter die Leistungserschleichung (Art. 150 StGB) entgegen weit verbreiteter Meinung[361] nicht vertretbar, weil die *Erlangungen eines immateriellen Gutes* (Werkdatei) einer *Sachleistung, nicht* etwa einer *Dienstleistung* gleichkommt. Es werden aber nur Dienstleistungen von Art. 150 StGB erfasst,[362] weil sich andernfalls die Schutzbereiche der Art. 143 ff. und des Art. 150 StGB überschneiden würden.

Offensichtlich bestehen hier Missverständnisse bezüglich der Abgrenzung zwischen immateriellen Sachleistungen und Dienstleistungen im Bereiche digi-

---

355 Andreas Donatsch, Strafrecht III, Delikte gegen den Einzelnen, 9. Aufl., Zürich 2008, S. 173 f.

356 Vgl. zusammenfassend Stratenwerth und Wohlers (Fn. 327), Art. 143 N 2 f.

357 Weissenberger (Fn. 353), Art. 143 N 15 m.w.N., hier gehe es um Urheberrechtsverletzungen, wettbewerbsrechtliche Verletzungen usw.

358 Stratenwerth und Jenny (Fn. 353), § 14 N 22 m.w.N.

359 Ablehnend auch Glarner (Fn. 151), S. 171, mit der Begründung, dass der Zweck einer Zugriffssicherung immer der Ausschluss Unberechtigter sei, gleichgültig, welche Erfordernisse erfüllt sein müssten, um eine Zugangsberechtigung zu erhalten.

360 Stratenwerth und Wohlers (Fn. 327), Art. Art. 143 N 4.

361 Stratenwerth und Jenny (Fn. 353), § 14 N 55 m.N.; ebenso Weissenberger (Fn. 353), Art. 150 N 23; Donatsch (Fn. 355), 238, beide trotz der Beschränkung des Angriffsobjekts auf Dienstleistungen. Glarner (Fn. 151), S. 178, erachtet die Generalklausel als anwendbar (Art. 150 Abs. 1 StGB). Korrekt dagegen Schmid (Fn. 333), § 9 N 25, 41 ff.; Trechsel (Fn. 341), Art. 150 N 3c «Inanspruchnahme der *Dienstleistungen* einer Datenverarbeitungsanlage» (meine Hervorhebung); Jörg Rehberg, Niklaus Schmid und Andreas Donatsch, Strafrecht III, Delikte gegen den Einzelnen, 8. Aufl., Zürich 2003, 219.

362 So Botschaft, BBl. 1991 II 1030 und die h.L. Trechsel (Fn. 348), Art. 150 N 2; Weissenberger (Fn. 353), Art. 150 N 4; Donatsch (Fn. 355), 237.

taler Datenverarbeitung. Zu den digitalen Sachleistungen zählen Software, Textdateien, digitale Bild-, Video- und Musikdateien. Beispiele für digitale Dienstleistungen sind Online-Beratungsdienste, die Rechenleistung eines Computers («Zeitdiebstahl»)[363] oder die Übertragungsleistung eines Netzwerkbetreibers.[364] Im Gegensatz zu letzteren befindet sich bei digitalen Sachleistungen am Schluss eine vollständige und dauerhafte Datei auf dem Speichermedium des Nutzers. Dienstleistungen sind dadurch charakterisiert, dass sie in der Regel nicht speicher- und übertragbar sind und dass ihre Erzeugung und Konsumtion zeitlich zusammenfallen. Zum Teil kann die digitale Sachleistung (digitale Textdatei) wie in unserem Beispiel nur zusammen mit einer digitalen Dienstleistung (Nutzung der Datenbank und Software) angeboten werden. Eine Leistungserschleichung könnte aber gleichwohl nur dann angenommen werden, wenn die Person in unserem Beispiel allein die Arbeitsleistung des Computers bzw. des Datenbankprogramms nutzen würde unter der zusätzlichen Voraussetzung, dass diese dem Publikum nur gegen Entgelt angeboten wird. Die Nutzung der Computerzeit und des Datenbankprogramms ist aber bei den meisten Anbietern kostenlos, während sich das zahlungspflichtige Angebot auf den Download der vollständigen Textdatei bezieht.[365]

cc. Wirkt die Schrankenregelung des Urheberrechts als Rechtfertigungsgrund im Computerstrafrecht?

