Gutachten

Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen

Prof. Dr. Andreas Pfitzmann
(Technischer Teil)

Prof. Dr. Ulrich Sieber
(Strafrechtlicher Teil)

erstellt im
Auftrag von

d m m v
Deutscher Multimedia Verband

VPRT
Verband Privater
Rundfunk und
Telekommunikation e.V.

Verband Privater Rundfunk und
Telekommunikation e.V.
Stromstraße 1
10555 Berlin
Tel.: 030 39880-0

Deutscher Multimedia Verband e.V.

Kaistraße 4
40221 Düsseldorf
Tel.: 0221 600456-0

Vorwort:

Angesichts der weltweit wachsenden Verbreitung von Internetanschlüssen und der steigenden Verfügbarkeit von Technologien zur Vervielfältigung digitaler Inhalte sehen sich die Produzenten und Anbieter von Inhalten - gleichgültig ob es sich um Filme, Software, Datenbankinhalte, Videos, Musik o.ä. in digitaler Form handelt - heute in zunehmendem Maße mit dem Problem digitaler Piraterie konfrontiert.

Unter Nutzung automatisierter Datenverarbeitung werden Delikte geplant, vorbereitet und ausgeführt, die sich gegen jede Art von Netzinfrastrukturen richten und eine Bedrohung für die Informationstechnologie und die gewerbliche Nutzung digitaler Infrastrukturen darstellen.

Für die Inhalteanbieter stellt sich daher die Frage, wie sie die unauthorisierte Nutzung, Vervielfältigung und Verbreitung ihrer Inhalte verhindern können, wenn sie diese Inhalte im Internet anbieten oder eine legale Vervielfältigung stattfindet.

Derzeit werden sowohl im privaten und gesellschaftlichen als auch im politischen und gesetzgeberischen Bereich Möglichkeiten diskutiert, die Interessen von Nutzern und Rechteinhabern zu einem zufriedenstellenden Ausgleich zu bringen.

Die auftraggebenden Verbände möchten mit dem Gutachten diese wichtige Diskussion unterstützen, so dass im Zusammenwirken aller am Markt sowie in Politik und Gesetzgebung Beteiligten eine befriedigende Lösung gefunden werden kann, um digitale Inhalte künftig besser zu schützen.

Berlin/Düsseldorf, im September 2002

Dr. Marcus Englert
Vize-Präsident des VPRT

Alexander Felsenberg
Vize-Präsident des dmmv

Technischer Teil

Verfasser:

Prof. Dr. Andreas Pfitzmann, Technische Universität Dresden
(Projektverantwortung)

Dr.-Ing. Hannes Federrath, Freie Universität Berlin
(Projektkoordination)

Dipl.-Inform. Markus Kuhn, University of Cambridge, England

Kurzfassung

Inzwischen existiert eine Vielzahl von Techniken zum Schutz von Rechten an digitalen Inhalten. Diese sog. Digital-Rights-Management-Systeme (DRM-Systeme) sollen möglichst unabhängig von der Distributionsform (Datenträger, Rundfunkübertragung, Kommunikationsnetze etc.) und vom Typ (Multimedia-Inhalt, ausführbare Software, Publikation etc.) der zu schützenden Inhalte die Rechte der an der Produktion, Verteilung sowie dem Konsum digitaler Inhalte Beteiligten schützen helfen.

Die meisten verfügbaren Systeme bieten allerdings keinen oder nur sehr begrenzten Schutz gegen starke (clevere, intelligente) Angriffe. Inhalte, die über CD, DVD und das Internet verbreitet werden, sind heute technisch katastrophal schlecht vor Verfälschung und unberechtigter Vervielfältigung geschützt. Dies gilt auch für urheberrechtlich geschützte Inhalte. Die bekannten technischen Schutzmaßnahmen helfen bestenfalls gegen Gelegenheitstäter und auch das nur solange, bis (möglicherweise, aber nicht notwendigerweise illegale) automatisierte Verfahren zur illegalen Nutzung veröffentlicht werden.

Um die durch gesetzliche Vorschriften allein schwierig kontrollierbare unrechtmäßige Nutzung geistiger Werke einzudämmen, wurden eine Reihe von technischen Maßnahmen entwickelt. Man kann die Maßnahmen danach unterscheiden, ob sie bereits die illegale Nutzungsmöglichkeit verhindern sollen oder nur die illegale Nutzung. Ein Beispiel für ersteres wäre, bereits die Erstellung illegaler Kopien zu verhindern, ein Beispiel für letzteres, nur die Verwendung illegaler Kopien zu erschweren.

Bei den technischen Komponenten von DRM-Systemen handelt es sich im Wesentlichen um auf die speziellen Gegebenheiten von Multimedia-Daten-Kommunikation zugeschnittene IT-Sicherheitssysteme. Das bedeutet, die Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit und Verfügbarkeit – in konkreten Ausprägungen z.B. Nicht-Konsumierbarkeit nicht bezahlter Inhalte, Unverfälschbarkeit urheberrechtlich geschützter Werke, Verhindern von Piraterie/Anfertigen illegaler Kopien – werden durch kryptographische, organisatorische und spezielle Sicherheitsmechanismen unter einem bestimmten Angreifermodell realisiert.

Insbesondere Verfahren, die das Kopieren von Inhalten verhindern sollen, sind deutlich unsicherer gegenüber Verfahren, die auf die Einschränkung illegaler Nutzungsmöglichkeiten zielen und damit robuster gegen Angriffe. Da digitale Daten verlustfrei vervielfältigt werden können, wird meist versucht, das Speicher- bzw. Übertragungsmedium schwer kopierbar zu machen oder – nachdem die Daten gelesen wurden – diese niemals vor der Ausgabe (Bildschirm, Lautsprecher etc.) in hoher Qualität (digital) abgreifbar zu machen bzw. noch innerhalb des speziell geschützten Bereiches, der meist in Hardware realisiert ist, in eine nur mit Verlusten kopierbare Repräsentation (z.B. analoges Signal) zu bringen.

Einige Verfahren sind ausschließlich in Software realisiert und bieten – da die Ausführung der Software nicht vor der ausführenden Maschine geschützt werden kann – nur sehr rudimentären,

begrenzten Schutz. Alle Software-Maßnahmen schützen die Anbieter von Inhalten selbst kurzfristig nahezu nicht vor Piraterie. Sogar technisch ungebildete Laien können zu Piraten werden, sofern sie sich der im Internet oftmals kostenlos angebotenen Software-Werkzeuge bedienen, die nahezu als Abfallprodukt der notwendigen Erforschung von Sicherheitsmechanismen entstehen oder von technisch gebildeten Interessierten aus diesen Ergebnissen leicht zusammengestellt werden können.

Mechanismen in Hardware gewährleisten einen besseren Schutz, verhindern Piraterie aber keinesfalls perfekt: Alle Hardware-Maßnahmen sind zumindest mittelfristig und bei Massenanwendungen in ihrer Sicherheit gefährdet, da oftmals überraschend einfache Möglichkeiten gefunden werden, die Sicherheit zu unterlaufen und bisher keine langfristig erprobten, für den Massenmarkt geeigneten Techniken zur Verfügung stehen. Zudem stellt sich die Frage, was Konsumenten motivieren sollte, diese Hardware zu erwerben oder auch nur zu nutzen.

Trotz ihrer weit gehenden Unwirksamkeit für den intendierten Zweck neigen Maßnahmen zum Schutz von Inhalten dazu, den Konsumenten durch den Anbieter bzgl. der Nutzung überwachbar zu machen. Neben der Frage der Zulässigkeit wirft dies verschärft die Frage der Akzeptanz dieser Maßnahmen durch datenschutzbewusste Konsumenten auf.

Inhaltsverzeichnis

1 Einführung

Für Menschen, die ihren Lebensunterhalt über Lizenzgebühren bestreiten, dürften die Digitalisierung und das Internet ein Segen und ein Fluch zugleich sein. Die Distributionsmöglichkeiten sind global und billig; die Digitalisierung ermöglicht den verlustfreien Transport zum Konsumenten, aber auch die sehr einfache Herstellung und illegale Verbreitung exakt gleicher Kopien, das bedeutet Kopien ohne Qualitätsverlust. Deshalb stellt sich die Frage, ob und wie Piraten daran gehindert werden können, illegale Kopien zu verbreiten. In dieser Studie werden die technischen Zusammenhänge und Möglichkeiten hierfür untersucht und bewertet.

Für eine Bewertung in Frage kommende Kriterien, teilweise nichttechnischer Natur, sind der Aufwand (speziell die Kosten und die Akzeptanz beim Konsumenten) und die Stärke (speziell gegen welche Stärke eines Angreifers/Piraten ein Schutzsystem noch hilft). Weitere Kriterien sind die Überwachbarkeit der Konsumenten sowie die Frage, wie technische Vorkehrungen das ungehinderte, legale Verbreiten von Kulturgütern beeinflussen.

Die Produkte von Autoren (auch Komponisten, Musikern, Filmproduzenten und Softwareentwicklern) zeichnen sich im Vergleich zu anderen Wirtschaftsgütern durch besonders niedrige Marginalkosten aus. Der Preis des Endproduktes besteht in erster Linie aus dem Autorenhonorar, Aufwendungen für Marketing, der Gewinnspanne für das Vertriebsnetz, sowie einer Risikoabsicherung für den ausstehenden Erfolg des Produktes. Die reinen Herstellungs- und Vertriebskosten einer einzelnen Kopie solcher geistiger Werke fallen in einer Endpreiskalkulation nur unwesentlich ins Gewicht. Ohne einen speziellen Schutz gegen die Nachahmung geistiger Produkte durch Konkurrenten wäre deren Produktion daher kaum mit der Aussicht auf attraktiven nachhaltigen finanziellen Gewinn verbunden. Das Ergebnis wäre ein Kulturangebot, welches in erster Linie von nicht-professionellen Autoren geschaffen wird, deren Erwerbstätigkeit nicht im Wesentlichen in der Schaffung geistiger Werke besteht.

Es besteht daher seit langem in der kulturinteressierten Bevölkerung Europas ein breiter Konsens, dass die rechtliche Einschränkung der Vervielfältigung im Interesse der Aufrechterhaltung eines reichhaltigen professionell produzierten kulturellen Angebotes wünschenswert ist. Daraus haben sich im Laufe der letzten beiden Jahrhunderte die einschlägigen nationalen Urheberrechtsgesetzgebungen und entsprechendes internationales Recht entwickelt.

Der bislang bestehende Schutz gegen die nichtautorisierte Nutzung und Vervielfältigung geistiger Werke nutzt in erster Linie den Umstand, dass zur qualitativ hochwertigen Vervielfältigung und Verteilung erhebliche Produktionsmittel (Druckereipressen, Schallplatten- oder CD-Pressen, Filmkopieranlagen, Lastwagen, Läden, etc.) notwendig sind, deren Betreiber vergleichsweise einfach auf die Einhaltung der Urheberrechtsgesetze hin kontrolliert werden konnten. Jede neue technische Entwicklung zur Vervielfältigung und mehrfachen Nutzung von Informationen und damit möglicherweise auch geistigen Werken wurde von der kulturschaffenden Industrie in der Vergangenheit stets mit Sorge verfolgt, so etwa öffentliche Bibliotheken, Radios, Fernseher, Tonbandgeräte, Bürokopierer, Magnetbandkassetten, Videorecorder, Datenfernübertragung, etc. Die Kulturindustrie reagierte auf diese Entwicklungen in erster Linie mit der

kontinuierlichen Einführung von Medien höherer Qualität (70-mm-Film mit Dolby-Surround Sound statt Videorecorder und Fernseher, CD statt Magnetbandkassette und FM-Radio), um sich für die Kunden in der Produktattraktivität deutlich von den immer weniger kontrollierbaren für Privatpersonen weitverfügbaren Vervielfältigungsmedien zu unterscheiden.

Da diese Qualitätsunterschiede immer geringer werden, steigt gleichzeitig auch die Attraktivität illegaler Kopien. Die Digitalisierung in Verbindung mit der weiten Verbeitung des Internet führte somit zu einer derartigen Verschärfung der Situation, dass sich Technologieunternehmen verstärkt mit der Entwicklung spezieller Sicherheitstechnologie zum Schutz digitaler Inhalte beschäftigten. Diese Technik soll dann die Rechte an digitalen Inhalten verwalten helfen. Neuerdings werden solche Systeme auch Digital-Rights-Management-Systeme (DRM-Systeme) genannt.

1.1 Digital Rights Management (DRM)

Die folgende Begriffsbestimmung für DRM-Systeme ist an [4, S.2ff] angelehnt:

DRM-Systeme sind elektronische Vertriebssysteme für digitale Inhalte. Sie ermöglichen die sichere Verbreitung digitaler Inhalte – unter anderem urheberrechtlich geschützte Musik-, Film- oder Sprachwerke – im Online- und Offline-Bereich, z.B. über das Internet, Datenträger (CompactDisc, MiniDisc etc.), mobile Abspielgeräte oder Mobiltelefone.

DRM-Systeme ermöglichen den Rechteinhabern einen sicheren Vertrieb zu berechtigten Nutzern, eine effektive und differenzierte Rechteverwaltung, weitgehende Kontrolle über die Verbreitung und Nutzung digitaler Inhalte und eröffnen so neue Nutzungsarten und Geschäftsmodelle (z.B. kostenpflichtiger Download, Abbonement von Inhalten, Pay-per-view/listen, file sharing).

In ihrer unflexibelsten Form verhindern DRM-Systeme, dass der Nutzer einen digitalen Inhalt kopieren kann. In ihrer flexibelsten Form erlauben DRM-Systeme die individuelle Abrechnung und Nutzung digitaler Inhalte ähnlich den Telefongebühren.

In DRM-Systeme werden auch Hoffnungen bezüglich der Reformierbarkeit des im Jahre 1965 eingeführten Pauschalabgabesystems für Datenträger und Kopiervorrichtungen gesetzt. Wenn Werke mittes DRM-Systemen geschützt werden können (Kopierschutz) und deren Nutzung individuell vergütet werden kann, seien die alten Pauschalabgabesysteme überflüssig geworden, argumentieren die Technologie-Provider, beispielsweise die Hersteller von CD-Brennern und die Anbieter von DRM-Verfahren.

Die alten Vergütungsmodelle haben ihren Ursprung in der damaligen Erkenntnis des Gesetzgebers, dass mit der Verbreitung privater Vervielfältigungstechniken (damals Tonbandgeräte und Kassettenrecorder) dem Endverbraucher die Nutzung geschützter Inhalte vornehmlich durch Rundfunkmitschnitte ermöglicht wird, die weder verhindert noch kontrolliert werden kann. Kopien waren aufgrund der Analogtechnik stets von minderer Qualität (verglichen mit dem Original). Mit der Digitalisierung und der breiten, kostengünstigen Verfügbarkeit digitaler Kopiertechnik (insbesondere CD-Brenner in PCs) erreicht eine Kopie jedoch exakt die Qualität des Originals. Hinzu kommt noch, dass mit Scannern, Farbdruckern und Spezialpapier heute sogar die CD-Booklets hochqualitativ reproduziert werden können.

Obwohl inzwischen auch DRM-Systeme verfügbar sind, die die gesamte Vertriebskette digitaler Inhalte abdecken, haben sie sich bisher noch nicht breit durchsetzen können. So fehlt es noch an passenden Geschäftsmodellen für die modernen Distributionsformen über das Internet. Dabei bietet gerade der Vertrieb über das Internet realistische Chancen für die schnellere, kostengünstigere und kundenorientiertere Verbreitung von Inhalten. Zumindest dürfte es an mangelnder technischer Kompetenz der Internetnutzer nicht scheitern: Wer es mit einer gehörigen Portion Enthusiasmus und Geduld schafft, über Peer-to-Peer-Filesharing-Systeme (siehe Abschnitt 3.6.2) kostenlos Musik herunterzuladen, wird auch keine Mühe haben, ein ansprechend gestaltetes, effizientes und gut bedienbares Bezahlsystem für digitale Inhalte zu nutzen. Ausserdem haben die Systeme zum kostenlosen File-Sharing ein hohes Image bei den Benutzern. Dieses Potential an Kundeninteresse und Kundenbindung ließe sich sicher auch bei einem Wechsel in die Legalität und Kommerzialisierung erhalten.

Die DRM-Techniken sind meist proprietär und noch nicht breit etabliert, und die Rechteinhaber (Künstler, Medienkonzerne) scheuen sich noch davor, eine bestimmte Technik zu lizenzieren. Aufgrund schlechter Erfahrungen im Bereich Datenträger- und Medienformate (beispielsweise existierten in der Anfangszeit der Heim-Videotechnik wenigstens drei Formate, von denen sich VHS im Heimbereich durchgesetzt hat) ist dieses Abwarten auch verständlich.

1.2 Ausgangslage aus technischer Sicht

Die folgenden Abschnitte analysieren die Ausgangslage und die daraus resultierenden Konsequenzen für die Entwicklung technischer Mechanismen zum Schutz digitaler Inhalte und zeigen technische Trends auf.

1.2.1 Technische Entwicklungen

In den vergangenen zehn Jahren erfolgten erneut eine ganze Reihe sich gegenseitig ergänzender enormer technischer Entwicklungen, die neue Vervielfältigungsmöglichkeiten geistiger Werke bieten und von der Kulturindustrie mit großer Sorge beobachtet werden:

- Frei programmierbare Universalcomputer (PCs) sind ein erschwingliches und populäres Haushaltsgerät geworden. Das anhaltend exponentielle Wachstum der Speicher- und Rechenleistung und die modulare Erweiterbarkeit erlaubt es, auf diesen Geräten heute Funktionen einfachst in Software zu realisieren, für die wenige Jahre zuvor noch sehr teuere spezielle Industrieausrüstung notwendig war.
- Die Digitalisierung des Telefonnetzes sowie die Entwicklung hochleistungsfähiger Glasfaser- und Kupferübertragungstechniken schaffte die Grundlage für den kostengünstigen und einfachen Zugang der gesamten Bevölkerung zu einer universell nutzbaren weltweiten digitalen Datenübertragungs- und Datenarchivierungs-Infrastruktur, dem Internet.
- Forschungsergebnisse in den Bereichen digitale Signalverarbeitung, Informationstheorie und Sinnesphysiologie ermöglichten die Entwicklung hocheffizienter Kodierverfahren für Bild- und Tonsignale (z.B. ISO MPEG), welche die Übertragung und Speicherung derartiger Daten zehn bis hundertfach effizienter gestalten als herkömmliche Distributionsformate.

- Die Unterhaltungselektronik- und Computerindustrie amortisierte die enormen Entwicklungs- und Investitionskosten für neue Speicher- und Übertragungstechnologien (CD, DVD, Firewire) durch Einsatz der gleichen Formate sowohl für den Vertrieb von geistigen Produkten als auch als Universalmedien für den Computergebrauch.

- Die dezentrale, oft nicht-kommerzielle, schnell-lebige und internationale Natur vieler über das Internet erreichbarer Dienste erschwert die Durchsetzung gesetzlicher Urheberrechtsbestimmungen, was sich insbesondere durch die derzeit noch im frühen Anfangsstadium befindliche Entwicklung anonymer und zensurresistenter Publikationsdienste verschärfen dürfte.

1.2.2 Konsequenzen

Das Ergebnis dieser Entwicklung ist, dass heute selbst technisch wenig versierten Privatleuten Haushaltsgeräte zur Verfügung stehen, mit denen geistige Werke effizient, bequem und ohne Qualitätsverlust vervielfältigt, archiviert, indiziert, gesucht und weltweit übertragen werden können. Betroffen davon sind insbesondere Musikaufnahmen in CD-Qualität, die heute auf eine Datenrate von 120–160 kbit pro Sekunde komprimiert werden können (MPEG Audio Layer 3) um dann mit etwa 60 kbit pro Sekunde über das Telefonnetz übertragen zu werden (ISDN, V.92). Damit beträgt die Ladezeit von Musik über das Internet derzeit etwa das doppelte der Spielzeit.

Verbesserte Kodierverfahren (z.B. MPEG-2 AAC+SBR) ermöglichen inzwischen über das Telefonnetz gar eine der Spielzeit entsprechende Ladezeit. Verbesserte und für Privathaushalte erschwingliche Internetzugangstechnologien (ADSL, Kabelmodems) verkürzen die Ladezeit weiter um einen Faktor 5–30. Zunehmend kritisch wird der Schutzbedarf für digitalisierte Kinofilme, da die typischen Filmlängen (90 min) und wesentlich höhere Datenraten von 4000–8000 kbit pro Sekunde zwar noch relativ lange Ladezeiten erfordern. Raubkopien von DVDs können allerdings bereits heute mit erträglichen Qualitätseinbußen auf einer CD-R untergebracht werden. Perfekte Raubkopien können jedoch künftig auch in Form von DVD-RW Medien in Umlauf gebracht werden.

Aufgrund der weiten Verfügbarkeit von Software-Entwicklungswerkzeugen für Heimcomputer sind heute frei verfügbare und privat entwickelte Kopier- und Abspielprogramme oft deutlich weiter entwickelt und schneller verfügbar, als dies die vergleichsweise langen Produktzyklen der etablierten Unterhaltungselektronikindustrie erlauben würden. Über das Internet finden sich heute schnell Gruppen von enthusiastischen Hobbyentwicklern zusammen, die derartige Systeme ohne kommerzielle Interessen gemeinsam entwickeln, verbessern und der Allgemeinheit frei zur Verfügung stellen. Produktzyklen für frei verfügbare Kopierhilfssoftware werden in Wochen statt wie im kommerziellen Bereich in Jahren oder Jahrzehnten gemessen.

Der Kampf gegen die illegale Bereitstellung und Nutzung urheberrechtlich geschützter Daten im Internet mit Hilfe technischer Mittel scheint angesichts der phantasievollen Umgehungsmöglichkeiten von Sperren aussichtslos. Die Markierung geschützter Inhalte mit Hilfe digitaler Wasserzeichen und digitaler Fingerabdrücke ermöglicht wenigstens die Verfolgung individuell markierter Kopien und besitzt damit für den Piraten abschreckende Wirkung.

Eine Verbreitung von digitalen 1:1-Kopien könnte mit Hilfe hardwaregestützter kryptographischer Verfahren verhindert werden. Allerdings sind solche Techniken sehr teuer und helfen in

der Praxis sehr wahrscheinlich auch nur eine begrenzte Zeit. Versuche, das Internet dermaßen zu verändern, dass die Benutzer bei allen Handlungen (egal, ob legal oder illegal) verfolgbar sind, scheitern technisch an der Verfügbarkeit und Nutzbarkeit von Anonymisierungsdiensten und dürften zudem in Konflikt stehen mit datenschutzrechtlichen Bestimmungen.

Kommunikation findet heutzutage über offene Netze statt. Das bedeutet, man hat sich auf wesentliche technische Standards zur Kommunikation geeinigt, deren Verwendung nicht durch Patente, Lizenzen o. ä. eingeschränkt wird. Das Internet ist ein solches offenes Netz. Die verteilte Netzstruktur des Internet besteht aus Rechnern vieler verschiedener Hersteller mit sehr unterschiedlicher Hardware- und Softwareausstattung, was die technische Offenheit unterstreicht. Damit die daraus resultierende Vielfalt kein Hindernis bei der weltweiten Kommunikation ist, wurden technische und organisatorische Kommunikationsvereinbarungen getroffen, an die sich alle Rechner des Internet halten müssen.

Die Vielfalt an Benutzern und Betreibern hat weiterhin die Konsequenz, dass man nicht davon ausgehen kann, dass sich alle Akteure im Internet kooperativ verhalten. Es existiert zwar eine sog. Netiquette, aber niemand ist gezwungen, sich daran zu halten. Nicht kooperatives Verhalten wird durch das Internet größtenteils noch nicht verhindert. Anders herum gesagt: Es existieren derzeit nur sehr wenige Sicherheitsfunktionen, die Betreiber und Benutzer vor Angriffen auf die Verfügbarkeit, Integrität, Zurechenbarkeit und Vertraulichkeit von Diensten und Daten schützen. Dieses Defizit muss für die ernsthaft geschäftsmäßige Anwendung des Internet, also für E-Business, beseitigt werden, sonst leidet auf lange Sicht die Vertrauenswürdigkeit eines „im Netz“ agierenden Unternehmens.

1.2.3 Technische Trends

Derzeit sind einige Trends zu beobachten, die auch ihre Auswirkungen auf Techniken zum Schutz digitaler Inhalte haben:

- **Konvergenz der Systeme:** Die Hersteller von Soft- und Hardware gehen zunehmend dazu über, mit einem einzigen System möglichst viele Formate, Standards, Kodierungen etc. zu unterstützen. Beispielsweise unterstützt Quicktime von Apple heute über 50 verschiedene Grafik-, Sound- und Videoformate. Set-Top-Boxen unterstützen teilweise mehrere Schutzsysteme (Multicrypt). Umgekehrt werden die gleichen Inhalte gleich für mehrere unterschiedliche Schutzsysteme ausgestrahlt, um sie auch auf verschiendenen Typen von Empfangsgeräten nutzen zu können (Simulcrypt). Die beiden Varianten sind in Abbildung 1.1 gegenübergestellt.

- **Schaffung von Plattformen:** Set-Top-Boxen werden universell. Personal Computer und Fernseher werden technisch immer ähnlicher. Mit der Multimedia Home Platform (MHP) verschmelzen beide Welten derart miteinander, dass technische Unterschiede kaum noch auszumachen sind.

- **Standardisierung:** Da proprietäre Systeme stets eine begrenzte Marktdurchdringung haben und für den Verbraucher wenig Nutzen bringen, soll nun über offene Standards versucht werden, gemeinsam den Durchbruch zuschaffen. MHP ist beispielsweise europaweit durch ETSI (European Telecommunications Standards Institute) standardisiert.

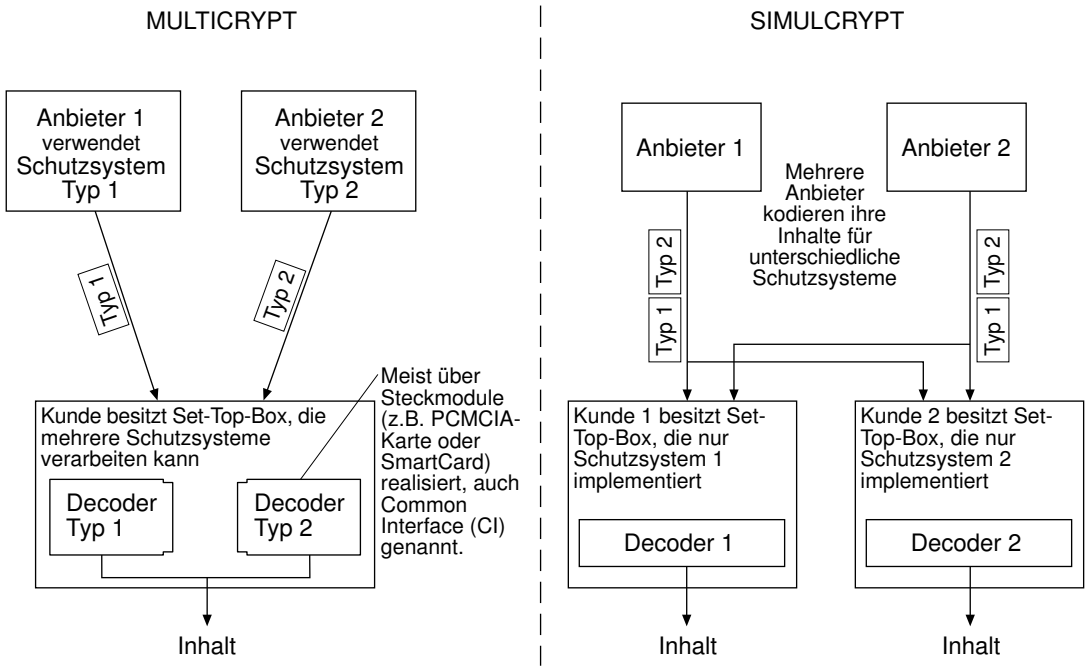

Abbildung 1.1: Gegenüberstellung von Multicrypt und Simulcrypt

1.3 Technische Grundlagen

Die folgenden Abschnitte vermitteln einige Grundlagen der IT-Sicherheit, benennen die heute üblichen Basistechniken der IT-Sicherheit, führen in die Grundverfahren der Distribution multimedialer Inhalte ein und erläutern kurz die heute üblichen Übertragungsprotokolle im Internet.

1.3.1 Schutzgüter, Bedrohungen und Schutzziele

In komplexen IT-Systemen, wie es unsere heutigen und zukünftigen Kommunikationsnetze sind, handeln verschiedene Subjekte (Organisationen, Personen). Sie können dabei nicht nur kooperieren, sondern auch konkurrieren (z. B. um Betriebsmittel), sabotieren (z. B. Kommunikation behindern, stören, blockieren, lahmlegen), fingieren (z. B. Identitäten vortäuschen, Daten verändern) oder abhören (z. B. bespitzeln, lauschen). Die Großrechner vor 25 Jahren waren streng bewacht, d.h. für sie galten Zugangskontrollmaßnahmen (Pförtner, Stahltüren etc.), die nicht leicht zu überwinden waren. Die Vernetzung von Rechnern blieb Spezialanwendungen vorbehalten.

IT-Systeme (einschließlich der Übertragungsstrecken) müssen außerdem gegen unbeabsichtigte Fehler und Ereignisse (z. B. höhere Gewalt, technische Fehler, Fahrlässigkeit, Programmierfehler, Verschleiß, Havarien) und beabsichtigte Angriffe (z. B. Abhören, Manipulation und Zerstören von Informationen, aber auch von Software und Hardware) von außen (z. B. Hacker oder Terroristen mit Sprengstoff) und innen (z. B. Administratoren, Programmierer) gesichert werden.

Seit den frühen 80er Jahren [55] findet sich eine Dreiteilung der Bedrohungen und korrespondierenden **Schutzziele** Vertraulichkeit, Integrität und Verfügbarkeit:

- Unbefugter Informationsgewinn, d.h. Verlust der **Vertraulichkeit** (Confidentiality),
- Unbefugte Modifikation von Informationen, d.h. Verlust der **Integrität** (Integrity) und
- Unbefugte Beeinträchtigung der Funktionalität, d.h. Verlust der **Verfügbarkeit** (Availability).

Die neuen Kommunikationsmedien sollen zunächst natürlich erwünschte Funktionen leisten, allerdings ebenso unerwünschte Funktionen oder Verhaltensweisen verhindern. Entsprechend lassen sich die großen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit verfeinern.

	Inhalte Worüber?	Umfeld Wer, wann, wo, mit wem, wie lange?
Unerwünschtes verhindern	Vertraulichkeit von Nachrichteninhalten	gegenseitige Anonymität der Anwender
	Verdecktheit von Nachrichteninhalten	Unbeobachtbarkeit der Anwender durch die Betreiber
Erwünschtes leisten	Integrität von Nachrichteninhalten	Zurechenbarkeit von Nachrichten zu Absendern
	Verfügbarkeit von Daten und Diensten	Erreichbarkeit von Anwendern

Tabelle 1.1: Gliederung von Schutzzielen

Sicherheit zu realisieren bedeutet, sich gegen einen **intelligenten Angreifer** bestimmter Stärke schützen zu können. Dieser Angreifer wird im Angreifermodell charakterisiert: Ein **Angreifermodell** definiert die Stärke eines Angreifers, gegen den ein bestimmter Schutzmechanismus (z.B. ein ganz bestimmtes Verschlüsselungsverfahren) gerade noch sicher ist. Dabei berücksichtigt das Angreifermodell folgende Aspekte:

1. Aktive oder passive Rolle des Angreifers:
   - Was kann der Angreifer maximal passiv beobachten?
   - Was kann der Angreifer maximal aktiv kontrollieren (steuern, verhindern) bzw. verändern?
2. Mächtigkeit des Angreifers:
   - Wieviel Rechenkapazität besitzt der Angreifer?
   - Wieviel finanzielle Mittel besitzt der Angreifer?
   - Wieviel Zeit besitzt der Angreifer?
   - Welche Verbreitung hat der Angreifer? Oder spezieller: Welche Leitungen, Kanäle, Stationen kann der Angreifer beherrschen?

Als potentielle Angreifer können Außenstehende, Teilnehmer, Betreiber, Hersteller, Entwickler und Wartungstechniker betrachtet werden, die natürlich auch kombiniert auftreten können. Außerdem kann man nach Angreifern innerhalb des betrachteten IT-Systems (Insider) und außerhalb (Outsider) unterscheiden. Die Feststellung, dass eine Instanz angreifen kann, ist nicht gleichzusetzen damit, dass sie wirklich angreift.

Grundsätzlich gilt: Man sollte einem Angreifer nie zuwenig zutrauen. Die Kosten, die ein Angreifer zum Knacken eines Systems aufwenden wird, müssen aber selbstverständlich in einem gesunden Verhältnis zu den Kosten des Schutzes stehen. Insofern mag ein Schutzmechanismus, der gegen einen „Gelegenheitstäter“ etwas hilft, aber nicht gegen einen professionellen Knacker, durchaus sinnvoll sein, wenn die Verluste hauptsächlich durch den Gelegenheitstäter auftreten. Die globale Verfügbarkeit von Informationen und automatisierten Tools im Internet lässt aber zunehmend die Grenzen zwischen Amateur und Profi verschwimmen, weshalb in der Praxis von einem starken Angreifer ausgegangen werden sollte.

In letzter Konsequenz heißt das: Experten werden Tools entwickeln, die jedermann in die Lage versetzen, gegen Copyright wie auch DRM-Techniken zu verstoßen, und dies vermutlich so, dass es der Enduser gar nicht merkt.

1.3.2 Basistechniken zum Schutz

Um die Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit und Verfügbarkeit in informationstechnischen Systemen zu realisieren, existieren Basismechanismen, die heute gut erforscht und teilweise auch benutzerfreundlich einsetzbar sind.

Die Vertraulichkeit von Nachrichten kann mit Hilfe von **Verschlüsselung** erreicht werden. **Message Authentication Codes** dienen dem Schutz von Nachrichten vor unerkannter Verfälschung auf den Übertragungswegen.

Mit Hilfe der **digitalen Signatur** ist Zurechenbarkeit realisierbar: Nachrichten können so ihrem „Unterzeichner“ eindeutig zugeordnet werden.

Die Anonymität und Unbeobachtbarkeit von Internet-Nutzern kann durch sog. **datenschutzfreundliche Techniken** realisiert werden. Im Bereich E-Commerce sind die bekanntesten Verfahren, die zur Klasse der anonymen Verfahren zählen, die digitalen anonymen Zahlungssysteme und Verfahren zum unbeobachtbaren Web-Surfen im Internet.

Die Verfügbarkeit von Daten und Diensten kann erreicht werden durch **Diversität und redundante Auslegung** von Leitungskapazitäten, Rechenressourcen und Datenspeichern.

Eine ausführliche Darstellung der Basistechniken zum Schutz vor intelligenten Angreifern ist z.B. in [20] zu finden.

Neben den Verschlüsselungsverfahren haben für den Bereich Digital Rights Management spezielle Techniken zum Schutz der Inhalte eine hohe Bedeutung. In Kapitel 2 werden die dort angewendeten Techniken vorgestellt.

1.3.3 Distribution von multimedialen Inhalten

Man kann Verteilung von multimedialen Inhalten unterscheiden nach Offline-Verteilung, z.B. über Compact Disc oder andere Datenträger und Online-Verteilung, z.B. per Rundfunk, über spezielle Verteilkabel, Telefon oder über das Internet.

	Online	Offline
Synchron	z.B. Rundfunk, Fernsehen, Webcasting, Simulcasting	—
Asynchron	z.B. Abruf von Webseiten im Internet	z.B. Distribution über Datenträger (CD, DVD)

Tabelle 1.2: Verteilungsformen von Inhalten

Online verteilte Inhalte können synchron und asynchron konsumiert werden. Synchron/asynchron bezieht sich auf den zeitlichen Zusammenhang zwischen Datenübertragung und Konsumierung (Tabelle 1.2).

- **Asynchron:** Inhalte, die auf einem Datenträger verteilt werden, können zu jeder beliebigen Zeit und auch mehrmals konsumiert werden.
- **Synchron:** Inhalte, die synchron übertragen werden (z.B. Rundfunk, Fernsehen, aber auch Streaming-Daten im Internet), müssen vom Konsumenten erst gespeichert werden, damit sie asynchron oder wiederholt konsumiert werden können.

Bei der synchronen Online-Übertragung im Internet unterscheidet man neuerdings noch nach Simulcasting und Webcasting. Unter Simulcasting wird die zeitgleiche Übertragung von terrestrischen Sendungen im Internet verstanden, während mit Webcasting die Nur-Internet-Übertragung gemeint ist.

Neben Offline/Online kann man auch nach der Eignung des Mediums zur Interaktivität unterscheiden. Interaktive Inhalte besitzen heute meist (aber nicht notwendigerweise) eine Online-Komponente.

Weiterhin ist zu unterscheiden, ob alle Konsumenten exakt gleiche Kopien des Inhaltes erhalten oder ob sie individualisierte, d.h. speziell auf sie zugeschnittene Kopien (z.B. mit eingebetteten Informationen über Kaufdatum, Besitzer etc.) erhalten. Die individualisierte Verteilung der Inhalte ist offline schwer bzw. nicht möglich und kann deshalb momentan praktisch nur für den Online-Abruf (ggf. mit anschließender erlaubter Speicherung des Inhalts) realisiert werden.

Bei der Distribution von Inhalten im Internet (egal, ob synchron oder asynchron) werden heute meist exakt gleiche Kopien an alle Konsumenten übermittelt.

Synchrone und asynchrone Distributionsformen sind von der leichten Kopierbarkeit im gleichen Maße betroffen, da es einfach möglich ist, die Inhalte digital aufzuzeichnen und ebenfalls asynchron (d.h. zeitversetzt) weiterzuverbreiten (siehe auch Abschnitt 3.6.2).

Der Vertrieb von Inhalten fand und findet aufgrund der teilweise unbefriedigenden Übertragungskapazitäten der Online-Anschlüsse privater Haushalte über Datenträger statt. Der Anteil der Online-Verteilung nimmt jedoch stetig zu, insbesondere im Audio-Betreich, wo die Übertragungskapazitäten inzwischen ausreichen.

1.3.4 Übertragungsprotokolle im Internet

Bevor näher auf den Schutz von Daten eingegangen wird, sollen einige Grundbegriffe der Übertragungsprotokolle im Internet eingeführt werden, da deren Verständnis die Voraussetzung für die Beurteilung der praktischen Anwendbarkeit der Schutzmechanismen ist.

Nutzerdaten werden im Internet mit Hilfe von zwei Übertragungsprotokollen transportiert, dem Transmission Control Protocol (TCP) und dem User Datagram Protocol (UDP), siehe Tabelle 1.3.

	TCP	UDP
Punkt-zu-Punkt	Etabliert, Beispiel: HTTP (WWW)	Etabliert, aber teilweise keine Quality-of-Service-Zusicherungen, Beispiel: Real Player
Multicast, Broadcast	—	In Entwicklung und Erprobung

Tabelle 1.3: Übertragungsprotokolle im Internet

Transmission Control Protocol (TCP)

Das Transmission Control Protocol (TCP) wird bei Punkt-zu-Punkt-Verbindungen zwischen zwei Endpunkten, z.B. einem Browser und einem Webserver eingesetzt. Bei TCP wird darauf geachtet, dass alle vom einen Endpunkt gesendeten Bits auch tatsächlich beim anderen Endpunkt ankommen und auch ihre Reihenfolge nicht durcheinander kommt. Falls Daten beim Transport verloren gehen, werden sie erneut gesendet (Retransmission). Dieses Transportprotokoll wird z.B. beim Transport von Webseiten, E-Mails, Dateien etc. angewendet, da man sicher gehen möchte, dass die Daten auch wirklich beim Empfänger ankommen.

Sollen mit Hilfe von TCP-Verbindungen viele Nutzer mit dem gleichen Inhalt von einem Server versorgt werden, muss jeder Nutzer eine eigene Verbindung zum Server aufbauen (Abbildung 1.2). Der Bedarf an Bandbreite wächst dadurch linear mit der Teilnehmerzahl, da der Server jeweils eine Verbindung pro Client und Request unterhält. Selbst wenn mehrmals die gleichen Inhalte vermittelt werden sollen, erfolgt keine Konzentration, etwa um Bandbreite zu sparen. Dass ein solches Vorgehen nicht besonders effektiv ist, liegt auf der Hand, allerdings ist TCP auch nicht unbedingt für solche Verkehrsformen wie Broadcasting gedacht gewesen.

Deshalb wird mit Hilfe einer Replikation des Datenbestandes (die Server R1 und R2, siehe Abbildung 1.3, werden mit Kopien der Inhalte des Servers versorgt) und sog. Caching-Techniken versucht, einen Lastausgleich und bessere Antwortzeiten zu erreichen. Einen solchen Service bietet z.B. die Firma Akamai (http://www.akamai.com/) an.

Die Replikation löst allerdings nicht das Grundproblem der Mehrfachverteilung von Informationen, sondern reduziert es nur, da es trotzdem vorkommen wird, dass mehrere Nutzer gleichzeitig den gleichen Inhalt von einem Server abrufen.

User Datagram Protocol (UDP)

Beim User Datagram Protocol (UDP) sendet der Sender Datenpakete aus. UDP ist ein verbindungsloses Protokoll und wird u.a. im Bereich Streaming angewendet. In Abhängigkeit von der Auslastung des Netzes erreicht dann z.B. ein Datenpaket des Multimedia-Streams den Empfänger rechtzeitig, zu spät (delayed) oder auch gar nicht (dropped). UDP wird

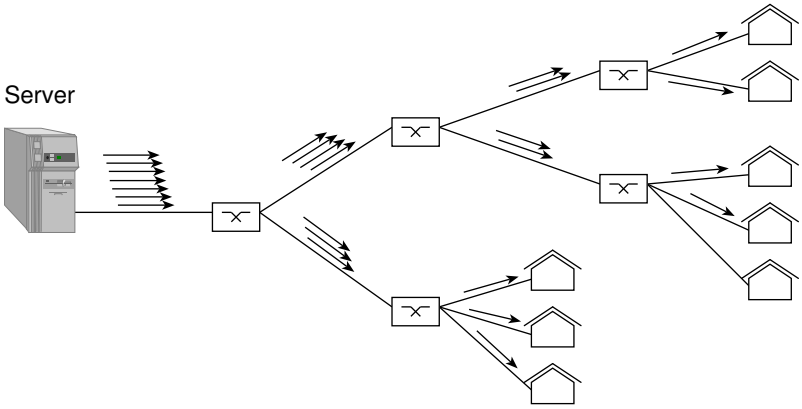

Abbildung 1.2: Punkt-zu-Punkt-Verbindungen

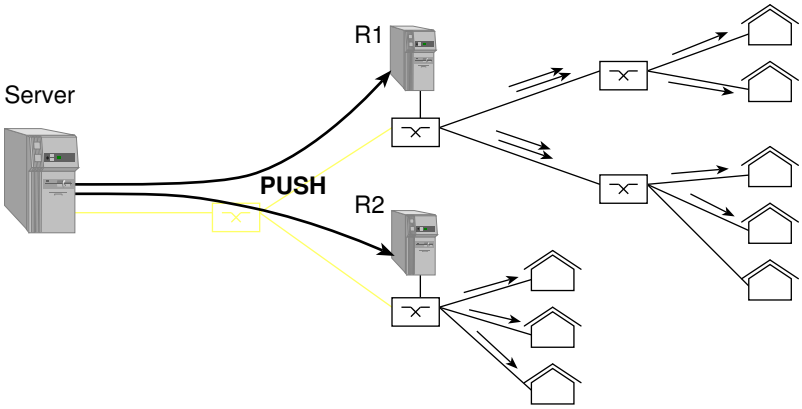

Abbildung 1.3: Replikation des Datenbestandes

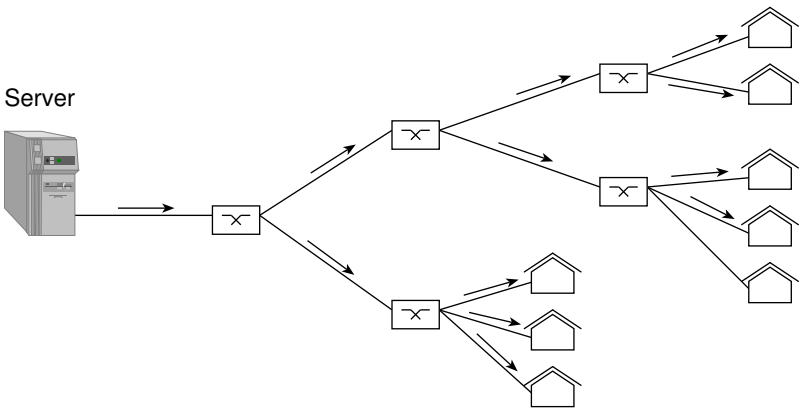

Abbildung 1.4: Multicast von Streamingdaten

hauptsächlich für Datenströme verwendet, bei denen eine Retransmission nicht möglich ist. Beispielsweise bei Audio- und Videoströmen, die synchron gesendet und konsumiert werden, ist es nicht sinnvoll, verloren gegangene Datenpakete erneut zu senden, da der fehlende „Abschnitt“ des Datenstroms zeitlich hinter dem aktuell gesendeten liegt. UDP-Pakete werden beispielsweise vom Real Player (http://www.real.com/) verarbeitet. Der Verlust von Datenpaketen macht sich je nach Kodierung der Medienströme durch Qualitätsverschlechterung oder Aussetzer bemerkbar.

Neben der Punkt-zu-Punkt-Übertragung von UDP-Paketen lassen sich auch Punkt-zu-Mehrpunkt-Übertragungen (Multicast, Broadcast) realisieren. Diese Klasse von UDP-Verkehr soll u.a. den Bereich des Webcasting abdecken (siehe Abbildung 1.4). Dabei verbindet sich ein Benutzer z.B. mit einen Videodatenstrom über eine sog. Multicast-Adresse (join). Dies wird durch das sog. Internet Group Management Protocol (IGMP) realisiert.

Derzeit wird massiv an der Zusicherung sog. Quality-of-Service-Merkmale (QoS) gearbeitet, um die auftretenden Verzögerungen und Datenverluste derart vorhersagen bzw. vermeiden zu können, dass dem Endbenutzer eine gleich bleibend hohe Qualität der Übertragung zugesichert werden kann. Die bisher entwickelten Protokolle tragen Namen wie Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP) und Real-Time Streaming Protocol (RTSP). Im Zusammenhang mit QoS existiert noch ein Resource Reservation Protocol (RSVP). In der gegenwärtigen Distributionspraxis im Internet spielen die genannten Protokolle noch keine große Rolle, was sich aber mit steigenden Übertragungskapazitäten ändern wird. An technischer Einführungsliteratur in die Multicastprotokolle kann [38] empfohlen werden.

2 Techniken zum Schutz

Um die gesetzlich schwierig kontrollierbare unrechtmäßige Verbreitung von schützenswerten Inhalten einzudämmen, wurden eine Reihe von technischen Maßnahmen vorgeschlagen. Eine Kategorisierung der Mechanismen ist schwierig, da die in der Praxis anzutreffenden DRM-Systeme meist eine Kombination mehrerer Mechanismen darstellen.

2.1 Übersicht

Wir verwenden für die Darstellung der Mechanismen folgende Gliederung:

1. **Kerntechniken der IT-Sicherheit, die auch im DRM-Bereich Anwendung finden.**
   - **Verschlüsselung:** Um individualisierte und kostenpflichtige Dienste vor unberechtigter Nutzung zu schützen, müssen die übertragenen Inhalte verschlüsselt sein.
   - **Schutz durch manipulationssichere Hardware:** Sicherheitsmechanismen verwenden (meist kryptographische) Geheimnisse, deren Kenntnis die Voraussetzung für die Nutzung der Inhalte ist. Die einzige derzeit halbwegs sichere Methode zur Aufbewahrung der Geheimnisse ist sog. Tamper-Resistant Hardware.
   - **Schutz durch Software-Kapselung:** Wenn schon keine Tamper-Resistant Hardware eingesetzt werden kann, weil die zu schützenden Inhalte beispielsweise auf einem handelsüblichen PC nutzbar sein sollen, so sollte wenigstens die Ausführungsumgebung, in der das Rechtemanagement erfolgt, gegen böswillige fremde Software (Trojanische Pferde, Sniffing- und Hacker-Software) geschützt sein. Ein Softwareschutz gegen Angriffe durch den Betreiber und Besitzer des Rechners ist dagegen heute aussichtslos.
2. **Speziell für DRM designte halbwegs starke Mechanismen zum Schutz.**
   - **Modifikation des analogen Endsignals:** Selbst wenn man DRM-Systeme so bauen würde, dass nur analoge Signale abgreifbar wären, sollte das Abgreifen und erneute Digitalisieren erschwert werden.
   - **Watermarking:** Damit urheberrechtlich geschützte digitale Mediendaten als solche erkennbar sind und auch nach Manipulationen erkennbar bleiben, werden sie mit digitalen Wasserzeichen versehen.
   - **Fingerprinting:** Für den Schutz der Urheberrechte an multimedialen Inhalten wird man zunehmend dazu übergehen, individualisierte Kopien zu verteilen, um eine Rückverfolgung des illegalen Distributionsweges zu ermöglichen.

3. **Schwache und mittelbar wirksame Mechanismen, die ernsthaften Angriffsversuchen nicht standhalten.**
   - Einbringen von Codes ohne besondere Sicherung,
   - bewusste Schaffung von Inkompatibilitäten, um die Nutzung legaler Inhalte einzuschränken,
   - das Aufspüren von illegalen Inhalten sowie
   - das Sperren bzw. Filtern dieser Inhalte.

Auf die genannten Techniken wird im Folgenden ausführlicher eingegangen.

2.2 Kerntechniken der IT-Sicherheit

In den folgenden Abschnitten werden die kryptographischen Grundverfahren und deren Anwendung für die Verschlüsselung von Inhalten und Medienströmen erläutert. Sichere DRM-Verfahren setzen eine Kapselung des Rechtemanagements voraus, die bevorzugt durch manipulationssichere Hardware oder notfalls durch geschützte Software-Ausführungsumgebungen, sog. Sandboxen, erfolgen sollte.

2.2.1 Kryptographische Grundverfahren

Kryptographie dürfte die mit Abstand ausgereifteste Technik sein, die auch sofort zur Verfügung steht, während die anderen teilweise noch im Entwicklungs- und Einführungsprozess sind. Man unterscheidet symmetrische und asymmetrische Verschlüsselungsverfahren. Wenn sowohl Sender als auch Empfänger über den gleichen kryptographischen Schlüssel verfügen, spricht man von symmetrischen Systemen, andernfalls von asymmetrischen.

Symmetrische Kryptosysteme

Die bekanntesten und ältesten kryptographischen Systeme sind symmetrische Systeme (siehe Abbildung 2.1). Ihre bekanntesten Vertreter sind DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) und AES (Advanced Encryption Standard).

Wenn eine Nachricht x verschlüsselt über einen unsicheren Kanal gesendet werden soll, muss der Schlüssel k bei Sender und Empfänger vorliegen. Für den Distributionsweg eines Inhaltes bedeutet dies, dass der Inhalt verschlüsselt verbreitet wird und beim Empfänger im Endgerät entschlüsselt wird. Um zu verhindern, dass der Empfänger unverschlüsselte digitale Kopien anfertigen und weiter verbreiten kann, muss u.a. der Schlüssel besonders gesichert, d.h. vor Kenntnisnahme durch den Empfänger geschützt, sein. Zusätzlich muss selbstverständlich auch das Abgreifen des unverschlüsselten digitalen Inhalts unmöglich gemacht werden. Als sicherheitstechnisch befriedigende Lösungen kommen hier nur Hardware-Lösungen (sog. Tamper-Resistant Hardware, siehe Abschnitt 2.2.3) in Betracht. Ein Softwareschutz ist völlig unsicher und kann mit sehr geringem Aufwand gebrochen werden. Die Konsequenz ist, dass der Schlüssel nach Bekanntwerden bei *allen Empfängern* ausgewechselt werden muss, was in der Praxis nahezu unmöglich ist.

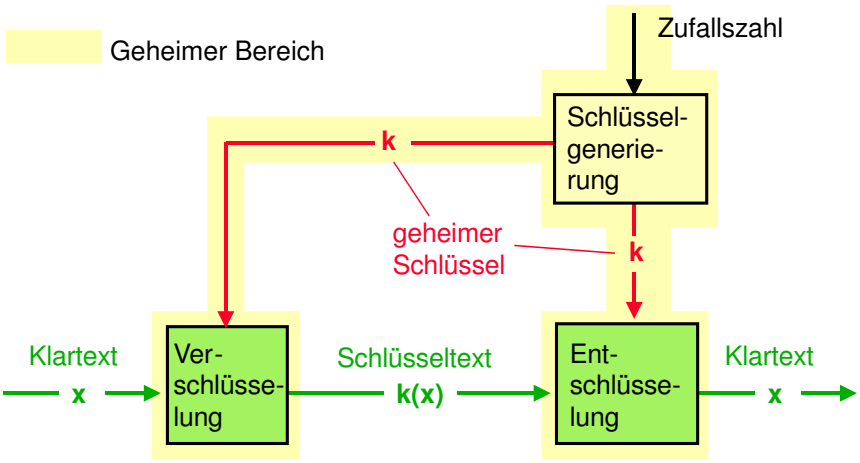

Abbildung 2.1: Symmetrisches kryptographisches System

Asymmetrische Kryptosysteme

Die bekanntesten asymmetrischen Systeme (siehe Abbildung 2.2) sind RSA und ElGamal (jeweils benannt nach ihren Erfindern Rivest, Shamir, Adleman bzw. ElGamal). Im Vergleich zu symmetrischen Kryptosystemen sind sie deutlich rechenaufwendiger (etwa Faktor 100 bis 1000).

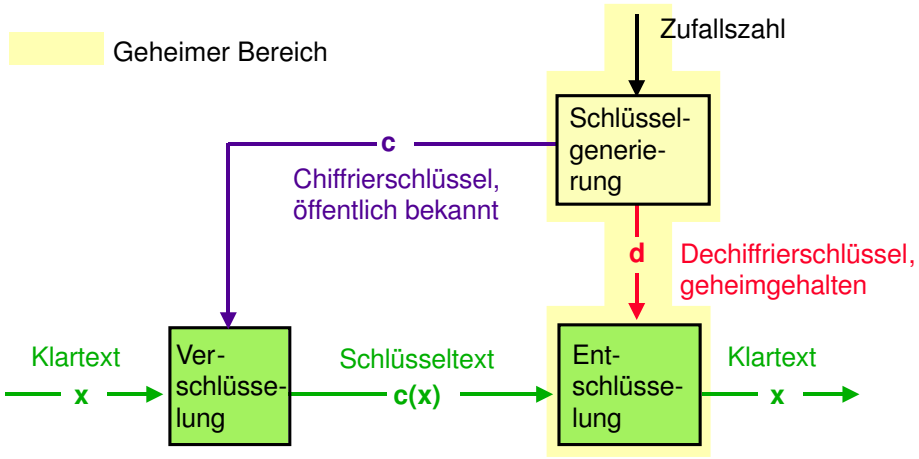

Abbildung 2.2: Asymmetrisches kryptographisches System

Asymmetrische Systeme wurden erfunden, um die Schlüsselverteilung zu vereinfachen. Hier sind zum Ver- und Entschlüsseln verschiedene Schlüssel *c* und *d* erforderlich, und nur *d* muss geheimgehalten werden. Damit man *c* tatsächlich nicht geheimhalten muss, darf *d* nicht mit vernünftigem Aufwand aus *c* zu bestimmen sein.

Hybride Kryptosysteme

Asymmetrische Systeme werden meist eingesetzt, um einen symmetrischen Session Key zu verschlüsseln und zum Teilnehmer zu übertragen (sog. hybride Kryptosysteme). Der Teilneh-

mer entschlüsselt den Session Key und verwendet ihn, um den Medienstrom, der seinerseits mit dem Session Key verschlüsselt wurde, wieder zu entschlüsseln. Die Konsequenz für die Distribution von Inhalten ist, dass jetzt *zusätzlich* vor der Übertragung der Inhalte an *jeden* der Sitzungsschlüssel gesendet werden muss. Dieses Vorgehen ist zwar aufwendiger, hat aber für die Online-Distribution folgende Vorteile:

1. Ein regelmäßiger Schlüsselwechsel ist möglich. Ein in der Vergangenheit kompromittierter Sitzungsschlüssel nützt dem Unberechtigten nur etwas bis zum nächsten Schlüsselwechsel.

2. Eine individualisierte Verteilung der Sitzungsschlüssel ist möglich, d.h. individualisierte Zugänge zu bestimmten Inhalten (On-Demand-Dienste) sind realisierbar.

Ersteres ist auch mit einem symmetrischen Schlüssel zur Session-Key-Verteilung möglich. Anstelle des asymmetrischen Schlüssels wird jedem Teilnehmer ein symmetrischer Schlüssel zugeordnet, mit dem der Session Key verschlüsselt wird. Dies ist in der Praxis meist effizienter, weil asymmetrische Verfahren rechenaufwendiger sind und bei sehr wenig zu übertragenden Bits zu einer Nachrichtenexpansion führen. Außerdem erhält der Empfänger den Schlüssel sowieso vom Sender, so dass der vereinfachte Schlüsselaustausch asymmetrischer Systeme nicht zum Tragen kommt.

Zweites ist auch einfacher mit anderen Techniken, z.B. dem Übertragen von individuellen Seriennummern (Freischalt-Codes), die das individuelle Freischalten der Inhalte nach Bezahlung übernehmen, möglich. Anstelle des Wechsels des Sitzungsschlüssels wird der Medienstrom stets mit einem festen Schlüssel verschlüsselt. Sobald die Abspiel-Hardware einen individuellen Freischalt-Code empfängt, entschlüsselt sie die Inhalte und gibt sie unverschlüsselt an das Ausgabegerät (Bildschirm, Lautsprecher etc.) weiter.

Geheimgehaltene Systeme

Insbesondere dann, wenn Sicherheitsmechanismen von Entwicklern entworfen werden, deren Kerngebiet nicht Sicherheit ist, sondern z.B. Nachrichtenformate, Kommunikationsprotokolle, Geräte- und Mediendesign (kurz: Laien auf dem Gebiet Sicherheit), entstehen meist proprietäre, d.h. nicht standardisierte Schutzmechanismen. Um einen vermeintlich besseren Schutz zu erzielen, wird das Design der Sicherung geheim gehalten. Dies bedeutet nicht zwangsläufig einen Sicherheitsgewinn, sondern kann umgekehrt zu einem Sicherheitsverlust führen, weil beim Design wichtige Angriffe übersehen wurden und dies zunächst niemand bemerkt. Später könnte erfolgreiches Reverse Engeneering (siehe Abschnitt 3.4) plötzlich zur Unsicherheit der gesamten im Einsatz befindlichen Technik führen.

Die Sicherheit des Verfahrens soll, wie es für gute Verschlüsselungsverfahren gilt, nur durch die Geheimhaltung eines kryptographischen Schlüssels erzielt werden. Daraus ergibt sich die Forderung, dass jeder Schutzmechanismus, der ernst genommen und auch rechtlichen Auseinandersetzungen stand halten soll, vollständig offen gelegt und seine Qualität durch Experten bestätigt sein muss. Ist man sich als Anbieter von Sicherheitstechnik seiner Sache jedoch sehr sicher und sind rechtliche Auseinandersetzungen nicht zu erwarten, kann Geheimhaltung des Designs eine zusätzliche Hürde für den Angreifer darstellen.

2.2.2 Verschlüsselung von Inhalten und Medienströmen

Die im vorangegangenen Abschnitt eingeführten kryptographischen Verfahren sollen nun für die Verschlüsselung von Inhalten in Online-Verbindungen und auf Datenträgern angewendet werden.

Verschlüsselung von Online-Verbindungen

Heutzutage existieren auch für den Schutz von Inhalten beim Streaming und Abruf über Netze derart ausgereifte Verschlüsselungsverfahren, dass bei richtiger Anwendung das Knacken der Verschlüsselung praktisch unmöglich ist. Für individualisierte und insbesondere kostenpflichtige Dienste sollten also, wann immer möglich, die Mediendaten verschlüsselt werden, um sie vor unberechtigtem Zugriff auf den Übertragungswegen zu schützen (Abbildung 2.3).

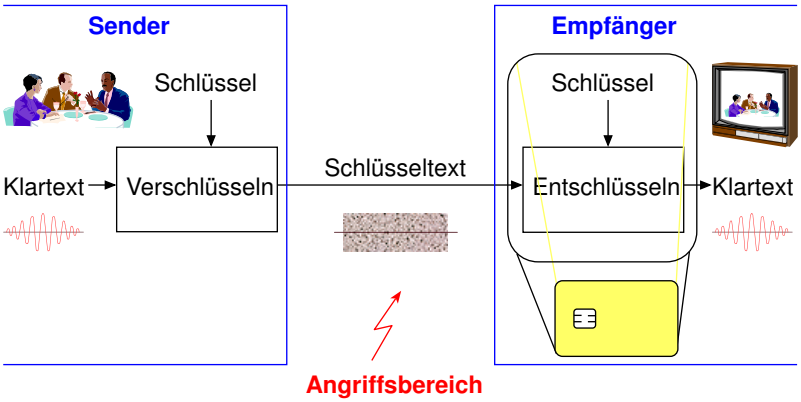

Abbildung 2.3: Verschlüsselung auf Übertragungswegen

Die individuelle Verschlüsselung (d.h. jeder Kunde besitzt einen anderen Schlüssel) hat allerdings den Nachteil, dass jeder Kunde einen anderen Medienstrom erhalten müsste, was wiederum mit einer enormen Verschwendung an Übertragungskapazität verbunden wäre (vgl. auch Abbildung 1.2), zumindest wenn alle Kunden zeitgleich mit den gleichen Mediendaten versorgt werden sollen.

In der Praxis wird deshalb meist ein einziger verschlüsselter Medienstrom übertragen. Alle Kunden erhalten den gleichen Schlüssel, der sich z.B. in einer Chipkarte oder in einer Set-Top-Box befindet und der das Gerät nie verlässt. Andernfalls wäre die illegale Verbreitung des Schlüssels möglich. Mit diesem Schlüssel kann dann ein temporär gültiger Sitzungsschlüssel entschlüsselt werden, mit dem der eigentliche Medienstrom verschlüsselt wurde. Solche Verschlüsselungstechniken werden heute noch nicht überall angewendet.

Das „Scrambling“ von einigen älteren Pay-TV-Kanälen basiert meist auf deutlich schwächeren Schutzmechanismen und kann nicht unbedingt als Verschlüsselung bezeichnet werden. Häufig werden die Daten nur „verschleiert“, was ernsthaften Angriffen nicht standhält.

Verschlüsselung von Datenträgern

Eine Möglichkeit, Inhalte, die auf einem Datenträger verteilt werden, zu schützen, besteht darin, die Daten auf dem Datenträger zu verschlüsseln und in einer separaten, ausforschungssicheren Hardware zu entschlüsseln (z.B. eine Chipkarte, die jedem Datenträger beiliegt, ähnlich einem Dongle, mit dem teure Software gegen Raubkopieren geschützt wird). Wie aufwendig der Nachbau eines solchen Hardware-Moduls ist, hängt vom Aufwand ab, mit dem die innere Struktur und die kryptographischen Geheimnisse, die ein solcher Baustein beherbergt, vor Reverse Engeneering (siehe Abschnitt 3.4) geschützt sind. Anhaltspunkte für entsprechende Sicherheitsstufen von Hardwarebausteinen finden sich in Abschnitt 3.2.

Das Abspielgerät besitzt einen Schacht für den Datenträger und einen für die Chipkarte. Eine digitale Kopie der verschlüsselten CD wäre damit ohne die zugehörige Chipkarte wertlos. Allerdings dürfen die entschlüsselten Daten im Abspielgerät nicht unberechtigt abgegriffen werden können, um aus ihnen eine unverschlüsselte digitale 1:1-Kopie herstellen zu können, was aber mit einem PC leicht möglich sein wird. Deshalb ist ein solches Verfahren in der Praxis untauglich und zudem teuer, weshalb es praktisch nicht angewendet wird.

Außerdem verhindert die reine Verschlüsselung der Inhalte auf dem Datenträger nicht das 1:1-Kopieren des (verschlüsselten) Mediums. Deshalb enthält das geschützte Medium neben den verschlüsselten Daten in der Regel noch ein Sondersignal, welches von allgemein zugänglichen Abspielgeräten für den Einsatz in Universalcomputern (PCs) zwar gelesen, aber nicht geschrieben werden kann. Das kann im Prinzip ein einzelnes Datenbit an einer ausgewählten, für Schreibsoftware unzugänglichen Stelle im Datenstrom sein, oder aber, falls Kompatibilität zu existierenden Medien eine Anforderung ist, ein ausgefeilterer Datenkanal, wie etwa bestimmte Kombinationen von Bitfehlern. Abspielgeräte entschlüsseln den Datenstrom nur, nachdem die Anwesenheit des Sondersignals festgestellt wurde. Eine etwas verfeinerte, aber prinzipiell äquivalente Form dieses Prinzips (in der eine Hierarchie aus Schlüsseln teil des Sondersignals ist) findet beispielsweise beim DVD-System Einsatz.

Die Verwendung eines einzigen oder einiger weniger Schlüssel hat den gravierenden Nachteil, dass viele Stellen (z.B. alle Hersteller von Player-Hardware) den Schlüssel erfahren müssen, um ihn in das Endgerät zu integrieren. Sobald eine Stelle „undicht“ wird (oder die Hardware unsicher), ist das gesamte Sicherheitssystem gefährdet. Dies ist beispielsweise beim Content Scrambling System (CSS) der DVD geschehen.

Mehrschlüsselsysteme für Online-Übertragung und Datenträger

Statt einen einzelnen Schlüssel zu benutzen, kann das Risiko etwas reduziert werden, indem eine Gruppe von Schlüsseln benutzt wird, von denen jedes Abspielgerät nur einen beherbergt, z.B. zwei Schlüssel pro Hersteller wie im DVD-System. Der Nutzdatenstrom wird mit einem für die jeweiligen Daten spezifischen Medienschlüssel verschlüsselt, und dieser Medienschlüssel wiederum wird mit allen Schlüsseln aus Abspielgeräten verschlüsselt, wovon jedes Abspielgerät nur einen beherbergt.

Im Prinzip könnten damit, sobald ein Schlüssel aus einem Abspielgerät erfolgreich ausgelesen wurde, die Hersteller von neuen Medien den betreffenden Medienschlüssel nicht mehr mit dem Schlüssel des kompromittierten Abspielgerätes verschlüsselt abspeichern. Dies hätte zur Folge,

dass die entwendete Schlüsselinformation nicht mehr genutzt werden kann, um von neu publizierten Medien den Kopierschutz zu entfernen. Auf der anderen Seite wären aber von dieser Maßnahme die Besitzer aller Abspielgeräte betroffen, die den gleichen nunmehr kompromittierten und aus dem Verkehr gezogenen Schlüssel benutzen. Zudem können mit dem kompromittierten Schlüssel immer noch alle älteren veröffentlichten Werke „entschützt“ werden, was immer noch einen erheblichen Schaden darstellen kann, solange die geschützten Daten nicht nur im Wesentlichen kurzzeitig von Wert sind (wie etwa bei Zeitungsnachrichten).

Mehrschlüsselsysteme werden inzwischen recht erfolgreich im Bereich der digitalen Pay-TV-Zugangskontrolle von mindestens einem Anbieter eingesetzt. Bei Pay-TV-Systemen werden die verteilten verschlüsselten Daten nicht von den Benutzern gespeichert, weshalb ein Austausch von Schlüsseln in dieser Anwendung wesentlich praktikabler ist. Die entsprechenden Systeme sind darauf vorbereitet, dass die Schlüsseldaten in einer Chipkarte untergebracht sind. Chipkarten sind ein Format, das sich insbesondere zum einfachen Postversand eignet. Bei modernen Pay-TV-Systemen besteht daher im Vergleich zu älteren Kopierschutzsystemen, die direkt in die Set-Top-Box integriert sind, kaum ein Bedarf für einen manipulationssicheren Baustein innerhalb der Set-Top-Box: Die Entschlüsselung wird direkt auf der Chipkarte durchgeführt. Der regelmäßige Austausch aller Kundenchipkarten ist im Pay-TV- wie auch im Bank-Bereich inzwischen ein Routinevorgang und bewirkt, dass Geheimschlüssel nach 1–3 Jahren ihren Wert verlieren, was bei Schutzkonzepten für gespeicherte Werke (z.B. DVD) nicht praktikabel ist.

Zusammenfassung

Der Sinn der Verschlüsselung der Nutzdaten ist es, dem Benutzer der Daten den freien Zugriff auf das unverschlüsselte, aber noch komprimierte und damit bequem transportierbare und mit beliebiger Hardware wiedergebbare Nutzsignal vorzuenthalten. Zu diesem Zweck müssen die Schaltfunktionen für

(a) die Erkennung des nicht kopierbaren Sondersignals bzw. der Authentisierung,

(b) die Entschlüsselung,

(c) die Dekompression, und vorzugsweise

(d) auch die Digital/Analog-Wandlung

sowie nach Möglichkeit sogar die physikalische Ausgabe in einer manipulationssicheren geschlossenen Einheit stattfinden, welche den externen Zugang zu Zwischenbearbeitungsschritten verhindert.

2.2.3 Manipulationssichere Hardware

Manipulationssichere Hardware wird zum Schutz von Geheimnissen, etwa Dekodierschlüsseln, und zur Authentisierung der Teilnehmer eingesetzt. Nach einer allgemeinen Problembeschreibung wird das Angreifermodell entwickelt. Schließlich werden die Grundverfahren zur Realisierung manipulationssicherer Hardware beschrieben.

Allgemeines

Die soeben beschriebenen Mechanismen verwenden (meist kryptographische) Geheimnisse, deren Kenntnis die Voraussetzung für die Nutzung der Inhalte ist. Um die Geheimnisse, die gewissermaßen den Anker der Sicherheit der Verfahren bedeuten, vor unberechtigter Verwendung und/oder Kenntnisnahme und womöglich Veröffentlichung zu schützen, müssen sie speziell gesichert werden.

Jedes Abspielgerät enthält dann versteckt innerhalb eines integrierten Schaltkreises die Schlüsselinformation, mit deren Hilfe der Nutzdatenstrom entschlüsselt werden kann. Die Entschlüsselung, digitale Decodierung und Digital/Analog-Wandlung des Nutzsignals sollte innerhalb eines einzigen manipulationssicher geschlossenen Bauteils stattfinden, so dass es extrem schwierig wird, an den entschlüsselten, aber noch digital komprimierten Datenstrom zu gelangen, welcher zum Anfertigen einer exakt identischen Kopie notwendig wäre.

Das Problem dieser Verschlüsselungstechniken ist die sichere Speicherung des Schlüssels (und ggf. auch des gesamten Verschlüsselungsverfahrens) in einem Abspielgerät. Sofern nicht jedes einzelne verkaufte Medium individuell für ein spezielles Abspielgerät verschlüsselt wird, was im Musikbereich mit der existierenden „Plattenladen“-Infrastruktur nicht praktikabel ist, aber für Onlineverkäufe durchaus vorstellbar wäre, so muss es letztendlich einen globalen Schlüssel geben, der in jedem Abspielgerät enthalten sein muss. Gelingt es jemandem, diesen Schlüssel aus einem Abspielgerät auszulesen, so bricht der gesamte Kopierschutz zusammen, da sich nun relativ leicht Software entwickeln lässt, die die Nutzdaten entschlüsselt und damit den Kopierschutz spurenlos entfernt. Dies ist beispielsweise im Spätsommer 1999 für den DVD-Kopierschutz geschehen, und das notwendige Wissen hat sich völlig unkontrollierbar in wenigen Tagen weltweit unter tausenden von technisch Versierten verbreitet. Es gab intensive rechtliche Bemühungen der DVD-Industrie, die Verbreitung eines in den Medien weithin diskutierten DVD-Entschlüsselungsprogramms („DeCSS“) zu unterdrücken, aber inzwischen existiert eine große Anzahl von unabhängigen Implementierungen dieses Entschlüsselungsverfahrens, einige davon weitgehend unbemerkt als Bestandteil normaler MPEG-Abspielsoftware.

Stärke des Angreifers

Die Sicherheit jeder kryptographischen Anwendung basiert letztendlich auf der physischen Sicherung der geheimen Schlüssel gegen den Zugriff durch Unbefugte. Da verteilte Computersicherheitsmechanismen in der Regel mit kryptographischen Techniken (z.B. Verschlüsselungs- und Signaturalgorithmen) realisiert werden, ist die Aufgabe eines manipulationssicheren Systems in der Regel, geheime Schlüssel zu schützen. Neben den eigentlichen Schlüsseln darf für den Angreifer natürlich auch die Ausführung der kryptographischen Algorithmen nicht beobachtbar sein, da aus dem Ablauf des Algorithmus die Schlüssel offensichtlich wären. Neben diesen primär zu schützenden Daten und Algorithmen kann ein manipulationssicheres System noch weitere Anwendungssoftware und andere Komponenten enthalten, die für die Sicherheit des Gesamtsystems relevant sind.

Die historisch ersten praktischen Überlegungen zum Schutz von geheimen Schlüsseln stammen – wie nicht anders zu erwarten – aus dem militärischen Bereich [31]. So wurden beispielsweise auf Kriegsschiffen die Codebücher zur Chiffrierung geheimer Funkmeldungen mit Gewichten versehen und mit wasserlöslicher Farbe gedruckt, so dass die streng geheimen Informationen bei

einem Überfall durch einfaches Überbordwerfen der Bücher schnell und zuverlässig vernichtet werden konnten. Andere Codebücher wurden auf Papier aus Nitrocellulose (Schießbaumwolle) gedruckt, damit sie im Notfall sekundenschnell rückstandsfrei verbrannt werden konnten. Spätere Beispiele von technisch sehr ausgefeilten manipulationssicheren Systemen aus dem militärischen Bereich sind die Sicherheitsmechanismen in Kernwaffen, die nach einem Diebstahl durch Terroristen das spaltbare Material unbrauchbar machen müssen sowie Sensoren, die zur Überprüfung von Abrüstungs- und Kernwaffenteststopp-Verträgen in anderen Ländern installiert werden [2]. Erst etwa 1985 begannen kommerzielle Computerhersteller (angefangen mit IBM) sich außerhalb militärischer Anwendungen mit Konzepten für manipulationssichere Hardware zu befassen. Die Anforderungen im zivilen Bereich unterscheiden sich dabei erheblich von den in Militärausrüstungen gängigen Verfahren. Kosten spielen eine entscheidende Rolle und pyrotechnische Selbstzerstörungsmechanismen sind im Unterhaltungselektronikbereich nicht akzeptabel.

Bislang werden in kommerziellen Anwendungen im Wesentlichen zwei Ansätze zum Entwurf manipulationssicherer Rechner eingesetzt, die im Folgenden näher erläutert sind.

Einchip-Systeme

Sofern die zu schützende Software nur wenige zehntausend Bytes lang ist, kann sie in nichtflüchtigem Speicher zusammen mit der CPU in einem einzigen Mikrocontroller-Chip untergebracht werden. Masken-ROM ist die kompakteste Speicherform auf einem Chip, aber da die Information durch das Chiplayout festgelegt ist, lässt sich ein ROM mit einem Elektronenmikroskop relativ problemlos auslesen. Selbst wenn die ROM-Bits sich nur durch die Dotierungsmuster unterscheiden lassen, stehen geeignete selektive Ätzverfahren zur Verfügung, um diese sichtbar werden zu lassen [37]. Zudem lassen sich Schlüsseldaten im ROM nicht nachträglich ändern oder löschen. Als nicht-flüchtige Speicher in Einchip-Systemen haben sich vor allem EEPROMs durchgesetzt. Dabei handelt es sich um Feldeffekttransistoren, deren Gate-Eingang völlig von isolierendem Material umgeben ist. Durch eine hohe Programmierspannung kann diesem *floating gate* ein bestimmtes Potential aufgezwungen werden, das dann den Schaltzustand des Transistors über viele Jahre hinweg bestimmt, womit ein Bit abgespeichert wird.

Eine sehr weit verbreitete Anwendungsform von EEPROM-Einchip-Systemen sind Chipkarten [30]. Dabei wird der Mikrocontrollerchip auf ein etwa 1 cm^2 großes dünnes Kunststoffplättchen geklebt, das auf der gegenüberliegenden Seite über meist sechs oder acht Kontaktflächen verfügt. Der Siliziumchip wird mit sehr dünnen Gold- oder Aluminium-Bondingdrähten wie in einem normalen Chipgehäuse mit den Kontaktflächen elektrisch verbunden und anschließend in Epoxid-Harz vergossen. Dieses Chipmodul wird zur besseren Handhabbarkeit in eine größere Kunststoffform integriert, zum Beispiel im ISO-Kreditkartenformat, im Miniaturkartenformat wie es bei GSM-Mobiltelefonen eingesetzt wird, oder in einer Plastikschlüsselform, wie sie bei einigen Pay-TV-Decodern zu finden ist.

Zu den Schwächen und Angriffsmöglichkeiten von Einchip-Systemen finden sich im Abschnitt 3.2 auf Seite 50 weitere Informationen.

Sichere Verpackung ganzer Baugruppen

Das grundlegende Problem von EEPROM-basierten Sicherheitsmodulen besteht darin, dass externe Energie benötigt wird, um die geheimen Daten vernichten zu können. Sobald der Angreifer diese Energiezufuhr unterbricht, sind die Daten gefangen und der Zugriff auf die Daten kann in aller Ruhe durchgeführt werden, ohne dass das Auslösen eines Alarmsystems befürchtet werden muss.

Eine attraktive Lösung besteht darin, die geheimen Daten in batteriegepuffertem statischem RAM (SRAM) unterzubringen. Da nun bereits eine Energiequelle erforderlich ist, um die Daten zu erhalten, kann die selbe Energiequelle auch zum Betrieb von wirkungsvollen Alarmmechanismen genutzt werden, die im Fall eines Eindringens in die Schutzhülle des Sicherheitsmoduls einfach die Stromversorgung des SRAM-Speichers unterbrechen. Der Angreifer kann nicht mehr ohne weiteres die Energiequelle entfernen, ohne dadurch die Daten zu gefährden. CMOS SRAM-Bausteine mit 128 Kilobyte Kapazität sind heute mit Erhaltungsströmen von unter 1 µA erhältlich, was eine kleine Lithiumbatterie problemlos mindestens ein Jahrzehnt zur Verfügung stellen kann.

In [56] wurde erstmals der Entwurf eines SRAM-Sicherheitsmoduls dokumentiert, in dem eine ganze Baugruppe mit einem Prozessor, mehreren Speicher- und Peripheriechips, einer kleinen Alarmschaltung und einer Batterie untergebracht ist. Diese Baugruppe wird auf allen Seiten völlig lückenlos und in mehreren Lagen mit einem 80 µm dünnen isolierten Draht umwickelt. Anschließend wird die so umwickelte Baugruppe in ein hartes Epoxid-Harz eingegossen. In diesem Kunststoff befinden sich Aluminium- und Siliziumflocken. Sie sollen die maschinelle Bearbeitung der Verpackung oder deren Entfernung durch einen UV-Laser ohne Beschädigung der Drahtumwicklung oder deren Isolation wesentlich erschweren. Die Isolation des Wickeldrahtes ist chemisch weniger widerstandsfähig als das Vergussmaterial, so dass bei einem Aufätzversuch mit großer Wahrscheinlichkeit Kurzschlüsse entstehen werden. Eine Schaltung aus Operationsverstärkern vergleicht ständig die Widerstände der beiden langen Drahtschleifen, die um die Baugruppe gewunden wurden. Wenn sich durch eine Unterbrechung oder einen Kurzschluss die Widerstandsverhältnisse deutlich ändern, so wird sofort die Spannungsversorgung der SRAM-Chips mit Masse kurzgeschlossen, so dass die Daten gelöscht werden. Diese Schaltung benötigt nur etwa 20 µA Strom.

Zu den Schwächen und Angriffsmöglichkeiten auf sicher verpackte Baugruppen finden sich im Abschnitt 3.2 auf Seite 52 weitere Informationen.

2.2.4 Sandbox-Verfahren

Sandbox-Verfahren dienen dem Schutz der Ausführungsumgebung und anderer Programme vor bösartigem Programmcode, der meist erst online und zur Laufzeit des Systems bekannt wird. Der Programmcode läuft deshalb zum Schutz innerhalb eines abgesicherten Bereiches – der Sandbox. Sandbox-Verfahren sind heute in allen gängigen Web-Browsern vorinstalliert und dienen zum Schutz des Surfers bzw. seines Rechners vor möglicherweise bösartigen Java-Applets. Allgemeiner formuliert, schützt die Sandbox vor bösartigen Inhalten. Sie muss also bereits auf der Plattform des Nutzers installiert sein und kann nicht erst duch die Inhalte selber bereitgestellt werden.

Die Ausführung fremder Softwareprogramme ist, sofern sie völlig ohne Einschränkungen ausgeführt werden, mit Risiken für die Ausführungsumgebung und andere in der Ausführungsumgebung laufende Programme verbunden. Beispielsweise könnte fehlerhafter oder absichtlich bösartiger Programmcode (malicious code), der von einem Web-Browser geladen und direkt auf dem Betriebssystem zur Ausführung gebracht wird (sog. aktiver Inhalt, beispielsweise ActiveX-Control), mit allen Rechten der Ausführungsumgebung (hier: Web-Browser) arbeiten, d.h. beliebige Dateien lesen, anlegen, meist auch löschen oder verändern. Weiterhin ist es nicht ausgeschlossen, dass ungewollte Interaktionen mit anderen momentan laufenden Programmen stattfinden. So könnte beispielsweise ein legal und kostenpflichtig bezogener Medienstrom unbemerkt vom malicious code „abgezweigt“ und ins Internet eingespeist werden, oder der malicous code kopiert sich die Zugangsdaten, um den Stream anschließend unberechtigt anzufordern.

Die Anforderung, dass eine Ausführungsumgebung sich selbst und die laufenden Anwendungen schützen muss, ist nicht neu. Jedes Betriebssystem ist gewissermaßen eine Ausführungsumgebung und muss selbst über Schutzmechanismen verfügen, etwa die Vergabe von Zugriffsrechten (z.B. Leserecht, Schreibrecht, Ausführungsrecht) und den Speicherschutz, d.h. Programme erhalten vom Betriebssystem zugeteilten Speicher und dürfen nur diesen verändern, andernfalls wird eine Speicherschutzverletzung gemeldet.

Die Schutzmechanismen des Betriebssystems sind jedoch für fremde aktive Inhalte, die möglicherweise erst zur Laufzeit des Systems geladen werden, viel zu grobkörnig und unflexibel.

So mag eine Pay-TV-Anwendung beispielsweise Zugriff auf eine Conditional-Access-Komponente der Set-Top-Box bekommen, ein über das Internet heruntergeladenes und in der Set-Top-Box als Videospiel ausgeführtes Spieleprogramm, das in Wirklichkeit ein trojanisches Pferd ist, mit dem die Encryption Keys des Nutzers unbemerkt ausspioniert werden sollen, darf dagegen keinen Zugriff erlangen. Die Set-Top-Box muss also in Abhängigkeit der Anwendung größtenteils ohne Zutun des Menschen entscheiden, welche Anwendungen welche Rechte erlagen dürfen.

Die Schutzmechanismen des Betriebssystems sind zudem vom Betriebssystem abhängig. Dies widerspricht jedoch dem Trend, aktive Inhalte auf verschiedenen Plattformen betriebssystemunabhängig, aber trotzdem sicher ausführen zu wollen. Deshalb hat man – je nach aktivem Inhalt – Auführungsumgebungen geschaffen, die die Schutzanforderungen betriebssystemunabhängig realisieren.

Sicherheit von Java, Java-Script, ActiveX-Controls und Plug-ins

Im Internet findet man aktive Inhalte in Form von ActiveX-Controls, Java-Applets und Java-Scripts.

Java-Applets werden durch die Ausführungsumgebung – meist als Java Virtual Machine (JVM) bezeichnet – vollständig abgeschottet. Die JVM verfügt über eine ausgefeilte Zugriffskontrolle. So besitzen Java-Applets standardmäßig keinerlei Lese- und Schreibrechte auf dem Rechner, auf dem sie ausgeführt werden. In diesem Sinn wird auch der Begriff Sandbox verwendet, da ein Java-Applet innerhalb des Sandkastens – jedes Applet hat seinen eigenen Sandkasten – beliebige Operationen ausführen darf, aber ihn nicht verlassen kann. Da dies jedoch Einschränkungen bzgl. der realisierbaren Anwendungen mit sich bringen würde (z.B. könnte ein Home-Banking-Applet dann nicht mit der HBCI-Chipkarte kommunizieren), dürfen

Java-Applets, die vom Benutzer als vertrauenswürdig eingestuft wurden, zusätzliche Rechte (Schreib-, Lese-, Ausführungsrechte) anfordern und nach Bestätigung durch den Endbenutzer auch erhalten. Um die Authentizität des Codes (als eine Voraussetzung für die Beurteilung der Vertrauenswürdigkeit des Bereitstellers des Applets) sicherzustellen, können Java-Applets digital signiert sein (code signing). Das Sicherheitsmodell von Java umfasst also eine Public-Key-Infrastruktur (PKI). Die zur Prüfung der Signaturen erforderlichen Zertifikate sind Bestandteil der JVM bzw. der Web-Browser. Da Java eine betriebssystemunabhängige Plattform ist, lassen sich Applets auch auf verschiedenen Rechnern, Devices und Betriebssystemen ausführen, sofern sie die Java-Plattform unterstützen.

Java-Scripts werden im Web-Browser ausgeführt und besitzen aufgrund des geringen Sprachumfangs bei richtig implementiertem und konfiguriertem Browser nahezu keine Möglichkeiten, ernsthaften Schaden anzurichten. In der Vergangenheit wurden allerdings wiederholt Sicherheitslöcher entdeckt, die meist auf Implementierungsfehler im Web-Browser zurückgingen. Beispielsweise bietet Georgi Guninski auf seiner Webseite http://www.guninski.com/ Sicherheitshinweise und Demonstrationen der Schwächen für alle gängigen Browser-Typen an.

ActiveX ist eine von Microsoft entwickelte proprietäre Schnittstellenbeschreibung zur Ausführung von betriebssystemabhängigem Programmcode. ActiveX-Controls werden nur sehr rudimentär in ihren Ausführungsrechten eingeschränkt. Im wesentlichen erhalten sie die betriebssystemabhängig vergebenen Rechte und sind insofern sehr gefährlich, da sie meist ohne Einschränkungen laufen. Der Chaos Computer Club konnte z.B. nachweisen, dass ein bösartiges ActiveX-Control selbständig Homebanking-Funktionen auslösen kann [15].

Multimedia Home Platform

Die Vorteile der Java-Plattform mit ihrer flexiblen Anwendungsgestaltung sollen künftig auch im Bereich interaktive Dienste und digitales Fernsehen genutzt werden. Mit der Multimedia Home Platform (MHP) wurde durch ETSI (European Telecommunications Standards Institute) ein offener Standard für das digitale Fernsehen der Zukunft geschaffen [16].

Mit MHP werden Personal Computer und TV mehr und mehr miteinander verschmelzen. Für den Verbraucher hat MHP den Vorteil, über eine Plattform, d.h. konkret über ein einziges Gerät viele Medien, Dienste und Programme empfangen zu können. Das Gerät wird meist eine Set-Top-Box sein, aber auch der Multimedia-PC ist als Endgerät denkbar.

Das Ziel von MHP ist u.a. die Realisierung von interaktivem Fersehen. MHP unterscheidet drei Profile der Interaktivität:

- Enhanced broadcasting, bei dem kein Rückkanal existiert,
- Interactive broadcasting mit Rückkanal sowie
- Internet access.

Bei den beiden Broadcasting-Profilen werden neben dem Fernsehbild (MPEG-Stream) noch zusätzliche Daten, z.B. sogenannte Xlets, übertragen. Ein Xlet ist im wesentlichen eine spezielle Form von Java-Applet, das in einer Ausführungsumgebung innerhalb einer Sandbox ausgeführt wird. Die Xlets werden dabei über ein „Objektkarussell“ ausgestrahlt, ähnlich dem heutigen Videotext. Die wesentlichen Unterschiede zwischen Xlets und Java-Applets bestehen in

- der Nutzbarkeit speziell für das Fernsehen konzipierter graphischer Bedienelemente, die Halbtransparenz unterstützen, z.B. Textfelder und Knöpfe, die das darunter liegende Fernsehbild nicht völlig verdecken,
- einem reduzierten Umfang an Java-Programmierbibliotheken, um MHP-fähige Geräte nicht unnötig zu verteuern,
- Synchronisationsfunktionen mit MPEG-Stream und Funktionen zu seiner Steuerung und ggf. weiteren Multimediadaten (z.B. Einblendungen)
- einer Conditional-Access-Schnittstelle, die für die Anbindung verschiedener Entschlüsselungssysteme von Pay-TV-Inhalten vorgesehen ist, sodass der Kunde auch tatsächlich viele Kanäle (auch unterschiedlicher Anbieter) mit einem einzigen Gerät empfangen kann.

MHP ist ein offener Standard, der problemlos auch auf einem PC implementiert werden kann. Die Offenheit des Standards legt es nahe, auch Implementierungen mit offengelegten Quelltexten von MHP zuzulassen und zu fördern. Dies würde zur Vermeidung von Programmierfehlern beitragen. In [18] wird beispielsweise der Vorschlag einer Open-Source-Implementierung von MHP gemacht.

Set-Top-Boxen, die MHP implementieren, werden teilweise auf Standardbetriebssystemen implementiert. Neben Windows-Betriebssystemen werden auch Linux sowie spezielle eingebettete Systeme verwendet.

Das Sicherheitsmodell von MHP ist dem von Java sehr ähnlich. Xlets können digital signiert sein und dürfen sich um weitere Rechte bewerben. Unsignierte Xlets dagegen haben nicht auf den vollen Funktionsumfang von MHP Zugriff.

Das insgesamt gut durchdachte Sicherheitsmodell von MHP enthält leider eine Funktionalität, die in der Praxis sehr gefährlich werden kann und die praktische Sicherheit stark reduziert: Das ansonsten konsequent angewendete Sandbox-Prinzip wird durchbrochen durch eine sog. Plug-in-Architektur, die es erlaubt, den Funktionsumfang (bzgl. dekodierbarer Formate) der Set-Top-Box zu erweitern [16, S.35f]. Plug-ins sollen sich jedoch ebenfalls authentisieren, um erweiterten Zugriff auf MHP-Komponenten zu bekommen. Genauere Informationen hierzu enthält der MHP-Standard nicht, man kann jedoch davon ausgehen, dass die Sicherheitsrisiken im schlimmsten Fall denen der Anwendung von Browser-Plug-ins oder ActiveX entsprechen und somit im Einzelfall ein ernstes Sicherheitsproblem darstellen können.

2.3 Spezielle DRM-Techniken

Neben den grundsätzlichen Sicherheitsmechanismen entstanden auf die Schutzziele von DRM-Systemen abgestimmte Sicherheitsmechanismen. Im Folgenden werden

- Modifikation des analogen Endsignals,
- Watermarking und
- Fingerprinting

behandelt.

2.3.1 Modifikation des analogen Endsignals

Selbst wenn die Entschlüsselung, Dekompression und Analogwandlung des Audio- oder Videosignals in einer manipulationssicher geschlossenen Einheit stattfindet, so steht dem Kopierer immer noch ein hochwertiges Analogsignal zur Verfügung, das sich wiederum Digitalisieren und Komprimieren lässt. Dieser Vorgang muss nur ein einziges Mal durchgeführt werden. Alle weiteren Kopien können völlig ungeschützt und digital vorgenommen werden. Das qualitativ hochwertige Anzapfen und Wandeln eines Analogsignals erfordert gewisse technische Sorgfalt, insbesondere wenn das Analogsignal bewusst nicht in einer gängigen Form zur Verfügung steht.

Allerdings sind entsprechende Adapterschaltungen von jedem elektronisch geschulten Techniker vergleichsweise leicht aus Standardkomponenten herzustellen. Immerhin wäre es möglich, wenigstens die Rückwandlung des Analogsignals durch Laien zu verhindern, indem keine externen Steckverbinder mit Analogsignalen vorgesehen werden und die Entschlüsselung und Analogwandlung in der Nähe von schwer zugänglichen Komponenten, etwa dem Hochspannungsteil eines Videomonitors oder in einem in den Lautsprecher oder Kopfhörer integrierten Baustein, durchgeführt wird. Viele Kunden werden aber durch die resultierende Inkompatibilität mit anderer Unterhaltungselektronik enttäuscht sein, da diese Einschränkungen der systemintegrierenden Grundidee des Multimedia-Gedanken zuwiderlaufen.

Im Falle von Flachbildschirmen als Wiedergabemedium ist es jedoch technisch praktikabel, die Entschlüsselung und die Bildausgabe so eng miteinander zu verbinden, dass sich selbst technische Experten einem erheblichen Aufwand gegenüber sehen, da Flachbildschirme mit hochgradig parallelen Ansteuersignalen arbeiten, es also im Gerät bei sorgfältig integrierter Entschlüsselungsfunktion keine einfach anzapfbare Analogform des Bildsignals gibt, wie dies bei Kathodenstrahlröhren der Fall ist.

Modifikationen des analogen Endsignals können auch dem Zwecke dienen, eine „Entdekomprimierung“ zu erschweren. Wärend bei einer normalen Komprimierung von audiovisuellen Daten immer Information verloren geht, besteht bei manchen Kompressionsverfahren die Möglichkeit, mit dem Wissen, dass ein analoges Signal durch einen exakt bekannten Dekompressionsalgorithmus aus unbekannten komprimierten Daten entstanden ist, diese komprimierte Form nahezu exakt zu rekonstruieren. Dadurch kann eine sorgfältige „Entdekomprimierung“ mit einer wesentlich geringeren Qualitätseinbuße verbunden sein als die erneute Anwendung des ursprünglichen Kompressionsalgorithmus. Die genauen Möglichkeiten und Grenzen der Entdekomprimierung sind bislang noch nicht hinreichend untersucht worden, aber neben der noch ausstehenden gezielten Entwicklung von Dekompressionsverfahren, die gegen diese Technik geschützt sind, besteht auch die Möglichkeit, durch Filterung und Addition eines kleinen Rauschsignals Entdekompressionsversuche zu erschweren.

Macrovision

Ein weiteres Beispiel für eine Modifikation des analogen Endsignals ist das Video-Kopierschutzsystem der kalifornischen Firma Macrovision [42, 46]. Dieses System nutzt die Tatsache aus, dass die Elektronik am Videoeingang von Fernsehern und VHS-Videorekordern unterschiedlich auf analoge Videosignale reagiert, welche die Fernsehnorm verletzen. Im Gegensatz zu Fernsehempfängern verfügen VHS-Videorekorder über eine automatische Pegelsteuerung, die in der Lage ist, Spannungsschwankungen im Eingangssignal automatisch auszuglei-

chen. Vorbespielte Videokassetten, die unter Verwendung des Macrovision-Kopierschutzes hergestellt wurden, enthalten in der Austastlücke (einem Teil des Bildsignals, der auf normalen Fernsehgeräten nicht sichtbar ist) Bereiche, in denen Spannungen außerhalb des normalen Helligkeitsbereiches auftauchen. Die automatische Pegelkontrolle in einem aufzeichnenden VHS-Heimrekorder reagiert auf diese Überspannungen durch Herunterregeln der Verstärkung, wodurch das beim Kopieren vom Rekorder aufgenommene Bild insgesamt dunkler wird. Da die Überspannungen ständig wechseln, springt die Helligkeit des aufgezeichneten Videosignals, was zu einer erheblich verschlechterten Widergabequalität des kopierten Videos führt.

Die Pegelsteuerung des Videosignals ist nicht zwingend erforderlich und nur sehr wenige Techniken zur Pegelsteuerung lassen sich durch das Macrovision-Verfahren so stark irritieren, dass es zu Problemen bei der Bildaufzeichnung kommt. Aus diesem Grund hat die japanische Firma JVC, die Lizenzgeberin für das heute dominierende analoge Heimvideoformat VHS ist, vor einiger Zeit die Lizenzbedingungen für Hersteller so geändert, dass eine bestimmte für Macrovision besonders empfindliche Pegelsteuertechnik für alle VHS-Videorekorder zwingend vorgeschrieben ist.

Der Macrovision Kopierschutz lässt sich technisch vergleichsweise einfach auf verschiedene Arten umgehen. Eine Möglichkeit ist die Deaktivierung der Pegelsteuerung im aufzeichnenden Videorekorder, was insbesondere bei älteren Geräten oft durch Austausch eines einzigen elektronischen Bauteils möglich ist. Eine weitere Möglichkeit sind externe Filterschaltkreise die zwischen den wiedergebenden und aufnehmenden Rekorder geschaltet werden. Sie lassen die sichtbaren Bildbestandteile eines Videosignals ungehindert passieren, aber die Synchronisationspulse und anderen Signale in der Austastlücke werden neu und somit frei von Überspannungen erzeugt. Die meisten Elektroniker mit guten Videotechnikkenntnissen werden kaum mehr als eine Woche benötigen, um durch Beobachtung des Videosignals mit einem Oszilloskop das Macrovision-Prinzip zu verstehen und eine einfache Version einer derartigen Kopierfilterschaltung zu entwickeln, die mit Hilfe von elektronischen Bauelementen realisiert werden kann. Solche Bauelemente finden auch in jedem Fernsehgerät Verwendung, sind in Bastelläden erhältlich und kosten insgesamt weniger als 50 EUR. Zahlreiche Beschreibungen von Macrovision-Filterschaltungen in Elektronikmagazinen und Internet-Seiten belegen dies.

Derartige Filterschaltungen waren auch einige Zeit kommerziell verfügbar, allerdings hat die Firma Macrovision sorgfällig fast jede denkbare Bauform schon vor Einführung des Systems patentieren lassen, und konnte somit den kommerziellen Vertrieb dieser Produkte recht erfolgreich mit rechtlichen Mitteln einschränken. Allerdings existiert eine Reihe von völlig legitimen Videotechnik-Produkten, die nicht speziell als Macrovision Kopierschutzfilter entwickelt wurden, die aber dennoch die Synchronpulse regenerieren und somit ganz nebenbei auch den Macrovision-Schutz vollständig entfernen. Dazu gehören zum Beispiel verschiedene Videoschnitt-Graphikkarten für PCs, professionelle Videoausrüstung zum Verbessern der Signalqualität in Videostudios (*time base correctors*), sowie verschiedene Videoeffekt-Geräte und Videorekorder, die nicht mit dem VHS-Standard arbeiten. Auch wenn das Macrovision System eine gewisse Hemmschwelle für den elektronisch unversierten Endkunden darstellt und verhindert, dass nur mittels einfachen Verbindens zweier Heimrekorder gute Kopien erstellt werden könnten, so lässt sich die Technik doch mit etwas Sachverstand und einer geringfügigen Investition mühelos umgehen.

Macrovision wird heute nicht nur in vorbespielten Videokassetten zum Verleih oder Verkauf eingesetzt, sondern auch in DVD-Abspielgeräten und Pay-TV-Zugriffskontrollsystemen. Bei

diesen findet nach Möglichkeit die Entschlüsselung, Dekompression, digital/analog-Wandelung und das Einfügen der Macrovision-Schutzimpulse in einem einzigen manipulationssicher gekapselten integrierten Baustein statt. Die Vertriebsfirma fügt dem komprimierten digitalen Videosignal vor der Verschlüsselung Steuerinformationen bei, die im Abspielgerät nach der Dekompression die Hinzufügung der Fernsehnorm-verletzenden Überspannungen auslösen. Somit lässt sich die Anfertigung von analogen Kopien mit einem Heimrekorder auch vom Analogausgang eines DVD-Players oder einer pay-per-view Set-Top-Box für ausgewähltes Material erschweren.

2.3.2 Watermarking zur Detektion von übertragenen Inhalten und zum Schutz vor Verfälschung

Beim Watermarking werden in digitale Mediendaten Informationen z.B. über den Urheber der Daten eingebettet. Die mit dem Original fest verbundene, eingebettete Information wird als Watermark bezeichnet (Abbildung 2.4). Dieser Einbettungsprozess muss so robust erfolgen, dass es unmöglich ist, das Watermark unberechtigt zu entfernen, wenn der Angreifer versucht, das Objekt zu manipulieren. Dabei sind viele verschiedene Manipulationen denkbar: Analog-Digital-Wandlung, Digital-Analog-Wandlung, Ausdrucken und erneutes Einscannen, Verändern von Größe, Auflösung, Abspielgeschwindigkeit, Farbtiefe, Kompression, Verzerrung, Ausschneiden von Bildteilen.

Es ist klar, dass das Watermark möglichst so in das digitale Objekt eingebracht werden muss, dass es nicht zu Beeinträchtigungen des Dokumentes kommt. So sollten Watermarks in Grafiken bzw. Videos nicht sichtbar, in Sounddateien nicht hörbar sein. Insofern sind die Watermarking-Verfahren verwandt mit der Steganographie [19, 44], wo versucht wird, geheime Daten unbemerkt und damit vertraulich in Hülldaten (z.B. Bilder, Musik) einzubetten.

Gegenwärtige Watermarkingtechniken arbeiten bevorzugt im Frequenzbereich (neben Raum- und Zeitbereich), den die digitalen Objekte abdecken [12, 54, 57]. Dazu werden sog. Spread Spectrum Techniken eingesetzt. Die Einbettung muss dabei auch in die Datenteile erfolgen, die auch nach einer verlustbehafteten Kompression, die nicht wahrnehmbare oder redundante Daten entfernt, noch vorhanden sind.

Die Information, die das Watermark trägt, ist vom Einsatzzweck (Urheberrechts- oder Eigentumsrechtsschutz) und der zur Verfügung stehenden Infrastruktur abhängig. Das kann z.B. eine Dokument-ID sein oder der Name des Autors.

Ein praktisches Anwendungsbeispiel für watermarkierte Ton- und Videodaten ist das automatisierte Erstellen von Distributionsprotokollen beim Webcasting: Ein Scanner, der z.B. von einer Verwertungsgesellschaft betrieben wird, analysiert die gesendeten Daten z.B. eines Webradios nach eingebetteten Watermarks, um anschließend die Rechte des Künstlers wahrnehmen zu können, Hitlisten zu erstellen etc.

Watermarking-Systeme besitzen neben der hier beschriebenen technischen Komponente auch eine organisatorische. Jedes digitale Objekt muss vor der Distribution in einer vertrauenswürdigen Registrierungsstelle gemeldet sein, damit zweifelsfrei nachvollziehbar ist, wer der Urheber eines Inhaltes ist. Da technisch nicht verhinderbar ist, dass ein bereits markierter Inhalt erneut markiert wird, muss der tatsächliche Urheber den Zeitpunkt seiner Markierung nachweisen können. Alternativ zur Registrierung kann auch ein von einer vertrauenswürdigen Stelle

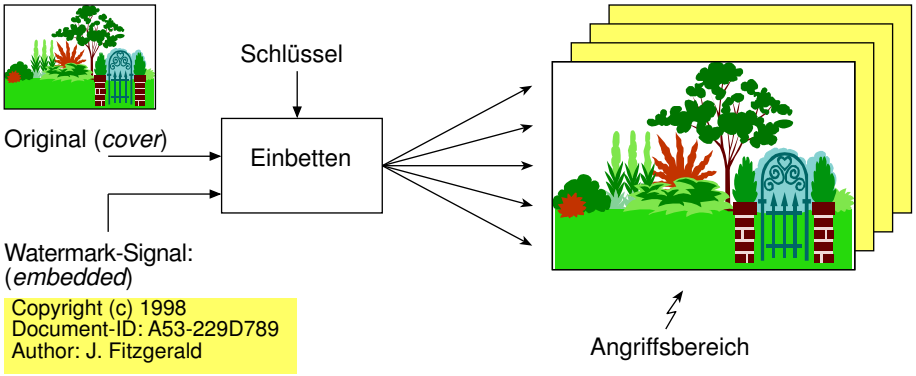

Abbildung 2.4: Distribution eines markierten digitalen Objekts

digital signiertes (und damit authentisches) Datum-Uhrzeit-digitales-Objekt-Kennzeichen Teil der einzubettenden Information sein. Da digitale Signaturen heute mehrere hundert bis einige tausend Bit einnehmen können, ist dies jedoch nicht in jedem Fall realisierbar, und um eine vertrauenswürdige dritte Stelle kommt man ebenfalls nicht herum.

Informationen zum momentan erreichbaren Sicherheitsniveau von Watermarking-Systemen finden sich in Abschnitt 3.3.

2.3.3 Fingerprinting zum Verhindern der nicht verfolgbaren Weitergabe von Inhalten

Sofern das Kopieren von Inhalten nicht verhindert werden kann, möchte man wenigstens abschreckende Maßnahmen ergreifen, die das unberechtigte Kopieren von Inhalten erkennbar und verfolgbar machen.