Die *zentrale Frage* ist nun, ob die *Schrankenregelung des Urheberrechts*[366] als *Rechtfertigungsgrund* im Kontext des Versuchs der unbefugten Datenbeschaffung anzusehen sei[367] oder nicht. Gemäss Art. 14 StGB verhält sich rechtmässig, wer eine gesetzlich erlaubte Handlung ausführt, auch wenn die Tat nach dem StGB oder einem andern Gesetz mit Strafe bedroht ist. Und gerade eine solche gesetzlich erlaubte Handlung kann aus Art. 39a Abs. 4 i.V.m. Art. 19

363 Es ist völlig klar, dass die Ergänzung von Art. 150 StGB nur die reine Rechnerleistung («Benützen einer Datenverarbeitungsanlage» oder «unerlaubte Verwendung von Programmen») und nicht etwa eine unbefugten Datenbeschaffung umfassen sollte, denn hierzu wurde ja eigens ein neuer Tatbestand ins Gesetz eingeführt (Art. 143 StGB). Technisch ging der Gesetzgeber damals von einem Zentralrechner-Terminal-Modell aus, in welchem die Datenverarbeitungsleistungen des Zentralrechners selbst noch erhebliche Kosten verursachten, siehe Botschaft, BBl. 1991 II 984 und 1030 f.

364 Vgl. spezifisch hierzu Redmer Luxem, Digital commerce, Electronic commerce mit digitalen Produkten, 2. Aufl., Lohmar/Köln 2001, S. 20. Allgemein zur Abgrenzung von Sachleistung und Dienstleistung Jörg Rösner, Service – ein strategischer Erfolgsfaktor von Industrieunternehmen? Hamburg 1998, 14 ff.

365 Die Botschaft, BBl. 2006, 3425, erwähnt nur den Schutz durch Art. 150bis StGB, der durch die URG-Revision nicht tangiert werde. Glarner (Fn. 230), S. 649, sieht in der Nichterwähnung von Art. 150 StGB ein redaktionelles Versehen.

366 Insbesondere die Werknutzung zum Eigengebrauch, vgl. Art. 19 Abs. 1, Art. 39a Abs. 4 URG.

367 So Glarner (Fn. 151), S. 172, allerdings ohne Begründung.

Abs. 1 lit. a URG hergeleitet werden.[368] Es handelt sich bei den Regelungen des URG über die Werknutzung nota bene nicht nur um das speziellere, sondern im Fall des Art. 39a Abs. 4 URG auch um das jüngere Gesetz.

In der parlamentarischen Debatte wurden die Konsequenzen für die Computerdelikte nicht diskutiert, obschon ein Hinweis auf die Problematik erfolgte.[369] Sie wird von der Rechtsprechung durch Auslegung zu ermitteln sein, wobei massgebend sein wird, ob zwischen dem Versuch der unbefugten Datenbeschaffung und Verletzung des Umgehungsverbots sowie der vollendeten Datenbeschaffung und der Verletzung des Vervielfältigungsrechts jeweils ein Verhältnis von Spezialbestimmung zu Grundtatbestand besteht. Anders gesagt fragt sich, ob der Tatbestand der unbefugten Datenbeschaffung ein anderes Unrecht definiert als die urheberstrafrechtliche Norm. Verneint man dies, erscheint es unlogisch, die rechtfertigende Wirkung von Art. 39a Abs. 4 URG beim Computerdelikt abzulehnen. Die Lehre äussert sich im Rahmen der Konkurrenzen zu diesem Verhältnis: Zwischen Art. 143 StGB und den Art. 67 und 69 URG soll echten Konkurrenz bestehen, da unterschiedliche Rechtsgüter betroffen seien.[370] Bei genauer Betrachtungsweise geht es aber immer um die Verfügungsmacht über geschützte Daten bzw. Werkdaten. Art. 143 StGB erfasst sowohl die Gefährdung durch Umgehung einer Zugriffssicherung (in der Versuchsvariante), die von Art. 69a Abs. 1 lit. a URG kriminalisiert wird, als auch die Verletzungen des Verfügungsrechts, die im spezifischen Urheberrechtskontext durch die Art. 67 und 69 URG abgedeckt werden. Somit ist bei Identität des Verfügungsberechtigten von unechter Konkurrenz auszugehen.[371] Die Rechtmässigkeit der Umgehung zum Zwecke einer gesetzlich erlaubten Verwendung überträgt sich somit auch auf die unbefugte Datenbeschaffung. Dass dies bei der Formulierung von Art. 39a Abs. 4 URG wohl kaum die Intention war, liegt auf der Hand.[372] Das