Kennzeichnung des Inhalts

Beim Fingerprinting werden in digitale Mediendaten Informationen über den Käufer eingebettet. Der Anbieter kennzeichnet jede verkaufte Kopie durch kleine Änderungen so, dass später beim Auffinden einer Raubkopie der ursprüngliche Käufer festgestellt werden kann. Dieses kundenindividuelle Watermarking wird *Fingerprinting* genannt. Fingerprinting-Verfahren werden u.a. in [7, 8, 17, 45, 50] vorgestellt.

Da nun mehrere Repräsentationen der Daten entstehen, die sich jeweils genau durch den Fingerprint unterscheiden, ergibt sich folgende Zusatzforderung: Ein Angreifer soll selbst dann nicht in der Lage sein, den Fingerprint zu entfernen, wenn er im Besitz mehrerer Kopien eines markierten Inhaltes ist (Kollusionsresistenz).

Die Anzahl der notwendigen Kopien zum Entfernen des Fingerprints bzw. zum Bilden eines anderen (entweder eines neuen oder einem anderen Käufer zugeordneten) Fingerprints wird als Kollusionsresistenz bezeichnet. Mit steigender Kollusionsresistenz wächst allerdings auch der Einbettungsaufwand der Verfahren.

Durch sog. asymmetrisches Fingerprinting [50] kann zusätzlich sichergestellt werden, dass der Anbieter des Medienstroms keine gefälschten „Beweise“ erzeugen kann.

Kennzeichnung des Schlüssels

Eine Sonderform des Fingerprinting ist die Schlüsselkennzeichnung. Sie wird angewendet, wenn die Verteilung von individuell markierten Inhalten zu aufwendig oder nicht möglich ist, z.B. auf Datenträgern (CD, DVD) oder beim Broadcasting (z.B. Pay-TV). Alle Kunden erhalten so gleiche digitale Daten.

Um die unberechtigte Nutzung der Inhalte durch Aussenstehende von vorn herein auszuschließen, werden die Inhalte verschlüsselt übertragen. Nun könnte jeder Kunde den Entschlüsselungsschlüssel in einem vor Ausforschung physisch sicheren Gerät (z.B. einer Chipkarte oder einem gekapselten Player) erhalten, um zu verhindern, dass er den Schlüssel unberechtigt weitergibt. Physischer Schutz gelingt jedoch bestenfalls für eine beschränkte Zeit, da immer wieder einmal neue Methoden zum unberechtigten „Auslesen“ von geheimen Informationen z.B. aus Chipkarten gefunden werden.

Besser wäre es also, wenn jeder Kunde einen eigenen individuellen Schlüssel zur Entschlüsselung des Medienstroms bekäme. Ein Verschlüsselungsverfahren, mit dem es möglich ist, einen einzigen verschlüsselten Medienstrom an alle Empfänger zu senden, der dann mit mehreren individuellen Schlüsseln entschlüsselt wird, wird als Gruppenverschlüsselung (auch: Broadcast Encryption) bezeichnet (Abbildung 2.5).

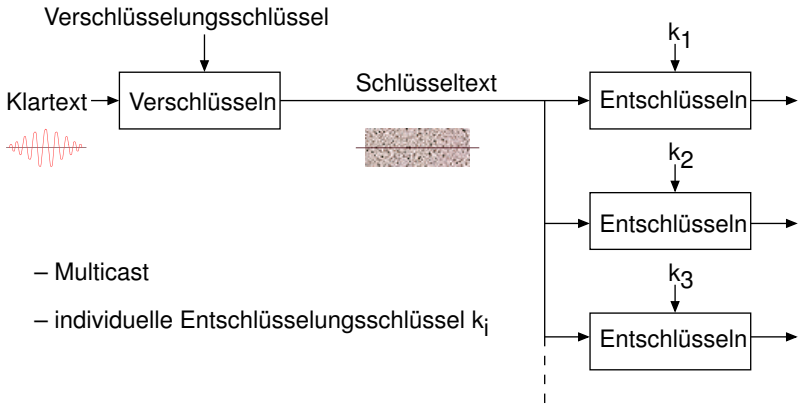

Abbildung 2.5: Gruppenverschlüsselung

Taucht ein Entschlüsselungsschlüssel illegal im Internet auf, kann der legale Besitzer ermittelt und ggf. verantwortlich gemacht werden für die unberechtigte Veröffentlichung des Schlüssels. Dieser Prozess der Rückverfolgung (Traitor Tracing) gelingt jedoch nur, wenn gespeichert wurde, welcher Kunde welchen Schlüssel erhalten hat. Zur Identifizierung des legalen Besitzers wird dann nicht der digitale Inhalt, sondern der Entschlüsselungsschlüssel mit einem Fingerprint versehen.

Zur eigentlichen Entschlüsselung des Medienstroms erhält der Kunde vom Anbieter den Schlüssel und weitere Berechnungsdaten, mit denen er den augenblicklichen Entschlüsselungsschlüssel berechnen kann.

Es muss verhindert werden, dass besonders böswillige Kunden, die sich gleich mehrere Schlüssel legal besorgen, aus ihnen einen neuen Schlüssel berechnen können. In diesem Fall wäre die Rückverfolgung entweder erfolglos (d.h. es wurde ein Schlüssel berechnet, der nicht

registriert ist) oder ein Kunde wird fälschlich beschuldigt (d.h. der berechnete Schlüssel ist identisch mit dem eines anderen Kunden).

Schlüsselmarkierung ist vor allem dort sinnvoll, wo der Wert der Daten im Vergleich zu den Kosten für die Verteilung relativ gering ist: Ein Pirat könnte einen Medienstrom mit einem legal erworbenen Schlüssel entschlüsseln und erneut (illegal und unverschlüsselt) verteilen, da die Inhalte selbst keine Rückschlüsse auf den Piraten zulassen [50].

Konkrete Verfahren für Schlüsselkennzeichnung werden beispielsweise in [10, 25, 48, 49] vorgeschlagen.

Kollusionsresistenz

Insbesondere Fingerprinting-Verfahren aber auch Watermarking-Verfahren (Abschnitt 2.3.2) und zum Teil kryptographische Verfahren generell (Abschnitt 2.2.1) müssen sicher gegen sog. Collusion Attacks sein. Ziel des Angreifers ist es,

- aus mehreren, individuell für verschiedene Konsumenten hergestellten Kopien des gleichen Inhalts diejenigen Stellen des Inhalts zu ermitteln, an denen ein rückverfolgbares Kennzeichen eingebracht wurde, oder
- aus mehreren zur Entschlüsselung desselben Inhalts geeigneten Schlüsseln einen neuen Schlüssel zu berechnen, der dann nicht mehr zurückverfolgbar ist.

Gute Fingerprinting-Verfahren halten in der Regel solchen gemeinschaftlichen Angriffen bis zu einem gewissen Grad (Kollusionsresistenz, Anzahl verfügbarer Kopien) stand. Diese Aussage bezieht sich natürlich nur auf Angriffe, die nicht auf die Watermarking-Eigenschaft jedes Fingerprints gerichtet sind: Fingerprinting kann nie sicherer sein als Watermarking.

Fingerprinting zur Detektion von Inhalten

Neben dem oben erläuterten Begriffsverständnis von Fingerprinting, das auf das *Einbringen* eines Fingerabdrucks des Käufers in den Inhalt zielt, existiert noch ein weiteres: Jeder Inhalt besitzt in sich eine einzigartige Charakteristik, die es möglich macht, ihn zu erkennen und von anderen zu unterscheiden. Dabei geht es weniger um Sicherheitseigenschaften, sondern um das automatisierte Erkennen von Strukturen. Der Inhalt selbst wird dabei nicht verändert.

Seit Jahren forscht man, um die Erkennungsrate und -geschwindigkeit solcher Verfahren zu verbessern. Ein Beispiel für eine solche Detektionstechnik ist AudioID, die am Fraunhofer Institut für Integrierte Schaltkreise (IIS-A) entwickelt wurde (http://golem.de/0201/17862.html). Um ein bekanntes Musikstück eindeutig identifizieren zu können, sollen nur wenige Sekunden Musikmaterial ausreichen. Über sogenannte Spektralflachheitseigenschaften einzelner Frequenzbänder des Musikstücks, die verglichen werden mit einer Datenbank, die die Fingerabdrücke aller detektierbaren Musikstücke enthält, wird das Musikstück erkannt.

Hier zeigt sich ein wesentlicher Unterschied zu Watermarking-Verfahren: Ein in den Inhalt eingebettetes Watermark enthält Daten (beispielsweise den Namen und Interpreten des Musikstücks), die durch den Extraktionsalgorithmus ausgelesen werden können und sofort, d.h. ohne zusätzliche Online-Verbindung zu einer Datenbank, zur Verfügung stehen.

Solche Fingerprinting-Techniken eignen sich beispielsweise zum Erstellen automatisierter Sendelisten von Rundfunk- und Fernsehsendungen. Als Detektionsmittel zum Aufspühren (Abschnitt 2.4.5) illegaler Angebote und anschließenden Filtern (2.4.6) sind sie bedingt geeignet. Auch zur Rückverfolgung (Traitor Tracing) eignen sie sich nicht.

2.4 Schwache Mechanismen

Neben den Kerntechniken, die in den vorangegangenen Abschnitten beschrieben wurden, existieren noch Mechanismen, die auch einen gewissen Schutz der Inhalte gegen unberechtigte Nutzung bieten. Im sicherheitstechnischen Sinn zählen sie aber nicht zu den Mechanismen, die gegen entschlossene, intelligente Angreifer schützen.

Diese „schwachen Mechanismen“ wirken somit bestenfalls unterstützend und vor allem gegen „unbedarfte Angriffsversuche“.

2.4.1 Einbringen von Codes ohne besondere Sicherung

Gerade in der Anfangszeit digitaler Kopierschutztechniken wurden entsprechende Codes in Inhalte eingebracht, die anzeigen sollen, welche Nutzungsrechte mit dem Inhalt verbunden sind. Aus dem Softwarebereich sind solche „Freischaltcodes“ seit langem bekannt. Leider können diese Codes leicht weitergegeben werden und im Internet wimmelt es nur so von Webseiten, die solche Registration Codes enthalten.

Solange diese Codes nicht so fest mit dem Inhalt selbst verbunden sind, dass der Inhalt nur mit dem entsprechenden Code nutzbar ist, sind solche einfachen Systeme leicht zu umgehen, was nachfolgend am Beispiel des Serial Copy Management Systems (SCMS) gezeigt werden soll. Ein ähnlich einfacher Mechanismus, den man ebenfalls unter die hier behandelte Kategorie zählen kann, ist der analoge Kopierschutzmechanismus von Macrovision (siehe Abschnitt 2.3.1).

Beispiel Serial Copy Management System

Eines der ersten digitalen Kopierschutzsysteme ist das Serial Copy Management System (SCMS), das im Jahre 1990 für den digitalen Home-Audio-Bereich auf Initiative der RIAA (Recoding Industry Association of America) eingeführt wurde.

Jeder digitale Audio-Recorder, d.h. momentan CD-R-Audio, MiniDisc (MD), Digital Audio Tape (DAT), der über einen digitalen SPDIF-Ausgang (Sony Philips Digital Interface) verfügt, muss auch SCMS implementieren.

SCMS-geschützte Inhalte enthalten alle 75 Datenblöcke (Frames) ein Kopierschutzbit, das entweder dauerhaft eingeschaltet, ausgeschaltet oder abwechselnd ein- und ausgeschaltet wird. In SCMS können demnach drei Situationen unterschieden werden:

1. **Frei kopierbare Inhalte:** Hier ist das Kopierschutzbit im Original dauerhaft ausgeschaltet, und die Inhalte können ohne Restriktionen kopiert werden. Das Kopierschutzbit der Kopie ist ebenfalls dauerhaft ausgeschaltet, so dass von der Kopie wieder Kopien angefertigt werden können.

2. **Einmal kopierbare Inhalte:** Hier ist das Kopierschutzbit im Original dauerhaft eingeschaltet. Eine von diesem Original angefertigte Kopie verändert das Kopierschutzbit so, dass es abwechselnd ein- und ausgeschaltet ist.

3. **Nicht kopierbare Inhalte:** Empfängt ein mit SCMS ausgestatteter Audio-Recorder Inhalte mit sich wechselndem Kopierschutzbit, verweigert er das Anfertigen einer Kopie.

SCMS kann in der Praxis leicht umgangen werden.

- Da Inhalte auf Audio-CD mit dem CD-Brenner eines PCs kopierbar sind, kann man selbst von einer Kopie mit sich wechselndem Kopierschutzbit weitere Kopien anfertigen. Die auf der CD vorhandenen Daten werden beim Brennvorgang nicht ausgewertet, sondern einfach 1:1 kopiert, womit der Inhalt des Kopierschutzbits für den Kopiererfolg unbedeutend ist.

- Einige Audio-Recorder (insb. solche für den professionellen und semiprofessionellen Bereich) werten das SCMS-Kopierschutzbit auf Wunsch des Nutzers nicht aus bzw. setzen es nach Bedarf.

  Unter http://www.american-digital.com/prodsite/product.asp?p=112&c=15 findet man beispielsweise die Produktbeschreibung des Marantz CDR631. Dort steht „SELECTABLE COPY PROTECTION: Bypass SCMS copy protection when duplicating a disc. Or set your own copy protection at the level you decide.“

- Am Markt sind Konverter erhältlich, die in den Signalweg zwischen Player und Recorder geschaltet werden und das SCMS-Kopierschutzbit nach Wunsch setzen.

  Unter http://www.midiman.net/products/m-audio/co3a.php wird beispielsweise ein „Coaxial, Optical AES/EBU Converter“ beschrieben. Zu SCMS steht dort: „Control over SCMS. If you use Minidisc technology, you probably know that your discs are encoded with SCMS (Serial Copy Management System), a kind of copy protection that prevents the data from being digitally copied. The CO3 gives you control over SCMS, enabling you to adjust those bits in the data stream to fit your needs.“

2.4.2 Regionale Kodierung

DVD-Medien und die zugehörigen Abspielgeräte besitzen Funktionen zur Auswertung eines sog. „Ländercode“, der der künstliche Marktseparation dient. In die Player-Hardware ist ein Schutzmechanismus integriert, der das Entschlüsseln verschlüsselter DVDs nur dann ermöglicht, wenn das Abspielgerät einen passenden Ländercode besitzt. Die Hersteller von DVD-Spielern haben meist das Ändern dieser Ländercodes vorgesehen, aber das Wechseln des Ländercodes auf eine maximale Anzahl begrenzt.

Hiermit bezweckt man, dass Inhalte, die in einem anderen Land oder Erdteil früher als in anderen auf den Markt kommen, nicht vorzeitig in anderen Ländern verbreitet werden. Da das Preisgefüge von Land zu Land sehr unterschiedlich sein kann (DVDs sind in den USA im Mittel etwa 30 Prozent günstiger als in Europa), will man die durch Export und Niedrigpreise entstehenden „Verluste“ begrenzen.

Einige Abspielgeräte besitzen jedoch Funktionen, mit denen man die Firmware des DVD-Spielers patchen kann, so dass der Ländercode (zwar umständlich), aber beliebig oft geändert werden kann. Entsprechende Software kann im Internet kostenlos heruntergeladen werden. Teilweise werden auch Geräte verkauft, die den Ländercode überhaupt nicht auswerten. Entsprechende Gerätelisten findet man in Internet beispielsweise unter http://www.zonefreedvd.com/ und http://www.codefreedvdplayers.com/.

Insofern schützt der Ländercode nicht perfekt und schon gar nicht vor ernsthaften „Knackversuchen“, Gelegenheitstäter werden jedoch abgeschreckt. Im Übrigen führt der Preisverfall bei Player-Hardware dazu, dass man sich künftig mehrere Abspielgeräte (oder Laufwerke im PC) leisten können wird.

2.4.3 Nichtkompatible Medien

Die für jedermann leichte und ohne Qualitätsverlust mögliche Kopierbarkeit der Audio-CD ist in erster Linie darauf zurückzuführen, dass in der Form von CD-ROM-Laufwerken heute billigste Audio-CD-Abspielgeräte vorliegen, mit deren Hilfe PC-Software direkt auf die digitalen Rohdaten des Mediums zugreifen kann. Dieses Problem könnte auf den ersten Blick dadurch umgangen werden, dass die Industrie sich darauf einigt, grundsätzlich ausschließlich physikalisch völlig inkompatible Medien für das Abspielen urheberrechtlich geschützter geistiger Werke auf der einen Seite und als Speichermedien für Universalcomputer auf der anderen Seite zu verwenden. Die Einhaltung derartiger Absprachen könnte ggf. in Form von entsprechenden Lizenzbedingungen für die der Speichertechnologie zugrunde liegenden Patente mit existierenden rechtlichen Mitteln gesichert werden.

Dieser Ansatz widerspricht natürlich völlig dem Ziel und Anspruch der Multimedia-Idee, demzufolge für den Konsumenten erhebliche neue und attraktive Möglichkeiten gerade durch die Integration aller verfügbaren Medien mit den flexiblen Softwaremöglichkeiten eines Universalcomputers (PC) entstehen. Nichtkompatible Medien bieten natürlich auch keine Schutzlösung für PC-Software, da diese immer in einem für den Computer lesbaren Format ausgeliefert werden muss.

2.4.4 Ausnutzung historischer Inkompatibilitäten

Angesichts des großen Interesses der Musikverlage, den Austausch komprimierter Musik-CDs über das Internet zu erschweren, wurden von zahlreichen Unternehmen verschiedene Schutztechniken für das existierende CD-System ersonnen (siehe z.B. [33]). Alle diese Verfahren basieren auf historisch bedingten kleinen Unterschieden im Verhalten von CD-ROM-Laufwerken in Computern und Audio-CD-Spielern. CD-ROM-Laufwerke sind in der Regel mit moderner Software ausgestattet und unterstützen mehr Kodieralternativen als die oft wesentlich älteren und einfacheren integrierten Schaltungen in Audio-CD-Spielern. Audio-CDs, die unter Anwendung dieser Schutzsystemen hergestellt wurden, verletzen gezielt die Spezifikation des CD-Standards in einer Art und Weise, welche von einfachen Abspielgeräten ignoriert wird, aber in Computerlaufwerken zu Fehlfunktionen führt. Beispiele dafür sind bestimmte sehr gezielt eingebrachte Bitfehler im Audiodatenstrom oder verwirrende Eintragungen in den Inhaltsverzeichnisdaten oder Zeitmarkierungen der CD.

Diese Techniken sind mit einer Reihe von Risiken verbunden. Zum einen erwartet ein Kunde, der eine Audio-CD erwirbt, natürlich, dass es sich dabei um ein korrekt der CD-Spezifikation entsprechendes Produkt handelt, und nicht um ein „gepanschtes“ Medium. Das Abspielen einer Audio-CD auf einem CD-ROM-Laufwerk ist ja für sich eine durchaus legitime Nutzung des Produktes, weshalb diese Art von Kopierschutz durch künstlich provozierte Inkompatibilität als Produktmangel gewertet werden und mit den entsprechenden Verbraucherschutzrechten angegangen werden kann. Auch lässt sich eine Unterscheidung zwischen CD-ROM-Laufwerken und Audio-CD-Abspielgeräten nicht immer klar und ohne Ausnahmen durchführen, da heute beide Arten von Geräten nicht selten auf den gleichen Schaltkreisen beruhen, weshalb der Kopierschutz auch die Käufer einiger neuerer reiner Audio-CD-Abspielgeräte treffen könnte. Aus diesem Grund werden gezielte Verletzungen des CD-Standards von Musikverlagen bislang nur in kleinen Pilotversuchen getestet.

Hinzu kommt noch, dass mit speziellen Programmen, die auf das „Clonen“ (Vervielfältigen eines Datenträgers inkl. etwaiger Fehlerstellen) spezialisiert sind, meist doch Kopien angefertigt werden können. Weitere Informationen zu Kopiervorrichtungen finden sich in Abschnitt 3.6.1.

2.4.5 Aufspüren von illegalen Inhalten

Soweit möglich, sollten die Schutzmechanismen Urheberrechtsverletzungen von vornherein verhindern. Da dies nicht perfekt möglich ist, wird es in der Praxis doch zu Piraterie und illegalem Angebot fremder Inhalte kommen. Im Folgenden werden Möglichkeiten zum Aufspüren und Verfolgen solcher Urheberrechtsverletzungen skizziert, bewertet und ihre Grenzen aufgezeigt. Die geschilderten Techniken (sowohl zum Aufspüren als auch zum Schutz davor) kommen ebenfalls bei anderen Tatbeständen (z.B. Aufspüren und Verfolgen von Kinderpornographie) zum Einsatz.

Die Tatsache, dass digitale Inhalte verlustfrei kopierbar sind, kann man sich zunutze machen: Jeder unveränderte Inhalt besitzt exakt das gleiche Bitmuster wie sein Original. Deshalb genügt eine einfache Vergleichsoperation über alle Inhalte auf Webservern, Datenbanken, File-Sharing-Systemen etc., um illegal abrufbare fremde Inhalte aufzuspüren. Hierzu verwendet man einen Scanner, der die erreichbaren Inhalte analysiert. Im Internet (hier: World Wide Web) könnte ein solcher Scanner z.B. in Kombination mit einer Suchmaschine (Web-Robot) betrieben werden, die ohnehin jeden erreichbaren Inhalt abruft und analysiert, in diesem Fall proaktiv, d.h. ohne konkreten Verdacht, dass tatsächlich eine Rechtsverletzung vorliegt.

In der Praxis gelten natürlich ein paar Einschränkungen bzgl. des erreichbaren Schutzes durch Scannen:

- Sollen die illegalen Inhalte nicht öffentlich, sondern illegal in einer geschlossenen Benutzergruppe angeboten werden, kann sie der Pirat verschlüsseln und sie somit vollständig vor dem Aufspüren schützen.
- Es ist möglich, das wahre Datenformat eines Inhalts unkenntlich zu machen (z.B. durch so simple Methoden wie Umbenennen einer Dateiendung von .mp3 zu .txt oder durch Entfernen von Headerinformation innerhalb der Datei), sodass der Scanner sie als nicht relevant einstuft. Hintergrund ist die Tatsache, dass der Scanner wegen des riesigen Datenvolumens zur Optimierung der Suchleistung nur nach typischen Dateitypen, z.B. Vi-

deos (.avi, .mov), Musik (.wav, .mp3), Bilder (.jpg) suchen wird. Hier hilft nur, alle Dateitypen nach den aufzuspürenden Bitmustern zu durchsuchen.

- Medienformate können (teilweise verlustfrei, teilweise verlustbehaftet) ineinander überführt werden, z.B. das Bildformat JPEG (.jpg) in das Format Portable Network Graphics (.png). Bei der vorhandenen Fülle an Medienformaten und Kodierverfahren müsste dann nach jedem möglichen Zielformat gesucht werden, was zu einer kombinatorischen Explosion der Möglichkeiten führt.

- Inhalte können neu digitalisiert werden, was aufgrund des stets vorhandenen Quantisierungsrauschens zu stochastischen Unterschieden zwischen Original und Kopie führen wird und nur durch inhaltsbasierte Analysen (also nicht den bloßen Vergleich von Bitketten, sondern durch „fortgeschrittene“ Methoden) und Extrahieren von Watermarks erkannt werden kann.

Hat man illegale Inhalte gefunden, können zusätzlich zu den möglicherweise bereits vorhandenen Beweisen noch die Protokolle (Log-Files) der Server, auf denen die Inhalte gefunden wurden, sichergestellt werden. Das Aufspüren von Rechtsverletzungen mittels Durchsuchen der vorhandenen Datenbestände muss natürlich auf legale Weise erfolgen, d.h. das Eindringen in fremde Server, um festzustellen, ob dort illegale Inhalte vorhanden sind, ist nicht erlaubt.

In diesem Sinn zwar wirkungsvoll, aber kritisch zu bewerten sind Methoden, bei denen man vorgeht wie ein Pirat: Eine Verfolgung ist theoretisch dadurch möglich, dass die Adressierungsinformation auf der Netzwerkebene verwendet wird, um den Anbieter bzw. Konsumenten zu verfolgen. Dies machen sich z.B. der Media Enforcer (http://mediaenforcer.tripod.com/enforcer/) und Zeropaid (http://www.zeropaid.com/busted) zunutze, um die IP-Adressen von Tauschhändlern herauszubekommen, z.B. indem sie Dateien mit eindeutig lautenden Dateinamen zum Download anbieten.

Unter http://dailynews.yahoo.com/h/zd/20011016/tc/riaa_we_ll_smother_song_swappers_1.html war im Internet weiterhin zu lesen, die Musikindustrie experimentiere mit einer neuen Methode gegen die Bereitstellung illegaler Inhalte im Internet, indem sie nach dem Aufspüren eines entsprechenden File-Sharing-Servers den Server blockieren könne und anschließend die Verbindungen zu Clients übernehme und die gewünschte Datei während des Downloads ausgetauscht werde. Ein Vorstoß seitens der RIAA (Recording Industry Association of America), solche Methoden im Rahmen eines im Oktober 2001 vom US-Kongress verabschiedeten Anti-Terror-Gesetzes zu legalisieren, scheiterten allerdings, berichtete das Online-Magazin Telepolis (http://www.heise.de/tp/deutsch/inhalt/te/9831/1.html).

Inhalte können auch durch bewusstes mehrfaches und langanhaltendes Abrufen den Server derart überlasten, dass er unter der Last zusammenbricht. Somit bekämen andere Interessenten keinen Zugriff zu den illegalen Inhalten mehr. Das Blockieren von Inhalten mit solchen Methoden ist gleichzusetzen mit einem Denial-of-Service Angriff und beeinträchtig somit alle Internet-Nutzer (auch solche, die den illegalen Inhalt nicht abrufen), da die Internet-Verbindungen verstopft werden. Gemäß der Task-Force „Sicheres Internet“ [29, 21] der Bundesregierung wäre ein solches Vorgehen seitens des Verfolgers höchstwahrscheinlich strafbar. Legalisierung würde in jedem Fall den Missbrauch von Denial-of-Service Angriffen fördern.

2.4.6 Zugriffsfilter und Sperren

Häufig stellen Internet Service Provider ihren Kunden speziell zugeschnittene Standarddienste zur Verfügung, bei denen eine grobe Vorauswahl der Inhalte und auch eine Sperrung bereits bekannter kritischer Inhalte erfolgt. Dies kann z.B. sinnvoll sein, wenn Eltern ihren Kindern den Zugang zum Internet ermöglichen wollen. So kann der Provider z.B. einen Filter für Spam-E-Mails, Werbe-E-Mails oder spezielle Webadressen (URLs) vorsehen, um seine Kunden nach ihren Wünschen zu schützen.

Umgekehrt betrachtet eigenen sich solche Filtermechanismen auch, um dem Nutzer den Zugang zu bestimmten Inhalten (z.B. rechts- oder sittenwidrige) zu verwehren.

Der Nutzer kann sich jedoch leicht über die Filterung hinwegsetzen, wenn er kein Filtern wünscht, was die Wirkung solcher gefilterter Dienstangebote teilweise in Frage stellt. Der Nutzer muss hierzu z.B. auf ungefilterte News-Server ausweichen, oder er benutzt sog. Proxy-Dienste (siehe auch Abschnitt 3.5).

Die Filterung von Inhalten setzt eine vorgeschaltete Bewertung nach vorgegebenen Kriterien (z.B. Qualität, Zulässigkeit, Rechtsverträglichkeit) voraus. Diese kann manuell (durch Menschen) oder automatisch (durch Maschinen) erfolgen.

Die automatisierte Kontrolle von Inhalten erfordert eine semantische Analyse von Daten. Computer sind jedoch bestenfalls in der Lage, syntaktische Auswertungen vorzunehmen. Folglich ist eine vollautomatische Filterung von Inhalten unmöglich. Halbautomatische Verfahren, d.h. eine Kombination von automatischer und manueller Bewertung sind jedoch möglich. Das Filtern von Inhalten ist selbstverständlich nur bei unverschlüsselter Nachrichtenübermittlung möglich.

Eine weitaus ausführlichere Diskussion zu den Folgen und der Wirkung von Sperrungen im Internet ist z.B. in [36] zu finden.

Automatische Bewertung aufgrund formaler Kriterien

Die einfachste und einleuchtendste Art der Bewertung ist das Überprüfen der Inhalte nach vorgegebenen Schlüsselworten. Dies eignet sich natürlich nur für Texte. Für Bilder und andere Medien bietet sich eine Überprüfung mit Hilfe von Checksummen an. Allerdings werden hier nur Inhalte erkannt, die dem Bewerter bereits vollständig bekannt sind und vom Sender nicht, d.h. nicht einmal in einem Bit, verändert wurden.

Ein Ansatz zu einer intelligenteren Bewertung von Inhalten ist das Content-based Database Retrieving (siehe z.B. http://wwwqbic.almaden.ibm.com), bei dem über die Angabe bestimmter Bildkriterien (z.B. Vorhandensein bestimmter Texturen, Farbzusammensetzung etc.) eine Bewertung möglich ist.

Im Audio-Bereich ist man inzwischen in der Lage, Musikstücke aus wenigen Sekunden Material zu erkennen.

Trotz der Fortschritte, die im Bereich der automatisierten Bewertung noch zu erwarten sind, können Fehleinschätzungen bei der automatisierten Bewertung in beide Richtungen auftreten: Einerseits können zu filternde Inhalte als einwandfrei erkannt werden, andererseits könnten auch Inhalte ohne Relevanz geblockt werden. Beispiele hierfür sind Diskussionsforen, die sich mit den Auswirkungen rechtswidriger, krimineller oder pornographischer Handlungen und Inhalte beschäftigen, ohne die Inhalte selber zum Gegenstand des Austauschs zu machen.

Manuelle Bewertung durch Dritte

Zunächst besteht natürlich die Möglichkeit, dass der Content Provider selbst seine Inhalte mit einer Bewertung versieht. Dies ist in Bereichen, in denen die Selbstregulierung greift, durchaus sinnvoll und hat in Systemen wie PICS (Plattform for Internet Content Selection) seine Berechtigung. Die Kombination mit dem unabhängigen Rating der Angebote durch unabhängige Dritte kann so eine qualitative Steigerung des Internetangebots nach sich ziehen, wie dies bei PICS der Fall ist. Infolge der Bewertung entstehen Sperrlisten, die entweder beim Provider oder auf dem lokalen Rechner des Benutzers vorhanden sind. Bei der Anforderung gesperrter Inhalte werden diese gar nicht erst vom Server angefordert. Filterkriterien, aus denen die Listen aufgebaut werden, können Rechneradressen (IP-Adressen), Webadressen (URLs), Namen von Newsgruppen, aber auch Message-IDs (besonders bei E-Mail und News-Beiträgen) sein.

Aufgrund der riesigen Datenmenge, die das Internet heute aufweist, ist eine vollständige Bewertung aller Inhalte aussichtslos. Die hinzukommende Dynamik der Inhalte macht eine dauerhafte und nachhaltige Bewertung unmöglich.

Rights Protection System (RPS)

Im Bereich Schutz der Urheberrechte wurde ebenfalls ein Filtersystem vorgeschlagen, um die illegale Verbreitung urheberrechtlich geschützter Materialien zu verhindern. Beim Rights Protection System [24] sollten die Internet Service Provider entsprechende Hard- und Software bei sich installieren.

Mit RPS wollte die Musikindustrie Grenzkontrollen im Internet einführen. Zugriffe aus Deutschland auf urheberrechtsverletzende Inhalte im Ausland sollten bei den wenigen deutschen Internet Service Providern mit einer Auslandsanbindung über einen den Routern vorgeschalteten Filter unterbunden werden. Dies sind in Deutschland nur etwa 50–70 Stellen.

RPS hat sich jedoch nicht durchgesetzt, einerseits wegen der hohen Kosten, andererseits wegen der generellen Kritik an Sperren und ihrer Wirkungslosigkeit gegenüber ernsthaften Umgehungsversuchen (siehe auch Abschnitt 3.5). Große Kritik gab es auch an dem Vorschlag, das RPS auf einem innerdeutschen zentralen Knotenpunkt, dem de-cix, zu installieren, da eine dortige Installation von RPS nicht der Grenzkontrolle, sondern die Überwachung des innerdeutschen Internetverkehrs gedient hätte.

3 Angriffstechniken und -werkzeuge

Trotz aller Bemühungen zeigen sich bei den existierenden Schutzsystemen immer wieder Schwächen, die von intelligenten Angreifern ausgenutzt werden, um Urheberrechte zu verletzen. Diese Schwächen lassen sich einteilen nach

- systematische Schwächen der Systeme und
- Schwächen bzw. Angriffsmöglichkeiten, die durch ungeeignete oder gar fehlerhafte Mechanismen hervorgerufen werden.

Oft haben auch der enorme Konkurrenzdruck und die immer kürzer werdenden Time-To-Market-Zyklen damit zu tun, dass Schutzsysteme bereits gebrochen sind, bevor sie weite Verbreitung erlangt haben. Die folgenden Abschnitte beschreiben typische Vorgehensweisen und Schwächen existierender Schutzsysteme.

3.1 Angriffe auf die verwendete Kryptographie

Kryptographische Mechanismen (siehe Abschnitt 2.2.1) sind, wenn sie gut gewählt und sorgfältig von Experten untersucht sind, aller Voraussicht nach nicht zu brechen. Die heute aktuellen Verfahren können daher guten Gewissens auch in DRM-Systemen zum Einsatz kommen.

3.1.1 Brechen der kryptographischen Mechanismen

Man unterscheidet verschiedene Stufen des Brechens kryptographischer Verfahren:

- **Vollständiges Brechen:** Finden des Schlüssels,
- **Universelles Brechen:** Finden eines zum Schlüssel äquivalenten Verfahrens,
- **Nachrichtenbezogenes Brechen:** Brechen für einzelne Nachrichten, ohne den Schlüssel selbst in Erfahrung zu bringen.
  - Selektives Brechen: für eine vom Angreifer bestimmte Nachricht (z.B. einen abgefangenen Schlüsseltext),
  - Existenzielles Brechen: für irgendeine Nachricht.

Dabei ist zu unterscheiden, ob ein Angreifer lediglich eimalige Kosten hat, um den verwendeten Schlüssel effizient knacken zu können, oder jeder Angriff auf eine Nachricht signifikante Kosten beim Angreifer verursacht. Ein Angreifer wird im Normalfall versuchen, an der schwächsten Stelle des Systems anzugreifen. Meist sind Angriffe auf die verwendete Kryptographie weniger aussichtsreich als z.B. das direkte Abgreifen des Klartextes (ggf. auch in leicht verminderter Qualität) oder Angriffe auf die physischen Sicherungsmaßnahmen (siehe Abschnitt 3.2) zur Geheimhaltung des Entschlüsselungsschlüssels.

3.1.2 Sicherheit aktueller Verfahren

Seit einigen Jahren existieren einige Kryptoalgorithmen, die nach dem Stand der Wissenschaft als *praktisch sicher* bezeichnet werden können. Praktisch sicher bedeutet, dass für den jeweiligen Algorithmus nach dem aktuellen Kenntnisstand keine effizienten Kryptanalyseverfahren bekannt sind. Zu diesen Algorithmen zählen z.B.:

- Triple-DES (Triple Data Encryption Standard) mit einer Schlüssellänge von 112 Bit,
- Rijndael, der neuer amerkanischer Verschlüsselungsstandard AES (Advanced Encryption Standard) ist, mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit,
- IDEA (International Data Encryption Algorithm) mit einer Schlüssellänge von 128 Bit,
- RSA, ein asymmetrischer Algorithmus, mit einer Schlüssellänge (Moduluslänge) von mindestens 1024 Bit.

Der in die Jahre gekommene DES (Data Encryption Standard) ist mit seiner geringen Schlüssellänge von 56 Bit nicht mehr sicher.

In jedem Fall können diese Algorithmen immer noch durch sog. **vollständiges Durchsuchen des Schlüsselraumes** (auch *Brute-force Attack* genannt) gebrochen werden. Wie aufwendig das praktisch ist, hängt von der Schlüssellänge des jeweiligen Algorithmus ab. Dabei ist zu beachten, dass die Schlüssellänge nie losgelöst vom Algorithmus betrachtet werden kann. So erreicht der asymmetrische Algorithmus RSA mit einer Schlüssellänge von 1024 Bit momentan etwa das gleiche Sicherheitsniveau wie der symmetrische IDEA mit 128 Bit.

Bei symmetrischen Systemen gelten derzeit 128 Bit Schlüssellänge als ausreichend. Wie hoch der finanzielle und zeitliche Aufwand für das Brechen eines symmetrischen Systems in Abhängigkeit der Schlüssellänge im Jahr 1995 war, zeigt die Tabelle 3.1 (nach [52, S.153]).

	Schlüssellänge in Bit					
Kosten in USD	40	56	64	80	112	128
100.000	2 s	35 h	1 Jahr	70.000 Jahre	10^{14} Jahre	10^{19} Jahre
1.000.000	0,2 s	3,5 h	37 d	7.000 Jahre	10^{13} Jahre	10^{18} Jahre
10.000.000	0,02 s	21 min	4 d	700 Jahre	10^{12} Jahre	10^{17} Jahre
100.000.000	2 ms	2 min	9 h	70 Jahre	10^{11} Jahre	10^{16} Jahre

Tabelle 3.1: Zeitlicher Aufwand für eine hardwarebasierte Brute-force Attack

Weiterhin hängt die notwendige Schlüssellänge von der Zeitdauer ab, die eine Information unbedingt geschützt bleiben muss. Muss die Information nur wenige Minuten bis Stunden

geschützt bleiben, z.B. weil sie anschließend sowieso öffentlich wird, genügen Schlüssellängen zwischen 64 und 128 Bit. Dies sind z.B. gebräuchliche Werte für Sitzungsschlüssel im Broadcasting. Für längerfristige Geheimhaltung sind heute Schlüssellängen ab 128 Bit zu wählen.

Nachdem kryptographische Algorithmen oder ganze Systeme veröffentlicht wurden, werden teilweise Fehler im Design entdeckt, die zur Unsicherheit führen. Grundsätzlich ist von der Nutzung selbst designter Krypto-Algrithmen abzuraten, wenn sie nicht ausgiebig durch die Krypto-Community untersucht worden sind. Zu hoch ist die Wahrscheinlichkeit, dass dem Designer Fehler unterlaufen sind, die dann von Hackern gnadenlos ausgenutzt werden können.

Auch bei der Umsetzung (Implementierung) von Krypto-Algorithmen treten immer wieder Fehler auf. Meist sind dies Unachtsamkeiten (kleine Programmierfehler mit großer Wirkung) und Unwissen des Entwicklers bzgl. der exakten Funktionsweise des Algorithmus. Seltener werden neue Angriffe entdeckt: So können beispielsweise Verzweigungen des Programmcodes innerhalb des Ver- oder Entschlüsselungsalgorithmus zu einem Informationsgewinn beim Angreifer über den Schlüssel führen (timing analysis, [34]). Bei Smart Cards konnte durch Messung des Stromverbrauchs der Karte während eines Verschlüsselungsvorgangs ebenfalls der nur auf der Karte vorhandene Schlüssel ermittelt werden, obwohl dies die Smart Card eigentlich hätte verhindern sollen (power analysis, [35]). Darüber hinaus müssen Entwickler auch bedenken, dass Angreifer gerade bei Chipkarten versuchen können, durch gezielte Misshandlung des Prozessors Fehlfunktionen auszulösen, durch die Zugriff auf sicherheitskritische Informationen erlangt werden kann (fault induction, [2, 43]).

3.2 Schwächen manipulationssicherer Hardware

Wir müssen davon ausgehen, dass der Angreifer technisch gut ausgebildet ist und über Ausrüstung zur Untersuchung und Änderung von elektronischen Schaltungen und hochintegrierten Halbleiterbausteinen verfügt. Bevor jedoch konkrete Angriffe diskutiert werden, sollen zunächst Angreiferklassen (Gefährlichkeitsklassen) und Schutzklassen eingeführt werden.

3.2.1 Gefährlichkeitsklassen

In [1] werden die beim Entwurf eines Systems zu berücksichtigenden Angreifer entsprechend ihren Möglichkeiten in drei grobe Gefährlichkeitsklassen eingeteilt:

- **Klasse I: Clevere Außenstehende.** Sie sind oft sehr intelligent, haben aber nur beschränktes Wissen über den Aufbau des untersuchten Systems. Sie haben nur Zugang zu mittelmäßig aufwendiger Ausrüstung (z.B. Lötkolben, Mikroskop, einfache Chemikalien, mechanische Werkzeuge, PC, In-Circuit-Emulator und Logik-Analysator). Sie nutzen oft existierende Schwächen des Systems aus, anstatt neue zu schaffen. Beispiele sind Studenten, Hobbyelektroniker oder Privatdetektive.
- **Klasse II: Erfahrene Insider.** Sie haben eine gezielte technische Ausbildung und viel Erfahrung. Sie haben unterschiedlich gutes Wissen über die Bestandteile des untersuchten Systems, aber prinzipiell Zugang zu Beschreibungen der technischen Einzelheiten. Oft haben sie auch Zugang zu anspruchsvoller Ausrüstung zur Untersuchung des Systems. Beispiele sind einzelne Mitarbeiter eines Systemherstellers oder -betreibers.

- **Klasse III: Zahlungskräftige Organisationen.** Sie sind in der Lage, Spezialistenteams mit Experten verwandter und sich ergänzender Ausbildung zusammenzustellen, die mit großen finanziellen Mitteln ausgestattet sind. Sie können eine detaillierte Analyse des untersuchten Systems durchführen, anspruchsvolle Angriffe entwickeln und haben Zugang zu den aufwendigsten Untersuchungshilfsmitteln (Chiptestarbeitsplätze, Elektronenmikroskope, Plasmaätzanlagen, Röntgengeräte, Elektronenstrahltester, Ionenstrahlarbeitsplatz, UV Lasersystem, usw.). Sie können eventuell auf erfahrene Insider als Teammitglieder zurückgreifen. Beispiele für Klasse-III-Angreifer sind die Labors von Geheimdiensten, von großen Mikroelektronikherstellern und einige kriminelle Vereinigungen.

3.2.2 Klassifikation von Schutzmechanismen

Der Aufwand der Schutzmechanismen, die in einem manipulationssicheren System eingesetzt werden müssen, hängt von den geschätzten Fähigkeiten und Mitteln des Angreifers ab. In [1] wird die Klassifikation von Schutzmechanismen in die folgenden sechs Stufen vorgeschlagen, abhängig von den Kosten, die aufgewendet werden müssen, um den Sicherheitsmechanismus zu überlisten:

- **Null:** Keine speziellen Sicherheitsvorkehrungen. Beispiel: ein normaler Bürocomputer.
- **Niedrig:** Es existieren einige einfache Sicherheitsmechanismen, die sich jedoch mit üblichen Laborhilfsmitteln und Werkzeugen wie Kneifzange, Lötkolben, Mikroskop, usw. umgehen lassen.
- **Mittel-Niedrig:** Teurere Werkzeuge sowie gewisses spezielles Wissen werden für einen erfolgreichen Angriff benötigt. Die Werkzeugkosten können im Bereich von etwa 500 bis 5000 US-Dollar liegen.
- **Mittel:** Spezielle Ausrüstung sowie spezielles Können und Wissen werden für einen erfolgreichen Angriff benötigt. Werkzeuge und Ausrüstung können im Bereich 50.000 bis 200.000 US-Dollar kosten. Der Angriff kann zeitaufwendig, aber letztendlich doch erfolgreich sein.
- **Mittel-Hoch:** Die erforderliche Ausrüstung ist zwar verfügbar, aber sehr teuer in der Anschaffung und im Betrieb und kann ebenfalls zwischen 50.000 bis 200.000 oder mehr US-Dollar kosten. Spezielles Können und Wissen ist notwendig, um die Ausrüstung einsetzen zu können. Mehr als ein aufwendiger Vorgang kann zur Überwindung der Sicherheitsmechanismen notwendig sein, so dass mehrere Experten mit sich ergänzendem Wissen zusammenarbeiten müssen. Der Angriff könnte letztendlich erfolglos bleiben.
- **Hoch:** Alle bekannten Angriffsversuche waren erfolglos. Eine Untersuchung durch ein Team von Spezialisten ist erforderlich. Sehr spezielle Ausrüstung ist erforderlich, die zum Teil erst entworfen und hergestellt werden muss. Die Gesamtkosten des Angriffs können mehrere Millionen US-Dollar übersteigen und es ist unsicher, ob der Angriff erfolgreich sein wird.

Diese Klassifikation von Sicherheitsmechanismen ist sicher sehr wertvoll für den Anwender eines Sicherheitsmoduls, da eine handfeste Aussage über den für einen Angriff notwendigen

Aufwand getroffen wird. Organisationen, welche Sicherheitsprodukte zertifizieren, vermeiden jedoch gerne konkrete Aussagen über die minimal erforderlichen Kosten eines erfolgreichen Angriffs, da eine gute Idee, eine sehr versteckte Sicherheitslücke oder eine neu verfügbare Technologie ganz unerwartet die Kosten des günstigsten möglichen Angriffs erheblich reduzieren kann.

Für Zertifizierungszwecke wurde daher in einer entsprechenden US-Norm [23] eine alternative Grobklassifikation von Sicherheitsmaßnahmen für manipulationssichere kryptographische Module vorgenommen. In den vier FIPS-Sicherheitslevels werden nur grundlegende Anforderungen an die Aufgaben der implementierten Schutzmechanismen gestellt, jedoch keine Aussagen über die Kosten eines Angriffs gemacht:

- **Sicherheitslevel 1:** Es werden nur Anforderungen an die verwendeten kryptographischen Algorithmen gestellt. Es werden keine besonderen physikalischen Schutzmaßnahmen verlangt, die über die normalen bei elektronischen Geräten üblichen geschlossenen Gehäuseformen hinausgehen.

- **Sicherheitslevel 2:** Das Sicherheitsmodul muss mit einem Siegel oder einem Schloss gesichert sein, oder in ein undurchsichtiges Material vergossen sein, so dass ein einfacher Manipulationsversuch durch die dabei entstandene Beschädigungen im Nachhinein offensichtlich wird.

- **Sicherheitslevel 3:** Ein Manipulationsversuch soll nicht nur im Nachhinein als Beschädigung erkennbar sein, sondern bereits während des Eingriffs vom Modul erkannt werden und zur sofortigen Vernichtung der im Sicherheitsmodul gespeicherten Geheimnisse führen. Ein einfaches Beispiel wäre ein sehr stabiles Gehäuse mit Schaltern, die beim Abnehmen des Gehäusedeckels sofort die gespeicherten Schlüsseldaten löschen, oder das Vergießen der Schaltung in sehr hartem Epoxid-Harz, um eine Beschädigung der Schaltung bei der Untersuchung wahrscheinlicher zu machen.

- **Sicherheitslevel 4:** Mit gewissem mechanischem Aufwand kann es immer noch relativ leicht möglich sein, die Alarmmechanismen von Level-3-Modulen zu umgehen, beispielsweise indem dünne Löcher an den Sensoren vorbei durch das Gehäuse gebohrt werden, über die der Zugang erfolgt. Level 4 verlangt einen umfassenden Eindringschutz von allen Seiten her. Das Eindringsensorsystem muss das Modul wie eine lückenlose Schutzhülle umgeben und im Falle eines Angriffs die Geheimdaten sofort löschen. Darüber hinaus muss durch Tests sichergestellt werden, dass bei variablen Umwelteinflüssen wie etwa Temperatur- und Spannungsschwankungen keine die Sicherheit des Moduls gefährdenden Systemzustände eintreten können. Alternativ können Sensoren eingesetzt werden, die bei ungewöhnlichen Umweltbedingungen wie etwa extremer Kälte eine Löschung der Geheimdaten auslösen.

Im Folgenden sollen nun konkrete Schwächen von manipulationssicherer Hardware und Ansatzpunkte für Angreifer beschrieben werden.

3.2.3 Einchip-Systeme

Die Sicherheit von Einchip-Systemen (Abschnitt 2.2.3, Seite 27) wurde von den Herstellern ursprünglich nur dadurch begründet, dass dem Angreifer die Systembusleitungen nicht zugänglich sind und er daher nur über die externen Schnittstellen mit der Anwendungssoftware kommunizieren kann. Ferner wurde von den Herstellern darauf hingewiesen, dass in EEPROM-Speichern die geheime Software nicht optisch sichtbar ist und lediglich als sehr empfindliches Ladungsmuster aufbewahrt wird, das sich beim Abätzen der oberen Schutzschichten sofort verflüchtigen wird.

Dennoch haben seit etwa 1994 regelmäßig Pay-TV-Piraten aus Chipkartenprozessoren mit gewissem Aufwand die geheimen Daten ausgelesen. Das Epoxid-Harz, in das der Chip eingebettet ist, kann mit rauchender Salpetersäure ($> 98\ \%\ HNO_3$) aufgelöst und mit Aceton entfernt werden [5]. Salpetersäure kann chemisch die in Siliziumchips eingesetzten Materialien Silizium, Siliziumoxid, Siliziumnitrit und Gold nicht angreifen. Das für Leiterbahnen auf den Chip aufgedampfte Aluminium überzieht sich sofort mit einer resistenten Schutzschicht (Al_2O_3) und wird daher ebenfalls nicht geschädigt.

Schon normale EEPROM-Mikrocontroller, die nicht speziell für Chipkarten- oder Sicherheitsanwendungen ausgelegt sind, versuchen, das unbefugte Auslesen der Daten zu verhindern. Sie verfügen über eine spezielle EEPROM-Speicherzelle mit einem Sicherheitsbit. Falls es gesetzt ist, wird das einfache Auslesen über die Programmierverifikationsfunktion des Prozessors verhindert. Jedoch ist immer noch bei vielen Mikrocontrollern dieses Sicherheitsbit in einer EEPROM-Zelle außerhalb der Fläche des normalen EEPROM-Speichers untergebracht. Der Angreifer muss daher nur die Chipverpackung wie beschrieben entfernen, den EEPROM-Speicher mit Farbe abdecken und die restliche Chipfläche mit UV-Licht bestrahlen, um das Sicherheitsbit zu löschen, ohne die Programmdaten zu vernichten. Anschließend können die Daten über den Programmiermodus ausgelesen werden. Diese Technik ist auch für Klasse-I-Angreifer durchführbar. Chipkartenprozessoren für Sicherheitsanwendungen verfügen aber in der Regel über bessere Schutzmechanismen.

Auch wenn es sehr schwierig ist, die Potentiale der EEPROM-Speicherzellen einer zugänglichen Chipoberfläche direkt auszulesen, so ist es doch relativ leicht möglich, Zugriff zu den Busleitungen zu bekommen. Nachdem die Epoxid-Harz-Verpackung des Chips entfernt wurde, befindet sich zwischen der Metallisierungsschicht, in der die Aluminiumverbindungen zwischen den Transistoren liegen, und der Chipoberfläche nur noch eine Passivierungsschicht. Diese robuste isolierende Schutzschicht aus Siliziumnitrit oder Siliziumoxid schützt die tieferen Schichten vor Beschädigung, Umwelteinflüssen und Ionenmigration. Sie lässt sich aber sehr einfach durch UV-Laserbeschuss entfernen, wozu ein spezielles Mikroskop mit Laseraufsatz eingesetzt wird. Anschließend kann der Angreifer feine Mikroprobing-Metallnadeln unter einem stark vergrößernden Mikroskop auf einem vibrationsgedämpften Arbeitstisch auf die ihn interessierenden Busleitungen setzen. Diese 0,5–2 µm spitzen Nadeln können über einen Vorverstärker mit einem Logik-Analysator verbunden werden, der dann die Vorgänge auf dem untersuchten Prozessorbus aufzeichnet [37].

Ein aufwendigeres Untersuchungsverfahren sind Elektronenstrahltester, bei denen der Chip wie in einem Elektronenrastermikroskop abgetastet wird [22]. Die Anzahl und Energie der von den Primärelektroden des Kathodenstrahls aus der Chipoberfläche herausgeschlagenen Sekundärelektroden geben Auskunft über das lokale elektrische Potential. Auf dem Bildschirm

des Elektronenstrahltesters sind daher die Spannungen auf den Leitungen des Chips als Helligkeitsunterschiede erkennbar (Spannungskontrast). Ein ebenfalls aufwendigeres, aber inzwischen in zahlreichen Labors verfügbares sehr leistungsfähiges Verfahren sind Ionenstrahlanlagen (FIB) [14], mit denen von der Chipoberfläche mit etwa 10 nm Auflösung in einer Vakuumkammer Material abgetragen oder deponiert werden kann. Dadurch lassen sich nachträglich auf einer Chipoberfläche Schaltungsänderungen durchführen und größere und damit leichter zugängliche Kontaktflächen anbringen. Diese Verfahren können bei Integrationsdichten und Frequenzen eingesetzt werden, bei denen Mikroprobing-Nadeln unzureichend sind.

Durch Beobachten der Busleitungen des Prozessors kann der geheime Speicherinhalt mitprotokolliert werden. Alternativ kann auch der Prozessor angehalten werden, und über die Busleitungen wird aktiv vom Angreifer der Speicher ausgelesen. Anschließend wird der vorgefundene Maschinencode disassembliert und ausgewertet, womit der Angriff auf das Einchip-System erfolgreich war.

Eine inzwischen gängige Schutzmaßnahme sind einige zusätzliche Metallisierungsschichten. Diese können zwar prinzipiell mit Ionenstrahlmanipulationsanlagen umgangen werden, allerdings erhöhen sie den Arbeitsaufwand für den Angreifer doch erheblich, insbesondere wenn die Chipoberfläche vor Aufbringen der Metallschutzschichten poliert wurde, so dass darunter liegende Strukturen nicht mehr an ihrem Höhenprofil erkennbar sind. Gute Metallschutzschichten sind nicht einfach homogene Flächen, sondern ein dichtes Netz aus Sensorleitungen, welche von der darunter liegenden Elektronik auf Kurzschluss oder Unterbrechung überprüft werden.

Durch systematisches Abätzen dünner Schichten des Chips und anschließendem vollständigen Fotografieren der Oberfläche des Chips kann ein hochauflösendes dreidimensionales Modell des Chips erstellt werden, aus dem dann mit Bildverarbeitungstechniken die Netzliste der Schaltung rekonstruiert werden kann [6]. Derartige den Chip zerstörende Verfahren helfen dem Angreifer, in Hardware implementierte kryptographische Algorithmen zu verstehen und einen Ausleseangriff auf einen anderen noch intakten Chip mit identischem Layout vorzubereiten.

Angesichts dieser heute in vielen besseren Mikroelektroniklabors verfügbaren Techniken erscheint es ausgesprochen schwierig, Schutzmechanismen höchster Sicherheit auf Chipebene zu realisieren. Die meisten heutigen Chipkarten dürften daher nur die Sicherheitsstufe **Mittel** (siehe Seite 48 auf der Skala nach [1]) erreichen, einige wenige ausgefeilte Chips von sehr erfahrenen Herstellern erreichen **Mittel-Hoch**. Einige Mikroelektronik-Labors bieten sogar kommerziell das Auslesen von einigen **Mittel-Niedrig** und **Mittel** Einchip-Systemen in Chipkarten und anderen Systemen als Dienstleistung für etwa zehntausend US-Dollar pro Chip an.

Für Einchip-Systeme stellt daher [23] keine speziellen Anforderungen an Schutzmaßnahmen auf dem Chip selbst, sondern nur an die Verpackung des Chips. Im Sicherheitslevel 4 muss der Chip in ein hartes undurchsichtiges Material eingegossen werden, dessen Härte- und Adhäsionseigenschaften es sehr wahrscheinlich machen, dass bei einem Versuch, die Verpackung mechanisch zu entfernen, der Chip ernsthaft beschädigt wird. Die Löslichkeitseigenschaften des Vergussmaterials sind so mit den auf dem Chip verwendeten Substanzen abzustimmen, dass Versuche, das Verpackungsmaterial chemisch aufzulösen, auch den Chip angreifen werden.

Derartige Sicherheitsverpackungen sind inzwischen kommerziell erhältlich, so beispielsweise das *ChipSeal*-System der Firma Dow Corning [9], oder das *Si-Shell*-System der Firma Schlumberger. Das *ChipSeal*-System wurde ursprünglich für den Einsatz in US-Militärausrüstung entwickelt, findet aber inzwischen auch in Systemen der Unterhaltungselektronik Verwendung,

so etwa in dem inzwischen vom Markt verschwundenen DVD-Verleihsystem DIVX, das ein anderes und bislang nicht kompromittiertes Verschlüsselungssystem hatte als die DVD.

3.2.4 Sichere Verpackung ganzer Baugruppen

Bei derartigen Sicherheitsmodulen (siehe auch Abschnitt 2.2.3, Seite 28) ist zu beachten, dass SRAM-Bausteine ihren Speicherinhalt bei Raumtemperatur für einige Sekunden ohne Versorgungsspannung erhalten können [53, 28]. Die verbliebene Ladungsverteilung in den Feldeffekttransistoren reicht aus, um das Flip-Flop beim Wiedereinschalten in den alten stabilen Zustand zurückkehren zu lassen. Diese Ladungsverteilung wird durch thermisches Rauschen langsam verändert. Durch Kühlung der ganzen Baugruppe auf etwa $-50\,^{\circ}$ Celsius kann das thermische Rauschen soweit verringert werden, dass sich die Information manchmal stundenlang ohne Versorgungsspannung halten kann.

Ein Angreifer könnte das Modul abkühlen und ohne Rücksicht auf den Alarmmechanismus die Verpackung schnell entfernen. Dann würde er den Kurzschluss, den der Alarmmechanismus ausgelöst hat, beseitigen und eine externe Versorgungsspannung anlegen, um anschließend das Modul auszulesen. Als Gegenmaßnahme sollte daher ein Sensor bei einer Abkühlung deutlich unter übliche Temperaturen ein Überschreiben der Daten auslösen.

Mit dieser Technik lassen sich Sicherheitsmodule entwickeln, die den FIPS Level 4 Anforderungen genügen, und auch einem Klasse-III-Angreifer einiges Kopfzerbrechen bereiten dürften. Ein möglicher Angriff wäre, bei Raumtemperatur mit speziell entwickelten Werkzeugen in Sekundenbruchteilen die Alarmmechanismen und die Batterie mechanisch abzutrennen, um ein aktives Überschreiben der Daten zu verhindern und dann sofort die Speicherbausteine mit einer externen Betriebsspannung zu versorgen. Ein anderer Angriffsansatz wäre, mechanisch die Drähte teilweise freizulegen, um mit einem sehr empfindlichen Spannungsmessgerät die Drahtwindungen nahe der Alarmschaltung ausfindig zu machen. Die an diesen Windungen anliegenden Potentiale werden dann mit einer externen Präzisionsspannungsquelle festgehalten, woraufhin der Angreifer die zwischen den extern spannungsstabilisierten Windungen liegenden anderen Drahtwindungen unterbrechen und den freigewordenen Raum für einen Zugang zum Inneren des Moduls nutzen kann.

Das physikalische Sicherungssystem des *IBM 4758 Transaction Security System* Moduls, das beispielsweise in vielen Geldautomaten eingesetzt wird, ist kurz in [1] beschrieben. Die äußere Schutzhülle besteht aus einer flexiblen Polyuretan-Folie, in die mehrere Lagen eines mit dotiertem und damit elektrisch leitfähigen Polyuretan gedruckten Sensorleitungssystem eingebettet werden. Da sich Leiter und Isolator chemisch nur geringfügig unterscheiden, ist es nicht mehr praktikabel, mit chemischen Mitteln wie beim Vorläufersystem die Drähte freizulegen und kurzzuschließen. Diese Alarmfolie umgibt die sicherheitsrelevanten Speicher-, Prozessor- und Verschlüsselungsbausteine völlig und schließt die Baugruppe hermetisch dicht ab. Die Widerstandsüberwachungsschaltung entspricht der in [56] beschriebenen. Das IBM 4758 Sicherheitsmodul war das erste nach FIPS Level 4 zertifizierte Sicherheitsmodul und dürfte nach einhelliger Ansicht von Fachleuten auch einem Klasse-III-Angreifer erhebliche Schwierigkeiten bereiten.

Das Schutzmembransystem, das die Firma Gore in Zusammenarbeit mit IBM für das IBM 4758 Modul entwickelte, ist inzwischen unter der Markenbezeichnung *D^3 Electronic Security Enclosure* auf dem Markt erhältlich [27] und verschiedene Hersteller arbeiten am Einsatz dieser

Schutztechnologie in wesentlich kleineren und kostengünstigeren Modulen als der etwa 2000 USD teuren für Bankanwendungen entwickelten IBM 4758.

Ein kleineres und wesentlich billigeres manipulationssicheres System ist der *iButton* der Firma Dallas Semiconductor (inzwischen Maxim). Dieses Modul ist eine kleine Stahlbüchse (5 mm hoch, 16 mm Durchmesser, einer Knopfzell-Batterie ähnlich), in der sich neben einer langlebigen Li-Batterie ein Sicherheitsmikroprozessor mit Metallschutzabdeckungen befindet, der seine Daten in batteriegepuffertem statischen RAM hält, welcher von mehreren Alarmmechanismen beim Öffnen der Büchse oder Verletzen der Chipoberfläche gelöscht wird.

Zusammenfassung

Zusammenfassend lässt sich sagen, dass die Entwicklung von für den Einsatz in der Unterhaltungselektronik geeigneten manipulationsresistenten Mikroprozessoren und Modulen derzeit noch am Anfang steht, es aber in den letzten fünf Jahren in diesem Bereich schon vielversprechende Fortschritte und eine erste Produktgeneration gegeben hat. Manipulationssichere Einchipsysteme sind insbesondere durch ihren niedrigen Preis (nur unwesentlich über dem anderer hochintegrierter Schaltungen) und ihre einfache Einsetzbarkeit mit konventioneller Bauteilebestückungstechnologie attraktiv für Hersteller, allerdings fehlt ihnen in der Regel der umfassende und ständig aktive Alarmmechanismus, der zum Schutz gegen Klasse III Angreifer wünschenswert ist, wie er bei Einsatz langlebiger identischer Schlüssel in einer großen Zahl von Abspielgeräten erforderlich wäre.

Die vielversprechendsten Schutzmaßnahmen für Einchipsysteme ohne dauerhafte Energiequelle sind extrem harte und gut mit dem Chipmaterial verbundene Verpackungsmaterialien, sowie obskure nicht-standard Schaltungstechniken und aufwendige Hardware-Implementationen der eingesetzten geheimzuhaltenden Sicherheitsmechanismen, um ein erfolgreiches Reverse Engineering so gut wie möglich zu erschweren, indem nicht nur Software, sondern auch Hardwareelemente rekonstruiert werden müssen.

Vielversprechender gegen Klasse-3-Angreifer sind aktive Schutzsysteme, die ggf. ganze Baugruppen, in welchen Schlüsseldaten in batteriegepufferten flüchtigen Speichern gehalten werden, hermetisch geschlossen umgeben und die bei Penetration der Schutzmembran die geschützten Daten umgehend dauerhaft löschen. Derartige Systeme erfordern aber nicht nur eine langlebige Batterie, sondern auch spezialisierte Fertigungstechnologie. Die einhergehenden Zusatzkosten von derzeit wohl mindestens 5–30 EUR pro Abspielgerät, das Risiko von verlorenen Daten durch Fehlalarme, sowie die batteriebedingt limitierte Lebensdauer von etwa einem Jahrzehnt machen diese im Prinzip heute schon ansatzweise verfügbaren Schutztechnologien noch etwas problematisch im breiten Einsatz in der Unterhaltungselektronik.

3.3 Schwächen von Watermarking-Systemen

Die Sicherheit von Watermarking-Verfahren gegenüber ernsthaften Angreifern lässt noch erheblich zu wünschen übrig. Es ist davon auszugehen, dass alle heute bekannten und alle zu erwartenden Watermarking-Systeme gebrochen werden in dem Sinne, dass Tools im Internet bereitgestellt werden, die das Watermark entfernen, ohne das Werk dabei wesentlich mehr zu verfälschen, als dies ursprünglich durch das Einbringen des Watermark geschehen ist.

3.3.1 Angriffe durch Transformationen

Eine generische Angriffsform besteht darin, das markierte Material so zu transformieren, dass es für den menschlichen Betrachter nur unwesentlich an Wert verliert, zugleich aber ein einfacher Detektor nicht mehr in der Lage ist, das Wasserzeichen zu erkennen. Die meisten Watermarkingleseverfahren lassen sich nicht durch die einfache Addition von sublimalen Störsignalen und Rauschen verwirren und überstehen dadurch beispielsweise die Quantisierungseffekte von verlustbehafteten Bildkompressionsverfahren wie JPEG meist unbeschadet. Jedoch reagieren sie oft sehr empfindlich auf selbst geringe und kaum wahrnehmbare geometrische oder zeitliche Verzerrungen, da sich dadurch Synchronisationspunkte verschieben.

Arbeiten mit dem Watermarking-Testprogramm StirMark [39] haben beispielsweise aufgezeigt, dass selbst viele Watermarkingverfahren, die noch gegen eine einzige geometrische Verzerrung eines Bildes robust waren (leichte Verschiebung, Streckung, oder Rotation), nach einer Kombination mehrerer solcher nichtwahrnehmbarer Schritte oder dem Einsatz von Verzerrungen, die bei der Entwicklung nicht berücksichtigt wurden (Scherung, Blähung, etc.), das Watermark nur noch in seltenen Fällen finden konnten. Ein über ein Bild gelegtes Gitter (siehe Abbildung 3.1) macht dies deutlich.

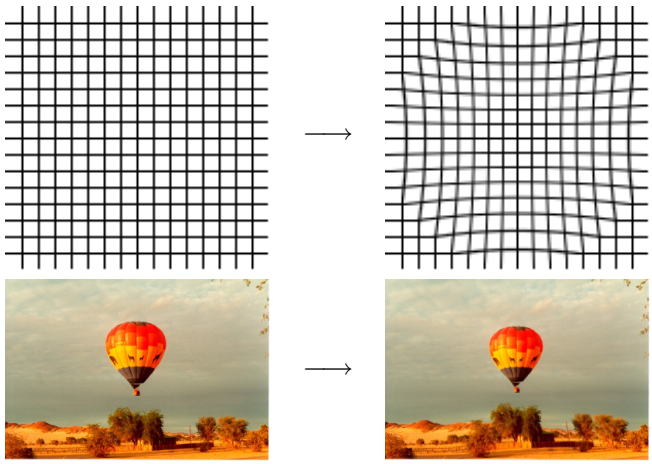

Abbildung 3.1: Stirmark Attack: Verbeulen eines Bildes

Das Watermark wurde dabei nicht wirklich entfernt und konnte nach Rücktransformation wieder zweifelsfrei nachgewiesen werden; es wurde nur für einfache und effiziente Detektoren unkenntlich. Spezielle forensische Watermarkingdetektoren sind durchaus in der Lage, eine große Zahl von Transformationsparametern auszutesten, um ein verbogenes Watermark wieder erkennbar zu machen, aber diese erfordern erhebliche Rechenzeit und lassen sich nicht praktikabel als billige Zusatzfunktion in einfachen Spielern einsetzen.

Solche Resultate zeigen, dass noch einiges an Forschungs- und Entwicklungsarbeit geleistet werden muss, bevor Watermarking-Verfahren ernsthaft gegen intelligente Angriffe sicher sind.

3.3.2 Mosaic-Angriff

Manchmal lassen sich gut gedachte Schutzmechanismen auch mit sehr primitiven, aber clever eingesetzten Mitteln aushebeln: Die Mosaic Attack [47] ist hierfür ein Beispiel. Watermarking-

Verfahren gehen davon aus, dass Manipulationen eines Inhaltes – z.B. Ausschneiden und Zerschneiden eines digitalisierten Fotos – das Watermark nicht unkenntlich machen sollen. Dies gelingt natürlich nur, wenn der Angreifer einen bestimmten Schwellenwert nicht überschreitet. Dieser sollte vom Urheber typischerweise so gewählt sein, dass der Bildinhalt für einen Piraten unbrauchbar bzw. nicht mehr wertvoll ist, wenn er den Schwellenwert überschreitet. Sobald der Angreifer einen sehr kleinen Bildausschnitt weiterverwendet, ist das Watermark nicht mehr detektierbar.

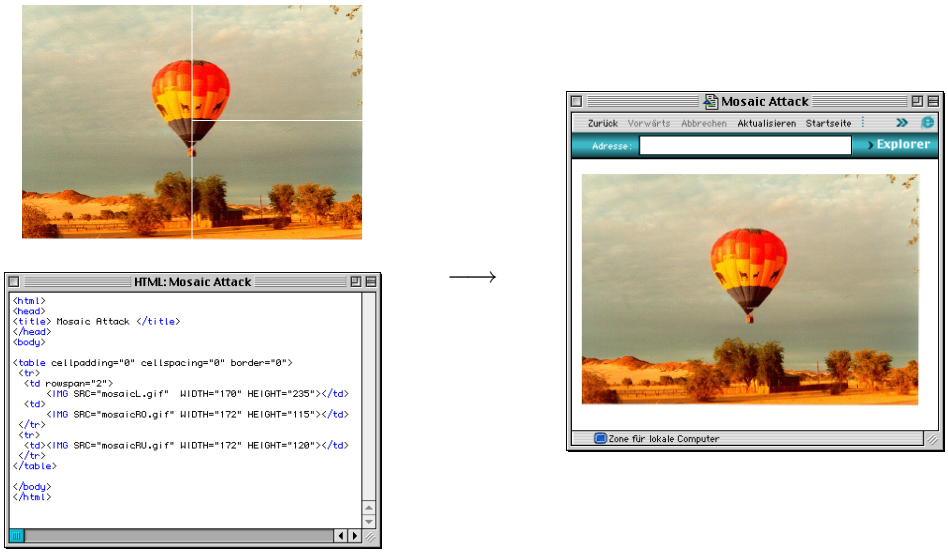

Abbildung 3.2: Mosaic Attack: Zerlegen eines Bildes

Die Mosaic Attack macht sich genau dies zunutze, allerdings so, dass der gesamte Bildinhalt ohne Verlust reproduzierbar ist, das Watermark aber trotzdem unerkennbar wird. Hierzu wird das Bild in viele kleine „Mosaikbausteine“ zerhackt, die anschließend für den Detektionsalgorithmus selbst dann unerkannt bleiben, wenn sie über einen geeigneten Mechanismus wieder zusammengesetzt und für den Betrachter zum ursprünglichen Bild reproduziert werden. Dies gelingt z.B. mit einer HTML-Seite, die aus einer (unsichtbaren) Tabelle besteht, deren Zellen die Mosaikbausteine (Teilbilder) enthalten (siehe Abbildung 3.2).

Ein Watermarkingleser darf daher beispielsweise bei HTTP-Zugriffen nicht auf einzelnen Bilddateien arbeiten, sondern muss die komplette Darstellungskette im Endgerät nachvollziehen (z.B. HTML-Layout, Java/JavaScript Interpretation, usw.), was den Rechenaufwand um Größenordnungen erhöht und den Einsatz von automatischen Echtzeit-Watermarkinglesern auf Breitbandkommunikationskanälen zur automatischen Filterung von geschütztem Material wesentlich problematischer macht.

3.3.3 Sensitivitäts-Angriff

Die heute bekannten Watermarking-Algorithmen basieren alle auf der Annahme, dass der Angreifer keine Kenntnis des zum Erkennen notwendigen Geheimschlüssels hat. Ein wirklich effektives und robustes asymmetrisches Watermarking-Verfahren, bei dem (analog zur asymmetrischen Kryptographie) die Kenntnis der im Watermarkdetektor eingesetzten Algorithmen

und Parameter nicht auch sofort zu einer recht offensichtlichen Methode zum Entfernen des Watermarks führt, ist nach unserem Kenntnisstand heute weder verfügbar noch in Aussicht. Man könnte deshalb annehmen, Watermarking-Verfahren müssten auch auf manipulationssichere Detektoren, die nicht für Reverse Engineering zugänglich sind, vertrauen.

Doch selbst bei Einsatz einer völlig geschützten Verpackung für den Detektor, kann dieser immer noch vom Angreifer zum Entfernen des Watermarks eingesetzt werden [13]. Dazu sucht der Angreifer mit einer Binärsuche zwischen einem Input mit und ohne Watermark nach einem Zwischenpunkt, an dem der Detektor gerade zwischen *Watermark vorhanden* und *nicht vorhanden* umschaltet. Anschließend wird die Eingabe so lange manipuliert, bis klar wird, welche lokalen Änderungen das Watermark erkennbar oder unkenntlich machen. Diese werden dann auf das markierte Bild angewendet, und somit wurde die kleinste Änderung angenähert, die das Watermark unkenntlich macht.

3.3.4 Weitere generische Angriffe

Viele erfolgreiche Angriffstechniken sind spezifisch für das jeweilige Watermarking-Verfahren, doch lassen sich auch einige weitere generische Verfahren nennen, welche die beschränkte Anwendbarkeit von Watermarking-Verfahren zu Kopierschutzzwecken verdeutlichen.

Sollte beispielsweise der Watermarking-Detektor nicht extrem sorgfältig in das Gesamtsystem integriert worden sein, so besteht die Gefahr, dass er einfach im Endgerät durch eine geringfügige Software- oder Hardware-Modifiktion deaktiviert wird, so dass sein – egal wie robustes – Ausgangssignal schlicht nicht mehr die illegitime Benutzung des Systems einschränkt.

Watermarks lassen sich durch Verschlüsselung der markierten Daten mühelos vollständig unkenntlich machen. Da moderne digitale Übertragungs- und Speichermedien mit beliebigen Bitströmen arbeiten, macht es für den Benutzer kaum einen Unterschied, ob Daten verschlüsselt oder im Klartext gehandhabt werden, insbesondere auf Universalcomputern und wenn die Verschlüsselung die Aktivierung unliebsamer inhaltabhängiger Kopierschutzmechanismen in Netzwerken und Speichergeräten ausschließt.

Watermarks für Videosignale bleiben oft über mehrere Einzelbilder hinweg konstant oder weisen andere Formen von Redundanz auf, um die notwendige Rechenleistung des Detektors zu beschränken. Da sich aber gleichzeitig die Bildinhalte rasch ändern, kann dies helfen, das Watermark vom Bild zu separieren. Ändert sich umgekehrt das Watermark von Einzelbild zu Einzelbild vollständig, so kann es durch Mittelung von sich weniger schnell ändernden Nachbarbildern abgeschwächt oder unkenntlich gemacht werden.

3.4 Reverse Engineering

Reverse Engineering von Systemen ist meist eine erlaubte Methode um zu verstehen, wie ein Mechanismus oder Gerät funktioniert und zudem eine sinnvolle Methode, um Schwächen zu finden, um die Systeme schrittweise zu verbessern. Der Verwertung der gewonnenen Erkenntnisse sind meist enge Grenzen gesetzt. Hierbei sollte man zusätzlich unterscheiden, ob durch Reverse Engineering speziell gesichertes Schlüsselmaterial oder lediglich ein Algorithmus, der vielleicht ohnehin patentrechtlich oder urheberrechtlich geschützt ist, an die Öffentlichkeit gerät. Bei derart geschützten Algorithmen ist auch der unberechtigte Nachbau illegal.

3.4.1 Nicht offengelegte kryptographische Algorithmen

Die Geheimhaltung von kryptographischen Verfahren – oftmals etwas geringschätzig als Security-by-obscurity bezeichnet – ist trotz gegenteiliger akademischer Lehrmeinung heute immer noch teilweise übliche Praxis, sowohl im kommerziellen als auch militärischen Bereich.

Eine der wesentlichen Grundanforderungen an moderne kryptographische Algorithmen ist, dass die gebotene Sicherheit ausschließlich auf der Geheimhaltung eines – im Notfall relativ leicht austauschbaren – kryptographischen Schlüssels beruhen soll. Alle weiteren Details des Verschlüsselungsverfahrens dürfen dem Gegner dagegen im Prinzip durchaus bekannt sein, ohne dass dadurch kryptoanalytische Angriffe praktikabel werden.

Dieses bereits 1883 von Kerckhoffs postulierte Prinzip [32] führte zur generellen Forderung nach einer vollständigen Offenlegung aller in sicherheitsrelevanten Anwendungen eingesetzten Kryptoalgorithmen. Dies ist auch heute zumindest im Bankwesen, bei digitalen Signatursystemen und bei Internet-Verschlüsselungssoftware dank entsprechender internationaler Standards weitgehend der Fall. Zahlreiche Fall-Beispiele belegen inzwischen auch deutlich, dass von kleinen und oft in der akademischen Kryptologie-Gemeinde nicht einschlägig bekannten „Experten“-Teams entwickelte und anschließend geheimgehaltene Verschlüsselungsverfahren oft erhebliche Schwächen aufweisen und nach Bekanntwerden von anderen Kryptologen oft innerhalb überraschend kurzer Zeit gebrochen werden, wie es beispielsweise beim Content Scrambling System (CSS) der DVD und verschiedenen Mobilfunk-Verschlüsselungsalgorithmen bereits geschehen ist.

Andererseits hat sich die Geheimhaltung der eingesetzen Algorithmen bei einigen Chipkarten-basierten Pay-TV-Systemen sogar als entscheidender Sicherheitsvorsprung bewährt. Bei Chipkartensystemen, in denen (in erster Näherung) alle Karten den gleichen Hauptschlüssel enthalten, ist der Schlüssel praktisch genauso gut oder schlecht austauschbar und vor Ausspähen geschützt wie der Verschlüsselungsalgorithmus. Der Einsatz eines bekannten Algorithmus gibt aber einem Angreifer mit verschiedenen Möglichkeiten zur Beobachtung und Manipulation der Hardware wichtige Informationen zur Planung und Durchführung eines Angriffs.

Einige Entwickler von Pay-TV-Chipkarten (z.B. NDS in Großbritannien) sind daher dazu übergegangen, in jeder Kartengeneration einen völlig neuen Verschlüsselungsalgorithmus als möglichst schwer durchschaubares Transistornetzwerk in Hardware zu implementieren. In der Praxis wird ein konkreter Angriffsversuch erheblich aufwendiger, wenn zunächst die Verdrahtung eines umfangreichen integrierten Schaltkreises rekonstruiert werden muss, um den zum Entschlüsseln notwendigen Algorithmus verstehen und auf den in einer Piratenkarte verwendeten Standardprozessor portieren zu können. Die eingesetzten Algorithmen werden dennoch nach Möglichkeit so gründlich geprüft werden müssen, dass sie selbst nach Bekanntwerden nicht notwendigerweise wesentlich unsicherer sind als bekannte Standardverfahren. Keinesfalls sollten durch die Geheimhaltung etwaige Schwächen des eigentlichen Algorithmus kaschiert werden, da dann Security-by-obscurity gegen ernsthafte Angreifer nichts helfen wird.

3.4.2 Reverse Engineering von Software

Reverse Engineering von DRM-Systemen ist nicht generell gleichzusetzen mit Piraterie. Beispielsweise könnte ein legal gekauftes und mittels eines DRM-Systems geschütztes Werk, das nur auf einem ganz bestimmten Betriebssystem oder einer Abspielsoftware nutzbar ist, den

verständlichen Wunsch seines Besitzers hervorrufen, es auch auf anderen Plattformen nutzbar zu machen.

Problematisch und keinesfalls von Dauer ist die durch „verworrenes Design“ erreichte Sicherheit von Softwarelösungen. Hierbei geht es lediglich darum, das Reverse Engineering des Programmcodes einigermaßen schwer zu machen.

Beispielsweise enthält der Microsoft Windows Media Player ein DRM-System (DRM2). Erwirbt der Nutzer eine Lizenz zum Abspielen eines Inhalts, kann er ihn jedoch nicht auf beliebiger Player-Soft- und -Hardware abspielen. Das DRM2-System wurde von Microsoft mit Blick auf erschwertes Reverse Engineering entwickelt. Eine (für den Außenstehenden) verworrene und unübersichtliche Struktur von Softwareobjekten soll die „Logik“ hinter dem System bestmöglich verstecken. Trotzdem ist es einem Programmierer gelungen, das System zu verstehen und ein Programm namens FreeMe [26] zu schreiben, mit dem Inhalte des Formats Windows Media Audio (WMA), für die eine Lizenz vorhanden ist, in einem auch für andere Player nutzbaren Format auf die Festplatte des Rechners abgespeichert werden können. FreeMe benutzt zum entschlüsseln die selben Funktionsaufrufe, die auch der Media Player nutzt, d.h. die DRM-Funktionen wurden nicht etwa „geknackt“, sondern vielmehr genutzt, um den Medienstrom abzuspeichern anstatt ihn auszugeben. Die technischen Details sind im Internet unter http://cryptome.org/ms-drm.htm veröffentlicht.

Ein weiteres Beispiel für den schwachen Schutz, den reine Softwarelösungen bieten, sind die in gängiger Abspielsoftware fehlenden Funktionen zum Abspeichern eines Medienstroms. Die Tatsache, dass eine Abspielsoftware (z.B. Windows Media Player oder Real Player) das Abspeichern nicht im Funktionsumfang anbietet, bedeutet keinesfalls, dass ein Pirat nicht in der Lage wäre, ein Programm zu schreiben, mit dem das Abspeichern möglich ist.

3.4.3 Begrenztheit reiner Softwarelösungen für DRM

Angesichts der weiten Verbreitung von Universalrechnern (PCs) und deren Multimedia-Möglichkeiten möchten die Inhalteanbieter verständlichweise auch diese Plattform mit Inhalten bedienen. Da PCs (zumindest bisher) sehr selten über entsprechende Hardware-Module verfügen, die zum Management der Rechte digitaler Daten geeignet wären, werden meist Lösungen für DRM in Software realisiert. In die Abspielsoftware oder sogar in die Betriebssystem-Software sind dann entsprechende DRM-Komponenten integriert. Nun leiden Softwarelösungen stets an dem Problem, dass die zu schützenden Geheimnisse, an denen die Sicherheit der DRM-Komponenten hängt, mehr oder weniger schutzlos dem Angreifer offenbart werden, da eine *physische* Kaselung in Software eben nicht möglich ist.

Insofern bleibt den Anbietern von Softwarelösungen nur ein Ausweg: Je verworrener, undurchschaubarer und unstrukturierter das Design der Software ist, umso schwerer wird es sein, und entsprechend lange wird es dauern, bis das System geknackt ist. Sobald dieser „Unsicherheitszustand“ bekannt ist, bekommen alle Nutzer über eine in das DRM-System integrierte Zwangs-Update-Funktion ein neues Stück Software, das wieder solange Schutz bietet, bis es ebenfalls geknackt ist u.s.w.

Wir wagen die These, dass je nach Motivation des Angreifers und Wert des Inhalts ein solcher Zyklus mit einer Periode von einigen Monaten oder länger beginnen kann, die Periode wird sich jedoch im Mittel verkürzen und kann nach mehreren erfolgreichen Hacks nur noch einige Tage

oder gar Stunden betragen. Der Grund hierfür liegt in der Tatsache begründet, dass der Vorrat an undurchschaubaren Konzepten und Denkstrukturen, die der Designer der DRM-Software besitzt und nutzen muss, um das Hacken zu erschweren, stets begrenzt ist. Man kann davon ausgehen, dass irgendwann die „guten Ideen“, die das Design verworrener machen, weitgehend erschöpft sein werden.

Folgender Vergleich mit der Sicherheit von Kryptographie verdeutlicht das Problem noch auf andere Weise: In den letzten 100 Jahren wurden höchstens 10–20 grundlegend verschiedene Ideen zum Design von Verschlüsselungsfunktionen vorgestellt, die sich bewährt haben. Diese kleine Zahl muss jedoch nicht erschrecken, da die Sicherheit eines Verschlüsselungsverfahrens nicht von der Geheimhaltung des Algorithmus, sondern vielmehr von dessen Parameter, dem Schlüssel, abhängen soll. Der Schlüsselraum heute sicherer Verfahren enthält aber zwischen 10^{20} und 10^{40} gleichwahrscheinliche Möglichkeiten. In Software, wo der Schlüssel als Teil der Daten innerhalb der Software gespeichert werden muss, kann er zur Sicherheit gegen Ausforschung nichts beitragen. Bei hardwarebasierter Kryptographie ist das grundsätzlich anders, da der Schlüssel das Hardware-Modul nicht verlässt: Die Hardware enthält den Schlüssel *und* den Algorithmus, so dass die Ver- und Entschlüsselung ebenfalls über das Hardware-Modul abläuft.

Den Anbietern von softwarebasierter DRM-Technik ist diese Problematik natürlich bekannt (vgl. die Vorträge von Industrievertretern auf der 2. Konferenz Digital Rights Management vom 29.–30. Januar 2002 in Berlin, http://www.digital-rights-management.de/) und sie versuchen, aus dieser Situation nach Möglichkeit noch das beste Sicherheitsniveau herauszuholen, da momentan aufgrund fehlender Hardwarebausteine in PCs keine andere Möglichkeit existiert.

Zusammenfassend muss gesagt werden, dass reine Softwarelösungen auf Dauer nicht geeignet sind, den Schutz digitaler Inhalte zu gewährleisten. Möglicherweise sind auch die Kosten für die Ausstattung von Geräten (PCs, Audio-, Videoabspielgeräte) mit entsprechenden Hardwarebausteinen momentan noch höher als die Verluste, die durch Piraterie und Verbreitung illegaler Inhalte entstehen.

3.5 Umgehen von Sperren und Filtern

Das Sperren von Internetangeboten (siehe auch Abschnitt 2.4.6) dient hauptsächlich dem Schutz des Endbenutzers. Wünscht er diesen Schutz nicht, hat aber sein Provider entsprechende Vorkehrungen getroffen, kann er sich über eine lokale Sperre leicht hinwegsetzen.

3.5.1 Methoden

Abbildung 3.3 zeigt die Umgehung einer Sperre durch den Client-Rechner, indem der Client auf einen sog. Proxy ausweicht, der innerhalb eines Providers 2 liegt und der den Zugang zu dem Server nicht gesperrt hat. Solange der Provider 1 den Zugang zu Provider 2 nicht ebenfalls sperrt oder Provider 2 nicht seinerseits den Zugang zu dem Server blockiert, gelingt dieses Ausweichen. Eine Sperre ist damit unwirksam, solange nicht alle Provider (weltweit) ebenfalls den Server blockieren.

Auch ein Server ist in der Lage, eine Sperrung zu umgehen, indem er z.B. alle Minuten seine IP-Adresse ändert. Bei Inhalten in Newsgruppen wird einfach ein Inhalt in andere, bisher un-

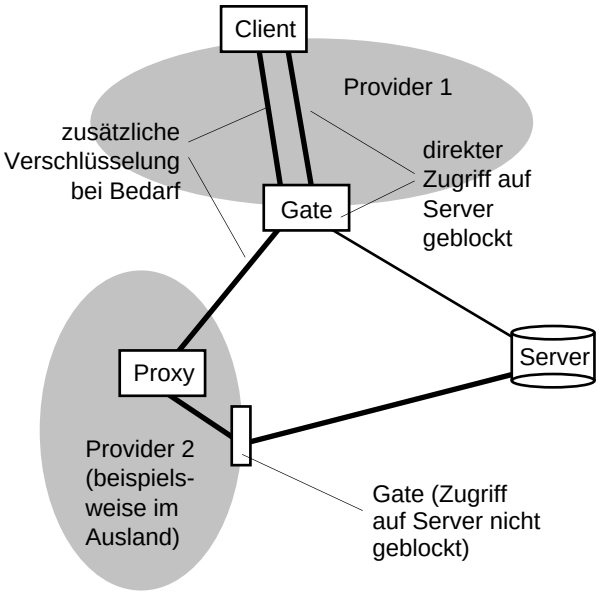

Abbildung 3.3: Ausweichen auf einen fremden Provider überbrückt die Sperre

verdächtige und einwandfreie Newsgruppen „gepostet“. Auch ein Namenswechsel der Newsgruppe bewirkt für einige (kurze) Zeit die ungefilterte Verbreitung von Inhalten. Generell ist es dem Content Provider möglich, falls er sich über eine Sperre hinwegsetzen möchte, sich dynamisch an die Filterkriterien anzupassen. Somit gelingt das Filtern und Sperren von Inhalten bestenfalls auf Zeit.

3.5.2 Konsequenzen

Eine reaktive Sperrung von Inhalten im Internet ist möglich und in vielen Fällen auch zumutbar. Eine proaktive Suche nach rechtswidrigen Inhalten kommt einer Massenüberwachung aller Kommunikation gleich und versagt, falls die Daten verschlüsselt werden. Dies gilt ebenso für Individualkommunikation (z.B. E-Mail) wie für geschlossene Benutzergruppen, die rechtswidrige Inhalte verschlüsselt austauschen.

Eine Sperre äußert sich als „technischer Defekt“. In einem verteilten System wie dem Internet, in dem niemand eine globale Übersicht über den Netzstatus hat, ist für einen Administrator die Einschätzung der Fehlerursache sehr schwer, möglicherweise gar unmöglich. So wird es häufiger zu Fehleinschätzungen (Fehler oder Sperre?) kommen, die eine Administration des Netzes erschweren. Folglich ist eine globale Übersicht über die Sperren notwendig.

Die manuelle Kontrolle aller Inhalte des Internet ist unzumutbar. Hat man ein Angebot als kritisch erkannt und möchte es sperren, beginnt der Wettlauf zwischen Anbieter und Filter, da der Anbieter sich an die Filterkriteren anpassen wird, um die Sperre zu umgehen. Solange ein Anbieter mit seinen rechtswidrigen Inhalten ins Ausland abwandern kann, sind lokale Sperrungen nur ein wenig wirkungsvolles Mittel; internationale Regelungen jedoch können greifen, da sie das Abwandern wirkungslos machen.

3.6 Missbräuchlich verwendbare Werkzeuge

In den folgenden Abschnitten sollen Werkzeuge (Hard- und Software sowie Internetdienste) diskutiert werden, die auch dazu benutzt werden können, um geschützte Inhalte unberechtigt zu vervielfältigen oder Spuren bei illegalen Handlungen zu verwischen, obwohl diese Werkzeuge ursprünglich nicht für diesen Zweck entwickelt wurden.

3.6.1 Kopiervorrichtungen (Grabber, Brenner)

Gemäß der Tabelle 1.2 aus Abschnitt 1.3.3 sollen Dienste, die synchron und online oder asynchron und offline verteilt werden, als klassische Distributionsformen bezeichnet werden. Eines der wesentlichen Merkmale der klassischen Distribution ist die Verteilung exakt gleicher Kopien an alle Konsumenten. Dies hat zur Folge, dass einer illegalen Kopie nicht anzusehen ist, wer die Kopie aus dem Original angefertigt hat und welchen Verteilweg sie genommen hat.

Ein Schutz vor Verbreitung digitaler 1:1-Kopien wurde in der Praxis bisher lediglich dadurch erreicht, dass das Herstellen solcher Kopien zu aufwendig oder zu teuer war. Die technische Entwicklung ermöglicht heute jedoch das preiswerte Anfertigen von Kopien.

Noch vor ein paar Jahren war das Anfertigen einer digitalen Kopie einer Musik-CD teurer als der Kauf der Original-CD. Heute lassen sich auf einer beschreibbaren Compact Disc (CD-R) mit einem handelsüblichen Computer digitale Kopien einer Musik-CD anfertigen. Der Rohling kostet weniger als 1 Euro und das Kopieren dauert maximal etwa 1 Stunde, typisch dürften 10 Minuten sein.

Die gleiche (technische und ökonomische) Situation könnte voraussichtlich in wenigen Jahren mit der Digital Versatile Disk (DVD) eintreten, auf der Videos und andere große Datenmengen gespeichert werden. Allerdings hat man sich bemüht, die Computerindustrie bei der Standardisierung der Kopierschutzmechanismen mit ins Boot zu bekommen, was seinerzeit bei der Festlegung des Audio-CD-Formats noch nicht der Fall war. Deshalb verfügen auch die in PCs eingebauten DVD-Laufwerke über Ländercode-Auswertung (Abschnitt 2.4.2). Besitzen diese PCs ausserdem Grafikkarten mit einer Videoausgabe (TV out, S-Video oder Composite-Signal), muss auch das Macrovision-Kopierschutzsystem (Abschnitt 2.3.1) implementiert sein.

Um die Situation im Musik-CD-Bereich nicht weiter zu verschlimmern, werden neuerdings vereinzelt Musik-CDs in einem Format erzeugt und verkauft, das in CD-ROM-Laufwerken von handelsüblichen PCs nicht problemlos gelesen werden kann. Bei der von Sony angewendeten Technik key2audio [33] werden bestimmte Datenbereiche (hier: das Inhaltsverzeichnis der CD), die nur von Computer-CD-ROM-Laufwerken gelesen werden, mit Daten beschrieben, die das CD-ROM-Laufwerk falsch interpretiert und damit „verwirrt“, so dass es das Abspielen der CD verweigert. Ein Audio-CD-Spieler wird dadurch nicht beeinträchtigt. Andere Verfahren verhindern zwar nicht das Abspielen einer Musik-CD auf einem Computer, sollen jedoch das Kopieren der digitalen Daten durch speziell aufgebrachte Fehler auf der Original-CD verhindern.

Leider sind Techniken wie key2audio völlig ungeeignet, das Anfertigen von Kopien *auf Dauer* zu verhindern, da es sich um schwache Schutzmechanismen handelt, die teilweise nur solange halten, bis jemand ein entsprechendes Auslese- und Kopierprogramm schreibt, mit dem der Schutz umgangen werden kann. Mit key2audio geschützte CDs können beispielsweise mit dem

Programm CloneCD problemlos kopiert werden, berichtete die Computerzeitschrift PC-Welt im Internet (http://www.pcwelt.com/ratgeber/hardware/17678/5.html).

Die Nutzungsqualität privat produzierter Kopien übertrifft derzeit oft sogar die von kommerziell erhältlichen Medien bei weitem. Eine gekaufte Musik-CD beispielsweise enthält ca. 70 Minuten Musik in einer vom Hersteller fest vorgegebenen Zusammenstellung. Eine privat erstellte Kopie dieser Musik auf einem DVD-RAM-Medium mit MPEG-Level-3 komprimierten Audiodaten hat bei vergleichbarer Qualität die fünfzigfache Spieldauer, überlässt dem Ersteller eine freie Auswahl der Zusammenstellung und Abspielreihenfolge, erlaubt die individuelle Ergänzung der Musik mit Zusatzinformationen und Auswahlmenüs. Darüber hinaus können sogar bequemst beim Vervielfältigen oder Abspielen Parameter frei modifiziert werden, die früher die Studiotechniker für alle Hörer fest vorgaben. Zum Beispiel kann die Lautstärkedynamik für bessere Hörbarkeit gegen Hintergrundgeräusche bei Autofahrten reduziert werden.

3.6.2 Peer-to-Peer-Netzwerke (P2P) und öffentliche File-Sharing-Systeme

Das Herstellen und die Re-Distribution (auch: Superdistribution, siehe auch Abbildung 3.4) von legalen wie illegalen Kopien kann heute über Dienste stattfinden, die teilweise darauf spezialisiert sind, bestimmte Medienformen möglichst unkontrollierbar zu verbreiten. Zur Verbreitung können verwendet werden:

- **Private Webpages**, News-Groups, E-Mail, auch wenn diese Dienste nicht spezialisiert sind auf bestimmte Medienformen,
- **Scour** (und Verwandte), ein „shared directory“, das mit komfortablen Suchfunktionen ausgestattet ist und spezialisiert, aber nicht beschränkt ist auf Bilder, Videos und Musikstücke (http://www.scour.com/),
- **Napster** (und Nachkommen), eine zentrale Vermittlungsdatenbank für MP3-Dateien; die Datei wird anschließend direkt zwischen dem Anbieter und Interessenten übermittelt, ohne durch den Napster-Server zu laufen (http://www.napster.com/),
- **Gnutella**, ein dezentralisiertes System, das zum Bereitstellen von beliebigen Inhalten geeignet ist. Bei Gnutella sind sowohl die Vermittlungsdatenbank als auch die Daten dezentralisiert (http://gnutella.wego.com/).

Über diese Dienste konnten Inhalte kostenlos angeboten und abgerufen werden. Die Systeme sind teilweise momentan nicht in Betrieb, da an der Erarbeitung von Geschäftsmodellen und Software für kostenpflichtigen Abruf (dann hoffentlich ausschließlich legal angebotener Inhalte) gearbeitet wird. Die Wiedergeburt von Napster & Co. hat jedoch weniger mit der zwischenzeitlichen Entwicklung besserer Schutzmöglichkeiten zu tun, als mit der Beliebtheit dieser Dienste in vergangenen Tagen. Man erwartet, dass die Nutzer trotzdem zu den ihnen „liebgewordenen“ Diensten zurückkehren werden.

Momentan laufende Systeme sind z.B. MusicCity Morpheus (http://www.musiccity.com/), Audiogalaxy Satellite (http://www.audiogalaxy.com/), BearShare (http://www.bearshare.com/) und iMesh (http://www.imesh.com/).

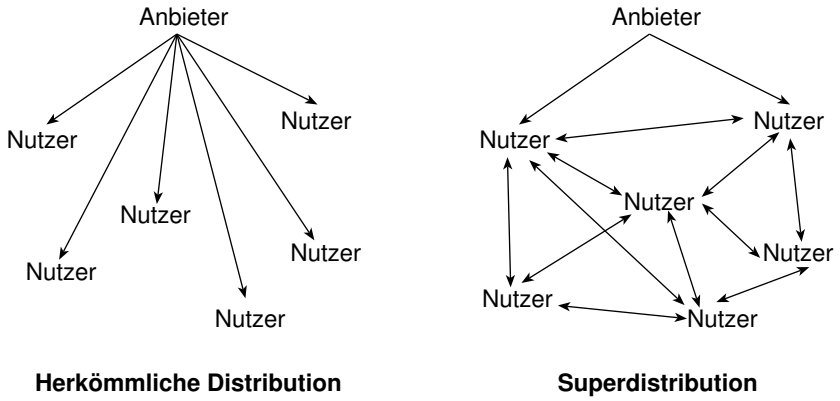

Abbildung 3.4: Superdistribution von Inhalten

Dabei wurde die Superdistribution nicht erst mit den Peer-to-Peer-Lösungen erfunden: Bereits Anfang der 80er Jahre wurde von dem Japaner Ryoichi Mori ein DRM-Konzept zur Verteilung von Inhalten entwickelt, bei dem keine Gebühr für den Erwerb, sondern für die Nutzung von Inhalten entstehen soll. Damit koppelt dieses Distributionskonzept die Vergütung von der Distribution der Inhalte ab [4, S.127ff].

Die illegale synchrone Re-Distribution von Rundfunk und Fernsehen, d.h. das unberechtigte „Ausstrahlen“ z.B. im Internet dürfte derzeit in den meisten Fällen noch am Mangel an technischer Ausstattung scheitern. Allerdings werden die Rechner und Internetverbindungen immer schneller. Software, mit der Jedermann seine eigene Internet-Radiostation betreiben kann, ist bereits am Markt. Beispiel Shoutcast: „SHOUTcast is Nullsoft’s Winamp-based distributed streaming audio system. Now you can listen to live streaming audio, and even broadcast your own SHOUTcast station from the comfort of your regular Internet connection.“ (http://www.shoutcast.com/).

Solche Programme sind sowohl für live- als auch für on-demand MP3 Internet Broadcast geeignet. Natürlich könnten diese Stationen auch mit fremden Inhalten gespeist werden.

3.6.3 Anonyme und unbeobachtbare Kommunikationsdienste

Die auf der Netzwerkebene des Internet vorhandene Adressierungsinformation kann verwendet werden, um den Anbieter bzw. Konsumenten von Inhalten zu verfolgen (siehe auch Abschnitt 2.4.5). Zeropaid (http://www.zeropaid.com/busted) betreibt beispielsweise einen Gnutella-Server, der die Interessenten von Kinderpornographie mit eindeutigen Dateinamen locken soll. Hinter den Dateien verbergen sich allerdings nicht die erwarteten Inhalte, jedoch erfährt Zeropaid die IP-Adresse des an dem Material Interessierten, um ihm anschließend möglichst das Handwerk zu legen.

Zukünftig könnten völlig legal angebotene Anonymisierer allerdings jegliche Verfolgung verhindern. Beispiele:

- **Anonymizer** (http://www.anonymizer.com/) ist ein anonymisierender Proxy-Server. Das bedeutet, der Abruf einer Webseite erfolgt nicht direkt durch den Benutzer, sondern stellvertretend durch den Anonymisierer. Der Betreiber des Webservers und dessen Log-Files haben somit keine verwertbaren Spuren zur Rückverfolgung des Piraten.

- **Freenet** (http://freenet.sourceforge.net/) ist ein dezentralisiertes System, bei dem sich Inhalte, sofern sie von anderen Nutzern tatsächlich abgerufen werden, nicht einfach löschen lassen, da sie sich durch eine spezielle Caching-Technik im „Freenet“ ausbreiten. Der Dienst wurde entwickelt, um free speech im Internet zu realisieren, d.h. unter anderem die Möglichkeit, unzensiert und anonym im Internet zu publizieren.

- **AN.ON** (http://anon.inf.tu-dresden.de/) ist ein eigenes Forschungsprojekt, welches ebenfalls belegt, dass die Anonymisierung von Internetzugriffen zwar aufwendig, aber technisch möglich ist. Zum unbeobachtbaren Surfen im Web ist das System JAP verfügbar.

Bezüglich des technischen Schutzes des Urheberrechtes sind Forderungen nach einem Verbot von privater, anonymer und unbeobachtbarer Kommunikation lediglich das Resultat unzureichender Schutzmechanismen im Vorfeld. Anstatt die Wirkung zu bekämpfen, sollte besser bei den technischen Ursachen begonnen werden, d.h. das leichte und unkontrollierte bzw. illegale Kopieren und Verbreiten von Inhalten muss erschwert oder von neuen Geschäftsmodellen und Diensten qualitativ und bzgl. Bequemlichkeit übertroffen werden.

3.6.4 Trojanische Pferde, Computerviren u. ä.

Viren, Würmer und Trojanische Pferde können nicht nur die Integrität und Verfügbarkeit von Daten und Programmen verletzen, sondern alle Schutzziele, also auch die Vertraulichkeit von Daten. Ein **Computervirus** ist ausführbarer Code, der sich in fremde Programme einpflanzt, dort ausgeführt wird und ggf. eine sog. **Schadensfunktion** ausführt. Ein **Wurm** ist ein ausführbares Programm, das sich über Computernetze verbreitet und ggf. eine Schadensfunktion ausführt. Ein **Trojanisches Pferd** ist ein Computerprogramm, das neben einer bekannten (vom Anwender gewünschten) Funktion eine (nicht gewünschte) Schadensfunktion ausführt.

Dies bedeutet, dass ein Angreifer z.B. einen Virus oder ein Trojanisches Pferd schreiben könnte, dessen Aufgabe es ist, fremde Festplatten, Computer und Computernetze nach urheberrechtlich geschütztem Material abzusuchen.

- Ein Pirat könnte so unberechtigt an die legal erworbenen Inhalte, Schlüssel etc. eines Anderen kommen und die ihn interessierenden Daten „absaugen“.

- Ein Verfolger könnte mit dieser Methode versuchen, illegal vorhandes Material aufzuspüren und entsprechende Maßnahmen (z.B. Löschen, Strafverfolgung) einleiten.

Beides ist unter normalen Umständen illegal. Technisch gesehen beruht die Angriffsmöglichkeit über trojanische Pferde und Computerviren auf einer fehlenden (z.B. in DOS, Windows 95/98/ME, MacOS bis Version 9) oder schlecht eingesetzten Zugriffskontrolle. Insofern ließe sich zumindest die Virenproblematik durch entsprechend stärkere Beachtung und sichere Vor-Konfiguration von Zugriffskontrollmechanismen durch die Hersteller von Betriebssystemen halbwegs in den Griff bekommen. Gegen trojanische Pferde hilft, sobald man die Virenproblematik zufriedenstellend gelöst hat, trotzdem nur der sensible und bewußte Umgang der Benutzer mit ausführbaren fremden Inhalten: Da man einem trojanischen Pferd die Hinterlist zunächst nicht ansieht, muss man der Korrektheit der Funktionalität (hier: Ausschließlichkeit der dokumentierten Funktionalität) vertrauen.

4 Konsequenzen und Sekundäreffekte

Für den Verbraucher bzw. Konsumenten von Inhalten entstehend durch die technisch unterstützte Sicherung des Urheberrechtes Konsequenzen und Sekundäreffekte, auf die in den folgenden Abschnitten eingegangen wird. Dies betrifft insbesondere die informationelle Selbstbestimmung der Konsumenten und den Verbraucherschutz.

4.1 Sicherung der informationellen Selbstbestimmung

In seinem sehr gut geschriebenen Überblickpapier „Golden Times for Digital Rights Management?“ nennt Tomas Sander im Kapitel „2.1 Dependable Digital Rights and Portability“ folgendes Fernziel: „The ultimate challenge is to bind digital rights to a person, and not to a (set of) device(s).“ Dies macht das Spannungsverhältnis zwischen informationeller Selbstbestimmung und dem effektiven Schutz digitaler Inhalte deutlich.

4.1.1 Unbeobachtbarkeit und Anonymität

Informationelle Selbstbestimmung der Nutzer digitaler Inhalte bedeutet, dass sie so weit wie möglich autonom und frei bestimmen,

- wem sie ihre Nutzung digitaler Inhalte wann und unter welchen Umständen wie weit offenbaren (Unbeobachtbarkeit der Nutzung) und
- wem sie ihren Erwerb digitaler Inhalte zur Kenntnis gelangen lassen (Anonymität des Erwerbs).