368 Die Botschaft, BBl. 2006, 3425, bleibt in diesem Punkt völlig unklar: «Sie [die Bestimmung des Art. 39a Abs. 4 URG] lässt indessen den durch Artikel 150bis StGB gewährleisteten Schutz von Zugangskontrollen für den elektronischen Geschäftsverkehr unberührt.» Das bezieht sich ja nur auf den abstrakten Gefährdungstatbestand der Herstellung und des Inverkehrbringens von Materialien zur unbefugten Entschlüsselung codierter Angebote und kann auch so gelesen werden, dass der durch andere Strafnormen gewährleisteten Schutz (insbes. des Art. 143 Abs. 1 StGB) durch Art. 39a Abs. 4 URG gerade betroffen werde. Siehe auch Glarner (Fn. 230), S. 649 f.: «… wird dadurch zumindest die Möglichkeit eröffnet, dass ein solches im URG legiferiertes Recht auch bei der Anwendung der Straftatbestände von Art. 150, 150bis oder 143 StGB als gesetzlicher Rechtfertigungsgrund herangezogen werden könnte. Im Resultat besteht somit die Gefahr, dass Geschäftsmodelle wie iTunes den ihnen bisher zugestandenen strafrechtlichen Schutz verlieren, da sich der Täter auf sein Recht auf Privatgebrauch berufen kann.»

369 Votum J. Alexander Baumann, AB 2007 N 1351.

370 Stratenwerth und Jenny (Fn. 353), § 14 N 34; Weissenberger (Fn. 353), Art. 143 N 38 je m.N.

371 Gl.M. Niklaus Schmid (Fn. 333), § 4 N 131; Glarner (Fn. 151), S. 173.

372 So schon Glarner (Fn. 230), S. 650, der daher zu Recht empfahl, den Schutz technischer Massnahmen in Art. 39a resp. 69a URG auf Nutzungskontrollsysteme zu beschränken, während die Verletzung von Zugangskontrollen alleine durch die Art. 143 ff. StGB geahndet werden sollte.

Resultat ist aus der Sicht der Rechteinhaber auch stossend, muss aber als Konsequenz einer Gesetzgebung hingenommen werden, welche Reflexwirkungen im Strafrecht nicht wirklich beachten will.[373]

Der Rechtsschutz der Computerstrafnormen lässt sich *de lege ferenda* mit einer Beschränkung der rechtfertigenden Wirkung von Art. 39a Abs. 4 URG auf das Urheberrecht erzielen. Ein einfacher Vorbehalt zugunsten anderer Bundesgesetze löst das Problem:

Art. 39a Abs. 4 URG (Ergänzungsvorschlag)

[4] Das Umgehungsverbot dieses Gesetzes kann gegenüber denjenigen Personen nicht geltend gemacht werden, welche die Umgehung ausschliesslich zum Zweck einer gesetzlich erlaubten Verwendung vornehmen. *Vorbehalten bleiben die Verbote anderer Bundesgesetze.*

Damit wäre zwar Art. 69a URG weiterhin ein symbolischer Straftatbestand,[374] aber ein gleichzeitig erfüllter Verstoss gegen Art. 143 StGB und allenfalls andere Strafbestimmungen des Computerstrafrechts wäre dann sicherlich nicht mehr gerechtfertigt. Zu Beginn der nationalrätlichen Beratung der URG-Revision äusserte der damalige Bundesrat Christoph Blocher einen weiteren Grund für die Zurückhaltung im Strafrecht:

> «Wir haben auch darauf geschaut, dass das Gesetz durchsetzbar ist. Wenn Sie zu strenge Regeln für die Eigennutzung im häuslichen Bereich setzen, können Sie sie gar nicht durchsetzen, ausser man würde die Polizei in Privathaushalten abklären lassen, ob jemand zum Eigengebrauch etwas auf eine leere Kassette übernommen hat. Auch wenn es vielleicht richtig wäre, das zu verbieten: Es wäre nicht durchsetzbar.»[375]

Abgesehen davon, dass «leere Kassetten» im digitalen Umfeld nicht mehr zum Einsatz kommen, würde Blochers Standpunkt auch einen Verzicht auf das Computerstrafrecht nahelegen. Denn: Hacking, unbefugte Datenbeschaffung, Datenbeschädigung und Leistungserschleichungen werden ebenfalls zumeist im häuslichen Bereich ausgeführt.

b. Umgehung einer Nutzungskontrolle

Ausserdem stellt sich die Frage nach der Strafbarkeit der Umgehung der Nutzungskontrolle.