Die heute weitestgehend gegebene Unbeobachtbarkeit der Nutzung digitaler Inhalte wird untergraben, wenn Inhalteanbieter oder ihre Vertriebspartner

- zum Zwecke der Einzelnutzungsabrechnung (Pay-per-use) detaillierte Abrechnungen vom Endsystem des Nutzers erhalten oder gar
- zum Zwecke der Freischaltung jeder einzelnen Nutzung eine Anfrage erhalten, um die entsprechende Autorisierungsnachricht an das Endsystem des Nutzers zu schicken, ohne die dieses den Inhalt nicht nutzen lässt.

Maßnahmen, die die Untergrabung der Unbeobachtbarkeit der Nutzung begrenzen, sind wenig detaillierte Einzelnutzungsabrechnungen, die in keinem Fall den genauen Nutzungszeitpunkt

enthalten sollten sowie möglichst wenige Angaben über die im Detail genutzten Inhalte. Anzustreben ist, dass die Einzelnutzungsabrechnung nur die für den Abrechnungszeitraum insgesamt zu zahlenden Entgelte als eine Summe ausweist. Aus Sicht der Unbeobachtbarkeit der Nutzung und damit des informationellen Selbstbestimmungsrechts extrem bedenklich sind Systemgestaltungen, die für jede Einzelnutzung Autorisierungsnachrichten erfordern, da dann der zeitliche Ablauf der Nutzung durch den Nutzer dem Inhalteanbieter oder seinem Vertriebspartner offenbar wird. Hier bliebe dann nur noch die Möglichkeit, eine anonyme Nutzung zuzulassen.

Der heute weitgehend gegebene anonyme Kauf digitaler Inhalte wird untergraben, wenn Inhalteanbieter oder ihre Vertriebspartner

- Käufer oder
- deren mit einer Identität versehene Geräte

identifizieren.

Hierbei ist nicht nur zu betrachten, welche Identifikation der Inhalteanbieter oder sein Vertriebspartner vornimmt, sondern auch, welche mittelbare Identifikation etwa durch das verwendete Zahlungssystem (z.B. Kreditkarten) erfolgt.

Beobachtungsmöglichkeiten über Seriennummern von Geräten sind bereits seit langem Realität. So verfügen beispielsweise Digital-Audio-Recorder, die mit dem Serial Copy Management System (SCMS, siehe Abschnitt 2.4.1) ausgestattet sind, über einen Recorder Unique Identifier (RID), ein 97 Bit langer Code, bestehend aus einem Herstellercode, einer Typnummer und einer eindeutigen Seriennummer des eingebauten Laufwerks. Jeder mit einem solchen Recorder aufgenommene Inhalt enthält alle 100 Datenblöcke des Audio-Datenstroms diesen RID. Der RID wurde eingeführt, um die Quelle unautorisierter Kopien besser verfolg- und identifizierbar zu machen.

Sind die verwendeten Maßnahmen zum Schutz der digitalen Inhalte technisch nicht sicher, was zumindest in der überschaubaren Zukunft der Fall sein wird, so arbeiten alle Möglichkeiten, den Nutzern Unbeobachtbarkeit zu gewähren bzw. den Käufern Anonymität, klar gegen die im Interesse der Inhalteanbieter anzustrebende Risikobegrenzung durch Beobachtbarkeit und Nachverfolgbarkeit der Ausnutzung von Sicherheitslücken.

4.1.2 Fälschliche Beschuldigung

Um bei Weiterverbreitung digitaler Inhalte „beweisen“ zu können, wer sie weiterverbreitet hat, wird die Identität des Käufers bzw. Nutzers in den digitalen Inhalt eingebettet (Fingerprinting). Neben der bereits bei der Beschreibung von Fingerprinting in Abschnitt 2.3.3 dargelegten Unsicherheit – sie ist noch größer und grundlegender als bei Watermarking – aller bisher bekannten Verfahren (Fingerprints können leicht entfernt werden), bieten Fingerprints noch zwei weitere Unsicherheiten. Diese können leicht zu fälschlichen Beschuldigungen führen:

- Derjenige, der den Fingerprint in den digitalen Inhalt einbringt, kennt exakt die gleiche Fassung des Inhalts wie derjenige, der den mit dem Fingerprint versehenen Inhalt erhält. Wird der mit dem Fingerprint versehene Inhalt an unbefugter Stelle aufgefunden, kann die undichte Stelle bei jedem von beiden liegen. Ein Beweis im Sinne des Zivilrechtes kann mit diesem Hilfsmittel allein also nicht geschaffen werden.

- Dass der mit einem Fingerprint versehene Inhalt an unbefugter Stelle aufgefunden wird, muss nicht auf böswillige Absicht oder auch nur Billigung eines der beiden Beteiligten beruhen. Heutige IT-Systeme sind größtenteils so komplex und unsicher, dass auch der Systembetreiber sich ihrer Funktion nicht sicher sein kann. Dies gilt insbesondere für alle IT-Systeme, wo Software dynamisch nachgeladen werden kann.

Aus den genannten Gründen müssen „Beweise“ für Urheberrechtsverletzungen, die Systeme zum Schutz digitaler Inhalte liefern, mit einer gehörigen Portion Skepsis betrachtet werden.

4.2 Langfristige Sicherung des Verbraucherschutzes

Die Akzeptanz von Schutzsystemen durch den Endverbraucher hängt auch davon ab, ob seine Interessen langfristig gewahrt bleiben. Die beiden folgenden Abschnitte betrachten diesen Aspekt für die Archivierung von Kulturgütern und die Situation, wenn die immer schneller werdenden Technologiezyklen den Wunsch des Verbrauchers nach Anpassung legal erworbener Inhalte an neue Technik entstehen lassen.

4.2.1 Kopierschutz vs. Archivierbarkeit von Kulturgütern

Hauptaufgabe von öffentlichen Bibliotheken ist es, den Kulturbesitz einer Gesellschaft zu erhalten, zu erweitern und möglichst vielen Benutzern zugänglich zu machen [40, 3]. Um diese Aufgabe zu vereinfachen, ist in vielen Ländern das Urheberrecht an eine Abgabepflicht von Belegexemplaren gebunden. Verleger geistiger Werke sind beispielsweise in Großbritannien verpflichtet, ein Belegexemplar an die British Library zu senden, und fünf weitere nationale Copyright-Bibliotheken haben das Recht, kostenlos ein Exemplar anzufordern. Der langfristige Erhalt dieses Bestandes über mehrere Jahrhunderte erfordert nicht nur die sorgfältige Aufbewahrung und Pflege, sondern auch die Überführung in andere, besser archivierbare Medien. So laufen derzeit etwa in zahlreichen Nationalbibliotheken große Projekte, um signifikante Teile des Buchbestandes einzuscannen, also in eine digitale und damit problemlos beliebig oft verlustfrei kopierbare Form zu wandeln. Die Abgabepflicht für Belegexemplare beschränkt sich derzeit oft noch auf gedruckte Werke, aber eine Erweiterung auf elektronische Werke inklusive Datenbanken, Computersoftware- und Spiele, etc. wird derzeit erwogen. Das Britische National Sound Archive verfügt beispielsweise bereits über eine Million privater und kommerzieller Tonträger [40].

Diese Arbeit zum langfristigen Erhalt von geistigen Werken könnte aber in absehbarer Zeit durch hocheffektive Kopierschutzmechanismen in elektronischen Medien gefährdet werden. Sicherlich werden für Werke, die in den Jahren nach der Erstveröffentlichung Popularität genießen, die Verleger selbst am Erhalt und der kontinuierlichen kommerziellen Verfügbarkeit des Produktes interessiert sein. Ein guter und langfristig wertvoller Bibliotheksbestand ist jedoch weniger nach dem aktuellen Interesse der Benutzer für den Bestand zu beurteilen, sondern danach, ob die Bibliothek auch in der Lage ist, in fernerer Zukunft noch ein umfassendes und unvoreingenommenes Abbild des gesamten kulturellen Geschehens über verschiedene Epochen hinweg zu erhalten, inklusive möglichst vieler auf Anhieb vielleicht weniger erfolgreicher Werke, von denen einige eventuell erst nach Jahrzehnten oder Jahrhunderten auf Interesse stoßen.

„Wie jedes Eigentum unterliegt auch das geistige Eigentum gewissen Schranken im Rahmen der Sozialpflichtigkeit. Ein der Öffentlichkeit – auf welche Weise auch immer – zugänglich gemachtes Werk ist durch seine Veröffentlichung Teil der Gesellschaft geworden – wie das Bundesverfassungsgericht formuliert hat. Es sollte ihr zur ungehinderten Nutzung zur Verfügung stehen.“ [3].

Bibliotheken kämpfen bereits jetzt mit einem enormen Erhaltungsproblem, das den Bestand fast aller gedruckter Werke der letzten 150 Jahre bedroht. Während sorgfältig hergestellte klösterliche Schriften aus dem Mittelalter noch heute in hervorragendem Zustand erhalten sind, so hat ein Großteil der im 20. Jahrhundert gedruckten Literatur nur eine Lebenserwartung von 50–80 Jahren [51]. Da sich seit etwa 1840 in der Papierherstellung eine kostengünstige Harz-Alaun-Leimung durchgesetzt hat, enthält modernes Papier Schwefelsäure und säurebildende Substanzen, die im Zusammenwirken mit der allgegenwärtigen Luftfeuchte die Zellulosefasern des Papiers im Lauf der Jahre brüchig werden lassen. Es wurde beispielsweise in den USA geschätzt, dass dort 70–90 Prozent der Dokumente vom Papierzerfall betroffen sind und bereits 15–30 Prozent heute nicht mehr benutzbar sind. Eine Untersuchung des Deutschen Bibliotheksinstituts ergab, dass in Deutschland in wissenschaftlichen Bibliotheken etwa 60 Millionen Bücher und in Archiven etwa 350 km Regallänge vom Zerfall bedroht oder schon betroffen sind. Ohne entsprechende Maßnahmen wird damit das geistige Erbe der Menschheit des 20. Jahrhunderts nicht für die Nachwelt erhalten bleiben.

Mit dem breiten Einsatz hocheffektiver Kopierschutztechnik im Publikationswesen der Zukunft droht Bibliotheken nichts anderes als eine Wiederholung des aktuellen Säureproblems mit Druckmedien im nächsten Jahrhundert für digital gespeicherte Werke.

Mit ständig steigenden Integrationsdichten digitaler Datenträger reduziert sich auch immer weiter die physikalische Redundanz der Datenrepräsentation und damit auch die langfristige Lesbarkeitsdauer des Mediums.

Kopierschutzmechanismen könnten künftig Bibliotheken nicht nur an der Übertragung alter Werke auf neuere, zeitgenössische, kompaktere und preiswertere Datenträger hindern und damit ein enormes Kostensparpotential für Bibliotheken und Archive eliminieren. Sie verhindern notwendigerweise auch die Anfertigung von Kopien für den Fernverleih und die Rettung des Datenbestandes am Ende der Haltbarkeit des Mediums.

4.2.2 Legitimes Kopieren und Reverse Engineering

Gleichwertig neben dem Interesse der Verleger geistiger Werke daran, eine gewinnschädigende unlautere Weitergabe an andere Benutzer zu vereiteln, bestehen auf Seiten vieler Kunden eine Reihe von durchaus legitime Bedenken gegen den Einsatz umfassender Kopierschutzmechanismen, vergleichbar mit den Sorgen der Archive und Bibliotheken.

Digitale Speichertechnologien (derzeit hauptsächlich magnetische, optische, und magnetooptische Plattenspeicher als austauschbare Medien oder fest gekapselte Laufwerke, sowie Halbleiterspeicher) unterliegen derzeit und auf absehbare Zeit hinaus einem exponentiellen Leistungswachstum in Merkmalen wie etwa Kapazität, Geschwindigkeit, Gewicht, Energieverbrauch, und Geräuschentwicklung. Schnelle Technologiezyklen machen Medien oft innerhalb von weniger als einem Jahrzehnt obsolet, und Kunden sind daher daran interessiert, erworbene geistige Werke selbstständig auf modernere Medien übertragen zu können. In gewisser Weise wären unflexible Formen von Kopierschutzmechanismen, die diesen Konsumentenanforderungen nicht

nachkommen, in etwa vergleichbar mit beispielsweise einer hypothetischen Buchdrucktechnologie, bei welcher der Kunde nur mittels seiner zum Kaufzeitpunkt aktuellen Lesebrille den Text lesen kann. Auch wenn zum Erwerbszeitpunkt dem Kunden der erkaufte Nachteil nicht bewusst wird, so sind die Nutzungsrechte doch nach einiger Zeit erheblich eingeschränkt.

Kontinuierlicher Gebrauch geht bei allen physikalischen Medien mit der Gefahr einher, dass die Medien durch erhöhte Temperatur und Erschütterungen sowie mechanischen Abrieb schneller altern als die gewünschte Nutzbarkeitsdauer des Produktes, die sich bei vererbten Bibliotheken oft über mehrere Generationen hin erstrecken kann, dies erlaubt. Moderne Speichermedien sind oft sehr sensibel gegenüber ungeeigneten Umwelteinflüssen und es besteht ständig die Gefahr, dass durch einen Unfall oder kurzfristige unsachgemäße Handhabung die Lesbarkeit der Daten beeinträchtigt wird. Im Bereich von Computersoftware herrscht daher ein seit langem akzeptiertes Gewohnheitsrecht, welches es Kunden erlaubt, sich Sicherheitskopien der erworbenen Medien zu erstellen.

Manche der zuvor genannten Bedenken wie etwa die Übertragbarkeit auf modernere Medien ließen sich gegebenenfalls durch geeignete „Online-Authentisierungstechniken“ praktikabel begegnen, aber um diese nutzen zu können, ist der Kunde darauf angewiesen, dass der Hersteller auch nach vielen Jahren noch die Möglichkeit bietet, Nutzungslizenzen von einem Medium oder Abspielgerät auf ein anderes zu übertragen. Dies ist insbesondere problematisch, wenn der Hersteller inzwischen das Geschäft aufgegeben hat.

Im Falle von Computersoftware kommt als weitere Kundensorge hinzu, dass ein umfassender Kopierschutz auch eine Inspektion der ausgeführten Maschineninstruktionen vereiteln würde, was erheblich die Möglichkeiten der Kunden reduzieren würde, das Produkt im Rahmen von Produkthaftungsansprüchen oder Patentlizenzforderungen eingehend zu untersuchen.

4.3 Fazit und offene Fragen

Momentan sind die verfügbaren Systeme zum Schutz von Inhalten systematisch unsicher.

Die existierenden Systeme haben trotz (oder gerade wegen) ihrer Unsicherheit Sekundäreffekte für Datenschutz und Verbraucherschutz, indem sie die Beobachtbarkeit und das Profiling der Nutzer ermöglichen oder wenigstens nicht verhindern. Weiterhin wird die freie und uneingeschränkte Nutzung von legal erworbenen Inhalten verhindert.

Wenn die existierenden Systeme tatsächlich sicher wären, bzw. wenn irgendwann sichere Systeme entwickelt und am Markt sein sollten, dann hätten sie auch Auswirkungen auf die Archivierbarkeit und die zeitlose Verfügbarkeit der über sie gesicherten Inhalte. Hier sollte man ggf. den Weg gehen, öffentliche Archive mit Kopien der Inhalte zu versorgen, die auch tatsächlich archivierbar und (zeitlos) nutzbar sind.

Die stärkere Verbreitung von DRM-Technik wirft im übrigen einige Fragen auf, die aus unserer Sicht bisher noch nicht ausreichend in der Öffentlichkeit diskutiert sind:

- Sind die Endverbraucher ausreichend geschützt und wer wird zukünftig ihre Rechte wahrnehmen?
- Brauchen wir möglicherweise für die Zukunft neue „Codes of Conduct“ für den Umgang mit Forschungsergebnissen über die Unsicherheit von Sicherungssystemen generell, da bereits heute Gesetze existieren, die die Freiheit wissenschaftlicher Arbeit beeinflussen?

- Welche Implikationen haben DRM-Systeme für die wissenschaftliche Arbeit? Das (wachsende) Angebot an momentan kostenlos und frei abrufbaren wissenschaftlichen Publikationen im Internet könnte mit der Einführung von DRM-Systemen schlagartig sein Ende finden.
- Im engeren Sinn stellt sich deshalb die regulatorische Frage, ob und ggf. wer den Zugang und die Nutzung von Information kontrollieren darf. Keinesfalls sollte Technik hier den Einscheidungsrahmen einschränken.

5 Zusammenfassung

In den vorangegangenen Kapiteln wurden Verfahren zum Schutz digitaler Inhalte vorgestellt und bewertet. Die dargestellten Angriffsmethoden machen deutlich, dass die Verfahren in der Praxis keinen perfekten Schutz gewährleisten können.

Nachfolgend sollen die Problematik, die Lösungsansätze und der Stand der Technik noch einmal kurz zusammengefasst werden.

Generelles Schutzziel von DRM-Systemen

DRM-Systeme sollen den Rechteinhabern einen sicheren Vertrieb, differenzierte Rechteverwaltung und eine Kontrolle der Nutzung digitaler Inhalte ermöglichen.

Das Paradoxe an DRM-Systemen ist, dass man einem Kunden einen Inhalt in einer bestimmten Weise zugänglich machen will und muss, ihn gleichzeitig aber daran hindern möchte, *alles* (= beliebiges) damit tun zu können. Sichere Technik, die einem Kunden erlaubte Nutzungsmöglichkeiten einräumt und unerlaubte technisch verhindert oder wenigstens erschwert, ist dabei nur ein Baustein eines DRM-Systems.

Ineinandergreifen von Technik und Recht

Insgesamt erstreckt sich der Schutz nach [4, S.263] über drei Ebenen, die ineinander greifen: Neben

- **Technik**, die ihrerseits durch einen rechtlichen Umgehungsschutz geschützt werden kann, tragen noch
- **Nutzungsverträge** zwischen Kunden und Anbietern, die ihrerseits schützbar sind durch Technik sowie diese wiederum durch den rechtlichen Umgehungsschutz sowie
- **Technologie-Lizenzverträge**

zum Schutz bei (siehe auch Abbildung 5.1). Dieses Ineinandergreifen soll bewirken, dass bei Versagen einer Ebene hoffentlich die nächste einspringt, um die Rechteinhaber zu schützen.

Systematik

Aus technischer Sicht, die ja Gegenstand der vorliegenden Studie ist, stellt sich die Situation folgendermaßen dar. Um das oben formulierte Schutzziel zu erreichen, benötigt man einen

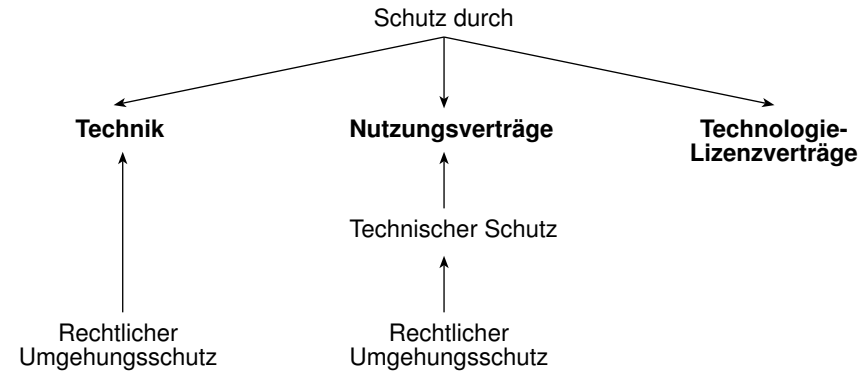

Abbildung 5.1: Unterschiedliche Schutzmechanismen in DRM-Systemen nach [4]

geschützten Bereich GB im Verfügungsbereich VB des Kunden. Dieser GB schützt den Rechteinhaber vor dem Kunden. Daraus folgt, dass GB für den Kunden nicht voll zugänglich sein darf, d.h. GB muss ausforschungssicher gegenüber dem Kunden sein. Diese Forderung entspricht exakt der Forderung, die beispielsweise an Telefon-Wertkarten gestellt werden. Hinzu kommt noch, dass der Inhalt, der dem Kunden zugänglich sein soll, in einer Repräsentation ausgegeben werden muss, die vom Kunden entweder nicht ohne großen Aufwand vervielfältigt werden kann oder den Käufer identifizier- und verfolgbare Informationen eingebettet haben muss, die vom Kunden nicht ohne weiteres entfernbar sind.

Informatischer Ansatz

Für die Analyse von Sicherheitseigenschaften ist die Ausführungs-Schichtenstruktur der beteiligten IT-Systeme grundlegend: Hierbei führt die Schicht i die Objekte der Schicht $i+1$ aus, wobei die Objekte der Schicht i wiederum durch Schicht $i-1$ ausgeführt werden können. Typische Ausführungs-Schichtenstrukturen heutiger IT-Systeme sind (siehe Abbildung 5.2): Die Hardware (Schicht 1: ICs, Leiterbahnen, Fest- und Wechselplatten, u.a. Bauteile angeordnet in Baugruppen, z.B. Prozessor, Arbeitspeicher, Netzwerk-, Audio- und Videokarten, etc.) führt die Systemsoftware (Schicht 2: Betriebssystem, Treiberprogramme etc.) direkt aus. Hardware und Systemsoftware zusammen führen Anwendungssoftware (Schicht 3: Textverarbeitung, Audio-Player, Video-Player, etc.) aus. Die Anwendungssoftware schließlich führt Text(verarbeitung) aus, spielt Tondateien, zeigt Videosequenzen, etc., d.h. führt die Objekte der Ebene 4 aus.

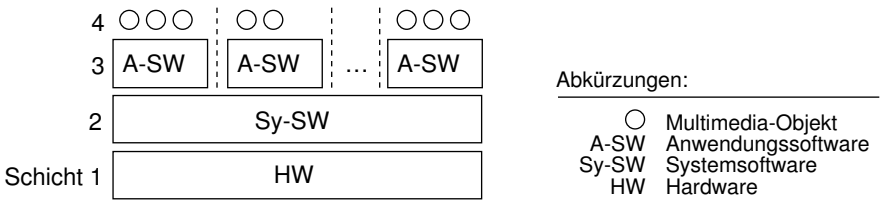

Abbildung 5.2: Ausführungs-Schichtenstruktur

Je nach Anbieter ist der zu schützende Inhalt unterschiedlich: Hardwarehersteller sehen ihre Bauteile als Content, Ersteller der Systemsoftware sehen Systemsoftware als zu schützen-

den Inhalt, Ersteller der Anwendungssoftware sehen beispielsweise Textverarbeitungssoftware, Audio- und Video-Player-Software als Inhalt und Künstler sowie Medienagenturen sehen Tondateien, Videosequenzen etc. als Inhalt.

Grundlegend gilt nun: Ein Schutz der Objekte der Schicht *i* vor den Objekten der darunterliegenden Schichten ist nicht effizient möglich, denn diese müssen die Objekte der Schicht *i* ja ausführen und zumindest insoweit elementar hantieren und „verstehen".

Schutz einer Tondatei vor Missbrauch erfordert Schutz des Audio-Players vor Manipulation. Der Schutz des Audio-Players erfordert wiederum Schutz der Systemsoftware vor Zweckentfremdung und dies schließlich wiederum Schutz der Hardware vor Manipulation — alles jeweils natürlich bezogen auf das konkrete IT-System, auf dem die Tondatei legitimerweise gespielt werden soll.

Bewertung

Im Kapitel 2 wurden Techniken zum Schutz digitaler Inhalte beschrieben. In Tabelle 5.1 werden die Mechanismen noch einmal zusammenfassend dargestellt. In Kapitel 3 wurden die Schwächen von und Angriffsmöglichkeiten auf die Mechanismen vorgestellt.

Man kann davon ausgehen, dass DRM-Systeme zukünftig auch eingesetzt werden, um Hardware- und Softwareplattformen technisch und vertraglich abzusichern, d.h. DRM-Systeme könnten zu einem festen Bestandteil der IT-Infrastruktur auch in Bereichen werden, in denen es nicht nur um mediale Inhalte geht. Die Technik von DRM-Systemen stützt sich im wesentlichen auf grundsätzliche IT-Sicherheitstechniken und ist insofern geeignet, nicht nur multimediale Inhalte, sondern auch beispielsweise Software zu schützen. Insofern deckt diese Studie jede momentan mögliche Form von „Inhalt" und alle derzeit üblichen Distributionsformen (z.B. Online-Dienste und Online-Übertragung, Software-Verteilung und Datenträgeraustausch) ab.

Versuche, den Schutz von Inhalten ausschließlich in Software zu realisieren, sind nahezu hoffnungslos. Dies zeigen die Erfahrungen beim Kopierschutz im Softwarebereich. Für wertvolle Software werden deshalb auch dort Hardwaresysteme (Dongles) eingesetzt.

Verfahren in oder zumindest unter Verwendung von Hardware gewährleisten begrenzten Schutz, da das Knacken der Hardware meist aufwendiger ist. Auch diese Verfahren sind weit entfernt von perfekter Sicherheit.

Da insbesondere die Verfahren, die das Kopieren von Inhalten *verhindern* sollen, nur wenig Sicherheit bieten, wächst die Nachfrage nach Verfahren, die das Kopieren und verbreiten erkennbar und verfolgbar machen. Dies ist auch insofern verständlich, dass Inhalte auch angezeigt bzw. abgespielt werden müssen, d.h. der Schutz sich auch auf die Ausgabekomponente erstrecken müsste, wo die Inhalte hochqualitativ (meist sogar digital) zur Verfügung stehen sollen.

Ausblick

Kriminelle Inhalte ebenso wie die kriminelle Verbreitung von Inhalten im Internet können, wie auch in anderen Medien, nicht einfach toleriert werden. Sie müssen in allen Medien angemessen bekämpft und möglichst verhindert werden. Alle Wege zur Bekämpfung müssen allerdings die Grundentscheidung zwischen Freiheit und Kontrolle treffen. Es gibt neben kulturellen (siehe

Absch.	Schutzsystem/ Technik	Schutzprinzip/ techn. Basis	Was wird bewirkt bzw. verhindert?	Bemerkungen
Präventive Verfahren				
— Verfahren basierend auf physischem Schutz, z.B. in Hardware (HW)				
2.2.3	Dongles	phys. HW-Schutz	verhindert unberechtigte Nutzung von Software	sicher, solange Dongle nicht kopierbar, obwohl Kopieren der Software möglich
2.2.3	Physisch gekapselte (Player)-HW	phys. HW-Schutz	verhindert Abgreifen des digitalen (ggf. entschlüsselten) Medienstroms	mit Aufwand gut, aber nicht perfekt möglich
2.4.3	Inkompatible Formate, Fehlerstellen auf physischem Medium	phys. HW-Schutz, Anbringen eines Sondersignals	verhindert Kopieren durch Aufbringen nicht kopierbarer Stellen auf phys. Medium	sicher, solange keine geeigneten Lese-/Schreibgeräte existieren, meist jedoch gebrochen
— Verfahren basierend auf Software-(SW)-Schutz				
2.2.4	Sandbox	Einkapselung fremder SW	schützt vor bösartiger fremder SW	kein Schutz vor der eigenen Ausführungsumgebung (lokaler PC und dessen Benutzer)
2.4.1	SW-Codes	Geheimhaltung des Codes	verhindert unberechtigte Nutzung, Kopieren möglich	schwacher Schutz, da Codes leicht weitergegeben werden können, meist durch Security-by-obscurity realisiert
3.4.3	DRM-Software	Security-by-obscurity	soll unberechtigte Nutzung des Inhalts verhindern	leicht knackbar, deshalb meist mit einer Zwangs-Update-Funktion ausgestattet, um sicheren Zustand zeitweise wieder herzustellen
— Verfahren zur Absicherung des Distributionsweges				
2.2.2	Verschlüsse-lung	Geheimhaltung eines Schlüssels, Kryptographie	soll unberechtigte Nutzung verhindern und unberechtigtes Kopieren des entschlüsselten Inhalts verhindern, Kopieren des Verschlüsselten leicht	Verhindern der Weitergabe des Schlüssels wie auch des Entschlüsselten ist essentiell, setzt für sichere Anwendung physische Kapselung der Entschlüsselung *und* Digital-Analog-Wandlung voraus
2.3.2	Watermarking	Einbringen eines nicht entfernbaren Sondersignals	soll Wiedererkennung des markierten Inhalts bewirken	Sondersignal kann beliebige Information (z.B. über den Urheber) tragen, Kopieren des markierten Inhalts möglich
2.3.3	Fingerprinting, Traitor Tracing	Kryptographie	bewirkt die Rückverfolgung illegaler Kopien zum legalen Käufer, Kopieren des markierten Inhalts möglich	setzt voraus, dass Inhalte nicht gegen den Willen (oder ohne das Wissen) des legalen Käufers mit Hackermethoden kopiert werden können, sonst fälschliche Beschuldigung
— Codierung mittels Metadaten				
2.4.1	Codes ohne Sicherung	Anbringen eines Kodes	soll Kopieren über mehrere Generationen erschweren	sehr schwacher Schutz, da Codes völlig ungesichert sind und verändert werden können
2.4.2	Regionale Codierung	Anbringen eines Kodes, Verschlüsse-lung des Inhalts	künstliche Marktseparation	Wirkungsvoll, solange Player-Laufwerke noch teuer sind
Reaktive Verfahren				
2.4.5	Aufspüren illegaler Kopien	Inhaltsbasierte Analyse	Rückverfolgung zum Verursacher	zusammen mit Fingerprinting wirkungsvoller
2.4.6	Filter/Sperren	Blockieren des Zugangs	soll den Abruf illegaler Inhalte verhindern	kann meist leicht umgangen werden

Tabelle 5.1: Zusammenfassung der Mechanismen

Abschnitt 4) vor allen Dingen auch technische Gründe, sich für die Freiheit zu entscheiden. Dies darf allerdings nicht missverstanden werden als Aufforderung zur Verbreitung rechtswidriger Inhalte im Internet. Toleranz wäre hier eine Schwäche.

Kopierschutztechniken, technische Nutzungsbeschränkungen und reaktive Verfahren zur Verfolgung (Internet-Kontrollen) sind momentan noch technisch mangelhaft und werden es solange sein, bis international anwend- und durchsetzbare Regeln gelten. Anbieter rechtswidriger Inhalte weichen bei Sperrung beispielsweise auf Server im Ausland aus. Das Internet ist faktisch ein internationales Netz. Wenn Schutzsysteme wirkungsvoll sein sollen, bedarf es erstens eines internationalen Konsens, was rechtswidrige Inhalte sind, und zweitens einer international anerkannten Organisation, die dafür sorgt, dass die Regeln international eingehalten werden.

Der Europarat hat auf die neuen Risiken beispielsweise mit der „Cybercrime Convention“ [11] reagiert, die der Anfang eines internationalen Regelungswerkes zur Verfolgung von Straftaten im und durch das Internet sein soll. Neben Verletzungen des Urheberrechts und der Bereitstellung anderer illegaler Inhalte soll vor allem auch die Verfolgung von Denial-of-Service-Angriffen verbessert werden. Dann wären auch Besitz und Herstellung von Anleitungen und Software zur Begehung von Computerkriminalität strafbar.

Ein weiterer Versuch zur Harmonisierung der Gesetze, die das Internet besser regulierbar machen sollen, ist die „Hague Convention on Jurisdiction and Foreign Judgements in Civil Matters“ [41]. Forderungen nach stärkeren Möglichkeiten, Internet-Benutzer zu kontrollieren, sind Ausdruck des Ohnmachtsgefühls der Regulierer, aber kein Mittel zur Stärkung des mündigen „Internet-Bürgers“.

Technisch mangelhafte Schutzsysteme werden dazu führen, dass Laien in die Sperre laufen. Technisch Versierte lassen sich durch verbesserte Kontrollmöglichkeiten nicht abschrecken. Etwas platt formuliert: Schwache Schutzsysteme schützen vor den Dummen und machen aus den vermeintlich Cleveren Helden.

Politische und gesellschaftliche Diskussion

Die politische und gesellschaftliche Diskussion zu den Folgen des Digital Rights Management wird national wie international auch heftig im Internet geführt. Eine Sammlung solcher Beiträge findet sich unter http://www.inf.tu-dresden.de/~hf2/drm/.

Eine der Botschaften lautet: Nichts ist fataler als ein falsches Sicherheitsgefühl bei den Menschen. Politische Entscheidungen für eine stärkere Kontrolle der Internet-Benutzer werden vielleicht das Sicherheitsgefühl der Menschen stärken, faktisch aber keine höhere technische Sicherheit bieten können.

Dank

Ein herzliches Dankeschön für kleinere und größere Zuarbeiten sowie Unterstützung bei der Recherche, Aufbereitung und Durchsicht des Manuskripts geht an Miriam Busch, Dr. Christian Dressel, Kristian Köhntopp und Stefan Köpsell.

Literaturverzeichnis

[1] D. G. Abraham, et al.: Transaction Security System. IBM Systems Journal 30/2 (1991) 206–229.

[2] Ross J. Anderson, Markus G. Kuhn: Tamper Resistance – a Cautionary Note. In: Proc. Second USENIX Workshop on Electronic Commerce. Oakland, California, Nov. 18–21 1996, 1–11.

[3] Urheberrecht in der Informationsgesellschaft. Gemeinsames Positionspapier von BDB und DBI, Juli 1998. http://www.dbi-berlin.de/dbi_ber/recht/urh-einl.htm.

[4] Stefan Bechthold: Vom Urheber- zum Informationsrecht – Implikationen des Digital Rights Management, Schriftenreihe Information und Recht 33. Verlag C. H. Beck, München, 2002.

[5] F. Beck: Integrated Circuit Failure Analysis – A Guide to Preparation Techniques. John Wiley & Sons, New York, 1998.

[6] S. Blythe, et al.: Layout Reconstruction of Complex Silicon Chips. IEEE Journal of Solid-State Circuits 28/2 (1993) 138–145.

[7] D. Boneh, M. Franklin: An efficient public key traitor tracing scheme. In: Advances in Cryptology – CRYPTO ’99, Lecture Notes in Computer Science 1666. Springer-Verlag, Berlin, 1999, 338–353.

[8] D. Boneh, J. Shaw: Collusion secure fingerprinting for digital data. IEEE Transactions on Information Theory 44/5 (1998) 1897–1905.

[9] Chipseal Tamper Resistant Composite, Dow Corning. http://www.se-com.com/secom/sp/dow.html.

[10] B. Chor, A. Fiat, M. Naor: Tracing traitors. In: Advances in Cryptology – CRYPTO ’94, Lecture Notes in Computer Science 839. Springer-Verlag, Berlin, 1994, 480–491.

[11] Draft Convention on Cybercrime. http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm.

[12] Ingemar Cox, Joe Kilian, Tom Leighton, Talal Shamoon: A Secure, Robust Watermark for Multimedia. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, Lecture Notes in Computer Science 1174. Springer-Verlag, Berlin, 1996, 185–206.

[13] Ingemar J. Cox, Jean-Paul M. G. Linnartz: Some General Methods for Tampering with Watermarks. IEEE Journal on Selected Areas in Communications 16/4 (1998) 587–593.

[14] J. H. Daniel, D. F. Moore, J. F. Walker: Focused Ion Beams for Microfabrication. Engineering Science and Education Journal (1998) 53–56.

[15] Lutz Donnerhacke, Steffen Peter: Vorsicht, Falle! iX 3 (1997) 90.

[16] Digital Video Broadcasting (DVB): Multimedia Home Platform (MHP) Specification 1.0. European Telecommunications Standards Institute, ETSI TS 101 812 V1.1.1 (2000-07).

[17] Cynthia Dwork, Jeffrey Lotspiech, Moni Naor: Digital Signets: Self-Enforcing Protection of Digital Information. In: Proc. 28th ACM Symposium on the Theory of Computing. Philadelphia, Pennsylvania, USA, 22.–24. Mai 1996, 489–498.

[18] Joachim Euchner: Proposal for an open MHP-Implementation. http://www.linuxtv.org/developer/mhp302.html.

[19] Hannes Federrath: Steganographie in Rechnernetzen. In: Tutorium „Sicherheit in Netzen“ der 13. DFN-Arbeitstagung über Kommunikationsnetze. Düsseldorf, 26.–28. Mai 1999. http://www.inf.tu-dresden.de/~hf2/publ/1999/Fede1_99DFNStego.pdf.

[20] Hannes Federrath, Andreas Pfitzmann: Bausteine zur Realisierung mehrseitiger Sicherheit. In: Günter Müller, Andreas Pfitzmann (Hg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison-Wesley-Longman, 1997, 83–104. http://www.inf.tu-dresden.de/~hf2/publ/1997/FePf_97Baust/.

[21] Frank W. Felzmann: Die Task Force „Sicheres Internet“. KES Zeitschrift für Kommunikations- und EDV-Sicherheit 16/3 (2000) 61–68.

[22] H. P. Feuerbaum: Electron Beam Testing: Methods and Applications. Scanning 5/1 (1982) 14–24.

[23] Security Requirements for Cryptographic Modules. FIPS PUB 140-1, Federal Information Processing Standards Publication, National Institute of Standards and Technology, U.S. Department of Commerce, 11. Jan. 1994.

[24] FITUG: IFPI Rights Protection System – A Compiled Fact Sheet. ftp://ftp.fitug.de/pub/eu/RPS02.PDF.

[25] E. Gafni, J. Staddon, Y. L. Yin: Methods for Integrating Traceability and Broadcast Encryption. In: Advances in Cryptology – CRYPTO ’99, Lecture Notes in Computer Science 1666. Springer-Verlag, Berlin, 1999, 372–387.

[26] Clemens Gleich: Entfesselte Musik – Microsofts neues Digital Rights Management ausgehebelt. ct 23 (2001) 62.

[27] Gore D^3 Electronic Security Enclosures. http://www.goreelectronics.com/products/specialty/electronic_security_enclosures.cfm.

[28] Peter Gutmann: Data Remanence in Semiconductor Devices. In: Proc. 10th Usenix Security Symposium. Washington, D.C., 13.–17. Aug. 2001.

[29] Heise-News: Schily empfiehlt Sofortmaßnahmen für sichereres Internet, 25. Apr. 2000. http://www.heise.de/newsticker/data/fm-25.04.00-000/.

[30] Identification cards – Integrated circuit(s) cards with contacts. ISO 7816, International Organization for Standardization, Geneva.

[31] D. Kahn: The Codebreakers – The Story of Secret Writing. Macmillan, New York, 1967.

[32] Auguste Kerckhoffs: La cryptographie militaire. Journal des sciences militaires, Vol. IX, 5–38, Jan. 1883, 161–191, Feb. 1883. http://www.cl.cam.ac.uk/~fapp2/kerckhoffs/.

[33] Will Knight: Sony locks CDs to stop internet copying. The New Scientist Online. http://www.newscientist.com/news/news.jsp?id=ns99991336.

[34] P. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Advances in Cryptology – CRYPTO '96, Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1996, 104–113.

[35] P. Kocher, J. Jaffe, B. Jun: Differential Power Analysis. In: Advances in Cryptology – CRYPTO '99, Lecture Notes in Computer Science 1666. Springer-Verlag, Berlin, 1999, 388–397.

[36] Kristian Köhntopp, Marit Köhntopp, Martin Seeger: Sperrungen im Internet. Datenschutz und Datensicherheit DuD 21/11 (1997) 626–631.

[37] Oliver Kömmerling, Markus G. Kuhn: Design Principles for Tamper-Resistant Smartcard Processors. In: Proc. USENIX Workshop on Smartcard Technology (Smartcard '99). USENIX Association, Chicago, Illinois, USA, 10.–11. Mai 1999, 9–20.

[38] D. Kosiur: IP Multicasting. Wiley, 1998.

[39] Markus Kuhn, Fabian Petitcolas: Stirmark, 1997. http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/.

[40] Petra Labriga: Die Britische Nationalbibliothek auf dem Weg zur elektronischen Bibliothek. Bibliotheksdienst /6 .

[41] Julia Lawlor: From the Trenches: Do laws know no bounds?, 16. Okt. 2001. http://www.redherring.com/index.asp?layout=story_imu&doc_id=1570020357&channel=10000001.

[42] Macrovision Video Copy Protection. http://www.macrovision.com/solutions/video/copyprotect/.

[43] D. P. Maher: Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective. In: Proc. Financial Cryptography, FC '97, Lecture Notes in Computer Science 1318. Springer-Verlag, Berlin, 1997, 109–121.

[44] Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist. Datenschutz und Datensicherheit DuD 18/6 (1994) 318–326.

[45] Moni Naor, Benny Pinkas: Threshold Traitor Tracing. In: Proc. 18th Annual International Cryptology Conference, Lecture Notes in Computer Science 1462. Springer-Verlag, Berlin, 1996, 502–517.

[46] Antti Paarlahti: Macrovision FAQ, v1.1, Tampere, Finland, 1995. http://ee.tut.fi/~pam/macrovision/macrov_faq_v1.1.txt.

[47] Fabien A. P. Petitcolas, Ross Anderson, Markus G. Kuhn: Attacks on copyright marking systems. In: David Aucsmith (Hg.): Proc. 2nd Workshop on Information Hiding, Lecture Notes in Computer Science 1525. Springer-Verlag, Berlin, 1998, 218–238.

[48] Birgit Pfitzmann: Trials of traced traitors. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, Lecture Notes in Computer Science 1174. Springer-Verlag, Berlin, 1996, 49–64.

[49] Birgit Pfitzmann, Michael Waidner: Kopierschutz durch asymmetrische Schlüsselkennzeichnung mit Signeten. In: Verläßliche IT-Systeme, GI-Fachtagung VIS ’97, DuD Fachbeiträge. Vieweg-Verlag, Wiesbaden, 1997, 17–32.

[50] Birgit Pfitzmann, Michael Waidner: Kopierschutz durch asymmetrisches Fingerprinting. Datenschutz und Datensicherheit DuD 22/5 (1998) 258–264.

[51] H. Reinitzer: Papierzerfall – Kulturzerfall? Über die Probleme der Bewahrung des ‚geistigen Erbes‘. Bibliotheksdienst 28/12 (1994) 1911–1925.

[52] Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2. Aufl. John Wiley & Sons, New York, 1996. (Die deutsche Übersetzung ist bei Addison-Wesley-Longman erschienen.).

[53] Sergei Skorobogatov: Low Temperature Data Remanence in Static RAM. University of Cambridge Computer Laboratory, 2001. http://www.cl.cam.ac.uk/~sps32/sram_article.pdf.

[54] Joshua Smith, Barrett Comiskey: Modulation and Information Hiding in Images. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, LNCS 1174. Springer-Verlag, Berlin, 1996, 207–226.

[55] Viktor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols. ACM Computing Surveys 15/2 (1983) 135–170.

[56] Steve H. Weingart: Physical Security for the μABYSS System. In: Proc. 1987 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 27.–29. Apr. 1987, 52–58.

[57] Jian Zhao: Look, it’s not there. Byte 22/1 (1997) 7–12.

Strafrechtlicher Teil

Verfasser:

Prof. Dr. Ulrich Sieber, Ordinarius für Strafrecht, Informationsrecht und Rechtsinformatik an der Ludwig-Maximilians-Universität München

Inhaltsverzeichnis

I. Einführung

Das vorliegende Gutachten entstand im Auftrag des Deutschen Multimedia Verbandes (dmmv) e.V. und des Verbandes Privater Rundfunk und Telekommunikation (VPRT) e.V. Es untersucht die Frage, inwieweit die in den neuen Medien digital verbreiteten geistigen Werke strafrechtlich angemessen geschützt sind und ob insoweit gesetzliche Neuregelungen erforderlich sind.

Das Hauptziel des Gutachtens liegt dabei im rechtspolitischen Bereich. Es soll darüber hinaus jedoch auch für die Nutzer die Grenzen des strafrechtlich verbotenen Tuns aufzeigen sowie den Strafverfolgungsbehörden, den betroffenen Opfern und ihren Verbänden eine praktische Handreichung für die bessere Beurteilung der einschlägigen Delikte geben. Diese letztgenannte Zielsetzung ist insbesondere deswegen von Bedeutung, weil die Arbeit an dem vorliegenden Gutachten gezeigt hat, dass der Schutz geistiger Güter im Bereich der neuen Medien nicht nur gesetzliche Neuregelungen erfordert, sondern vor allem auch eine bessere Umsetzung bereits bestehender Normen.

Die Anwendbarkeit des geltenden Rechts de lege lata und das Erfordernis strafrechtlicher Regelungen de lege ferenda können nur im Hinblick auf konkrete Angriffsformen sowie die konkrete Bedrohungssituation der potentiell schutzwürdigen Rechtsgüter beurteilt werden. Das vorliegende Gutachten analysiert deswegen zunächst in einem ersten empirischen Teil, welche digital verkörperten Güter zur Zeit durch welche Angriffsformen und Täterstrukturen bedroht sind. Der zweite Teil des Gutachtens untersucht dann, inwieweit diese Angriffsformen durch das geltende Recht erfasst werden. Im dritten Teil werden auf der Grundlage der empirischen Analyse sowie der rechtlichen Beurteilung abschließend Vorschläge für eine effektive rechtliche Schutzstrategie und für gesetzliche Neuregelungen unterbreitet.

II. Empirische Grundlagen

A. Betroffene Güter

Seit die Rechtsordnung Werke der Literatur, Wissenschaft und Kunst schützt, stellt sich auch das Problem der unberechtigten Vervielfältigung dieser Werke sowie der Verbreitung der so hergestellten Kopien. Waren Raubkopien in der traditionellen „analogen“ Welt teilweise noch – etwa durch Abschreiben oder Abmalen – aufwändig herzustellen und – etwa bei analogen Audiokopien – auch von wesentlich schlechterer Qualität als das Original,[1] so änderte sich dies mit der Digitalisierung und der massenhaften Verbreitung von Personal Computern (PC) vollkommen. Heute bietet jeder Standard-PC vielfältige und vor allem einfach zu bedienende Möglichkeiten zur Kopie und Verbreitung urheberrechtlich geschützter Werke. Diese Kopien erfolgen dabei häufig ohne oder gegen den Willen des Berechtigten, da – wie das Gutachten von *Pfitzmann*/*Federrath*/*Kuhn* zeigt – Kopierschutzmechanismen im weitesten Sinne entweder nicht funktionieren oder relativ leicht umgangen werden können.

Besonders betroffen vom Problem der digitalen Piraterie sind dabei Computersoftware sowie Audio- und Videodaten. Sie stehen deshalb auch im Focus der folgenden Untersuchung. Daneben findet sich digitale Piraterie allerdings auch im Bereich von Bildern und Texten, etwa bei elektronischen Büchern (so genannten E-Books), für welche die folgenden Ausführungen zu den Schutzmechanismen und Angriffsszenarien entsprechend gelten (z.B. im Hinblick auf die im Internet angebotenen Tools, die ein Umgehen des Kopierschutzes von PDF-Dateien ermöglichen).[2] Hinzu kommen – urheberrechtlich nicht geschützte – Daten wie Aktienkurse oder Wirtschaftsdaten. Die im Folgenden analysierten Angriffe auf Computersoftware sowie Audio- und Videodaten stehen daher prototypisch für die Verletzung geistiger Werke in der modernen Informationsgesellschaft.

1. Software

a) Legaler Markt

Den weltweit wirtschaftlich bedeutendsten Bereich der von Raubkopien betroffenen digitalen Inhalte stellen derzeit die Softwareprodukte dar. Trotz des schwierigen wirtschaftlichen Umfeldes im Jahr 2001 sind die Umsatzzahlen im Bereich der Software nach wie vor beeindruckend. So wurden nach einer Studie der Diebold Deutschland GmbH im Bereich der Systemsoftware (insbesondere Betriebssysteme) und der Standardapplikationen (insbesondere Officeanwendungen) in Deutschland im letzten Jahr ca. 14 Milliarden Euro umgesetzt.[3] Software-Projekte

1. Siehe auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 8.
2. Vgl. http://www.heise.de/newsticker/data/daa-28.06.01-001/ (Stand: 12.8.2002).
3. Vgl. http://www.diebold.de/media/pdf/IT-Trends_2002_.pdf?sid=76c3d84f95a8c762eb4c9e68ed

(insbesondere Individualentwicklung, Customizing) erzielten einen Umsatz von ca. 9 Milliarden Euro.[4] Dies entspricht im Vergleich zum Jahr 2000 sowohl bei der Systemsoftware als auch bei den Software-Projekten in etwa einer Steigerung von 8%.[5] Auch für das Jahr 2002 wird in beiden Bereichen wieder mit einer Wachstumssteigerung von ca. 8% gerechnet, was einem Gesamtmarktvolumen von insgesamt ca. 25 Milliarden Euro entspricht. Die wirtschaftliche Bedeutung der Softwarebranche lässt sich auch daran ablesen, dass Software nach einer Studie des European Information Technology Observatory (EITO) auf dem europäischen Markt – neben den informationstechnischen Dienstleistungen – mit einer Wachstumsrate von ca. 11,5% im Jahr 2002 den wichtigsten Wachstumsmotor im Bereich der Informationstechnik darstellt.[6] In Europa wird der Sektor der Informationstechnik nach dieser Studie im Jahr 2002 ein Marktvolumen von etwa 289 Milliarden Euro erreichen. Die Bedeutung der Softwarebranche zeigt sich eindrucksvoll schließlich auch darin, dass in Deutschland zur Zeit über 390.000 Beschäftigte in den Bereichen Software und IT-Services beschäftigt sind.[7] Die Softwarepiraterie betrifft damit nicht nur individuelle Einzelinteressen, sondern einen für die Volkswirtschaft wichtigen Industriezweig.

b) Piraterie

Für die betroffenen Hersteller stellt die Softwarepiraterie ein gravierendes wirtschaftliches Problem dar. Aufgrund der Ungewissheit über die einschlägige Dunkelziffer und mangels völlig branchenunabhängiger Gutachten gibt es für diesen Bereich zwar keine verlässlichen neutralen Zahlen. Eine Studie im Auftrag der Business Software Alliance (BSA) – einem Interessenverband vor allem der Softwareindustrie – schätzte die weltweiten Verluste durch Raubkopien von Softwareprodukten im Jahr 2000 jedoch auf 11,75 Milliarden US-Dollar.[8] Unterstützt wird dieser Befund durch eine Konsumentenbefragung der BSA, wonach 25% derjenigen Personen, die im Internet Software downloaden, erklärten, sie würden niemals für Software bezahlen.[9] Für die Bundesrepublik Deutschland ergeben sich nach der BSA-Studie bei einer Raubkopie-Rate von 28% Verluste in Höhe von ca. 635 Millionen US-Dollar. Deutschland rangiert damit bei den Verlusten der Industrie in West-Europa auf Platz eins, gefolgt vom Vereinigten Königreich und Frankreich.[10] Der Verband der Unterhaltungssoftware Deutschland (VUD) geht davon aus, dass es sich bei 25% der eingesetzten Computer- und Videospiele um Raubkopien handelt.[11] In anderen Staaten ist der Anteil der Raubkopien noch höher. Nach Presseberichten arbeiten z.B. in Taiwan selbst die meisten Regierungsstellen mit Raubkopien, was den taiwanesischen Premierminister nun allerdings zu einem Eingreifen veranlasst haben soll.[12]

5db604 (Stand: 12.8.2002).

4. Vgl. http://www.diebold.de/media/pdf/IT-Trends_2002_.pdf?sid=76c3d84f95a8c762eb4c9e68ed5db604 (Stand: 12.8.2002).
5. Vgl. http://www.diebold.de/media/pdf/IT-Trends_2002_.pdf?sid=76c3d84f95a8c762eb4c9e68ed5db604 (Stand: 12.8.2002).
6. Vgl. http://www.eito.com/PAGES/EITO/ABSTRACT/pr191001.htm (Stand: 12.8.2002).
7. Vgl. http://nachrichten.t-online-business.de/busi/them/nach/cebi/ar/info/ar-it-branche-selbstbewusstsein,templateId=Content.jsp,iID=764970.html (Stand: 12.8.2002).
8. Vgl. http://www.bsa.org/resources/2001-05-21.55.pdf, S. 1 (Stand: 12.8.2002).
9. Vgl. http://www.bsa.org/resources/2002-05-29.117.pdf (Stand: 12.8.2002).
10. Vgl. http://www.bsa.org/resources/2001-05-21.55.pdf, S. 5 (Stand: 12.8.2002).
11. Vgl. http://www.stern.de/computer-netze/spezial/raubkopieren/artikel_45741.html?seite=3 (Stand: 12.8.2002).
12. Vgl. http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3081237.htm

Den wirtschaftlich schwerwiegendsten Bereich stellen die professionellen Raubkopierer – insbesondere in Asien und Osteuropa – dar.[13] Dort werden in großen Kopierwerken Raubkopien kommerzieller Softwareprodukte erstellt und anschließend auf dem freien Markt vertrieben.[14] So konnte z.B. in Kuala Lumpur die Software Microsoft WindowsXP, die offiziell ab ca. 150 US-Dollar verkauft wird, für 1,50 US-Dollar erworben werden.[15] Die Raubkopien entsprechen dabei nicht nur inhaltlich dem Original, sondern imitieren es auch in Bezug auf die Beschriftung der Datenträger und die Verpackung der Software.