> Beispiel: Ein Film wird als Video-on-Demand-Datensatz angeboten. Ein Kopierschutzmechanismus ist in die Datei integriert, ebenso ein Verfallsmechanismus, der das Wahrnehmbarmachen des Films auf 48 Std. beschränkt. Der Nutzer kann die Film-

373 Neben den Hinweisen von GLARNER (Fn. 230), S. 649 f. lagen auch verwaltungsinterne Stellungnahmen von Seiten des Bundesamtes für Justiz vor, die auf die Sprengkraft des Regelungsansatzes aufmerksam machten.

374 Dieser Tatbestand würde nur dann Wirkung entfalten, wenn der Tatbestandsausschluss nach Art. 39a Abs. 4 URG abgeschafft würde.

375 Christoph Blocher, AB 2007 N 1201.

datei über ein elektronisches Netzwerk frei auf sein Speichermedium (DVD-Recorder; Computerfestplatte; anderes Speichermedium) herunterladen, was zur Erlangung einer dauerhaften Kopie der Filmdatei führt. Vorstellbar wäre auch, dass der Verfallmechanismus programmtechnisch die Selbstlöschung der Datei bewirken würde. Eine Person umgeht nun durch ein nicht näher zu spezifizierendes Vorgehen die genannten Nutzungskontrollen. Sie tut dies in der Absicht, eine dauerhafte Kopie der Filmdatei auf einem eigenen Speichermedium abzuspeichern. Diese Handlung wird zum Eigengebrauch ausgeführt.

Geht man wiederum davon aus, dass die Bestimmung des Art. 39a Abs. 4 URG sämtliche Tathandlungen von der Strafbarkeit nach Art. 69a Abs. 1 lit. a URG ausnimmt, die ausschliesslich für gesetzlich erlaubte Verwendungen vorgenommen werden, wäre die geschilderte Handlung *urheberstrafrechtlich nicht erfasst.* Wie weiter oben schon erwähnt wird der grösste Teil der potentiellen Umgehungshandlungen von Art. 69a Abs. 1 lit. a URG nicht erfasst. Dadurch besteht die Gefahr, dass die Anbieter die Schweiz bzw. Schweizer Konsumenten von Online-Geschäftsmodellen, welche auf dem Prinzip eines befristeten oder anderweitig eingeschränkten Werkzugangs für entsprechend tiefes Entgelt beruhen,[376] ausschliessen werden. Denn: Die hierfür erforderlichen Schutzmechanismen, meist am Download-File angebracht und auf dem eigenen Speichermedium oder Wiedergabegerät des Nutzers wirksam, könnten in der Schweiz sanktionslos umgangen, sämtliche derartige Geschäftsmodelle folglich unterlaufen werden.

Bezüglich der computerstrafrechtlichen Erfassung dieses Verhaltens liegt es noch näher als bei der Umgehung der Zugangskontrolle die Schrankenregeln des Urheberrechts[377] als Rechtfertigungsgrund im Kontext von Art. 143 Abs. 1 StGB oder anderer Strafbestimmungen anzusehen.[378] Die Auffassung, dass die Anfertigung einer Privatkopie[379] faktisch ein gesetzlich garantiertes Recht der Nutzer sei, führt zur paradoxen Rechtsüberzeugung, dass bei der Nutzung urheberrechtlicher Werke erlaubt sei, was im sonstigen elektronischen Geschäftsverkehr verboten ist.

Schliesslich ist im Zusammenhang mit dem Video-on-Demand-Datensatz mit 48-Stunden-Nutzungsfrist die Subsumtion unter Art. 150 StGB in der jetzigen Fassung nicht möglich,[380] weil auch bei dieser Nutzungsform durch einen rechtmässigen Download der Filmdatei eine dauerhafte Kopie auf dem eigenen Speicher- und Wiedergabegerät des Nutzers hergestellt wird. Das materielle Legalitätsprinzip (Art. 1 StGB) schliesst aus, dass aus einer rechtmässigen Erlan-

376 Also statt auf «virtuellem» Kauf auf «virtueller» Miete oder «virtuellem» Kinobesuch beruhen.

377 Insbesondere die Werknutzung zum Eigengebrauch, vgl. Art. 19 Abs. 1, Art. 39a Abs. 4 URG.

378 Glarner (Fn. 230), S. 649, geht davon aus, dass Nutzungen, sofern durch die Schutzschranke gedeckt, ungeahndet bleiben müssten.

379 Hierunter würde auch die Kopie zum Eigengebrauch fallen, die von einer nur zur temporären Nutzung überlassenen Werkdatei gezogen wird.

380 A.M. wohl Glarner (Fn. 230), S. 649, bezüglich des die «Zugriffssperre umgehenden Nutzers».

gung eines immateriellen Gutes per Analogie plötzlich die «Erschleichung einer Leistung» gemacht wird. Es handelt sich vielmehr um die Anmassung eines Verfügungsrechts über immaterielle Güter (urheberrechtliche Nutzungsbefugnis). Ausserdem wird der Anbieter häufig eine dauerhafte Kopie gar nicht anbieten wollen, auch nicht «gegen Entgelt».

D. Fazit

Die Untersuchung hat gezeigt, dass die Cyberkriminalität viele Dimensionen aufweist und sich aufgrund der vielfältigen Einsatzmöglichkeiten der IKT-Infrastruktur zu einem immer zentraleren gesellschaftliches Problem entwickelt. Die Grenzenlosigkeit des Cyberspace fordert die nationale Kriminalpolitik heraus, wirksame materielle und formelle Rahmenbedingungen für die internationale Strafverfolgung zu schaffen.

Der Überblick über die verschiedenen internationalen Initiativen zeigt, dass ein immer engmaschigeres System von konventionalrechtlichen Vorgaben herangewachsen ist, die einerseits zu einer Harmonisierung der wichtigsten Straftatbestände im Bereich der Cyberkriminalität führen, andererseits ein strafprozessuales Instrumentarium etablieren, dass die schnelle und international vernetzte Beweiserhebung und -sicherung gewährleistet.

Als Fallstudie wurde das Urheberstrafrecht herausgegriffen, in welchem sich die generellen Trends spiegeln. Verletzungen der Urheberrechte und verwandten Schutzrechte zählen zu den häufigsten Straftaten im digitalen Umfeld. Da diese Massendelikte mit zivilrechtlichen Klagen kaum unter Kontrolle zu bringen sind, wächst das Bedürfnis nach strafrechtlichen Lösungen:

> «The war on music-file sharing shows two contesting sides. On the one hand we see an industry that keeps suing in defense of its copyrights – already for several years now stooping to the level where its legal arrows are aimed at its own customers, finally even *invoking criminal law.* On the other hand, we see a ‹community› employ peer-to-peer communication services that become more and more intractable to authorities and that consequently *become attractive for criminal use.*»[381]

Völkerrechtlich wurde in diesem Bereich in relativ kurzer Zeit ein System etabliert, dass eine Kriminalisierung im Vorfeld der Verletzung von Urheberrechten und verwandten Schutzrechten favorisiert. Im Zentrum steht dabei die rechtliche Flankierung und Absicherung technischer Schutzmechanismen.

Betrachtet man die Umsetzung der internationalen Vorgaben im Rahmen der Revision des schweizerischen Urheberrechts, so muss man aus einer strafrechtlichen Froschperspektive festhalten, dass die Strafnormen des neuen URG er-

381 Aernout Schmidt, Understanding the war, in: Aernout Schmidt, Wilfred Dolfsma und Wim Keuvelaar (eds.), Fighting the war on file sharing, The Hague 2007, S. 135–212, S. 135 (meine Hervorhebungen).

hebliche Mängel aufweisen. Die Strafnormen für den Umgehungsschutz und zur Verhinderung von Vorbereitungshandlungen werden – falls die Analyse dieser Studie zutrifft – kaum von praktischer Relevanz sein. Die maximale Reichweite der Schrankenbestimmungen, insbesondere des rechtmässigen Eigengebrauchs, lassen die neuen Strafbestimmungen sogar weitgehend als symbolische Gesetzgebung erscheinen. Die Neuregelung enthält zudem mehrere dogmatische Fehlkonstruktionen, mit denen sich die Strafverfolgung und Rechtsprechung schwer tun werden. Ausserdem blieben die Vorgaben der Convention on Cybercrime völlig unbeachtet. Schliesslich hat der Schweizer Gesetzgeber bewusst eine Lösung gewählt, die dem europäischen und internationalen Schutzstandard in mehreren Punkten nicht entspricht. Mit den neuen Instrumenten wird es kaum gelingen, das angestrebte Ziel eines besseren direkten Schutzes der Urheber und Leistungsschutzberechtigten in der Schweiz zu erreichen.