Bei den Vertriebswegen der Raubkopien lassen sich vor allem zwei Formen unterscheiden: Zum einen erfolgt die Verbreitung auf Datenträgern, die entweder von professionellen Tätern in großem Umfang produziert oder von privaten Gelegenheitstätern erstellt werden; in jüngster Zeit treten dabei neben den klassischen Verkauf der Datenträger häufig Angebote zum Kauf von Raubkopien bei den Online-Auktionsanbietern. Zum anderen werden die Raubkopien über das Internet verbreitet, wobei sämtliche Internet-Dienste (z.B. WWW, FTP, Usenet, IRC, Instant Messaging, File-Sharing-Systemen) genutzt werden. Bei dieser Verbreitung von Raubkopien im Internet spielen vor allem spezielle WWW-Seiten sowie die so genannten File-Sharing-Systeme eine zentrale Rolle. Das nach wie vor größte Problem stellen dabei Internetseiten dar, auf denen kommerzielle Softwareprodukte kostenlos zum Download angeboten werden. Regelmäßig handelt es sich um so genannte „Warez-Sites“, auf denen üblicherweise nicht nur die Software zum Download bereit steht, sondern auch Seriennummern sowie „Hacks“ und „Cracks“, welche die Umgehung von Kopierschutzmechanismen ermöglichen. Gelegentlich dienen die über das WWW erreichbaren Warez-Sites auch nur dazu, die „Interessenten“ zu FTP-Servern weiterzuleiten, da diese Server insbesondere im Falle ihrer Entdeckung schnell geschlossen und genauso schnell unter einer neuen Adresse wieder eröffnet werden können.

Die Situation für die Hersteller kommerzieller Software hat sich dabei noch dadurch verschärft, dass – wie bereits erwähnt – inzwischen auch die so genannten File-Sharing-Systeme zum Austausch von raubkopierten Softwareprodukten genutzt werden. Bei den File-Sharing-Systemen handelt es sich um Peer-to-Peer-Systeme, bei denen sich die Raubkopien nicht auf dem zentralen Server eines Dritten befinden, sondern direkt zwischen den Nutzern bzw. deren Computersystemen ausgetauscht werden. Damit wird die Verfolgung von Raubkopierern deutlich erschwert, da es an dem Betreiber eines zentralen Server fehlt, gegen den im Falle seiner Entdeckung rechtliche Schritte eingeleitet werden können. Das selbe gilt im übrigen für den Austausch von Raubkopien in privaten Chaträumen oder über Instant-Messaging-Programme.

2. Audio-Daten

a) Legaler Markt

In dem bereits seit längerem bestehenden Markt der Audioinhalte wird der Wandel des Raubkopierens durch die Digitalisierung besonders deutlich: Als Thomas Edison im Jahre 1877 den

(Stand: 12.8.2002).

13. Vgl. dazu die Übersicht unter http://www.stern.de/computer-netze/spezial/raubkopieren/artikel_45704.html (Stand: 12.8.2002).
14. Vgl. http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/hob-13.01.00-001/ (Stand: 12.8.2002).
15. Vgl. http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/ps-25.09.01-000/ (Stand: 12.8.2002).

Phonographen (d.h. die Audioaufzeichnung auf einer Zinnwalze) erfand,[16] war nicht vorstellbar, dass sich das Anhören von Musik mittels einer „Tonkonserve“ einmal zu einem Massenmarkt entwickeln würde. Es dauerte dann auch bis zum Jahr 1947 bis die ersten Langspielplatten auf den Markt kamen.[17] Musikpiraterie war zu dieser Zeit und auch später allerdings kein sehr großes Problem, da es zumindest für die Masse der Verbraucher keine Geräte zu kaufen gab, die eine Überspielung von Schallplatten auf ein anderes Medium ermöglicht hätten. Dies änderte sich allerdings grundlegend, als die Firma Philips im Jahr 1963 die Audiokassette einführte und in den Folgejahren von der Firma Dolby die Rauschunterdrückung für Audiokassetten entwickelt wurde:[18] Ab diesem Zeitpunkt konnte praktisch jedermann Kopien von Schallplatten in zumindest akzeptabler Qualität erstellen. Eine „Explosion“ erlebte der Audiokassettenmarkt dann ab dem Jahr 1979 als Sony den so genannten Walkman[19] – einen portablen Audiokassettenspieler – in den Vertrieb brachte.

Trotz der einfachen und insbesondere billigen Kopierbarkeit von Schallplatten wurde die Plattenindustrie durch das Problem der Raubkopien jedoch noch nicht in gravierender Weise bedroht, da Audiokassetten nicht die Tonqualität von Schallplatten erreichen, die Tonqualität einer Audiokassette aufgrund des mechanischen Bandabriebs im Lauf der Zeit stark abnimmt und vor allem eine Abgabe für Audiokassetten und entsprechende Abspielgräte eingeführt wurde, so dass eine finanzielle Kompensation der Urheber und anderer Rechteinhaber erfolgen kann. Ab dem Jahr 1982 wandte sich dann das Blatt zunächst weitgehend zugunsten der Phonoindustrie, als von den Firmen Sony und Philips die bis heute für Audioaufzeichnungen übliche Audio Compact Disc (Audio-CD) eingeführt wurde, die digitale Aufzeichnungen beinhaltet und damit verlustfrei beliebig oft abgespielt werden kann.[20] Da es zu diesem Zeitpunkt nur die analoge Audiokassette als Medium zur Überspielung von Audio-CDs gab, bestand kein all zu großes wirtschaftliches Risiko, auch weil der Qualitätsunterschied zwischen beiden Trägermedien signifikant ist und – wie bereits erwähnt – entsprechende Abgaben zu entrichten sind.

Die Phonoindustrie versuchte daher auch in der Folgezeit darauf zu achten, dass jede Kopie von einer CD – egal auf welches Medium – entweder mit einem Qualitätsverlust behaftet oder eine digitale Aufnahme gänzlich unmöglich war. Auf letzterem Prinzip beruht z.B. das Serial Copy Management System (SCMS) aus dem Jahr 1990, welches in jedem digitalen Audio-Aufnahmegerät implementiert ist und steuert, ob digitale Audiodaten nicht, nur einmal oder beliebig oft auf einen anderen digitalen Datenträger kopiert werden dürfen.[21] Diese Strategie zur Eindämmung von Raubkopien funktionierte so lange, wie es für den Verbraucher keine Möglichkeit gab, digitale Daten 1:1 zu kopieren oder auszulesen, da in diesem Fall z.B. auch die SCMS-Daten einfach mitkopiert, nicht aber ausgewertet werden.[22] Mit der massenhaften Verbreitung von Heim-PCs und darin eingebauten CD-Brennern ab ca. 1998 änderten sich dann jedoch die „Machtverhältnisse“. Nun konnte und kann der Verbraucher Kopien von Audio-CDs ohne oder ohne merklichen Qualitätsverlust erstellen, indem er die Audiodaten direkt auf einen so genannten CD-Rohling „brennt“ oder die Audiodaten von der CD ausliest und in einen anderes Datenformat konvertiert sowie wieder auf einem digitalen Datenträger abspeichert.[23] Be-

16. Vgl. http://bnoack.com/history/history-de.html (Stand: 12.8.2002).
17. Vgl. http://bnoack.com/history/history-de.html (Stand: 12.8.2002).
18. Vgl. http://bnoack.com/history/history-de.html (Stand: 12.8.2002).
19. Vgl. http://bnoack.com/history/history-de.html (Stand: 12.8.2002).
20. Vgl. http://bnoack.com/history/history-de.html (Stand: 12.8.2002).
21. Siehe dazu näher *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 38 f.
22. Siehe *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 39.
23. Siehe auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 8.

liebtestes Format zur Komprimierung von Audiodateien ist dabei das MP3-Format (MPEG[24] Audio Layer 3), welches von *Pfitzmann*/*Federrath*/*Kuhn* näher erörtert wird.[25] Wie drastisch dieser technikbedingte Wechsel der „Machtverhältnisse“ tatsächlich ist, zeigt sich sehr deutlich an den aktuellen Marktdaten: Nach einer Umfrage des Bundesverbandes der deutschen phonographischen Wirtschaft e.V. wurden im Jahr 2001 insgesamt 182 Millionen CD-Rohlinge privat mit Musik bespielt, aber „nur“ 173,4 Millionen kommerzielle Musik-CDs verkauft.[26]

Dieser Bedrohung versucht die Audioindustrie heute mit verschiedenen Strategien zu begegnen. Zum einen wird mittels Kopierschutzverfahren versucht, die Erstellung von Kopien zu verhindern.[27] Zum anderen wird der Versuch unternommen, den Tausch von Audiodateien im Internet zu unterbinden.[28] Darüber hinaus setzt man auch auf neue Datenträgerformate. So sind die Nachfolger der Audio-CD bereits auf dem Markt. Es handelt sich dabei um die Super Audio CD (SACD) der Firma Sony und um die Audio-DVD. Beide Tonträgerformate haben für die Phonoindustrie den Vorteil, dass sie besser vor unberechtigten Kopiervorgängen geschützt sind und zudem auch noch keine Hardware für die entsprechenden Formate verfügbar ist bzw. die Kosten für das „Equipment“ noch in keinem Verhältnis zum Preis kommerzieller Audio-CDs stehen. Das Verkaufsargument der Musikbranche für die neuen Tonformate ist im übrigen die gegenüber einer konventionellen Audio-CD deutlich bessere Tonqualität (höhere Abtastrate und Mehrkanalton).[29] Die Phonoindustrie setzt damit wieder auf die bewährte Strategie, Tonträger anzubieten, die mit der selben Klanggüte (noch) nicht kopiert werden können.

b) Piraterie

Im Bereich digitaler Audiodaten findet die Piraterie heute insbesondere auf zwei verschiedene Arten statt. Zum einen werden Originale von Audio-CDs nicht nur für den privaten Gebrauch, sondern in großem Umfang oder auch gewerblich auf wiederbeschreibbare CD-Rohlinge kopiert („gebrannt“). Zum anderen werden urheberrechtlich geschützte Musikstücke im Internet vor allem über so genannte File-Sharing-Systeme – wie KaZaA oder Morpheus – von den Nutzern direkt über PCs getauscht und dann häufig wiederum auf einen CD- oder DVD-Rohling kopiert. In beiden Fallkonstellationen kam den Nutzern bisher zugute, dass Audio-CDs nicht kopiergeschützt waren und daher leicht kopiert bzw. über das Internet verbreitet werden konnten. Teilweise tauchen Musikstücke aber auch schon vor ihrer offiziellen Veröffentlichung auf CD im Internet auf, so dass die Vermutung nahe liegt, dass z.B. Studiopersonal heimlich Mitschnitte erstellt und diese dann über das Internet zugänglich macht.[30]

24. MPEG steht für „Motion Pictures Expert Group“. Diese Gremium setzt die Standards fest für die Kompression von Video- und den dazugehörigen Audiodaten, vgl. http://mpeg.telecomitalialab.com/ (Stand: 12.8.2002).
25. Vgl. *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 10.
26. Vgl. http://www.spiegel.de/wirtschaft/0,1518,188274,00.html (Stand: 12.8.2002).
27. Siehe hierzu unten II. B. 1. c).
28. Siehe dazu unten II. B. 2. b).
29. Vgl. in diesem Zusammenhang auch die Ausführungen von Gebhardt vom Bundesverband Phono e.V., abrufbar unter http://www.tagesschau.de/aktuell/meldungen/0,2044,OID680658_TYP4,00.html (Stand: 12.8.2002).
30. So vermutlich geschehen mit dem Musikalbum „Heathen Chemistry“ der britischen Rockband Oasis, vgl. http://www.spiegel.de/kultur/musik/0,1518,192938,00.html; siehe in diesem Zusammenhang aber auch http://www.heise.de/tp/deutsch/inhalt/musik/12411/1.html (Stand: 12.8.2002).

Besonders schwer hat die Phonoindustrie unter der Verbreitung raubkopierter Musikstücke zu leiden. So geht die deutsche Musikwirtschaft nach eigener Aussage z.B. für das Jahr 2000 von einem Umsatzverlust durch Raubkopien von 645 Millionen DM[31] (ca. 330 Millionen Euro) und für das Jahr 2001 von sinkenden Umsätzen – hauptsächlich verursacht durch Raubkopien – von über 10% bzw. 700 Millionen Euro aus.[32] Dies beruht vor allem darauf, dass auf über 50% der insgesamt in Deutschland verkauften CD-Rohlinge Musik kopiert wird, die entweder von einer Original Audio-CD stammt oder die kostenlos aus dem Internet von den Nutzern downgeloadet wird.[33] So wurden nach einer Schätzung von *Gebhardt* vom Bundesverband Phono e.V. im Jahr 2001 in Deutschland insgesamt 492 Millionen Musikstücke aus dem Internet downgeloadet.[34] Das Problem verdeutlicht auch eine Studie der Firma MORI (Market & Opinion Research International), wonach im Jahr 2000 in Europa über 20 Millionen Erwachsene Musik aus dem Internet herunterluden und 45% dieser Personen die so bezogenen Musikstücke auf einen CD-Rohling kopierten.[35] Ähnlich stellt sich die Situation auch in den USA dar: Nach einer Studie des Marktforschungsinstituts Odyssey haben in den USA in den letzten sechs Monaten über 40 Millionen US-Konsumenten im Internet Musikstücke downgeloadet bzw. ausgetauscht.[36] Nach Angaben der „International Federation of the Phonographic Industry“ (IFPI) fiel im Jahr 2001 der weltweite Umsatz im Musikbereich um 5% auf ca. 33,7 Milliarden US-Dollar (ca. 38 Milliarden Euro). Zumindest einen Teil dieses Rückgangs führt die IFPI auf das Problem der Raubkopien zurück, ohne allerdings genaue Zahlen liefern zu können.[37] Daneben leiden auch die Musik-Einzelhändler unter dem Problem der Raubkopien, da immer weniger Audio-CDs käuflich erworben werden. Allerdings wird sich deren Situation – trotz sicherer Kopierschutzmechanismen – vermutlich auch in der Zukunft kaum bessern, da die von der Phonoindustrie forcierte Einführung kommerzieller Tauschbörsen im Internet zu einem weiteren Rückgang der Verkaufszahlen im Einzelhandel führen wird.

Angesichts dieser für die Phonoindustrie prekären Situation tauchen immer wieder Pressemeldungen auf, dass die Musikindustrie bewusst minderwertige – z.B. mit Störgeräuschen versehene – Audiodateien in den Online-Tauschbörsen anbietet. Minderwertige Audiodateien sind für den Nutzer beim Download als solche nicht erkennbar und sollen nach diesen Meldungen beim Abspielen ein „Frusterlebnis“ erzeugen.[38] Daneben kursieren auch Gerüchte, dass in den Tauschbörsen bewusst Viren von den Rechteinhabern eingesetzt werden, um den Tausch urheberrechtlich geschützter Inhalte zu sabotieren.[39] Nahrung erhalten diese Gerüchte nicht zuletzt

31. Vgl. http://www.ifpi.de/jb/2001/jb01b.html (Stand: 12.8.2002).
32. Vgl. http://www.ifpi.de/news/news-175.htm und http://www.heise.de/newsticker/data/anw-16.04.02-004/. Interessant ist daran auch, dass die Phonoindustrie damit bereits im vierten Jahr hintereinander einen Umsatzrückgang hinnehmen muss, vgl. http://www.ifpi.de/jb/2001/jb01b.html (Stand: 12.8.2002).
33. Vgl. http://www.ifpi.de/news/129/DigitaleAufnahmen2001.ppt. Allerdings ist in diesem Kontext zu beachten, dass ein Zusammenhang zwischen dem illegalen Download von Musikstücken und dem aktuellen Umsatzrückgang der Phonoindustrie immer wieder bestritten wird, vgl. http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=176497 und http://www.heise.de/newsticker/data/anw-10.05.02-005/ (Stand: 12.8.2002).
34. Vgl. http://www.tagesschau.de/aktuell/meldungen/0,2044,OID680658_TYP4,00.html (Stand: 12.8.2002).
35. Die Studie wird zitiert im IFPI Music Piracy Report 2001, S. 4, vgl. http://www.ifpi.org/site-content/library/piracy2001.pdf (Stand: 12.8.2002).
36. Vgl. http://www.newsbytes.com/news/02/175893.html (Stand: 12.8.2002).
37. Vgl. http://www.nytimes.com/2002/04/17/technology/17MUSI.html (Stand: 12.8.2002).
38. Vgl. http://www.spiegel.de/netzwelt/netzkultur/0,1518,206714,00.html (Stand: 9.8.2002).
39. Vgl. http://www.spiegel.de/netzwelt/netzkultur/0,1518,206714,00.html (Stand: 9.8.2002).

dadurch, dass in den USA inzwischen im Repräsentantenhaus des US-Kongresses ein Gesetzentwurf eingebracht wurde, der es Rechteinhabern erlauben würde, mit Hackingmethoden gegen die Verbreitung von urheberrechtlich geschützten Werken vorzugehen ohne dabei für die Blockierung, Zerstörung usw. ihrer Werke haftbar zu sein.[40] Unter rechtlichen Gesichtspunkten führt dies zu der Frage, inwieweit derartige Vorgehensweisen – falls sie tatsächlich erfolgen sollten – durch Notwehr oder Notstand gerechtfertigt wären.[41]

3. Video-Daten

a) Legaler Markt

Die Entwicklung kommerzieller Videoprodukte für den Endverbraucher sowie der privaten Videoaufzeichnung begann – zumindest im Bereich des Massenmarktes – letztlich erst mit der Erfindung des VHS-Video-Recorders durch die Firma JVC im Jahre 1976.[42] Davor war es für Privatpersonen nicht bzw. nur schwer möglich und vor allem teuer, Videoinhalte – insbesondere Fernsehprogramme – aufzuzeichnen. In den ersten Jahrzehnten nach der Einführung des Videorecorders gab es dann zunächst noch keine digitalen Videoquellen, so dass es sich lediglich um analoge Videoaufzeichnungen handelte, die systembedingt keine perfekte Bildqualität liefern. Der Reiz, die Inhalte von Videokassetten oder auch von Fernsehrprogrammen zu kopieren, hielt sich deshalb in Grenzen. Zudem wurde analog zur Audiokassette auch für Videokassetten und entsprechende Abspielgeräte eine Urheberabgabe eingeführt. Auch hier trat ein grundlegender Wandel erst mit der Einführung der Digitaltechnik und insbesondere der DVD bzw. des digitalen Fernsehens ein.[43]

Im Videosektor wird der legale Markt seit ca. 2 Jahren vor allem durch den Verkauf und die Vermietung von Video-DVDs getragen, auf denen insbesondere Spielfilme digital und daher in exzellenter Bild- und Tonqualität abgespeichert sind. So besitzen nach einer Focus-Studie inzwischen rund 3 Millionen Bundesbürger einen DVD-Player und bereits im ersten Halbjahr 2001 hatte der DVD-Kaufmarkt ein Volumen von 303 Millionen DM (ca. 155 Millionen Euro).[44] Insgesamt wurde für 2001 in Deutschland mit einem Absatz von rund 3 Millionen DVDs gerechnet.[45] Bis Ende 2002 rechnen die Hersteller von Unterhaltungselektronik damit, dass in Deutschland 5,2 Millionen Haushalte mit einem DVD-Player ausgestattet sein werden.[46] Dabei

40. Vgl. H.R. 5211, 107. Kongress, abrufbar unter http://thomas.loc.gov; siehe auch http://www.heise.de/tp/deutsch/inhalt/te/12978/1.html (Stand: 9.8.2002).
41. In Deutschland ist die Frage bisher kaum geklärt, inwieweit die Inhaber von Urheberrechten sich bei der Rechtsdurchsetzung, z.B. beim Eindringen in fremde Rechnersysteme zwecks Feststellung von Raubkopien, auf die Rechtfertigungsgründe der Notwehr und des Notstandes berufen können. Diese Rechtfertigungsgründe dürften – vor allem auch wegen des Erfordernisses der „Gegenwärtigkeit“ des Angriffs im Sinne von § 32 StGB sowie wegen der Angemessenheitsklausel von § 34 StGB – jedoch nur in Sonderfällen zur Anwendung kommen.
42. Vgl. http://www.jvc.ch/de/inside/inside.htm (Stand: 12.8.2002).
43. Siehe in diesem Zusammenhang auch die Entscheidung des Berufsgerichts im Fall „MPAA gegen Corley und 2600 Enterprises“, abrufbar unter http://cryptome.org/mpaa-v-2600-cad.htm (Stand: 12.8.2002).
44. Vgl. http://medialine.focus.de/PM1D/PM1DN/PM1DNA/DOWNLOAD/01uelekt.pdf, S. 7 f. (Stand: 12.8.2002).
45. Vgl. http://medialine.focus.de/PM1D/PM1DN/PM1DNA/DOWNLOAD/01uelekt.pdf, S. 8 f. (Stand: 12.8.2002).
46. Vgl. http://www.spiegel.de/netzwelt/technologie/0,1518,192043,00.html (Stand: 12.8.2002).

ist davon auszugehen, dass Video-DVDs schon in wenigen Jahren die analogen VHS-Kassetten nahezu vollständig verdrängt haben werden.

Daneben spielt das kostenpflichtige aber auch das frei empfangbare digitale Fernsehen eine gewisse Rolle bei der Verbreitung von Video-Inhalten, insbesondere von Spielfilmen, TV-Serien und Sportereignissen. Die Abonnentenzahl der digitalen Pay-TV Anbieter bleibt allerdings europaweit hinter den Erwartungen der Anbieter zurück, was auch damit zusammenhängt, dass inzwischen nahezu alle Fernsehsender frei empfangbare digitale Fernsehprogramme über Satellit oder Kabelnetz anbieten.[47]

Schließlich werden Videos – insbesondere Spielfilme – seit einiger Zeit auch direkt über das Internet vermarktet. Allerdings befindet sich dieser Markt gerade erst im Aufbau und entsprechende Angebote leiden noch unter einem relativ geringen Angebot und dem Fehlen einer flächendeckenden Verbreitung von Breitbandzugängen zum Internet. Letzteres ist deshalb von großer Bedeutung, weil Videoinhalte aufgrund der anfallenden riesigen Datenmengen – unabhängig davon, ob sie downgeloadet oder gestreamt werden – mindestens einen DSL- oder einen vergleichbar schnellen Anschluss beim Nutzer voraussetzen.

b) Piraterie

Ebenso wie im Audiobereich besteht auch im Videobereich ein „massenhaftes“ Piraterieproblem erst seit der Digitalisierung von Videoinhalten. Hierbei können drei Hauptproblemfelder identifiziert werden:

- Die unberechtigte Vervielfältigung von DVD-Filmen und deren Verbreitung im Internet,
- die Nutzung des digitalen Pay-TV ohne entsprechende Bezahlung sowie
- die Aufnahme von Fernsehprogrammen mittels PC oder anderer digitaler Aufzeichnungsgeräte und die anschließende Verbreitung über das Internet.[48]

Eine aktuelle Studie der Unternehmensberatungsfirma Viant schätzt, dass etwa 400.000 bis 600.000 Filme pro Tag im Internet downgeloadet werden.[49] Beim Online-Auktionshaus ebay konnten Raubkopien des Spielfilms „Herr der Ringe“ von Dritten erworben werden, obwohl dieser Film bisher nur in den Kinos läuft und daher z.B. nicht auf DVD erhältlich ist.[50] Ebenso konnten unter der inzwischen gesperrten Adresse „www.movie88.com“ illegal erstellte Kopien von Spielfilmen zum Preis ab einem US-Dollar pro Film downgeloadet werden.[51] Was den Bereich des digitalen Pay-TV angeht, so gehen die betroffenen Anbieter – insbesondere aufgrund des Einsatz von so genannten Piraten-SmartCards[52] – von europaweiten Verlusten von

47. Vgl. z.B. die Sendertabelle für Satellitenprogramme unter http://www.digitv.de/programme/frequenzen.shtml und die Sendertabelle für Kabelprogramme der Firma Kabel & Medien Service unter http://www.atcable.de/produkte/kms/programme.cfm (Stand: 12.8.2002).
48. Hierzu gehören z.B. Digital Receiver mit eingebauter Festplatte oder reine Festplatten-Recorder; vgl. in diesem Zusammenhang auch http://www.gigalaw.com/articles/2001-all/isenberg-2001-11-all.html (Stand: 12.8.2002).
49. Vgl. http://www.viant.com/pages2/downloads/innovation_copyright_2.pdf (Stand: 12.8.2002).
50. Vgl. http://www.pcwelt.de/news/internet/23032/ (Stand: 12.8.2002).
51. Vgl. http://www.heise.de/newsticker/data/anw-12.04.02-000/ (Stand: 12.8.2002).
52. Siehe dazu näher unten II. B. 3. c).

mehreren hundert Million DM pro Jahr aus.[53] Allein der Pay-TV Anbieter Premiere rechnet mit mindestens 500.000 illegalen Zuschauern.[54] Besitzer des in den USA erhältlichen digitalen Videorecorders ReplayTV 4000 können das laufende Fernsehprogramm aufzeichnen und diese Aufzeichnungen z.B. im Internet anderen zugänglich machen.[55] Aufgrund dieser Situation rechnet die US-amerikanische Filmindustrie für das Jahr 2002 mit Einnahmeausfällen von drei bis vier Milliarden Euro.[56] Für Deutschland geht die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) davon aus, dass Raubkopien von DVDs und Videos einen Schaden von „20% des Gesamtaufkommens im deutschen Filmmarkt anrichten“.[57]

4. Konsequenzen

Die vorangehenden Ausführungen machen im Hinblick auf die rechtspolitische Beurteilung deutlich, dass die Piraterie digitaler Güter nicht nur die Interessen einzelner Personen oder Verbände betrifft, sondern volkswirtschaftlich wichtige Industrien bedroht und in besonders zukunftsträchtigen Bereichen den Schutz des geistigen Eigentums in Frage stellt. Der Blick auf die historische Entwicklung der Raubkopien zeigt, dass es dabei heute nicht um eine Verbesserung der Rechtsposition des geistigen Eigentums geht, sondern um eine notwendige Anpassung der Schutzrechte an die großen Veränderungen der Informationsgesellschaft, die sich insbesondere in den letzten zehn Jahren seit der Entwicklung neuer Kopiertechniken und des Internets ergab.

B. Vertriebswege, Schutzmechanismen und Angriffsformen

Die rechtliche Beurteilung der Vorbereitung, der Erstellung und des Vertriebs von Raubkopien hängt nicht nur vom Tatobjekt, sondern vor allem vom modus operandi der Täter ab. Die deswegen zu analysierenden konkreten Angriffsformen der Täter sind ihrerseits durch die Vertriebsformen und Schutzmechanismen der Industrie bestimmt, deren Kenntnis damit ebenfalls Voraussetzung für eine rechtliche Beurteilung der Raubkopien ist. Für die rechtliche Beurteilung de lege lata ist damit nicht so sehr die – für das Gutachten von *Pfitzmann*/*Federrath*/*Kuhn* relevante – allgemeine Frage nach der Wirksamkeit technischer Schutzmechanismen entscheidend, sondern der konkrete Handlungsablauf in den einschlägigen praktischen Fällen. Damit ist

53. Vgl. http://www.golem.de/0112/17243.html (Stand: 12.8.2002).
54. Vgl. http://www.tvforen.de/frameset.php3?frame=%2Fphorum%2Fread.php3%3Ff%3D4%26i%3D3749%26t%3D3749 (Stand: 12.8.2002).
55. Vgl. http://www.heise.de/newsticker/data/anw-12.04.02-000/. Um hiergegen vorzugehen, hatten vor allem die großen US-amerikanischen Filmstudios gegen den Anbieter des ReplayTV 4000 ein Urteil erwirkt, welches diesen unter anderem verpflichtete, zu überwachen, welche Programme von den Kunden versendet werden; vgl. http://www.siliconvalley.com/mld/siliconvalley/3186191.htm, http://www.wired.com/news/politics/0,1283,52498,00.html und http://news.com.com/2100-1023-912561.html. Allerdings hat sich die Anbieterfirma Sonicblue gegen dieses Urteil rechtlich bisher erfolgreich gewehrt, vgl. http://news.com.com/2100-1040-914370.html?tag=prntfr (Stand: 12.8.2002).
56. Vgl. http://www.chip.de/news_stories/news_stories_8720802.html (Stand: 12.8.2002).
57. Vgl. http://www.heise.de/newsticker/data/anw-21.04.02-000/ (Stand: 12.8.2002).

vor allem eine *systematische* Beschreibung der Vertriebswege, der Schutzmechanismen und der Angriffstechniken erforderlich, um bei der rechtlichen Beurteilung nicht zufällig ausgewählte Einzelfälle, sondern die einschlägige Gesamtstruktur beurteilen zu können.

Bei der damit zunächst interessierenden Distribution von digitalen Inhalten durch die Industrie kann grob zwischen einer Offline-Verteilung (Datenträger) und einer Online-Verteilung (insbesondere Internet und Rundfunk) unterscheiden werden, wobei die Inhalte – abhängig von der Distribution – entweder asynchron (mehrmals und zu beliebiger Zeit) oder synchron (während der Übertragung) konsumiert werden können.[58] Da sich zum einen die verwendeten Schutzmechanismen und zum anderen auch die verschiedenen Angriffstechniken je nach Verteiltyp stark unterscheiden, wird bei der Beschreibung der Vertriebswege der Industrie im folgenden zwischen digitalen Inhalten auf Datenträgern, digitalen Inhalten im Internet und Inhalten im digitalen Rundfunk unterschieden. Dabei erfolgt jeweils zunächst ein knapper allgemeiner Überblick, gefolgt von der Darstellung der verwendeten Schutzmechanismen und der in der Praxis auftretenden Angriffsszenarien.

1. Vertrieb über Datenträger

a) Vertriebsmedien

Praktische Bedeutung als Distributions-Datenträger für digitale Daten (Software, Spiele, Audio und Video) haben aufgrund des großen Speicherbedarfs dieser Inhalte heute nur noch CD-ROMs und DVDs. Daher beschränken sich die folgenden Ausführungen zu den Schutzmechanismen und Angriffsszenarien auf diese Datenträger. Insbesondere Disketten spielen aufgrund ihrer geringen Kapazität beim Vertrieb kommerzieller Software und anderer digitaler Güter heute keine relevante Rolle mehr.

CDs fassen standardmäßig 650 MByte Daten bzw. als Audio-CD 74 Minuten Musik oder in der nicht mehr ganz standardkonformen Variante 700 MByte Daten bzw. 80 Minuten Musik.[59] DVDs sind in verschiedenen Varianten erhältlich und können auf beiden Seiten (Single Sided [SS] / Double Sided [DS]) bis zu zwei „Datenschichten“ (Single Layer [SL] / Dual Layer [DL]) enthalten. Daraus ergeben sich bei DVDs folgende Datenkapazitäten: 1) 4,7 GByte (über zwei Stunden Video) bei SS/SL, 2) 8,5 GByte (über vier Stunden Video) bei SS/DL, 3) 9,4 GByte (über 4,5 Stunden Video) bei DS/SL und 4) 17 GByte (über acht Stunden Video) bei DS/DL.[60] Diese Daten machen deutlich, welche Datenvolumina bei der Erstellung von Raubkopien auf einem einzelnen Datenträger gespeichert werden können.

Bei CDs und DVDs besteht die Aufgabe der verwendeten Schutzmechanismen darin, sicherzustellen, dass diese Datenträger nicht mittels professioneller Kopierstationen oder eines CD- oder DVD-Brenners 1:1 kopiert werden können, dass Daten – z.B. Spiele – nicht von einer CD oder DVD auf die Festplatte eines Computers kopiert und ohne Verwendung des betreffenden

58. Vgl. *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 15 f.
59. Vgl. http://www.tecchannel.de/hardware/403/12.html. Daneben gibt es neuerdings auch noch CD-Rohlinge mit einer Kapazität bis zu 99 Minuten, die allerdings sehr problematisch in der Handhabung sind, vgl. dazu http://www.feurio.com/faq/faq_writer_99mincdr.shtml (Stand: 12.8.2002).
60. Vgl. http://www.techtv.com/products/hardware/jump/0,23009,2419968,00.html (Stand: 12.8.2002).

Datenträgers benutzt werden können und dass Inhalte – wie Audio- oder Videodateien – nicht kopiert und z.B. über das Internet verbreitet werden können. Beim Vertrieb über Datenträger hängen die einsetzbaren Schutzmechanismen – anders als beim Vertrieb über das Internet – dabei davon ab, ob es sich um Daten mit Software, um Audiodaten oder um Videodaten handelt. Im Hinblick auf die rechtliche Beurteilung ist daher weiter im Hinblick auf diese Datenarten sowie die insoweit eingesetzten Schutzmechanismen und Angriffsformen zu differenzieren.

b) Schutzmechanismen und Angriffsformen bei Software-CDs

Zum Schutz von Daten-CDs mit Software kommt heute entweder eine so genannte Zwangsaktivierung zum Einsatz oder aber es werden spezielle Kopierschutzverfahren verwendet. Beide Vorgehensweisen werden daher im folgenden kurz dargestellt. Nicht näher eingegangen wird auf den Schutz von Software mittels Hardware-Schutzstecker (so genannte Dongles), da diese wegen ihrer schlechten Handhabbarkeit für den Bereich des Massenmarktes keine wesentliche Bedeutung haben.

Zwangsaktivierung

Die Datenträger von Softwareprodukten – also z.B. CDs mit Software – sind häufig nicht mit einem speziellen Kopierschutz versehen, so dass mittels eines CD-Brenners ohne Schwierigkeiten eine Kopie erstellt werden kann. Das häufige Fehlen eines Kopierschutzes beruht dabei darauf, dass das Problem bei CDs mit Softwarepaketen nicht primär in der Erstellung einer Kopie der CD besteht. Das Problem liegt vielmehr darin, dass das Softwarepaket nicht nur auf dem Computersystem des Käufers der Software, sondern auch auf vielen anderen Computersystemen unberechtigterweise installiert wird. Es muss daher verhindert werden, dass beliebig viele Installationen mittels ein und der selben Daten-CD durchgeführt werden. Aus diesem Grund wird bei der Installation der betreffenden Software regelmäßig die Eingabe einer Seriennummer oder eines Product-Key verlangt und nur im Falle der Eingabe einer gültigen Seriennummer kann der Installationsprozess fortgesetzt werden. Hierbei gilt es aber zu beachten, dass dies keinen wirklichen Schutz garantiert, da „gültige“ Seriennummern oder Product-Keys entweder von dem Inhaber einer Original-CD weitergegeben oder auch auf einschlägigen Seiten im Internet abgerufen werden können.

Aufgrund der soeben dargestellten Problematik ist inzwischen insbesondere die Firma Microsoft dazu übergegangen, beispielsweise bei der Installation ihrer Softwareprodukte OfficeXP, WindowsXP und Visio2002 nicht nur die Eingabe eines Product-Key, sondern auch eine so genannte Produktaktivierung zu verlangen. Bei dieser – bislang am weitesten fortgeschrittenen und deswegen im folgenden auch im Mittelpunkt stehenden – Form der Zwangsaktivierung wird der Nutzer der entsprechenden Software nach der Installation aufgefordert, sein Softwarepaket bei Microsoft entweder per Telefon oder über das Internet aktivieren zu lassen, wobei dem Nutzer allerdings ein gewisser zeitlicher Spielraum überlassen bleibt. So kann z.B. das Softwarepaket OfficeXP 50mal ohne Produktaktivierung gestartet werden. Erst ab dem 51. Start ist eine Verwendung des Produkts nicht mehr möglich. Die Produktaktivierung beruht im Kern auf der Übertragung einer so genannten Installations-ID an Microsoft.[61] Die Installations-ID selbst setzt sich dabei aus zwei unterschiedlichen Komponenten zusammen, der so genannten

61. Vgl. http://www.microsoft.com/germany/themen/piraterie/prod_funk.htm (Stand: 12.8.2002).

Product-ID und einem Hashwert (Prüfsumme).[62] Dabei dient die Product-ID der eindeutigen Kennzeichnung des Software-Produkts und wird aus dem während der Installation eingegebenen Product-Key generiert. Der erwähnte Hashwert wird dagegen aus zehn verschiedenen Hardwarekomponenten desjenigen Computersystems gebildet, auf dem das Softwarepaket installiert wurde, wodurch eine „Bindung“ der Software an ein bestimmtes Computersystem erreicht wird.[63] Erfolgt die Produktaktivierung über das Internet, so wird die erwähnte Installations-ID an Microsoft gesendet, dort verarbeitet und eine digital signierte Aktivierungsbestätigung auf dem Computersystem des Nutzers abgelegt.[64] Damit ist das Software-Produkt „freigeschaltet“ und kann ohne Einschränkungen genutzt werden. Erfolgt die Aktivierung per Telefon, so muss der Nutzer die Installations-ID – es handelt sich dabei um eine 50-stellige Nummer! – einem Kundendienstmitarbeiter von Microsoft mitteilen. Der Nutzer erhält dann vom Kundendienstmitarbeiter eine 42-stellige Bestätigungs-ID, die er an einer bestimmten Stelle des Softwareprodukts eingeben muss.[65] Nach der Eingabe der Bestätigungs-ID ist das Produkt wiederum freigeschaltet.

Das soeben dargestellte Aktivierungs-Verfahren stellt allerdings zunächst einmal nur sicher, dass das selbe Softwarepaket nicht gleichzeitig auf verschiedenen Computersystemen installiert werden kann. Es besteht aber auch noch die Gefahr, dass der Inhalt einer Festplatte vollständig dupliziert wird, mithin also ein so genanntes Festplatten-Image erstellt wird. Ein solches „Image“ – mitsamt der darin enthaltenen Aktivierung des Softwarepaktes – kann ohne weiteres auf die Festplatte eines anderen Computersystems überspielt werden. Daher prüfen die oben erwähnten Software-Produkte von Microsoft bei jedem Start auch, ob sich die Hardwarekonfiguration des Computersystems inzwischen geändert hat. Ist dies der Fall, so muss eine Neuaktivierung durchgeführt werden. Dabei stellt sich allerdings das Problem, dass die Nutzer häufig einzelne Hardwarekomponenten – z.B. die Sound- oder Grafikkarte – ihrer Computersysteme austauschen. Deshalb wird eine Neuaktivierung nur erforderlich, wenn eine wesentliche Änderung der Hardware vorliegt. Zudem können über das Internet pro Jahr bis zu vier Aktivierungen durchgeführt werden.[66]

Im Hinblick auf die Umgehung der Zwangsaktivierung wird in der Presse immer wieder darüber berichtet, dass es Hackern inzwischen gelungen ist, die Produktaktivierung aushebeln zu können. Bei dieser Aushebelung werden einige Dateien ausgetauscht sowie ein so genannter „Patch“ angewendet.[67] Danach kann die entsprechende Software angeblich auf beliebig vielen Computersystemen installiert werden. Hinzu kommt, dass für den Unternehmensbereich spezielle Versionen der betreffenden Softwareprodukte existieren, die nur die Eingabe eines „Master-Key“ erfordern. Hierdurch soll der „Verwaltungsaufwand“ in Unternehmen bei der Installation insbesondere der betroffenen Microsoftprodukte minimiert werden, der in diesem Bereich unter Umständen nicht mehr akzeptabel wäre, wenn mehrere hunderte oder tausende von Softwarepaketen einzeln aktiviert werden müssten. Allerdings ist es Hackern wohl gelun-

62. Vgl. http://www.microsoft.com/germany/themen/piraterie/produktaktivierung/WPA_technisch.doc (Stand: 12.8.2002).
63. Vgl. http://www.microsoft.com/germany/themen/piraterie/produktaktivierung/WPA_technisch.doc (Stand: 12.8.2002).
64. Vgl. http://www.microsoft.com/germany/themen/piraterie/prod_funk.htm (Stand: 12.8.2002).
65. Vgl. http://www.microsoft.com/germany/themen/piraterie/prod_funk.htm (Stand: 12.8.2002).
66. Vgl. zu den näheren technischen Einzelheiten http://www.microsoft.com/germany/themen/piraterie/produktaktivierung/technisch/default.htm (Stand: 12.8.2002).
67. Vgl. http://www.cosmiverse.com/tech11010101.html (Stand: 12.8.2002).

gen, diese „Master-Keys“ auch bei „normalen“ Versionen von WindowsXP und OfficeXP zu einer Freischaltung einsetzen zu können. Schließlich wurde inzwischen bekannt, welche Hardwarekomponenten bei der Aktivierung herangezogen werden und welche davon ausgewechselt werden können, ohne dass eine erneute Aktivierung notwendig wird. Dies führt dazu, dass ein bereits freigeschaltetes Softwareprodukt unter bestimmten Voraussetzungen auf einem anderen, aber ähnlich konfigurierten Computersystem verwendet werden kann, ohne dass eine Aktivierung notwendig wird.

Spezielle Kopierschutzverfahren

Sofern spezielle Kopierschutzverfahren zum Einsatz kommen, hängt die Art der verwendeten Verfahren von der Aufgabenstellung ab: Soll „nur“ sichergestellt werden, dass die auf dem Original-Datenträger befindliche Software nach dem Kopieren auf einen anderen Datenträger nicht verwendet werden kann oder soll ein Kopieren der Daten generell unterbunden werden?

Bindung an den Original-Datenträger

In den meisten Fällen reicht es aus, wenn die Software lediglich von einem Original-Datenträger installiert werden kann bzw. nur in Verbindung mit dem Originaldatenträger eingesetzt werden kann. Dies ergibt sich daraus, dass regelmäßig die auf einem Datenträger gespeicherte Software zunächst auf der Festplatte eines Computersystems installiert werden muss, damit sie vom Nutzer überhaupt verwendet werden kann.

Zur Erreichung dieses Ziels wird von den verschiedenen in der Praxis erhältlichen Kopierschutzverfahren folgendes Verfahren angewandt: Auf dem Original-Datenträger werden „Informationen“ so abgespeichert, dass diese – zumindest in der Theorie – nicht mittels professioneller Kopierstationen oder mittels eines Brenners auf einen Datenrohling kopiert werden können, so dass sich auf der Kopie weniger Daten befinden als auf dem Original.[68] Während des Software-Installationsvorgangs oder während der Ausführung einer bestimmten Applikation wird dann überprüft, ob die „Information“ auf dem Datenträger vorhanden ist. Ist dies nicht der Fall, so bricht der Installationsvorgang ab, oder die Applikation kann nicht verwendet werden. Auf diesem Prinzip beruhen z.B. die Kopierschutzverfahren „Alcatraz“,[69] „FADE“,[70] „Phenoprotect“,[71] „Ring PROTECH“,[72] „Roxxe“,[73] „SafeDisc“[74] und „SecuROM“.[75] So werden bei den weit verbreitenden Verfahren „SafeDisc“[76] und „SecuROM“[77] Teile der Daten auf dem Original-Datenträger verschlüsselt[78] und dort zusammen mit einer digitalen Signatur oder einem sonstigen „Code“ abgespeichert. Diese digitalen Signaturen oder Codes können jedoch

68. Siehe auch den Überblick unter http://www.chip.de/produkte_tests/unterseite_produkte_tests_8636379.html (Stand: 12.8.2002).
69. Vgl. http://www.kochdigi.com/en/1/product_d_6.html (Stand: 12.8.2002).
70. Vgl. http://www.codemasters.com/news/displayarticles.php?showarticle=235&PHPSESSID=88982a1b8df05ec45f9f9e1398fd23f4 (Stand: 12.8.2002).
71. Vgl. http://www.codecult.com/home.html (Stand: 12.8.2002).
72. Vgl. http://dev.ed-contrive.co.jp/proring/ (Stand: 12.8.2002).
73. Vgl. http://www.roxxe.cz/ (Stand: 12.8.2002).
74. Vgl. http://www.macrovision.com/solutions/software/cdrom/pccdrom/index.php3 (Stand: 12.8.2002).
75. Vgl. http://www.securom.com/ (Stand: 12.8.2002).
76. Vgl. http://www.macrovision.com/solutions/software/cdrom/pccdrom/index.php3 (Stand: 12.8.2002).
77. Vgl. http://www.securom.com/solution/howdoes.html (Stand: 12.8.2002).
78. Siehe zu den kryptographischen Grundverfahren und zum Angriff auf die verwendete Kryptographie *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 20 ff., S. 45 ff.

nicht – wie oben bereits erwähnt – mittels eines Brenners kopiert werden. Fehlen aber diese Informationen, so können die (teilweise) verschlüsselten Daten nicht entschlüsselt werden, so dass entweder der Installationsvorgang abbricht oder die Ausführung einer Applikation verweigert wird. Eine interessante Variante hierzu stellt das Verfahren „FADE“ dar,[79] welches zum Schutz von Datenträgern mit Spielesoftware zum Einsatz kommt. Fehlt auf einer Kopie der erforderliche „Code“, so wird die Installation des betreffenden Spiels nicht etwa abgebrochen, sondern ordnungsgemäß durchgeführt. Auch lässt sich das Spiel zunächst normal benutzen. Nach einer gewissen Zeit werden jedoch automatisch bestimmte Einstellungen und Merkmale des Spiels abgeschaltet und zwar solange, bis es völlig unspielbar geworden ist.

Für derartige Kopierschutzverfahren existieren jedoch Tools, die entweder die Erstellung einer lauffähigen Kopie durch einen CD-Brenner ermöglichen oder die einer Applikation bei der Installation bzw. Ausführung im Wege einer Emulation „vorgaukeln“, sie würde von einem Original-Datenträger aus gestartet. Daneben finden sich im Internet auch exakte Beschreibungen, welche Einstellungen bei den Tools zu verwenden sind, um ein bestimmtes Kopierschutzverfahren aushebeln oder umgehen zu können.

Unterbindung der Kopie

Andere Verfahren setzen bereits beim Kopiervorgang selbst an und versuchen, diesen zu unterbinden. So haben z.B. mit dem Verfahren „LockBlocks“[80] geschützte Datenträger zwei „Kreise“ von ca. 5 mm Breite auf der Oberfläche, welche dazu führen, dass ein Datenbrenner an der entsprechenden Stelle „hängen bleibt“ und den Kopiervorgang abbricht. In eine ähnliche Richtung gehen auch Verfahren, bei denen sich auf dem Original-Datenträger vermeintlich sehr große so genannte Dummy-Dateien befinden, wodurch dem Brenner beim Kopieren „vorgegaukelt“ wird, die Größe des Datenträgers bewege sich außerhalb der üblichen Spezifikationen, was dazu führen kann, dass die Brennsoftware den Kopiervorgang abbricht. Dies hängt damit zusammen, dass z.B. eine Standard-CD – wie bereits erwähnt[81] – ein definiertes Fassungsvermögen von 650 MB bzw. 74 Minuten hat und das Brennprogramm erwartet, dass sich die zu kopierende Datenmenge in diesem Rahmen hält. Sind jedoch die zu kopierenden Daten vermeintlich größer – z.B. 1 GB –, so kann die Brennsoftware diese nicht verarbeiten.

Auch insoweit existieren Tools und Beschreibungen, welche eine Aushebelung der Kopierschutzverfahren ermöglichen. Insbesondere der „Kopierschutz“ mittels Dummy-Dateien lässt sich relativ leicht umgehen.[82]

c) Schutzmechanismen und Angriffsformen bei Audio-CDs

Im Falle von Audio-CDs wird bei den Schutzmechanismen ein anderer Ansatz als bei den Software-Datenträgern versucht, da diese Audio-CDs problemlos in „dummen“ Laufwerken, wie Stand-alone CD-Playern, funktionieren müssen. Audio-CDs werden deshalb bei der Herstellung so „manipuliert“, dass sie zwar von Stand-alone CD-Playern abgespielt werden können,

79. Vgl. http://www.codemasters.com/news/displayarticles.php?showarticle=235&PHPSESSID=88982a1b8df05ec45f9f9e1398fd23f4 (Stand: 12.8.2002).
80. Vgl. http://www.cdrinfo.com/Sections/Articles/Specific.asp?ArticleHeadline=CD%20Protection%20Overview&index=6 (Stand: 12.8.2002).
81. Siehe oben II. B. 1. a).
82. Siehe dazu unten II. B. 1. c).

nicht aber von CD-ROM, CD-R- oder CD-RW-Laufwerken in Computern.[83] Hierbei kommen vor allem zwei Grundprinzipien zum Einsatz.[84]

Zum einen werden Veränderungen am Inhaltsverzeichnis (sog. Table of Contents, TOC) einer Audio-CD dahingehend vorgenommen, dass dort beispielsweise falsche Sektorengrenzen für die Musikdaten angegeben werden. So kann dort z.B. die Gesamtlaufzeit einer Audio-CD mit 30s vermerkt sein, obwohl die Audio-CD tatsächlich eine Gesamtspieldauer von 60 Minuten hat. Wird eine solche Audio-CD in einem Stand-alone CD-Player abgespielt, so wird die in der TOC vermerkte Gesamtlaufzeit nicht beachtet und die CD ganz normal abgespielt. CD-Laufwerke in Computern beachten aber sehr wohl den TOC-Eintrag und brechen daher das Abspielen der CD oder das Auslesen der Audio-Daten z.B. nach 30 Sekunden ab. Dieses unterschiedliche Verhalten beruht darauf, dass Stand-alone CD-Player nicht „intelligent“ genug sind, um auf die Vorgaben des Inhaltsverzeichnisses reagieren zu können, d.h. es wird zwar im Display des Stand-alone CD-Players eine „falsche“ Gesamtlaufzeit (z.B. 30 Sekunden) angezeigt, aber gleichwohl werden die einzelnen Stücke auf der Audio-CD korrekt wiedergegeben.

Zum anderen werden die Audio-CDs mit Datenfehlern versehen, die CD-Laufwerke in PCs so „verwirren“, dass die Audio-Daten auf einem PC nicht mehr abgerufen werden können.[85] Dies geschieht meist dadurch, dass eine so genannte Multisession-CD mit zwei Sessions (Bereichen) erzeugt wird, wobei die zweite Session fehlerhaft ist.[86] Stand-alone CD-Player können durch diese Manipulation normalerweise nicht beeinflusst werden, da sie nur so genannte Single-Session-Geräte sind, d.h. sie greifen nur auf die erste Session einer Audio-CD zu und können daher auch nicht durch eine fehlerhafte zweite Session „verwirrt“ werden. Ganz anders stellt sich die Situation bei den CD- bzw. kombinierten CD/DVD-Laufwerken in einem PC dar. Diese Laufwerke sind Multisession-fähig, d.h. sie können die zweite fehlerhafte Session erkennen und darauf zugreifen. Erfolgt aber ein derartiger Zugriff auf die fehlerhafte Session, führt dies dazu, dass das CD-Laufwerk den Dienst verweigert oder sogar einen Absturz des PCs verursacht. Laut Presseberichten gilt dies z.B. für die Audio-CD „A New Day Has Come“ der Sängerin Céline Dion, die in einem Computerlaufwerk einen Systemcrash verursacht.[87] Weil dies aber bei den Konsumenten für Unmut sorgt und auch bei der Elektronikindustrie auf Bedenken stößt,[88] versucht man die Betroffenen durch „Zugaben“ zu zufrieden zu stellen. So sollen Musikstücke, die sich z.B. auf einer Audio-CD mit dem Kopierschutzverfahren der Firma SunnComm befinden, zukünftig ausgelesen und per E-Mail verschickt werden können. Die Musikstücke sind dann allerdings nur für eine bestimmte Zeit anhörbar und „deaktivieren“ sich danach automatisch.[89]

Daneben gibt es Verfahren, die nicht korrigierbare Fehler vortäuschen, wodurch wiederum die „intelligenten“ CD-Laufwerke in Computern nicht in der Lage sind, diese Audio-CDs fehlerfrei auslesen zu können. Werden Musikstücke von derartig geschützten Audio-CDs mittels eines

83. Siehe zum Ganzen auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 40 f.
84. Siehe auch die Übersicht unter http://www.chip.de/produkte_tests/unterseite_produkte_tests_8636379.html (Stand: 12.8.2002).
85. Siehe auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 40 f.
86. Diese zweite Session kann auch „brauchbare“ Daten enthalten, z.B. komprimierte und geschützte Audiodaten, die mittels eines speziellen Players über einen PC abgespielt werden können.
87. Vgl. http://www.heise.de/newsticker/data/ghi-14.05.02-001/ und http://www.newscientist.com/news/news.jsp?id=ns99992271 (Stand: 12.8.2002).
88. Vgl. http://www.tagesschau.de/aktuell/meldungen/0,2044,OID686646_TYP4,00.html (Stand: 12.8.2002).
89. Vgl. http://news.com.com/2102-1023-882221.html (Stand: 12.8.2002).

PCs ausgelesen (gerippt) und z.B. in das MP3-Format umgewandelt, so enthalten die MP3-Dateien starke Störgeräusche, welche die Dateien unbrauchbar machen oder der Kopiervorgang bricht sogar ganz ab.

Die heute regelmäßig in der Praxis verwendeten Kopierschutzverfahren für Audio-CDs „Cactus Data Shield 100, 200 und 300“[90] der Firma Midbar Tech, „key2audio“[91] der Firma Sony sowie „MediaCloQ“[92] der Firma SunnComm beruhen auf einer Kombination der oben dargestellten Prinzipien, d.h. es werden „falsche“ Inhaltsverzeichnisse auf der Audio-CD abgelegt und es handelt sich um eine Multisession-CD bestehend aus einer Audio- und einer Datensession. Am verbreitetsten dürfte das Kopierschutzverfahren „key2audio“ sein, welches sich zur Zeit auf ca. 10 Millionen Audio-CDs weltweit befindet.[93] Das Kopierschutzverfahren „SafeAudio“[94] der Firma Macrovision verwendet darüber hinaus nicht korrigierbare Fehler zum Schutz von Audio-CDs.

Ein „Kopierschutzeffekt“ kann sich im übrigen auch dadurch einstellen, dass die bisher übliche Audio-CD durch neue Formate – wie Audio-DVD oder Super Audio CD (SACD) – abgelöst werden. Die neuen Formate können in identischer Qualität bisher nicht oder nur mit großem Aufwand kopiert werden, da z.B. geeignete DVD-Brenner und DVD-Rohlinge bisher sehr teuer sind und sich zudem noch kein Standard für wiederbeschreibbare DVDs herausgebildet hat.[95]

Die eben erwähnten Kopierschutzverfahren können allerdings aktuell noch nicht verhindern, dass die geschützten Musikstücke mit entsprechender Software ausgelesen und im Internet verbreitet werden können.[96] Die Softwareprodukte ermöglichen dabei entweder das „Rippen“ (Auslesen) der Audiodaten oder zumindest eine fehlerfreie 1:1-Kopie von CD zu CD. Einschlägige Programme sind im Internet erhältlich und den interessierten Personen bekannt. So ermöglicht z.B. die Brennsoftware „CloneCD“ trotz des Einsatzes von Audio-Schutzmechanismen in den allermeisten Fällen die Erstellung voll funktionsfähiger 1:1-Kopien von Audio-CDs. Daneben besteht regelmäßig auch die Möglichkeit, die Audiodaten an einem analogen Ausgang – z.B. eines CD-Laufwerks – abzugreifen und diese über eine Soundkarte wieder zu digitalisieren.[97] Das selbe gilt, wenn der Ausgang eines Audiogerätes – z.B. eines Stand-alone CD-Players – mit dem Eingang einer Soundkarte verbunden wird. Aufgrund dieser Angriffsmöglichkeiten sind z.B. sämtliche Musikstücke der Audio-CD „A New Day Has Come“ der Sängerin Céline Dion in den gängigen File-Sharing-Systemen abrufbar, obwohl die Audio-CD mit dem Kopierschutzverfahren „key2audio“ geschützt ist. Dies bestätigt die von *Pfitzmann*/*Federrath*/*Kuhn* geäußerten Bedenken zur Wirksamkeit derartiger Verfahren.[98]

90. Vgl. http://www.midbartech.com/ (Stand: 12.8.2002).
91. Vgl. http://www.key2audio.com/start/default.asp (Stand: 12.8.2002).
92. Vgl. http://www.sunncomm.com/ (Stand: 12.8.2002).
93. Vgl. dazu auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 61 f. sowie http://story.news.yahoo.com/news?tmpl=story&u=/bpihw/20020403/en_bpihw/dion_s_new_cd_crashing_party_for_some_users (Stand: 12.8.2002).
94. Vgl. http://www.macrovision.com/solutions/audio/ (Stand: 12.8.2002).
95. Augenblicklich konkurrieren die Formate DVD-Ram, DVD-RW und DVD+RW um die Gunst der Konsumenten.
96. So auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 41.
97. Siehe auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 32.
98. VGl. *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 11.

d) Schutzmechanismen und Angriffsformen bei Video-DVDs

Einen Sonderfall beim Vertrieb über Datenträger stellen Video-DVDs dar, weil bei ihnen ganz spezielle Kopierschutzverfahren zum Einsatz kommen. Dabei ist von Bedeutung, dass der Kopierschutz bei Video-DVDs immer ein Zusammenspiel der DVD selbst mit einem DVD-Player (hard- oder softwarebasiert) ist.

Aus Sicht der Spielfilmproduzenten – insbesondere aus den USA – ergibt sich dabei allerdings zunächst das Problem, dass die Verwertung von Spielfilmen – Kino, DVD, Pay-TV und Free-TV – nicht auf der ganzen Welt mit der gleichen Geschwindigkeit ablaufen kann. So kommt z.B. ein Spielfilm aus den USA regelmäßig einige Monate später in die europäischen wie in die US-amerikanischen Kinos. Dies hängt meist mit der notwendigen Synchronisation der Filme zusammen, die eine gewisse Zeit in Anspruch nimmt. Dies kann aber faktisch dazu führen, dass ein bestimmter Spielfilm, der z.B. in Deutschland gerade erst im Kino zu sehen ist, in den USA bereits auf DVD erhältlich ist. Um sich nun das „Kinogeschäft“ nicht dadurch zu verderben, dass sich z.B. deutsche Kunden lediglich die US-amerikanischen DVDs anschauen, wurde von den großen Filmstudios eine Aufteilung der Welt in acht Regionen beschlossen.[99] So handelt es sich z.B. bei Nordamerika um die Region 1 und bei Europa sowie dem Nahen Osten um die Region 2. Um nun eine gewisse regionale Abschottung erreichen zu können, dürfen in Europa verkaufte DVD-Player nur DVDs abspielen, die mit dem Regionalcode 2 versehen sind oder keiner bestimmten Region zugeordnet sind. Dies führt dann – zumindest theoretisch – dazu, dass auf diesen Geräten keine US-amerikanischen DVDs abgespielt werden können. Region-2-DVDs kommen erst dann auf den europäischen Markt, nachdem die entsprechenden Filme bereits in den europäischen Kinos vorgeführt wurden.

Darüber hinaus werden die Inhalte von Video-DVDs mittels des so genannten „Content Scrambling Systems“ (CSS) geschützt.[100] Die Video-Daten befinden sich dabei als so genannte VOB-Dateien verschlüsselt[101] auf der DVD und können nur ausgelesen – d.h. angeschaut oder kopiert – werden, wenn ein gültiger Entschlüsselungsschlüssel zur Verfügung steht. Derartige Entschlüsselungsschlüssel sind z.B. in der Hardware von Stand-alone DVD-Playern implementiert.[102] Wird eine Video-DVD in einen solchen Player eingelegt, so versucht dieser den Inhalt der DVD mit den ihm zur Verfügung stehenden Entschlüsselungsschlüssel zu decodieren. Dies gelingt allerdings nur, wenn es sich um einen „zugelassenen“ Schlüssel handelt.[103] Alle zugelassen Schlüssel sind der DVD bekannt. In der Praxis bedeutet dies allerdings, dass ein bestimmter Hersteller von Stand-alone DVD-Playern nur einen bestimmten Satz von Entschlüsselungsschlüssel besitzt und diesen in allen seinen Geräten verwendet.

Schließlich setzen DVD-Player auch noch das so genannte Macrovision-Verfahren ein.[104] Dabei handelt es sich um eine Manipulation des analogen Endsignals, wodurch zwar die Elek-

99. Siehe zur regionalen Kodierung *Bechtold*, Vom Urheber- zum Informationsrecht, München 2002, S. 110 ff. und *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 39 f. und *Himmelein*, Kino auf der Scheibe, c't Heft 9/2002, 114, 119.
100. Vgl. *Bechtold*, oben Fn. 99, S. 108 f. Siehe in diesem Zusammenhang auch die Entscheidung des Berufsgerichts im Fall „MPAA gegen Corley und 2600 Enterprises“, abrufbar unter http://cryptome.org/mpaa-v-2600-cad.htm (Stand: 12.8.2002).
101. Siehe zu den kryptographischen Grundverfahren, zur Verschlüsselung von Inhalten und Medienströmen und zum Angriff auf die verwendete Kryptographie *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 20 ff., S. 45 ff.
102. Siehe *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 24 f.
103. Siehe *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 24 f.
104. Vgl. den Überblick bei *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 32 ff.

tronik am Videoeingang eines Fernsehers nicht beeinflusst wird, aber sehr wohl die Elektronik am Videoeingang eines Videorecorders.[105] Analoge Aufzeichnungen werden so grundsätzlich unterbunden.

Sämtliche beschriebenen Schutzmechanismen bei Videoinhalten auf DVDs können jedoch heutzutage umgangen werden. Der Schutz mittels verschiedener Ländercodes hat schon deswegen keine Wirkung, weil sich die meisten Stand-alone DVD-Player entweder code-free schalten lassen, d.h. der Region Code der DVD wird nicht beachtet, oder aber es kann beliebig oft zwischen den verschiedenen Ländercodes hin- und hergeschaltet werden.[106] Das selbe gilt im übrigen auch für DVD-Laufwerke in Computersystemen, da diese meist mittels eines so genannten Firmware-Updates code-free geschaltet werden können. Die auf dem PC installierte Abspielsoftware kann mittels kostenlos erhältlicher Tools ebenfalls so beeinflusst werden, dass jede beliebige DVD abgespielt wird.

Bei verschlüsselten Inhalten sind – wie bereits erwähnt – die Entschlüsselungsschlüssel innerhalb der Hardware der „Knackpunkt“ beim Schutz von Video-DVDs. Sind diese Entschlüsselungsschlüssel vor Angriffen nicht ausreichend geschützt, so kann ein Hacker in den Besitz „offizieller“ Entschlüsselungsschlüssel gelangen und damit jede beliebige Video-DVD auslesen.[107] Dies erfolgte bereits vor ca. 2,5 Jahren durch den norwegischen Hacker Jon Johansen und führte dazu, dass ein kleines – DeCSS genanntes – Computerprogramm erstellt wurde, welches das Auslesen kopiergeschützter Video-DVDs ermöglicht.[108] In der Praxis wird dieses Programm – in Verbindung mit weiteren Programmen – häufig dazu verwendet, die Daten der Video-DVDs vom Kopierschutz zu „befreien“, auszulesen und auf der Festplatte eines Computersystems abzuspeichern.[109] Meistens werden die sehr umfangreichen Daten – eine Video-DVD hat regelmäßig ein Datenvolumen zwischen 5 und 8 GB – anschließend auch noch mittels spezieller Kompressionsverfahren verkleinert.

Aufgrund der eben genannten Umgehungsmöglichkeiten wurden Softwareprogramme entwickelt, welche die Videodaten von einer DVD auslesen (so genanntes „Rippen“) und zur „Weiterbearbeitung“ bereitstellen. Üblicherweise werden die Videodaten auf der Festplatte eines PCs abgespeichert und anschließend von den Nutzern in ein anderes Videoformat – vor allem DivX sowie MPEG-1[110] – zum Zwecke der Komprimierung umgewandelt. Nicht selten werden die von den Nutzern so bearbeiteten Daten dann über die File-Sharing-Systeme des Internets zum Download angeboten oder in Form einer so genannten Video CD (VCD) bzw. Super Video CD (SVCD) auf einen handelsüblichen CD-Rohling zum Zwecke der Eigennutzung oder der Weitergabe kopiert.[111] Inzwischen existieren sogar Programme, die es dem Nutzer gleich in einem „Arbeitsgang“ ermöglichen, auf einfache Art und Weise Video-DVDs auszulesen, zu komprimieren und gegebenenfalls wieder auf einen Datenrohling (CD- oder DVD-Rohling) zu kopieren. Es ist daher auch nicht verwunderlich, dass Medienberichten zu Folge inzwischen bis zu eine Million Video-Dateien von Spielfilmen pro Tag im Internet downgeloadet werden.[112]

105. Siehe *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 32 f.
106. Siehe dazu auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 40.
107. Siehe *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 24.
108. Siehe in diesem Zusammenhang auch die Entscheidung des Berufsgerichts im Fall „MPAA gegen Corley und 2600 Enterprises“, abrufbar unter http://cryptome.org/mpaa-v-2600-cad.htm (Stand: 12.8.2002) sowie *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 26.
109. Siehe auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 26.
110. Vgl. http://mpeg.telecomitalialab.com/ (Stand: 12.8.2002).
111. Siehe in diesem Zusammenhang auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 10.
112. Vgl. http://www.wired.com/news/print/0,1294,50798,00.html (Stand: 12.8.2002).

2. Vertrieb über das Internet

a) Vertriebene Güter

Über das Internet vertreibt die Industrie heute vor allem Softwareprogramme. Diese stehen dort zum direkten Download bereit, wobei insbesondere zwischen dem Vertrieb von kommerzieller Software, Shareware, und Freeware unterschieden werden muss. Kommerzielle Softwareprodukte können legal auch im Internet nur nach vorheriger Bezahlung – regelmäßig mit Kreditkarte – direkt bezogen werden. Dabei erhält der Kunde in diesem Fall einen Installationscode – z.B. per E-Mail – zugeschickt, welcher bei der Installation der Software eingegeben werden muss. Eine Weitergabe dieser Software bzw. des Installationscodes an Dritte ist untersagt. Sharewareprogrammen können dagegen zunächst kostenlos bezogen und benutzt werden – häufig allerdings nur mit einem eingeschränkten Funktionsumfang –, müssen jedoch nach Ablauf eines bestimmten Zeitraums vom Nutzer ebenfalls käuflich erworben werden. In diesem Fall erhält der Nutzer nach der Bezahlung einen so genannten Freischaltcode und kann erst nach dessen Eingabe die Software unbeschränkt verwenden. Die Shareware darf dabei Dritten nur ohne den Freischaltcode überlassen werden. Freeware ist dagegen ohne jede Einschränkung und Kosten verwendbar und darf auch an beliebige Dritte weitergegeben werden.

Der legale kommerziellen Vertrieb digitaler Audio- und Videodaten im Internet[113] hat dagegen noch keine große Bedeutung erlangt. Das Internet dient in diesem Bereich eher Promotionszwecken oder gleich dem Austausch von Raubkopien, wobei die Daten selbstverständlich ohne jeden Schutzmechanismus vertrieben werden. D.h.: Das Internet steht heute noch eher am Ende der legalen „Verwertungskette“ digitaler Audio- und Videoinhalte. Allerdings darf nicht übersehen werden, dass es auch erste Ansätze zu einem kommerziellen legalen Vertrieb dieser Inhalte im Internet gibt. So bietet z.B. die Firma RealNetworks in den USA Abonnements zu monatlichen Festpreisen an, die einen Abruf von Audio- und Videodaten über das Internet ermöglichen. Die Daten werden dabei dem Nutzer in einem von RealNetworks entwickelten Format zu Verfügung gestellt und können auch nur mit der entsprechenden Software dieser Firma abgespielt werden. Die Software selbst enthält Schutzmechanismen, die sicherstellen sollen, dass die Daten z.B. nur über einen bestimmten Zeitraum oder nur auf einem PC abgespielt werden können und nicht auf einen Datenträger kopiert werden können. Allerdings missfällt insbesondere die fehlende Kopierbarkeit der Daten vielen Konsumenten. Daher wollen es die kommerziellen Musikanbieter „Listen.com“[114] und „BurnItFirst.com“[115] zukünftig zulassen, dass Kunden ihrer Abrufdienste eine bestimmte Anzahl der downgeloadeten Musikstücke auf eine CD kopieren können.

Auch in Deutschland gibt es bezüglich einer Online-Distribution von Audio- und Videoinhalten erste Ansätze: So bietet die Firma Arcor seit etwa einem halben Jahr im Internet Spielfilme über ein Video-on-Demand-System an. Die Spielfilme, welche in einem Format des Windows-Mediaplayer vorliegen, können nach dem Download 24 Stunden lang angeschaut werden und deaktivieren sich automatisch nach Ablauf dieser Frist.[116] Auch die Internet-Tochter T-Online

113. Vgl. zu den verwendeten Übertragungsprotokollen im Internet *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 16 ff.
114. Vgl. http://news.com.com/2100-1023-883154.html (Stand: 12.8.2002).
115. Vgl. http://news.com.com/2102-1023-893707.html (Stand: 12.8.2002).
116. Vgl. http://www.arcor.de/tzWRUvckywWTtssk4MpObg/vod/vod_1_0.jsp. Ein ähnliches Angebot plant ab Juni 2002 auch der Hamburger Stadtnetzbetreiber HanseNet, vgl. http://w1.hansenet.de/hnet2001/1,1346,1563-menueliste-141__19340,00.html (Stand: 12.8.2002).

der Deutschen Telekom ist seit der Cebit 2002 in diesem Bereich aktiv und stellt über ein spezielles Portal[117] kostenlose, aber auch kostenpflichtige Audio- und Videodaten sowie Computerspiele zum Abruf bereit.

b) Schutzmechanismen

Beim Vertrieb von Software über das Internet bestehen die Schutzmechanismen darin, dass kommerzielle Softwareprodukte erst nach Bezahlung downgeloadet werden können und auch erst zu diesem Zeitpunkt der Installationscode zur Verfügung gestellt wird. Shareware ist vor allem dadurch geschützt, dass sie ohne Bezahlung nur für einen bestimmten Zeitraum bzw. nur mit einem eingeschränkten Funktionsumfang genutzt werden kann.

Anders sieht die Situation bei den im Internet vertriebenen Audio- und Videodaten aus. Da in den aktuellen Computersystemen keine Hardwarekomponenten eingebaut sind, die direkt einen Schutz digitaler Inhalte garantieren, bleibt augenblicklich nur ein Rückgriff auf softwarebasierte Lösungen. Hierbei spielen vor allem Digital-Rights-Management(DRM)-Systeme eine entscheidende Rolle, die als Teil einer Abspielsoftware – z.B. bei Musik- oder Videoplayern – die Rechteverwaltung übernehmen. Einen näheren Überblick zu den DRM-Systemen geben *Pfitzmann*/*Federrath*/*Kuhn*, die auch die oben dargestellten Kopierschutzverfahren bei Datenträgern unter den Begriff des DRM fassen.[118] Das Prinzip derartiger DRM-Systeme sieht grob folgendermaßen aus: Der Anbieter eines digitalen Inhalts – z.B. eines Films – wandelt diesen in ein bestimmtes Format um und verschlüsselt ihn.[119] Der zur Entschlüsselung notwendige Schlüssel wird dann bei einem Dritten in Form einer Lizenz hinterlegt. Möchte ein Nutzer den verschlüsselten Inhalt nutzen, so muss er – regelmäßig gegen ein Entgelt – die Lizenz mit dem entsprechenden Entschlüsselungsschlüssel erwerben. Daneben kann die Lizenz noch weitere Regeln enthalten, etwa wie oft oder wie lange der erworbene Inhalt abgespielt werden kann und ob ein Transfer auf andere Datenträger zulässig ist.[120] Der Ablauf enthält somit immer folgende Schritte: 1) Sicheres Verpacken der digitalen Inhalte, 2) Lizenzierung durch den Rechteinhaber, 3) Sichere Weitergabe an den Nutzer und gegebenenfalls 4) Bezahlung des erworbenen Inhalts durch den Nutzer.[121] DRM-Lösungen bieten z.B. die Firmen IBM, Microsoft und RealNetworks an.[122] DRM-Techniken können nicht nur für reine Internetangebote verwendet werden, sondern z.B. auch, um den individuellen Zugriff auf Datenträger – wie CDs und DVDs – zu regeln. So kann z.B. die Möglichkeit des Kopierens einer Audio-CD davon abhängig gemacht werden, dass sich der Nutzer zuvor – regelmäßig gegen Entgelt – über das Internet registriert und die entsprechende Lizenz erwirbt.[123] Dies wirft allerdings ernste datenschutzrechtliche Frage auf, da diese Techniken zumindest potentiell zur Anlegung von Nutzerprofilen geeignet sind. Ungelöst ist in diesem Bereich zudem auch noch, welche Abrechnungsmodelle bei der Bezahlung von Kleinbeträgen (so genanntes Micropayment) zur Anwendung kommen sollen. Zwar gibt es

117. Siehe http://www.vision.t-online.de (Stand: 12.8.2002).
118. Technischer Teil, S. 8 f.
119. Siehe zu den kryptographischen Grundverfahren, zur Verschlüsselung von Inhalten und Medienströmen und zum Angriff auf die verwendete Kryptographie *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 20 ff., S. 45 ff.
120. Siehe z.B. zur Architektur des Windows Media Rights Managers http://www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.asp (Stand: 12.8.2002).
121. Vgl. http://www.druck-gegen-abgaben.de/pressroom/pdf/news_02.pdf (Stand: 12.8.2002).
122. Vgl. http://www.druck-gegen-abgaben.de/pressroom/pdf/news_02.pdf (Stand: 12.8.2002).
123. Vgl. http://www.druck-gegen-abgaben.de/pressroom/pdf/news_02.pdf (Stand: 12.8.2002).

bereits einige Anbieter – wie z.B. click&buy,[124] net900[125] oder Paybox[126] –, jedoch hat sich noch kein Anbieter eine dominierende Marktposition erobern können, was dazu führt, dass auch die potentiellen Kunden erst einmal abwarten, welcher Anbieter sich durchsetzen wird. Daher weisen auch *Pfitzmann*/*Federrath*/*Kuhn* zurecht darauf hin, dass es aktuell noch an „passenden Geschäftsmodellen für die modernen Distributionsformen über das Internet“ fehlt.[127]

Daneben können auch Watermarking- und Fingerprinting-Techniken zum Schutz digitaler Inhalte verwendet werden.[128] Beim Watermarking werden den digitalen Daten weitere Daten hinzugefügt – wie z.B. der Name des Autors –, wodurch eine Nachverfolgung der berechtigten und vor allem auch unberechtigten Verbreitungswege möglich wird.[129] Beim Fingerprinting werden dagegen Informationen über den berechtigten Erwerber in den digitalen Inhalt eingebettet, so dass eine Bindung des Inhalts an eine bestimmte Person erfolgt.[130] Beide Techniken garantieren also – isoliert angewendet – nicht die Unterbindung einer unberechtigten Verbreitung digitaler Inhalte, sondern dienen der „Abschreckung“, da entweder der Urheber seine Urheberschaft mittels des Watermarks nachweisen kann oder mit dem im Fingerprint enthaltenen Erwerber ein Verantwortlicher zur Verfügung steht, auf den zurückgegriffen werden kann. Allerdings kommen bei den oben erwähnten DRM-Systemen auch Watermarking- und Fingerprinting-Techniken zum Einsatz.

c) Angriffsformen

Die Angriffsmöglichkeiten auf DRM-Systeme zeigt ein erfolgreicher Angriff des anonymen Hackers „Beale Screamer“ auf das DRM-System von Windows Media (WMA).[131] Dieses System der Firma Microsoft soll dafür Sorge tragen, dass insbesondere Audiodateien im Windows Media Format nicht (beliebig) kopiert oder nur entsprechend der erworbenen Lizenz genutzt werden können. Der Hackerangriff ermöglichte es jedoch, dass Audiodateien beliebig oft kopiert werden konnten.[132] Allerdings betraf der Angriff nur eine spezielle Version des DRM (Version 7) von Windows Media, so dass die Firma Microsoft mit einem Update des DRM zunächst einmal weitere Angriffe unterbinden konnte.[133] An dem Fall ist interessant, dass der Angriff die Vertreter von Microsoft nicht beunruhigte, da sie selbst davon ausgingen, dass kein DRM-System unverwundbar ist und auf bekannt gewordene erfolgreiche Angriffe mit Verbesserungen reagieren wollen.[134] An dieser Aussage zeigt sich aber auch das grundlegende Problem von DRM-Systemen: Letztlich handelt es sich um einen Hase-Igel-Wettlauf zwischen DRM-Produzenten und Hackern, und es ist nicht abzusehen, wer hier letztlich gewinnen wird. *Pfitzmann*/*Federrath*/*Kuhn* gehen jedenfalls davon aus, dass „unendliche“ Verbesserungen

124. Vgl. http://www.firstgate.de/ (Stand: 12.8.2002).
125. Vgl. http://www.in-medias-res.com/inmediasres/net900/kundeninfo.htm und http://www.telekom.de/dtag/presse/artikel/0,1018,x635,00.html (Stand: 12.8.2002).
126. Vgl. http://www.paybox.de/ (Stand: 12.8.2002).
127. Siehe Technischer Teil, S. 9.
128. Vgl. dazu näher *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 34 ff.
129. Siehe *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 34 f.
130. Siehe *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 35 ff.
131. Vgl. http://www.itworld.com/AppDev/1471/IDG011024microsofthack/ (Stand: 12.8.2002); siehe in diesem Zusammenhang auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 58 f.
132. Vgl. http://news.com.com/2100-1023-274721.html (Stand: 12.8.2002).
133. Vgl. http://www.itworld.com/AppDev/1471/IDG011024microsofthack/ (Stand: 12.8.2002).
134. Vgl. http://www.itworld.com/AppDev/1471/IDG011024microsofthack/ (Stand: 12.8.2002).

der DRM-Systeme nicht möglich sind, weil irgendwann alle Verbesserungsideen aufgebraucht sind.[135] Dies liefe im Endeffekt dann auf einen „Sieg“ der Hacker hinaus.

Im übrigen bieten auch die oben erwähnten Watermarking-Techniken keinen ausreichenden Schutz, da im Internet Tools zur Verfügung stehen, die eine Entfernung der Watermarks ermöglichen.[136] Eine Vertiefung dieser Angriffstechniken kann hier unterbleiben, da die entsprechenden Fragen im dem Gutachten von *Pfitzmann*/*Federrath*/*Kuhn* ausführlich analysiert sind.

3. Vertrieb über den digitalen Rundfunk

a) Vertriebswege

Digitaler Rundfunk wird in Europa und auch in vielen anderen Ländern der Welt nach dem so genannten Digital Video Broadcasting (DVB) Standard ausgestrahlt. Festgelegt wird dieser Standard vom Digital Video Broadcasting Project, dem mehr als 300 Rundfunkanbieter, Hard- und Softwarehersteller, Netzwerkbetreiber und weitere Gremien angehören.[137] Der Standard unterteilt sich weiterhin insbesondere in DVB-Satellite (DVB-S)[138] sowie DVB-Cable (DVB-C)[139] und definiert diesbezüglich Sondervorgaben für die Satelliten- bzw. Kabelübertragung von digitalen Rundfunkprogrammen. Zukünftig wird noch die terrestrische Verbreitung digitaler Programme nach dem DVB-T Standard hinzutreten, welche die herkömmliche analoge terrestrische Verbreitung vollständig ablösen wird.[140] Allerdings befindet sich der Einsatz dieses Übertragungsweges momentan noch in der Erprobungsphase.[141] Bei allen Übertragungswegen gilt, dass die digitalen Daten im MPEG-2 Format[142] – einem Kompressionsverfahren der Motion Pictures Expert Group – übertragen werden.[143]

Bei digitalen Inhalten im Rundfunk muss – wie bereits erwähnt[144] – zunächst zwischen Hörfunk- und Fernsehprogrammen im frei empfangbaren digitalen Rundfunk und solchen im Pay-TV unterschieden werden. Auch bei Ersteren stellt die digitale Aufzeichnung der dort gesendeten Inhalte ein Problem dar, da diese anschließend leicht im Internet verbreitet werden können und damit beliebigen Personen weltweit zugänglich gemacht werden. Dies steht dann aber meist im Gegensatz zu den erworbenen Lizenzen der ausstrahlenden Fernsehanstalt, die regelmäßig eine Beschränkung auf ein bestimmtes Sendegebiet – sprich eine bestimmte Region – vorsehen. Hinzu kommt, dass durch die Verbreitung im Internet der Wert dieser Inhalte wesentlich minimiert wird, da ihre „Exklusivität“ verloren ist. Zudem kann sich ein mittelbarer Verlust daraus ergeben, dass weniger Nutzer die regulären Fernsehprogramme anschauen, wodurch die Quote und damit auch die erzielbaren Werbeeinnahmen sinken. Gerade bei beliebten US-amerikanischen Serien wird dieses Problem heute schon sichtbar. So besorgen sich

135. Technischer Teil, S. 58 f.
136. Siehe dazu näher *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 53 ff.
137. Vgl. http://www.dvb.org/dvb_membership/framesets/about-fr.html (Stand: 12.8.2002).
138. Vgl. http://www.dvb.org/asp/st-list.asp?cat=10 (Stand: 12.8.2002).
139. Vgl. http://www.dvb.org/asp/st-list.asp?cat=10 (Stand: 12.8.2002).
140. Vgl. http://www.ndr.de/technik/dvbt/ (Stand: 12.8.2002).
141. Vgl. den Überblick zu den Pilotprojekten unter http://www.digitv.de/dvbt/dvbtpilot.shtml (Stand: 12.8.2002).
142. Vgl. http://mpeg.telecomitalialab.com/ (Stand: 12.8.2002).
143. Vgl. http://www.dvb.org/dvb_membership/framesets/about-fr.html (Stand: 12.8.2002).
144. Siehe oben II. A. 3. a).

beispielsweise Fans der Serien „Friends“ oder „Futurama“ die Originale in englischer Sprache über die File-Sharing-Systeme des Internets, ohne auf eine Ausstrahlung z.B. durch eine deutsche Fernsehanstalt zu warten.

In gleicher Weise sind digitale Inhalte im Pay-TV betroffen. Dabei ergibt sich neben den soeben dargestellten Schwierigkeiten das Problem, dass Angreifer versuchen, ohne Bezahlung die entsprechenden Sendungen anzuschauen. In Deutschland betrifft dieses Problem die bisher einzigen kostenpflichtigen digitalen Pay-TV Anbieter Premiere[145] und Mediavision.[146]

b) Schutzmechanismen

Zum Schutz kostenpflichtiger digitaler Hörfunk- und Fernsehprogramme werden so genannte SmartCards[147] in Verbindung mit speziellen Digitalempfängern (Digital Receiver oder auch Set-Top-Box genannt) eingesetzt.[148] Das Zusammenspiel dieser Komponenten lässt sich in groben Zügen folgendermaßen veranschaulichen: Die digitalen Pay-TV Programme werden aktuell über Satellit oder Kabel im MPEG-2 Format[149] verschlüsselt ausgestrahlt. Möchte der Kunde digitale Pay-TV Programme ansehen oder anhören, so muss er zunächst eine SmartCard[150] – es handelt sich dabei um eine Chipkarte mit eingebauter „Intelligenz“ – von seinem Pay-TV Anbieter über ein Abonnement erwerben. Auf dieser Smartcard befinden sich Informationen – so genannte Schlüssel – die eine Entschlüsselung der gesendeten Daten ermöglichen.[151] Daneben wird ein Digital Receiver benötigt, der ein entsprechendes Einschubfach für die SmartCard bereitstellt und den vom entsprechenden Pay-TV Anbieter verwendeten Verschlüsselungsstandard unterstützt. Es handelt sich dabei z.B. bei dem deutschen Pay-TV Anbieter Premiere um das Verschlüsselungsverfahren Betacrypt bzw. Betacrypt2.[152] Der Digital Receiver selbst – bei Premiere dbox genannt – kann entweder vom Pay-TV Anbieter direkt erworben oder gemietet werden. Es besteht häufig aber auch die Möglichkeit, den Digital Receivern eines Drittanbieters einzusetzen. Entscheidend ist dabei immer, dass das so genannte Conditional Access Modul (CA-Modul)[153] innerhalb eines Digital Receivers die SmartCard des Pay-TV Anbieters „verarbeiten“ kann. Dies beruht darauf, dass direkt innerhalb dieses CA-Moduls zum einen die Überprüfung erfolgt, ob es sich um eine zulässige SmartCard des Pay-TV Anbieters handelt, und zum anderen die Entschlüsselung der gesendeten Informationen selbst erfolgt. Damit ist der Kunde gezwungen, stets darauf zu achten, dass er einen Digital Receiver erwirbt, der zumindest auch das CA-Modul seines Pay-TV Anbieters unterstützt.[154] Um dies zu erleichtern, werden die Inhalte teilweise für unterschiedliche Schutzsysteme kodiert (so genanntes Simulcrypt);[155] auch

145. Vgl. http://www.premiere.de/ (Stand: 12.8.2002).
146. Vgl. http://www.mediavision.de/ (Stand: 12.8.2002).
147. Siehe in diesem Zusammenhang auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 27 f.
148. Siehe *Scheffler*, Einsatz einer Pay-TV Piraten-SmartCard – strafrechtliche Würdigung, CR 2002, 151.
149. Siehe http://mpeg.telecomitalialab.com/ (Stand: 12.8.2002).
150. Vgl. http://sage.guug.de/lokal/karlsruhe/2002-01-21/smartcard/smartcard.pdf (Stand: 12.8.2002).
151. Siehe *Scheffler*, CR 2002, 151 und *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 23 ff.
152. Vgl. http://www.set-top-box.de/codiert/betacrypt.php. Weitere verwendete Verschlüsselungsverfahren sind Conax, Cryptoworks, Irdeto, MediaGuard (SECA), NagraVision, Viaccess, VideoGuard (NDS), siehe http://www.set-top-box.de/codiert/cas.php (Stand: 12.8.2002).
153. Siehe auch *Scheffler*, CR 2002, 151.
154. Vgl. http://www.set-top-box.de/codiert/simulcrypt.php (Stand: 12.8.2002).
155. Siehe *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 11 f.

wird angestrebt, dass zukünftig alle Digital Receiver für digitales Pay-TV über eine standardisierte Schnittstelle verfügen, ein so genanntes Common Interface (CI), welches die CA-Module sämtlicher Pay-TV Anbieter aufnehmen kann.[156] Im Hinblick auf die Schutzmechanismen und Risiken der zukünftigen Verschmelzung von interaktiven Diensten und digitalem Fernsehen nach dem Multimedia Home Platform (MHP) Standard wird auf die Ausführungen von *Pfitzmann*/*Federrath*/*Kuhn* verweisen.[157]

Die frei empfangbaren digitalen Hörfunk- und Fernsehprogramme sind dagegen nicht vor einer digitalen Aufzeichnung geschützt, d.h. mit der entsprechenden Hardware-Ausstattung[158] sind digitale Kopien problemlos möglich. Dabei ergibt sich für die Raubkopierer der zusätzliche „Vorteil", dass digitale Rundfunkprogramme – wie bereits erwähnt[159] – schon komprimiert im MPEG-2 Format[160] angeliefert werden, mithin also ohne großen Aufwand abgespeichert und weiterverwendet werden können.[161] Es handelt sich hiermit um ein klassisches Beispiel dafür, dass auch synchron distributierte digitale Inhalt leicht asynchron weiterverwendet werden können.[162] Allerdings werden in den USA bereits Überlegungen dahin gehend angestellt, Geräte, die das frei empfangbare oder verschlüsselte digitale High Definition Television (HDTV) – ein spezieller Standard des digitalen Fernsehens – empfangen können, so zu modifizieren, dass digitale Aufzeichnungen der gesendeten Inhalte nicht oder nur in verminderter Qualität möglich sind.[163]

c) Angriffsformen

Die Angriffe auf digitale Güter im Rundfunk beruhen darauf, dass viele PCs heute mit so genanten TV-Karten ausgerüstet sind, die nicht nur eine Betrachtung des laufenden – analogen und digitalen – Fernsehprogramms ermöglichen, sondern auch die – zeitgesteuerte – digitale Aufzeichnung dieser Programme. Anschließend können die so gewonnenen Daten wiederum „nachbearbeitet" und – vor allem im Internet – weiterverbreitet werden. Dass dies auch tatsächlich geschieht, zeigen die File-Sharing-Systeme, in denen man rund um die Uhr beliebte TV-Serien – oft im US-amerikanischen Original – abrufen kann.

Besonders problematisch ist dies vor allem für die Anbieter von analogen und/oder digitalen Pay-TVs – wie z.B. Premiere in Deutschland –, da deren verschlüsselte Programme ebenfalls „gehackt" werden können. Im Hinblick auf die analogen Pay-TV-Angebote gilt dies im übrigen schon lange: Für nahezu jeden gängigen TV-Kartentyp gibt es im Internet detaillierte Beschreibungen und Hinweise auf die notwendige Software. Aber auch für den Bereich der verschlüsselten digitalen Pay-TV-Angebote findet man im Internet inzwischen ein kostenlos erhältliches Softwareprogramm, welches es im Zusammenspiel mit einer speziellen DLL-Datei ermöglicht,

156. Man bezeichnet dies auch als Multicrypt, vgl. *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 11 f. und http://www.set-top-box.de/codiert/simulcrypt.php (Stand: 12.8.2002).
157. Technischer Teil, S. 30 f.
158. Siehe dazu unten II. B. 3. c).
159. Siehe oben II. B. 3. a).
160. Vgl. http://mpeg.telecomitalialab.com/ (Stand: 12.8.2002).
161. Siehe dazu auch *Weiner*, TV orbital, c't Heft 9/2002, 146, 148.
162. Siehe auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 16.
163. Vgl. oben Fn. 55 sowie http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20020408/tc_usatoday/4005904 und http://www.newsbytes.com/news/02/176149.html (Stand : 12.8.2002).

diese Sender allein mit Hilfe dieser Software zu entschlüsseln.[164] Zusammenfassend bedeutet dies: Wer heute über eine digitale TV-Karte in seinem PC und über einen Internetzugang verfügt, ist mit etwas Geduld ohne weiteres in der Lage, jedes gesendete Fernsehprogramm – egal ob analog oder digital bzw. unverschlüsselt oder verschlüsselt – kostenlos zu betrachten, digital aufzuzeichnen und weiterzuverarbeiten.

Schließlich sind die Anbieter des digitalen Pay-TVs auch dann vom Problem der Piraterie betroffen, wenn kein PC mit einer entsprechenden digitalen TV-Karte zur Verfügung steht. Zwar benötigt man zur Entschlüsselung des digitalen Pay-TV gleichwohl spezielle Hardware und zwar einen so genannten Digital-Receiver[165] sowie eine SmartCard des Pay-TV-Veranstalters, die in den Digital Receiver eingeschoben werden muss und auf der sich die notwendigen Informationen zur Entschlüsselung befinden. Allerdings ist es Hackern schon vor einiger Zeit gelungen, sowohl die benötigen Digital Receiver als auch die SmartCards nachzubauen.[166] „Hauptangriffsziel" ist dabei die SmartCard:[167] Zum einen werden Original-SmartCards, die vom Kunden nur für die Freischaltung eines kleinen Teils eines digitalen Pay-TV-Angebots erworben oder die vom PayTV-Anbieter bereits wieder gesperrt wurden, so modifiziert, dass weitere Teile bzw. das gesamte digitale Pay-TV-Angebot eines Veranstalters angeschaut werden können.[168] Daneben bieten professionelle Hacker so genannte Digital Pirate SmartCards an, die wie die originalen SmartCards funktionieren und bei denen die Hacker im Falle technischer Gegenmaßnahmen der PayTV-Anbieter sogar ein Update zum Zwecke der Reaktivierung offerieren. Weiterhin werden auf frei erhältlichen beschreibbaren SmartCards (z.B. Goldwafer-Karten) die zur Entschlüsselung benötigten Daten abgespeichert, d.h. es wird ein Nachbau einer Original SmartCard hergestellt.[169] Die hierfür notwendigen Daten selbst können im Internet abgerufen werden. Schließlich kommen Karten-Emulatoren zum Einsatz, die dem Digital Receiver „vorgaukeln", es befände sich eine ordnungsgemäße Karte im Gerät.[170] Die Emulation selbst wird von einer Software übernommen, die ebenfalls im Internet abgerufen werden kann.

Der Vertrieb der Piraten-SmartCards wird dabei ebenso wie der anderer illegaler Tools dadurch getarnt und erleichtert, dass die Distribution der Hardware und die Distribution der Software getrennt werden, um beide bei isolierter Betrachtung legal erscheinen zu lassen. So kann z.B. eine SmartCard nicht nur für Zwecke der Piraterie digitaler Güter verwendet werden, sondern auch für die Steuerung von Garagentoranlagen. Die Händler dieser sog. Dual-use-Produkte berufen sich dann beim Vertrieb der Hardware auf den legalen Zweck des Produkts, profitieren jedoch beim Absatz erheblich von der illegalen Verwendung ihrer Systeme. Die gleiche „Dual-use-Problematik" stellt sich auch beim Vertrieb von Software, die sowohl für die Datensicherung als auch für das Hacking von Systemen verwendet werden kann. Soweit für den illegalen Einsatz Daten (wie z.B. bestimmte Codes) erforderlich sind, die eindeutig nur für illegale Zwecke eingesetzt werden können, so werden diese Daten über Web-Server im Ausland vertrieben, de-

164. Vgl. http://www.chip.de/news_stories/news_stories_8644266.html und http://www.disc4you.de/news/april2002/042902_03.html (Stand: 12.8.2002).
165. In Deutschland ist dies die dbox.
166. Vgl. http://www.chip.de/praxis_wissen/praxis_wissen_96550.html (Stand: 12.8.2002).
167. Siehe dazu näher *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 50 ff.
168. Eine in dieser Form manipulierte Karte wird als Modified Original SmartCard (MOSC) bezeichnet, vgl. *Scheffler*, CR 2002, 151 und http://www.chip.de/praxis_wissen/unterseite_praxis_wissen_96643.html (Stand: 12.8.2002).
169. Nachbauten von SmartCards werden auch als Digital Pirate SmartCard (DPSC) bezeichnet, vgl. *Scheffler*, CR 2002, 151 und http://www.chip.de/praxis_wissen/unterseite_praxis_wissen_96643.html (Stand: 12.8.2002).
170. Vgl. http://www.chip.de/praxis_wissen/unterseite_praxis_wissen_96643.html (Stand: 12.8.2002).

ren Betreiber schwer identifiziert oder zumindest schwer zur Rechenschaft gezogen werden können. Durch dieses „Aufsplitten“ der für die Piraterie erforderlichen Tools wird das Ziel angestrebt, den Vertrieb der erforderlichen einzelnen Komponenten möglichst weitgehend legal zu gestalten und die strafbaren Handlungen allein auf den „Endnutzer“ zu verlagern.

4. Konsequenzen

Die Analyse der Vertriebswege, der Schutzmechanismen und insbesondere der daran anknüpfenden Angriffstechniken zeigt, dass der modus operandi bei der Kopie digitaler Güter kein einheitliches Bild bietet, sondern in zahlreichen unterschiedlichen Formen erfolgt. Da für die einschlägigen Straftatbestände (wie § 106 UrhG, § 17 UWG, §§ 202a, 263a, 303a StGB) z.B. entscheidend ist, ob Urheberrechte, Betriebsgeheimnisse oder sonstige elektronisch gespeicherte Daten betroffen sind und ob der Täter die Daten vervielfältigt, sich verschafft, sie anderen mitteilt, sie verwertet oder sie verändert, muss die rechtliche Analyse zwischen zahlreichen unterschiedlichen Fallkonstellationen unterscheiden. Unterschiede aufgrund des Tatobjekts und des modus operandi ergeben sich für die vorgenannten Merkmale dabei nicht primär im Hinblick auf die betroffenen digitalen Güter, sondern vor allem im Hinblick darauf, ob durch den Angriff

- die Zwangsaktivierung von Software,
- die verschiedenen Kopierschutzverfahren für Daten,
- die Verschlüsselung von Daten und sonstige Funktionen von DRM-Systemen oder
- (in unterschiedlichen Formen) SmartCards

betroffen sind. Zwischen diesen unterschiedlichen Angriffsformen wird daher im rechtlichen Teil zu differenzieren zu sein, bevor die Einzelergebnisse zu einer Gesamtbeurteilung der rechtlichen Situation zusammengefügt werden können.

C. Verbreitung der digitalen Güter durch die Täter

Die Frage, ob digitale Güter von der Industrie über Datenträger, über das Internet oder über digitalen Rundfunk vertrieben werden, hat – wie dargestellt – Auswirkungen auf die einsetzbaren Schutzmechanismen sowie deren Umgehung durch die Täter. Der (legale) Vertriebsweg der Industrie entspricht dabei jedoch häufig nicht dem (illegalen) Vertriebsweg der Täter. So werden z.B. die Inhalte von legalen Musik-CDs illegal über das Internet angeboten; umgekehrt können die im Internet oder digitalen Rundfunk angebotenen Spielfilme und sonstigen Videoinhalte auch in körperlicher Form z.B. auf einer VCD oder DVD weiterverkauft werden. Die damit getrennt von den Vertriebswegen und Business-Modellen der Industrie zu analysierenden Vertriebswege der Täter haben dabei nicht nur für die rechtliche Beurteilung de lege lata, sondern vor allem auch für die Entwicklung von strafrechtlichen Präventionsstrategien Bedeutung.

Der damit für das vorliegende Gutachten essentielle Form des illegalen Vertriebs von digitalen Gütern erfolgte bis in die 90er Jahre des letzten Jahrhunderts nahezu ausschließlich mittels digitaler Datenträger (z.B. durch Software-Verkäufe auf Flohmärkten). Dies hat sich in den letzten Jahren allerdings entscheidend gewandelt. Zwar werden auch heute noch digitale Inhalte häufig mittels digitaler Datenträger weitergegeben – z.B. Raubkopien von Spiel- und Audio-CDs im Bereich der sog. Schulhofkriminalität. Aufgrund der größeren Bandbreiten und damit verbundenen höheren Übertragungsgeschwindigkeiten sowie der stark gesunkenen Telkommunikationskosten nimmt allerdings heute – nicht nur bei Software, sondern auch bei Audio- und Videoprodukten – vor allem der illegale Vertrieb über das Internet eine dominierende Rolle ein. Dabei können sich auch Überlappungen ergeben, wenn z.B. Software-CDs mit Raubkopien über Auktionshäuser im Internet zum Kauf angeboten werden.

1. Verbreitung von Raubkopien mittels Datenträger

Die Verbreitung von Raubkopien mittels Datenträger betrifft alle im vorangegangenen Teil dieses Gutachtens näher erörterten digitalen Inhalte. Softwareprodukte – insbesondere der großen Softwarehäuser – werden vor allem von gut organisierten Banden aus Asien und Osteuropa in professionellen CD-Presswerken raubkopiert und sind häufig auch rein äußerlich vom Original kaum zu unterscheiden. Daneben erfolgt die Weitergabe raubkopierter Datenträger auch im nicht organisierten privaten Bereich. Dies gilt vor allem für Spielesoftware, die nach wie vor massenhaft von Minderjährigen unter Umgehung der Kopierschutzmechanismen vervielfältigt und anschließend im Freundes- und Bekanntenkreis verteilt wird.[171] Insoweit hat sich keine Änderung zu früher ergeben, außer dass die Diskette von der CD abgelöst wurde.

Auch für Audio-CDs gilt im Prinzip das soeben zu den Softwareprodukten Gesagte: Audio-CDs werden entweder von organisierten Straftätergruppen in illegalen Presswerken – die in den letzten Jahren vor allem Russland zu einem Zentrum der Musikpiraterie machten[172] – nahezu perfekt gefälscht und auf den Markt gebracht oder es werden im privaten Bereich mittels der inzwischen weit verbreiteten CD-Brenner 1:1 Kopien erstellt. Dabei spielt eine maßgebliche Rolle, dass letzteres im Rahmen des § 53 UrhG – zumindest zur Zeit noch – in einem gewissen Umfang zulässig ist. Allerdings werden Kopien von Audio-CDs häufig nicht nur für einen eng umrissenen Personenkreis erstellt, sondern z.B. gleich für die gesamte Schulklasse.

Ein relativ neues Phänomen stellt die Verbreitung von digitalen Datenträgern mit Videoinhalten dar. Obwohl diese Datenträger – insbesondere DVDs – gegen unberechtigtes Kopieren geschützt sind, können die Schutzmechanismen – wie oben dargestellt – leicht umgangen werden. Dies hat dazu geführt, dass vor allem Spielfilme inzwischen massenhaft von DVDs ausgelesen und anschließend auf CDs weiter vertrieben werden. Eine besondere Bedeutung kommt dabei der Video CD (VCD) – und auch der Super Video CD (SVCD) – zu, da hierzu handelsübliche CD-R(W)-Rohlinge verwendet und diese mit den herkömmlichen CD-Brennern leicht erstellt werden können. Weil dazu aufgrund der geringen Speicherkapazität einer CD von bis zu 700 MByte eine erhebliche Kompression der DVD-Daten notwendig ist, müssen allerdings relevante Qualitätseinbußen bei der Bild- und Tonqualität hingenommen werden. Im übrigen spielt – soweit ersichtlich – die 1:1 Kopie von DVD auf DVD noch keine große Rolle, was wohl damit

171. Vgl. http://www.stern.de/computer-netze/spezial/raubkopieren/artikel_45741.html?seite=4 (Stand: 12.8.2002).
172. Vgl. http://www.iipa.com/rbc/2002/2002SPEC301RUSSIA.pdf (Stand: 12.8.2002).

zusammenhängt, dass die hierzu notwendige Hardware, d.h. DVD-Brenner und DVD-Rohlinge, noch relativ teuer sind und zudem die DVD-Rohlinge keine ausreichende Kapazität bieten.[173] Sollte sich allerdings nichts Grundlegendes ändern, so ist es sicher nur eine Frage der Zeit, bis auch Video-DVDs problemlos 1:1 kopiert werden können.

2. Verbreitung von Raubkopien über das Internet

Bei der – den Schwerpunkt der hier interessierenden Fälle bildenden – Verbreitung von Raubkopien im Internet ist keine Unterscheidung zwischen Software, Audio- und Videodaten erforderlich, da insoweit inzwischen nahezu alle verfügbaren Dienste des Internets zur Verbreitung genutzt werden. Allerdings ist der Schwerpunkt der zur Verbreitung der Raubkopien eingesetzten Internetdienste durchaus (noch) unterschiedlich: Während z.B. Raubkopien von Softwareprodukten nach wie vor häufig über spezielle WWW-Seiten (so genannte Warez-Sites) – unter Umständen in Verbindung mit FTP-Servern – zum Abruf bereit gestellt werden, findet der Austausch von Audio- und Videodaten im Internet primär über File-Sharing-Systeme bzw. Peer-to-Peer und über den Internet Relay Chat (IRC) statt. Aber auch insoweit ist seit einiger Zeit ein Wandel zu beobachten und inzwischen werden auch die Tauschbörsen im Internet massiv für die Verbreitung von raubkopierter Software verwendet. So können beispielsweise im Gnutella-Netzwerk rund um die Uhr sämtliche Versionen des Betriebssystems Microsoft Windows heruntergeladen werden, inklusive der notwendigen Hacks, Cracks und Seriennummern. Aber auch die Produkte anderer Softwarefirmen, wie beispielsweise Adobe und Symantec, sind nahezu vollständig über diesen Vertriebsweg abrufbar. Diese Entwicklung ist im übrigen nicht weiter erstaunlich, bieten doch die aktuellen File-Sharing-Systeme für die Täter den Vorteil, dass zur Distribution kein spezielles zentrales – und damit leicht angreifbares – Computersystem erforderlich ist, sondern ein unmittelbarer Kontakt zwischen Anbieter und Nachfrager hergestellt werden kann.

Die File-Sharing-Systeme[174] beruhen allesamt darauf, dass über das Internet sehr viele Nutzer über ein Netzwerk zusammengeführt werden und sich gegenseitig digitale Inhalte zum Austausch anbieten. Im Gegensatz zum klassischen Server-Client-Modell, bei dem alle Nutzer auf ein bestimmtes, die Daten anbietendes, Computersystem zugreifen, ist bei den File-Sharing-Systemen der Nutzer selbst derjenige, der die Daten anbietet. Der „Urvater“ eines solchen File-Sharing-Systems wurde von der Firma Napster entwickelt und angeboten. Über Napster war der Austausch von Audiodaten im MP3-Format möglich. Da sich zu den Hochzeiten von Napster teilweise mehrere hunderttausend Nutzer im System befanden, die mehrere Gigabyte an urheberrechtlich geschützten Audiodaten anboten, kam es in den USA auf der Grundlage des Digital Millennium Copyright Act (DMCA) zu einer Klage der Phonoindustrie. Die Klage hatte Erfolg, und es wurde Napster gerichtlich untersagt, weiter den Austausch urheberrechtlich geschützten Audiodaten zu unterstützen. Dies führte dazu, dass Napster zunächst einmal vom inzwischen neuen Eigentümer – der Bertelsmann AG – geschlossen wurde und nunmehr in eine kommerzielle Tauschplattform umgewandelt werden soll. Aufgrund finanzieller Schwierigkeiten ist allerdings das weitere Schicksal von Napster ungewiss.[175]

173. Spielfilme haben üblicherweise eine Größe zwischen 5 und 8 GByte, während DVD-Rohlinge aktuell nur eine Kapazität von bis zu 4,7 GByte anbieten, vgl. z.B. http://www.cdr-rohlinge-shop.de/DVDmedien.htm (Stand: 12.8.2002).
174. Siehe insoweit auch *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 62 f.
175. Vgl. http://www.heise.de/newsticker/data/hps-18.05.02-000/ und

Allerdings führte der gerichtliche Erfolg der Phonoindustrie keineswegs zu einem Ende des Austausches urheberrechtlich geschützter Audio-Dateien. Ganz im Gegenteil kamen – teilweise als Reaktion auf die Schließung von Napster – gleich eine Vielzahl neuer File-Sharing-Programme auf den Markt. Zu den bekanntesten Programmen gehören „eDonkey 2000“, „Filetopia“, „Grokster“, „KaZaA“, „Limewire“ oder „Morpheus“, wobei diese Liste in keiner Weise abschließend ist, da nahezu täglich neue Programme erscheinen. So listet z.B. die WWW-Seite „afternapster.com“ derzeit insgesamt 87 Programme auf, die einen Datenaustausch oder zumindest einen Abruf von Dateien im Internet ermöglichen. Im Gegensatz zu Napster können mittels dieser Programme nicht nur Audiodateien, sondern teilweise beliebige Dateiformate getauscht werden. Dies führt z.B. dazu, dass nicht nur Musikstücke eines bestimmten Künstlers oder einer bestimmten Band, sondern auch gleich die dazugehörigen Grafikdateien mit den Abbildern der CD-Hüllen und CDs angeboten werden. So kann der Nutzer der Tauschbörsen nicht nur inhaltlich gleiche, sondern auch äußerlich dem Original täuschend ähnlich sehende CD erzeugen. Die Zahl der den Programmen zugrunde liegenden File-Sharing-Netzwerke ist dabei wesentlich geringer. Die bekanntesten File-Sharing-Netzwerke sind das Gnutella-Netzwerk (Morpheus, Limewire usw.), das FastTrack-Netzwerk (KaZaA, Grokster usw.) sowie das OpenNap-Netzwerk (Napigator, WinMX usw.). Daneben gibt es aber auch Programme, wie „Share Sniffer“, die direkt über das Internet nach Computersystemen mit dem Betriebssystem Windows suchen und auf denen bestimmte Bereiche der Festplatte für jedermann frei zugänglich sind.

Aufgrund der Vielzahl von Programmen und Netzwerken hat sich für die Urheber und ihre Interessenverbände die Situation in der „Nach-Napster-Ära“ in vielerlei Hinsicht verschärft: Unterstützten die File-Sharing-Systeme früher nur den Austausch von Audiodateien im MP3-Format, so können heute in den meisten Systemen beliebige Dateien ausgetauscht werden. Dies führt momentan zu einem starken Anstieg des Austauschs von Spielfilmen und Fernsehprogrammen. Diese Entwicklung beruht darauf, dass viele Nutzer inzwischen ihre Breitband-Internetzugänge und ihre Flatrates (bei denen die Kosten für den Internetnutzung pauschal abgegolten werden) dazu missbrauchen, große Datenmengen im Internet zu tauschen. So gehen Schätzungen davon aus, dass der Spielfilm „Star Wars II – Angriff der Klonkrieger“ schon vor seiner Kinopremiere von bis zu einer Million Menschen gesehen wurde, da er in den Tauschbörsen des Internets bereits sechs Tage vorher abrufbar war.[176] Ein weiteres Problem ergibt sich daraus, dass die hinter den File-Sharing-Systemen und Programmen stehenden Firmen ihren Sitz nicht nur in den USA, sondern z.B. auch in Europa oder Australien haben und sich damit unter Umständen den strengen Regelungen eines bestimmten Landes leicht entziehen können. So entschied erst kürzlich ein Berufungsgericht in den Niederlanden, dass die Firma KaZaA BV, welche zum Klagezeitpunkt die Software KaZaA vertrieb und ihren Sitz in den Niederlanden hatte,[177] nicht für die Handlungen derjenigen Nutzer verantwortlich ist, die die Software zum Austausch urheberrechtlich geschützter Inhalte verwenden. Interessanterweise läuft parallel dazu auch in den USA ein Gerichtsverfahren gegen KaZaA BV sowie gegen die Firmen Grokster und MusicCity. Sollte das US-amerikanische Gericht zu dem gegenteiligen Ergebnis kommen, dass KaZaA BV für die Urheberrechtsverletzungen seiner Nutzer verantwortlich ist (was aufgrund des Urteils gegen Napster sehr wohl möglich ist), so stellt sich die Frage, ob dieses Urteil überhaupt gegen die niederländische Firmen vollstreckt werden kann. Schließlich ergeben sich Probleme daraus,

http://www.spiegel.de/wirtschaft/0,1518,196131,00.html (Stand: 12.8.2002).

176. Vgl. http://news.bbc.co.uk/hi/english/entertainment/film/newsid_1979000/1979844.stm (Stand: 12.8.2002).

177. Während des Verfahrens vor dem Ausgangsgericht wurde die Firma an das australische Unternehmen Sharman Networks verkauft.

dass manche File-Sharing-Systeme – wie z.B. Filetopia – die übermittelnden Daten verschlüsseln, so dass nicht ohne weiteres festgestellt werden kann, welche Daten überhaupt ausgetauscht werden.

3. Konsequenzen

Die vorangegangenen Ausführungen haben gezeigt, dass für die rechtliche Beurteilung der Angriffe auf Sicherungsmechanismen insbesondere zwischen Angriffen gegen die Zwangsaktivierung von Software, gegen die verschiedenen Kopierschutzverfahren für Daten, gegen die Verschlüsselung von Daten und sonstige Funktionen von DRM-Systemen sowie gegen die verschiedenen Formen von SmartCards unterschieden werden muss. Die Untersuchung der Vertriebswege der Raubkopierer macht für die rechtliche Beurteilung weitere Differenzierungen zwischen dem Vertrieb von körperlichen Datenträger und dem Vertrieb über das Internet notwendig, vor allem im Hinblick auf die Frage, ob das Angebot der entsprechenden Kopiervorlagen urheberrechtswidrig ist.

D. Täter, Nutznießer und Beteiligte

1. Einzelpersonen ohne gewerbsmäßige Zielsetzung

Einzelne Täter ohne gewerbliche Zielsetzung treten in dem vorliegend untersuchten Bereich vor allem in zweifacher Weise in Erscheinung. Zum einen werden sie als Angreifer[178] aktiv, indem sie als Insider (Hersteller, Betreiber, Entwickler usw.) oder als Outsider (Kunde, Teilnehmer, unbeteiligter Dritter usw.) die Schwächen der eingesetzten Kopierschutzmechanismen bei digitalen Inhalten ausloten und im Erfolgsfall die „Ergebnisse“ ihrer Arbeit entweder veröffentlichen oder gleich in ein Programm zur Umgehung der Kopierschutzmechanismen einbauen.[179] Zum anderen machen sich Einzelpersonen die vor allem im Internet erhältlichen Tools und Informationen zur Umgehung von Kopierschutzmechanismen dadurch zu Nutze, dass sie Raubkopien von Softwareprodukten oder Audio- und Videoinhalte erstellen. Die Raubkopien werden dann entweder selbst genutzt oder auf einem Datenträger bzw. im Internet Dritten zugänglich gemacht. Dabei sind vor allem drei Stufen des Vorgehens zu unterscheiden, welche für die rechtliche Beurteilung relevant sind:

- Auf der ersten Stufe der Deliktsverwirklichung werden zunächst Mittel zur Umgehung von Schutzmechanismen bei digitalen Gütern entwickelt. Dazu finden sich viele Internet-Nutzer oft weltweit zusammen, welche die eingesetzten Schutzverfahren auf ihre Vorgehensweise und Schwachstellen hin analysieren. Der Wissensaustausch erfolgt dabei in vielfältiger Art und Weise, z.B. in einschlägigen Hackerforen im Usenet, über WWW-Seiten oder auch auf Treffen der Hackerszene „in der realen Welt“. Die Motivation zum Knacken der Schutzmechanismen beruht dabei nicht zwingend darauf, dass primär eine

178. Siehe *Pfitzmann/Federrath/Kuhn*, Technischer Teil, S. 14, S. 47 f.

179. *Pfitzmann/Federrath/Kuhn weisen in diesem Zusammenhang darauf hin, dass man einem Angreifer niemals zu wenig zutrauen sollte. Vgl. dazu das genannte Gutachten, Technischer Teil, S. 14.*

Erstellung von Raubkopien erreicht werden soll. Vielmehr handelt es sich häufig um eine „gemischte“ Motivationslage: Ein Hauptgrund ist zunächst einmal die „sportliche“ Herausforderung, ob ein bestimmter Mechanismus geknackt werden kann oder nicht. Hinzu kommt die häufig auch vorhandene „anarchische Ader“, die den „Großkonzernen“ Paroli bieten und gegen die – aus Sicht der Hacker – zu hohen Preise von digitalen Gütern protestieren will. Hinzu treten aber auch weitere Gründe, die sich z.B. bei der Entwicklung von DeCSS zur Umgehung des Kopierschutzes von Video-DVDs zeigten:[180] Hier handelten die Hacker nach ihren Aussagen, weil es für PCs mit dem Betriebssystem Linux keinen DVD-Player gab und daher in Eigenverantwortung ein entsprechendes Programm entwickelt werden sollte. Zur Erreichung dieses Ziel war es unter anderem erforderlich, die Schutzmechanismen von Video-DVDs zu analysieren und eine Umgehungsmöglichkeit zu finden.

Die Ergebnisse der Hacker zur Umgehung von Kopierschutzmechanismen münden dabei häufig in die Erstellung kleinerer Tools oder auch umfangreicherer – teilweise sogar kommerzieller – Programme, welche die Umgehung der Schutzmechanismen ermöglichen. Allerdings werden diese Tools und Programme häufig nicht von den Hackern selbst, sondern von Dritten erstellt, die sich deren „Vorarbeiten“ zunutze machen. Diese Programme stehen dann im Internet oder auf CD-ROM als Freeware kostenlos zur Verfügung und werden dort als Shareware vertrieben oder sogar in Produkte implementiert, die im Einzelhandel erworben werden können. So fand z.B. das Programm DeCSS Einzug in eine Vielzahl von Programmen, die das Auslesen und Komprimieren von Video-DVDs sowie das Erstellen von VCD und SVCDs ermöglichen.[181] Das selbe gilt für Produkte, die eine Umgehung nahezu aller verwendeten Kopierschutzmechanismen bei Software- und Audio-CDs ermöglichen.[182]

Die Umgehung der Kopierschutzverfahren selbst erfolgt dann häufig durch die Nutzer, welche die angebotenen Programme auf dem heimischen PC einsetzen, um die digitalen Güter zu vervielfältigen und auch weiterzuverbreiten. Dabei kommt den Nutzern zugute, dass die entsprechenden Tools und Programme leicht zugänglich sind. Die Programme finden sich z.B. auf den CD-ROMs aller bekannten Computerfachzeitschriften, werden über die Newsletter dieser Zeitschriften vorgestellt und stehen häufig sogar auf deren Servern zum Download bereit. Die Nutzer müssen sich daher keineswegs in den „Untergrund“ des Internets begeben, um die Tools zu erhalten. Allerdings sind die Tools zur Umgehung der Kopierschutzmechanismen nicht immer einfach zu verstehen und zu bedienen. Technisch weniger versierte Nutzer hätten daher bei ihrer Verwendung sicher Probleme. Hier helfen jedoch die im Internet erhältlichen Hinweise sowie vor allem die Computerfachzeitschriften weiter, die nicht nur die Programme anbieten, sondern auch gleich deren Anwendung bis in alle Einzelheiten erklären, so dass der Nutzer eine perfekte Bedienungsanleitung erhält. Belegt wird dies durch wahllos herausgegriffene Titel einzelner Computerfachzeitschriften der letzten Monate: „So kopieren Sie jeden Film“, „So kopieren Sie sofort jede CD“, „DVDs entschlüsseln, abspielen, austricksen“, „Kopierschutz? Na und¡‘, „Alles übers Kopieren“, „Verbotene Utilities“, „Geknackt“ usw.

180. Siehe näher oben II. B. 1. d).

181. Vgl. z.B. die Übersicht unter http://www.chip.de/praxis_wissen/praxis_wissen_158622.html (Stand: 12.8.2002).

182. Vgl. z.B. die Übersicht unter http://www.chip.de/produkte_tests/produkte_tests_8635903.html und http://www.chip.de/praxis_wissen/praxis_wissen_8714369.html (Stand: 12.8.2002).

Die erwähnten Zeitschriften rufen dabei vordergründig nicht zur Verletzung von Urheberrechten auf, sondern erörtern die Programme und Tools stets unter dem Aspekt der Erstellung privater Sicherungskopien.

- Auf der zweiten Stufe der Deliktsverwirklichung erfolgt die Verwendung und vor allem Distribution der dann technisch nicht mehr geschützten digitalen Güter. Die Motive der einzelnen Nutzer hinsichtlich der Erstellung von Kopien digitaler Inhalte sind dabei sehr unterschiedlich: Ein häufig geltend gemachter Beweggrund ist die Erstellung von Sicherungskopien, um einer Beschädigung der Original-Software-CD vorzubeugen oder um für den CD-Player im eigenen Pkw eine Kopie zur Verfügung zu haben. Im Bereich der Audio-CDs kommt hinzu, dass oft eine kostenlose Kopie für Verwandte und enge Freunde erstellt wird. Allerdings liegen sehr häufig auch andere Motive vor: Spiele-Software, Audio-CDs und Video-DVDs werden bewusst nur einmal erworben und anschließend für den gesamten Freundeskreis oder z.B. gleich für die gesamte Schulklasse kopiert. Auch erfolgt ein Verkauf derartiger Raubkopien – bevorzugt in den Online-Auktionshäusern – als vermeintliche Originalsoftware.

  Die Distribution von Raubkopien erfolgt in massiver Weise vor allem auch direkt über das Internet. Hier werden – wie bereist erwähnt[183] – alle Dienste des Internets in Anspruch genommen. Allerdings kommt den dezentralen File-Sharing-Systemen eine entscheidende Rolle zu, da sie aufgrund ihrer Struktur einen einfachen und vor allem schnellen Datenaustausch direkt zwischen den einzelnen Internet-Nutzern ermöglichen. Daher dauert es – wenn überhaupt – auch nur Stunden, bis z.B. die Musikstücke einer kopiergeschützten Audio-CD in den Tauschbörsen des Internets angeboten werden.

- Auf der dritten Stufe werden die entschlüsselten und vertriebenen Daten dann massenhaft kopiert. Dies kann dabei auch durch Personen erfolgen, die weder Kopierschutzverfahren umgehen noch entsprechende Inhalte im Internet anbieten, sondern als bloße „Profiteure“ durch das „digitale Schlaraffenland“ streifen und sich dabei bedienen.[184] Vor allem die Online-Tauschbörsen im Gnutella- bzw. Fasttrack-Netzwerk ermöglichen ohne jede technischen Kenntnisse den Abruf riesiger Datenbestände an Software, Audio- und Videodaten.

Der Übergang zwischen der Piraterie durch Privatpersonen und der gewerblichen oder auch organisierten Straftatbegehung ist dabei oft fließend. Dies zeigt sich z.B. beim Hacking des digitalen Pay-TV Angebots von Premiere: In einem Fall boten z.B. zwei Soldaten aus Flensburg auf ihren WWW-Seiten kostenlos Anleitungen und Programme zum Erstellen und Freischalten illegaler SmartCards an, sie ermöglichten aber daneben auch den Verkauf illegaler SmartCards für kostenpflichtige Fernsehsender.[185]

2. Organisierte Straftätergruppen mit gewerbsmäßiger Zielsetzung

Die Entschlüsselung und der Vertrieb von digitalen Gütern erfolgt nicht nur durch Privatpersonen und „Hobby-Raubkopierer“, sondern auch durch gewerbsmäßig handelnde organisierte

183. Siehe oben II. C. 2.
184. Vgl. http://www.spiegel.de/spiegel/0,1518,186609,00.html (Stand: 12.8.2002).
185. Vgl. http://www.flensburg-online.de/polizei/01-2-13.html (Stand: 12.8.2002).

Straftätergruppen. Diese konzentrieren sich dabei vor allem auf den Vertrieb körperlicher Datenträger, denen durch Fälschung der Originalverpackungen häufig der Anschein einer legalen Kopie des Softwareprodukts oder der Musik-CD gegeben wird. Die von organisierten Straftätergruppen produzierten Raubkopien werden dabei vor allem auf dem Schwarzmarkt verkauft oder teilweise auch als vermeintliche Original-Software ahnungslosen Kunden – z.B. bei Online-Auktionshäusern – zum Kauf angeboten.

- Auf die Herstellung und den Vertrieb von raubkopierten Softwareprodukten sind dabei vor allem organisierte Straftätergruppen aus Fernost spezialisiert. Dies zeigte sich z.B. kürzlich bei der Operation „Cyberstorm“, die zur Verhaftung von 27 Raubkopierern insbesondere aus Taiwan führte. Diese hatten die Raubkopien in Taiwan herstellen lassen und anschließend einen Softwarepiraterie-Ring in den USA betrieben, der sich insbesondere auf den Verkauf von Raubkopien von Microsoft Produkten spezialisiert hatte.[186]

- Auch die Herstellung und der Vertrieb von Piraten-SmartCards sowie anderer Komponenten für digitale Pay-TV Angebote wird teilweise von organisierten Straftätergruppen betrieben.[187] So wurden beispielsweise Ende 2001 bei einer Razzia vor allem in Hamburg, dem Ruhrgebiet und Bayern 8000 illegale SmartCards für den Pay-TV Anbieter Premiere sowie Computer, Kartenlesegeräte und gestohlene Digital-Receiver beschlagnahmt.[188] Bei dem Hauptverdächtigen wurden in diesem Zusammenhang zudem 380.000 DM (ca. 194.000 Euro) und ein Auto sichergestellt.[189] Weiterhin wurden Anfang 2002 in Österreich mehrere Personen ermittelt, die illegale SmartCards für Premiere vertrieben.[190] Mitte März 2002 konnte ein weiterer Händlerring zerschlagen werden, der illegale SmartCards vertrieb; dabei wurden Ermittlungsverfahren gegen ca. 70 Beschuldigte eingeleitet, wobei der Hauptbeschuldigte gewerbsmäßig mit selbst programmierten SmartCards handelte.

- Organisierte Straftätergruppen finden sich schließlich auch im Bereich der Audio- und Videopiraterie. Insoweit haben sich organisierte Straftätergruppen vor allem auf das massenhafte Vervielfältigen von Audio- und Videodatenträgern spezialisiert. Dieses findet insbesondere in Russland und Asien in professionellen Presswerken statt. So geht die „International Intellectual Property Alliance“ in einer Studie für das Jahr 2002 davon aus, dass allein in Russland 17 Presswerke für digitale Datenträger mit einer Jahreskapazität von mindestens 150 Millionen Einheiten betrieben werden.[191] Im Videobereich tauchen zudem immer häufiger „Unternehmen“ auf, die ohne im Besitz entsprechender Lizenzen zu sein, Spielfilme – zum Teil sogar kostenlos – über das Internet anbieten. Dies gilt beispielsweise für die Internetangebote „movie88.com“ und „film88.com“, wobei sich letzteres auf einem Server im Iran befindet.[192]

186. Vgl. http://www.heise.de/newsticker/data/se-20.04.02-001/ und http://www.spiegel.de/netzwelt/politik/0,1518,192817,00.html (Stand: 12.8.2002).
187. Siehe http://www.heise.de/newsticker/data/cp-02.12.01-003/ (Stand: 12.8.2002) und *Pfitzmann*/*Federrath*/*Kuhn*, Technischer Teil, S. 48.
188. Vgl. http://www.heise.de/newsticker/data/cp-02.12.01-003/ und http://www.golem.de/0112/17243.html (Stand: 12.8.2002).
189. Vgl. http://www.digitv.de/news/viewnews.cgi?newsid1007215353,15684, (Stand: 12.8.2002).
190. Vgl. http://www.set-top-box.de/news/news.php?id=943 und http://www.digitv.de/news/viewnews.cgi?newsid1014388757,83847, (Stand: 12.8.2002).
191. Vgl. http://www.iipa.com/rbc/2002/2002SPEC301RUSSIA.pdf (Stand: 12.8.2002).
192. Vgl. http://www.heise.de/newsticker/data/wst-07.06.02-001 (Stand: 12.8.2002).

3. Beteiligte Unternehmen

Als Tatbeteiligte kommen weiterhin auch Unternehmen in Betracht, welche die für den Einsatz von File-Sharing-Systemen benötige Software distributieren. Es handelt sich dabei um Firmen wie Sharman Networks (Software KaZaA) oder StreamCast Media (Software Grokster und Morpheus).[193] Dabei ist allerdings zu beachten, dass diese Firmen – etwa im Gegensatz zur Firma Napster – keine zentralen Server betreiben, auf denen verzeichnet ist, welche Nutzer welche Dateien im Netzwerk anbieten. Vielmehr dient die Software dieser Firmen „nur“ dazu, dass die Nutzer selbst den Dateiaustausch in einem bestimmten Netzwerk organisieren, d.h. dass bei einer Suchanfrage die im Netzwerk befindlichen Computersysteme der Nutzer unmittelbar nach den entsprechenden Dateien abgesucht werden. Damit stellen z.B. die oben erwähnten Firmen den Nutzern letztlich nur eine „neutrale“ Software – im übrigen kostenlos – zur Verfügung, wobei allen Beteiligten bewusst ist, dass der ganz überwiegende Teil der ausgetauschten Daten urheberrechtlich geschützt ist. Dabei ist es keinesfalls zwingend, dass die Software auch auf einem proprietären Netzwerkprotokoll des betreffenden Softwareherstellers beruht. So basiert z.B. die Software Morpheus in ihren neuesten Version auf dem Gnutella-Netzwerk. Letzteres wird ebenfalls von keiner zentralen Stelle oder ähnlichem betrieben, sondern basiert auf offenen Standards, die von jedermann in der eigenen Software implementiert werden können.[194]

4. Konsequenzen

Die empirische Analyse zeigt damit auch im Hinblick auf die in Erscheinung tretenden Täter und ihre Motive ein heterogenes Bild. Der Täterkreis reicht von den – bei der Kopie von Software und Musik massenhaft in Erscheinung tretenden – Jugendlichen aller sozialer Schichten über gewinnsüchtige Händler bis zu den Mitgliedern organisierter Straftätergruppen. Die Handlungsmotive gehen vom bloßen Ehrgeiz beim Knacken von Sicherungsmechanismen über den Wunsch zur Erlangung einzelner kostenloser Vervielfältigungsstücke bis zum gewerbsmäßigen Gewinnstreben der Händler und Mitglieder organisierter Straftätergruppen.

Die Kenntnis dieser Tätergruppen und insbesondere ihrer Motive ist nicht nur für die fundierte rechtliche Beurteilung der Kopie digitaler Güter wichtig, z.B. im Hinblick auf die Merkmale des gewerbsmäßigen Handelns i.S.d. §§ 3, 4, 5 Zugangskontrolldiensteschutz-Gesetz (ZKDSG)[195] und der §§ 95a Abs. 3, 108b Abs. 2 und Abs. 3, 111a Abs. 1 Nr. 1b UrhG in der Fassung des Regierungsentwurfs für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft[196] oder das von § 17 UWG geforderte Handeln „zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen.“ Die Unterscheidung zwischen den verschiedenen Tätern und ihren Motiven ist darüber hinaus auch eine unverzichtbare Voraussetzung für die Entwicklung ange-

193. Vgl. http://www.nytimes.com/2002/04/17/technology/17MUSI.html (Stand: 12.8.2002).
194. Vgl. http://www.gnutellanews.com/information/what_is_gnutella.shtml (Stand: 12.8.2002).
195. Vgl. BGBl. I 2002, S. 1090 f. vom 22.3.2002; abrufbar unter http://217.160.60.235/BGBL/bgbl1f/bgbl102019s1090.pdf (Stand: 12.8.2002).
196. Der Regierungsentwurf ist abrufbar unter http://www.bmj.bund.de/images/11476.pdf. Siehe auch den zuvor veröffentlichten Referentenentwurf für das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft unter http://www.urheberrecht.org/topic/MultiMediaRiLi/RefEntw_Infoges_18_3_02.pdf (Stand: 12.8.2002).

messener Reformvorschläge, die Aussicht auf einen gesellschaftlichen Konsens und damit ihre Durchsetzbarkeit erstreben.

E. Praxis der Rechtsverfolgung

1. Rechtsverfolgung im Softwarebereich

Nach der Polizeilichen Kriminalstatistik der Bundesrepublik Deutschland wurden der Polizei im Jahr 2001 insgesamt 2.082 Straftaten im Bereich der Softwarepiraterie bekannt.[197] Davon entfallen 410 Fälle auf „Softwarepiraterie in Form gewerbsmäßigen Handelns“ während 1.672 Fälle die „private Anwendung z.B. Computerspiele“ betrifft. Diese Zahlen sind sehr gering. Einzelne Erfolge im Kampf gegen Raubkopierer ändern an diesem Ergebnis nichts. So wurden z.B. vor kurzem zwei Personen im Alter von 16 und 18 Jahren von der Verdener Polizei verhaftet, die über das Internet Raubkopien von Softwareprodukten – und auch von CDs sowie DVDs – anboten.[198] Bei der durchgeführten Hausdurchsuchung fand die Polizei ca. 1.000 Raubkopien.[199] Die oben angeführten Zahlen[200] zur Piraterie im Softwarebereich zeigen, dass es sich bei solchen Erfolgen in der rechtlichen Verfolgung jedoch nur um einen „Tropfen auf den heißen Stein“ handelt. Dass das Vorgehen der Behörden insoweit auch keinen abschreckenden Charakter hat, belegt schon der Blick in beliebige Tauschbörsen im Internet. Dort erhält man nahezu jede beliebige Software inklusive der notwendigen Seriennummern oder sonstigen notwendigen „Zusatzinformationen“.

Eine Rechtsverfolgung durch die betroffenen Rechteinhaber erfolgt vor allem durch die Firma Microsoft. Microsoft richtete zu diesem Zweck in den USA eine firmeninterne „Spezialeinheit“ ein, die aktuell aus 35 Mitgliedern besteht und Ermittlungen durchführt, Beweise sammelt sowie gegebenenfalls die Ermittlungsbehörden einschaltet.[201] Dabei wurden bis Mitte des Jahres 2000 ca. 43.000 Internet-Seiten mit Raubkopien aufgespürt und vom Netz genommen sowie rechtliche Schritte gegen mehr als 7.500 Betreiber von Websites in 33 Staaten eingeleitet.[202] Im bisher größten „Schlag“ gegen Raubkopierer in den USA wurden 2001 in Kalifornien 30.000 aus Taiwan stammende Raubkopien der Microsoft Betriebssysteme Windows ME und Windows 2000 beschlagnahmt.[203] Dies entspricht einem geschätzten Wert von ca. 100 Millionen Dollar. Schließlich führte die bereits erwähnte[204] Operation „Cyberstorm“ – ebenfalls wieder unter Mithilfe der Firma Microsoft – zur Verhaftung von 27 Raubkopierern aus Taiwan, die in den USA einen Softwarepiraterie-Ring betrieben und mit dem Verkauf insbesondere von Raub-

197. Vgl. Polizeiliche Kriminalstatistik für das Jahr 2001, 62; abrufbar unter http://www.bmi.bund.de/Annex/de_20088/Polizeiliche_Kriminalstatistik_als_PDF-Download.pdf (Stand: 12.8.2002).
198. Vgl. http://www.chip.de/news_stories/news_stories_8719178.html (Stand: 12.8.2002).
199. Vgl. http://www.chip.de/news_stories/news_stories_8719178.html (Stand: 12.8.2002).
200. Siehe oben II. A. 1. b).
201. Vgl. http://www.siliconvalley.com/mld/siliconvalley/3093841.htm (Stand: 12.8.2002).
202. Vgl. http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/chr-02.08.00-000/ (Stand: 12.8.2002).
203. Vgl. http://www.pcwelt.de/news/software/20261/ (Stand: 12.8.2002).
204. Siehe oben II. D. 2.

kopien von Microsoft Produkten dieser Firma einen Schaden von ca. 75 Millionen US-Dollar zufügten.[205]

2. Rechtsverfolgung im Audiobereich

Zieht man zur Bestimmung der Strafverfolgungspraxis im Bereich der Musikpiraterie in Deutschland die polizeiliche Kriminalstatistik des Jahres 2001 heran, so fällt zunächst auf, dass es in der Statistik – im Gegensatz zur Softwarepiraterie – keine eigenständige Rubrik für diesen Kriminalitätsbereich gibt. Berücksichtigt man weiterhin, dass bei den insgesamt 6.174 erfassten Fällen von Urheberrechtsverletzungen auch Verstöße gegen das Markengesetz, § 17 UWG, das Gerbrauchs- und Geschmacksmustergesetz, das Kunsturheberrechtsgesetz und das Patentgesetz mitgezählt werden und dass bereits 2.082 Strafverfahren in den Bereich der Softwarepiraterie fallen, so wird deutlich, dass nur ein sehr geringer Prozentsatz der erfassten Urheberrechtsverstöße die Verfolgung der Musikpiraterie betrifft.

Die Praxis der Rechtsverfolgung im Audiobereich zeichnet sich allerdings durch ein aktives zivilrechtliches Vorgehen der Phonoindustrie aus. So wurden nach Aussagen des Bundesverbandes Phono e.V. im Jahr 2001 über 1.300 Angebote mit urheberrechtlich geschützter Musik im Internet durch zivilgerichtliche Verfahren gesperrt.[206] Nach Angaben der Recording Industry Association of America (RIAA) stieg im Jahr 2001 die Zahl der Verhaftungen und Anklagen um 113% und die der Verurteilungen um 203% im Vergleich zum Vorjahr.[207]

Auch im Hinblick auf die rechtliche Verfolgung von Tauschbörsen-Betreibern konnte die Musikindustrie bereits einige Erfolge verbuchen. Bekanntestes Beispiel hierfür ist das zivilrechtliche Vorgehen gegen die Tauschbörse Napster. Die Tauschbörse Napster zeichnete sich dadurch aus, dass Millionen von Nutzern urheberrechtlich geschützte Musikstücke austauschten und zudem die Napster Inc. zentrale Server betrieb, auf denen Verzeichnisse mit den von den Nutzern angeboten Musikdateien geführt wurden. D.h., dass auch bei dieser Tauschbörse der Datenaustausch direkt zwischen den Mitgliedern erfolgte, aber nur über die zentralen Server der Napster Inc. abgefragt werden konnte, wer welche Musikdateien wo anbot. Daher beantragten Ende 1999 alle großen Plattenfirmen und einige Musiker eine einstweilige Verfügung gegen Napster Inc. wegen Unterstützung der Urheberrechtsverletzung der Napster-Mitglieder.[208] Der United District Court, Northern District of California gab diesem Antrag am 26. Juli 2000 statt und verbot der Napster Inc. jede Form der Durchführung oder Unterstützung von Urheberrechtsverletzungen.[209] Bereits am 28.Juli 2000 bestätigte auch der United States Court of Appeals for the Ninth Circuit (Berufungsgericht) die Entscheidung des Ausgangsgerichts.[210] In der Folgezeit wurde dann der Napster Inc. vom Ausgangsgericht[211] und auch vom Berufungsgericht[212]

205. Vgl. http://www.siliconvalley.com/mld/siliconvalley/3093841.htm und http://www.spiegel.de/netzwelt/politik/0,1518,192817,00.html (Stand: 12.8.2002).
206. Vgl. http://www.tagesschau.de/aktuell/meldungen/0,2044,OID681606_TYP4,00.html (Stand: 12.8.2002).
207. Vgl. http://www.chip.de/news_stories/news_stories_8722444.html (Stand: 12.8.2002).
208. Vgl. http://news.findlaw.com/cnn/docs/napster/riaa/napster_complaint.pdf (Stand: 12.8.2002).
209. Vgl. http://news.findlaw.com/cnn/docs/napster/riaa/court512aruling.pdf (Stand: 12.8.2002).
210. Siehe dazu die „Procedural History“ auf Seite 2 im „Memorandum“ des United States District Court, Northern District of California, abrufbar unter http://news.findlaw.com/hdocs/docs/napster/napster022102ord.pdf (Stand: 12.8.2002).
211. Vgl. z.B. http://news.findlaw.com/cnn/docs/napster/napster030601ord.pdf (Stand: 12.8.2002).
212. Vgl. http://news.findlaw.com/cnn/docs/napster/9thcir71801ord.pdf und

die Verpflichtung auferlegt, vollständig dafür Sorge zu tragen, dass urheberrechtlich geschützte Musikstücke nicht mehr getauscht werden können. Zu diesem Zweck mussten die Antragsteller der Napster Inc. Listen mit den Namen ihrer Künstler und den Titeln der urheberrechtlich geschützten Musikstücke übergeben, und es wurde ein technischer Berater zur Überwachung der Auflagen bestellt.[213] Im Falle der Unerfüllbarkeit dieser Forderung verlangten beide Gerichte eine Schließung der Tauschbörse.[214] Dies bedeutete faktisch das Ende von Napster in seiner ursprünglichen Form, denn der Napster Inc. gelang es aufgrund technischer Schwierigkeiten bewiesenermaßen nicht, den Austausch von urheberrechtlich geschützten Musikstücken vollständig zu unterbinden, so dass nur die vorübergehende Schließung der Tauschbörse übrig blieb. Hieran änderte auch die Übernahme der Tauschbörse durch die Bertelsmann eCommerce Group (BeCG) Ende 2000[215] nichts, da sich Bertelsmann mit den anderen Plattenlabels bisher nicht auf ein Ende des Rechtsstreits einigen konnte. Derzeit wird Napster in eine kommerzielle Tauschbörse umgewandelt, die nur noch lizenzierte Musikstücke anbieten und möglicherweise noch dieses Jahr ihren Regelbetrieb aufnehmen wird. Auch in Japan wurde die Firma MMO Japan Ltd., die ebenfalls eine Tauschbörse im Internet betrieb, vom einem Tokioter Bezirksgericht dazu verurteilt, ihren Internetdienst „File Rogue“ zu schließen.[216] Diesen Urteilen steht allerdings die Entscheidung eines holländischen Berufsgerichtes konträr entgegen, das eine urheberrechtliche Verantwortlichkeit des Softwareherstellers KaZaA BV für das File-Sharing-System „Fasttrack“ verneinte und die Verantwortlichkeit alleine bei den Nutzern der Tauschbörse sah.[217]

Bei der Bewertung dieser Urteile darf nicht übersehen werden, dass gerade Audiodaten nach wie vor massenhaft über die File-Sharing-Systeme des Internets getauscht werden. Daher haben – jedenfalls bisher – die gerichtlichen Erfolge der Phonoindustrie keinen Einfluss auf das illegale Angebot an Musikstücken. Wird ein File-Sharing-Anbieter zur Aufgabe gezwungen, stehen gleich mehrere gleichwertige Alternativen zur Verfügung und die Nutzer wechseln entweder einfach zu diesen über oder bemerken die Aufgabe gar nicht, weil das Funktionieren des zugrunde liegenden Netzwerks – z.B. Gnutella – nicht vom Vorhandensein eines bestimmten Anbieters abhängig ist. Das eigentliche Problem liegt damit darin, dass die Internet-Nutzer leicht den Kopierschutz digitaler Inhalte entfernen und anschleißend bequem von zuhause aus Dritten zur Verfügung stellen können.

3. Rechtsverfolgung im Videobereich

In Deutschland findet eine Verfolgung der digitalen Videopiraterie vor allem im Bereich von Pay-TV Angeboten statt. Ebenso wie im Bereich der Musikpiraterie ist allerdings mangels gesonderter statistischer Erfassung in der Polizeilichen Kriminalstatistik eine Aussage zur Menge der erfassten Fälle nur schwer möglich. Aus der Statistik lässt sich jedoch entnehmen, dass im Jahre 2001 in Deutschland 8.039 Fälle in der Rubrik „Betrug mit Zugangsberechtigungen zu

http://news.findlaw.com/hdocs/docs/napster/napster032502opn.pdf (Stand: 12.8.2002).

213. Vgl. z.B. http://news.findlaw.com/cnn/docs/napster/napster030601ord.pdf (Stand: 12.8.2002).
214. Vgl. http://news.findlaw.com/cnn/docs/napster/9thcir71801ord.pdf und http://news.findlaw.com/hdocs/docs/napster/napster032502opn.pdf (Stand: 12.8.2002).
215. Vgl. http://www.heise.de/newsticker/data/jk-04.11.00-004/ (Stand: 12.8.2002).
216. Vgl. http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20020411a8.htm und http://news.com.com/2100-1023-885233.html (Stand: 12.8.2002).
217. Vgl. http://news.com.com/2100-1023-885233.html und http://news.com.com/2100-1023-870396.html (Stand: 12.8.2002).

Kommunikationsdienste(n)“ registriert wurden. Gegenüber den im Jahre 2000 bekannt gewordenen 2.198 Fällen ist dies eine Steigerung von 265,7%.

Diese im Vergleich zur Software- und Audiopiraterie höhern Zahlen sowie die Konzentration auf die strafrechtliche Verfolgung im Pay-TV Bereich dürfte unter anderem darauf beruhen, dass die Anbieter von Pay-TV Angeboten eng mit den Strafverfolgungsbehörden zusammenarbeiten. So gab es insbesondere innerhalb der KirchGruppe eine Taskforce „E-Security“, die gegen die SmartCard-Piraterie im Bereich des Pay-TV Angebotes des Abosenders Premiere vorging und mithalf, dass diesbezüglich bundesweit momentan ca. 300 Ermittlungsverfahren durchgeführt werden.[218] Als Ergebnis dieser Zusammenarbeit konnten bei einer Großrazzia unter anderem in Hamburg, dem Ruhrgebiet und Bayern über 8.000 illegale SmartCards im Wert von ca. 1,6 Millionen DM (ca. 820.000 Euro) sowie Kartenlesegeräte und gestohlene Digital-Decoder sichergestellt werden.[219] In einem anderen, im August 2001 eingeleiteten Ermittlungsverfahrens wird einem Spanier vorgeworfen, über 3.000 gestohlene Digital-Decoder und über 10.000 SmartCards angekauft und weiterverkauft zu haben. Dieses Ermittlungsverfahren führte Ende Juli 2002 in 15 Bundesländern zu einer Durchsuchung von über 90 Wohnungen und Büros.[220]

Auch in Österreich führte die Zusammenarbeit bereits zu Fahndungserfolgen: So konnte ein Elektrohändler im Bezirk Wels und eine Person in Wien ermittelt werden, die illegale SmartCards für Premiere zusammen mit Digital-Decodern vertrieben.[221]

In den USA ist im Hinblick auf die Rechtsverfolgung im Bereich der „Videopiraterie“ vor allem das US-amerikanische Gerichtsverfahren der Motion Picture Association of America (MPAA)[222]gegen Eric Corley und sein Unternehmen „2600 Enterprises“ Inc. interessant. Wie oben bereits erwähnt,[223] wird für das Auslesen von kopiergeschützten Videoinhalte auf DVDs vor allem das Programm DeCSS benötigt. Corley hatte im November 1999 diese Programm – welches im September 1999 von dem norwegischen Teenager Jon Johansen und weiteren unbekannten Personen entwickelt worden war – auf seiner Web-Site „www.2600.com“ zum Download bereitgestellt und zudem mehrere Links auf andere Web-Sites gesetzt, die dieses Programm ebenfalls zum Abruf anboten. Daraufhin wurde Corley zusammen mit seinem Unternehmen von der MPAA dahin gehend verklagt, zukünftig dieses Programm weder direkt noch per Link zum Abruf bereitstellen zu dürfen. Sowohl der United States District Court for the Southern District of New York[224] (Ausgangsgericht) als auch der United States Court of Appeals for the Second Circuit[225] (Berufungsgericht) verurteilten die Beklagten entsprechend dem Antrags der MPAA.

218. Vgl. http://www.digitv.de/news/viewnews.cgi?newsid1007296982,42273, (Stand: 12.8.2002).
219. Vgl. http://www.premiereworld.de/cgi-bin/WebObjects/PWPortal.woa/11/wo/EQ5VvrY6sHrM28vfkWo5rxMxDTg/11.0.8.3.3.3.0.5.1.0.0.NMEdiWOContainerSlotNC.0.PWEdiWOOneRowTextTeaserNC.3.0, http://www.golem.de/0112/17243.html und http://www.spiegel.de/netzwelt/technologie/0,1518,170818,00.html (Stand: 12.8.2002).
220. Vgl. http://www.premiereworld.de/cgi-bin/WebObjects/PWPortal.woa/42/wo/w63OIFsJ8nFf3FET6vz1VEhauVP/8.0.8.3.3.3.0.4.0.0.PWEdiWOTextLinkNC (Stand: 9.8.2002).
221. Vgl. http://www.digitv.de/news/viewnews.cgi?newsid1012823642,55273, und http://www.digitv.de/news/viewnews.cgi?newsid1014388757,83847, (Stand: 12.8.2002).
222. Zu ihr gehören die Filmstudios Universal City Studios Inc., Paramount Pictures Corporation, Metro-Goldwyn-Mayer Studios Inc., Tristar Pictures Inc., Columbia Pictures Industries Inc, Time Warner Entertainment Company L.P., Disney Enterprises Inc. und Twentieth Century Fox Film Corporation.
223. Siehe oben II. B. 1. d).
224. Siehe http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/00-08592.PDF (Stand: 12.8.2002).
225. Siehe http://cryptome.org/mpaa-v-2600-cad.htm (Stand: 12.8.2002) und Computer und Recht

Ihre Rechtsgrundlage finden beide Urteile in Bestimmungen[226] des 1998 in Kraft getretenen Digital Millennium Copyright Act (DMCA), die auf den Vorgaben der WIPO-Verträge „WIPO Copyright Treaty“ (WCT) und „WIPO Performances and Phongrams Treaty (WPPT) aus dem Jahre 1996 beruhen[227] und die festlegen, dass wirksame Kopierschutzmechanismen digitaler Inhalte weder umgangen noch Tools oder sonstige Hilfestellungen zur Verfügung gestellt werden dürfen, die eine entsprechende Umgehung ermöglichen. Verfassungsrechtliche Bedenken der Beklagten im Hinblick auf eine Einschränkung der Meinungsfreiheit (Free Speech) wiesen beide Gerichte mit dem Argument zurück, dass die einschlägigen Bestimmungen des DMCA nicht den Inhalt selbst betreffen – und somit inhalts-neutral sind –, sondern lediglich die Umgehung von wirksamen Schutzmechanismen.[228] Die hierbei entstehenden mittelbaren Auswirkungen auf die freie Meinungsäußerung sind nach Ansicht der Gerichte gerechtfertigt, da der Schutz der Urheberrechtsinhaber in diesem Fall Vorrang hat und zudem die gesetzlichen Einschränkungen noch angemessen sind.[229] Gleichwohl hatte dieser juristische Sieg der MPAA keine praktischen Auswirkungen, da DeCSS – wie bereits erwähnt – inzwischen in einer Vielzahl von Programmen zum Auslesen von DVDs eingesetzt wird. Mithin kann diesem Urteil nur eine symbolische Wirkung zugesprochen werden. Zudem hat inzwischen das US-amerikanische Unternehmen „321 Studios“ – welches die Software „DVD Copy Plus“ zur Erstellung von Sicherungskopien von DVDs herstellt und vertreibt – Klage vor einem US-amerikanischen District Court eingereicht.[230] Ziel der Klage ist es, dass die Erstellung einer Sicherungskopie einer DVD trotz Umgehung der Kopierschutzmechanismen für zulässig erklärt und damit ein Verstoß gegen den DMCA verneint wird.[231]

Weiterhin sind die Gerichtsverfahren der MPAA und anderer Betroffener gegen ICRAVETV und RecordTV von Bedeutung. ICRAVETV bot von Canada aus im Internet Spielfilme und Fernsehsendungen US-amerikanischer Sendeanstalten – welche das Unternehmen zuvor legal auf terrestrischem Weg empfangen und anschließend digitalisiert hatte – weltweit für Nutzer an.[232] Diese Vorgehensweise stellte nach Ansicht des von MPAA-Mitgliedern angerufenen Gerichts aber eine Urheberrechtsverletzung dar und wurde deshalb untersagt.[233] Interessanterweise handelte es sich dabei um ein Urteil eines US-amerikanischen Gerichts (dem United States District Court for the Western District of Pennsylvania), welches sich trotz eines kanadischen Anbieters wegen der Abrufbarkeit der Inhalte in den USA für zuständig erklärte. Auch im Falle von RecordTV ging es darum, dass Fernsehsendungen unberechtigterweise digital aufgezeich-

International (CRI) 2002, 50 ff. Siehe in diesem Zusammenhang auch http://www.wired.com/news/politics/0,1283,52609,00.html und http://www.2600.com/news/display.shtml?id=1233 (Stand: 12.8.2002).

226. Vgl. 17 U.S.C. § 1201(a) und (b); der DMCA ist abrufbar unter http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2281enr.txt.pdf (Stand: 12.8.2002). Siehe auch *Friedman*, CRi 2002, 40 f.
227. Siehe zu den WIPO-Verträgen insb. *Wand*, Technische Schutzmaßnahmen und Urheberrecht, München 2001, S. 24 ff.
228. Vgl. http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/00-08592.PDF und http://cryptome.org/mpaa-v-2600-cad.htm (Stand: 12.8.2002) sowie *Friedman* CRi 2002, 40 ff.
229. Vgl. http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/00-08592.PDF und http://cryptome.org/mpaa-v-2600-cad.htm (Stand: 12.8.2002) und *Friedman* CRi 2002, 40, 44 f.
230. Vgl. http://www.heise.de/newsticker/data/vza-24.04.02-001/ und http://news.com.com/2100-1023-889455.html (Stand: 12.8.2002).
231. Vgl. http://www.321studios.com/PR_complaint.htm (Stand: 12.8.2002).
232. Siehe *Handa*, CRi 2002, 46 ff.
233. Vgl. http://www.mpaa.org/Press/iCrave_Findings.htm (Stand: 12.8.2002) und *Handa*, CRi 2002, 46, 47.

net und anschließend im Internet zum Abruf bereit gestellt wurden.[234] Die Beklagte kam einem Gerichtsurteil durch einen Vergleich zuvor und anerkannte, dass es sich bei den vorgenommenen Handlungen um Urheberrechtsverletzungen handelt.[235]

4. Konsequenzen

Die Rechtsverfolgung bei Angriffen auf digitale Güter wird sowohl im Software- als auch im Audiobereich im wesentlichen von den Geschädigten betrieben. Im Videobereich sind die staatlichen Strafverfolgungsorgane zwar stärker präsent, jedoch dürfte auch dies wesentlich auf Initiativen der privaten Rechteinhaber beruhen. Vergleicht man den Umfang der raubkopierten Güter mit den entsprechenden Maßnahmen der Rechtsverfolgung, so ergreift letztere allerdings nur einen Promilleanteil der einschlägigen Verhaltensweisen. Eine wirksame Strafverfolgung fehlt damit in weiten Bereichen fast völlig.

Sofern diese Situation nicht durch rechtliche Reformen und Verwaltungsmaßnahmen im Bereich der Ermittlungsbehörden geändert werden kann, muss in den rechtspolitischen Überlegungen nicht nur das Strafrecht berücksichtigt, sondern vor allem auch geprüft werden, wie die private Rechtsverfolgung (z.B. durch Normierung von Auskunftsansprüchen oder von zivilrechtlich durchsetzbaren Sanktionen) gestärkt werden kann.

F. Zusammenfassung und Folgerungen

1. Verbreitung und Schäden der Raubkopien

Die vorstehende Analyse hat gezeigt, dass alle digitalen Güter trotz des Einsatzes von Schutzmechanismen in gravierender Weise von Piraterie betroffen sind. Der Schwerpunkt der Schäden liegt dabei im Bereich der Software-, Audio- und Videopiraterie. Aber auch andere Inhalte, wie elektronische Bücher oder ganz allgemein elektronische Texte, werden unter Umgehung von Schutzmechanismen illegal verbreitet und genutzt.

Die digitale Piraterie verursacht dabei sowohl im Software- als auch im Audio- und Videobereich weltweit Schäden in Milliardenhöhe. In Deutschland entstand der Softwarebranche nach eigenen Angaben z.B. im Jahr 2000 ein geschätzter Schaden von 635 Millionen US-Dollar. Die Musikindustrie geht in Deutschland im Jahr 2001 von einem Verlust von ca. 700 Millionen Euro aus und auch die Filmwirtschaft vermutet, dass der jährlich verursachte Schaden in etwa 20% des Gesamtaufkommens der deutschen Filmwirtschaft ausmacht. Dabei entfällt ein Großteil der Schäden auf den Softwarebereich. Dies sagt jedoch nichts über die Häufigkeit von Pirateriehandlungen aus, sondern beruht vor allem darauf, dass die einzelnen Softwareprodukte im Vergleich zu Audio- und Videoinhalten einen größeren Wert darstellen. Im Hinblick auf die Deliktshäufigkeit dürfte der Download und der Austausch von Musikstücken sowie von Spielfilmen als Massenphänomen dagegen zahlenmäßig deutlich vor der Verbreitung von Softwareraubkopien liegen.

234. Vgl. http://www.mpaa.org/Press/RecTVComplaint.pdf (Stand: 12.8.2002).
235. http://www.mpaa.org/Press/RecTVSettlementRelease.htm (Stand: 12.8.2002).

Die derzeitige Entwicklung des Massenphänomens „Raubkopieren“ führt jedoch nicht nur zu hohen wirtschaftlichen Schäden. Sie stellt auch eine ernste wirtschaftliche Gefahr für die betroffenen Inhaltsanbieter – wie Softwarehersteller, Künstler, Musikproduzenten, Filmschaffende, Filmstudios, Rundfunkanbieter und sonstige Medienkonzerne – dar. Sie gefährdet darüber hinaus auch die Entwicklung neuer Geschäftsmodelle und Technologien, da viele Content-Anbieter wegen fehlender effektiver Schutzmaßnahmen für digitale Inhalte auf eine digitale Vermarktung ihrer Inhalte verzichten oder nur in einem beschränkten Umfang aktiv werden. Damit leidet auch die Entwicklung des E-Commerce und des Internets insgesamt, die durch attraktive Angebote mit hohen Anforderungen an Speicher- und Übertragungskapazitäten gefördert wird. Die Schädigung der einschlägigen Industrien verletzt mittel- und langfristig vor allem auch die Interessen der Verbraucher und Konsumenten, die bei einem Rückgang der einschlägigen Investitionen keine qualitativ hochwertigen Angebote mehr bekommen werden.

2. Versagen der bisherigen technischen Schutzmaßnahmen

Die Industrie entwickelt im Moment neue Schutzsysteme und insbesondere auch neue Businessmodelle, die zur Verbreitung von Premium-Inhalten auf Bezahlsysteme zurückgreifen. So bieten z.B. die Firmen Arcor, Real oder auch der Musikanbieter „popfile.de“ im Internet kostenpflichtige Video- bzw. Audioinhalte an. Die empirisch-kriminologische Analyse belegt allerdings, dass die bisher entwickelten Schutzmaßnahmen bis heute nicht in der Lage waren, das Phänomen der Raubkopien auf Dauer wirksam zu verhindern. Die Geschichte der Piraterie geistiger Güter zeigt vielmehr, dass – vor allem im Bereich der digitalen Güter – neu entwickelte Schutzmaßnahmen nach kurzer Zeit stets wieder umgangen werden können. Die bisherige Erfahrung mit der Verbreitung von Raubkopien lässt daher vermuten, dass dies auch in der Zukunft so sein wird und technische Schutzmaßnahmen den Zugriff auf digitale Güter stets nur für eine begrenzte Zeit verhindern und im übrigen nur unwesentlich erschweren können. Das technische Gutachten von *Pfitzmann*/*Federrath*/*Kuhn* bestätigt dies in allgemeiner Form.

Versucht man, dieses Defizit im Bereich der technischen Schutzmaßnahmen durch rechtliche Maßnahmen auszugleichen, so müssen zunächst die Gründe für das Scheitern der technischen Schutzmaßnahmen und für die große Verbreitung der Raubkopien analysiert werden. Vor allem im Hinblick auf die Konzeption rechtlicher Schutzstrategien ist dabei von Bedeutung, dass das Phänomen der Raubkopien nicht nur auf der Schwäche der technischen Schutzmaßnahmen beruht, sondern auf mehreren Faktoren:

- Zunächst ist es in der Tat nicht möglich, die digitalen Güter nur in einer Form zu verbreiten, die auf Dauer nicht kopierbar ist. Dies beruht zum einen auf der – in dem Gutachten von *Pfitzmann*/*Federrath*/*Kuhn* näher belegten –Tatsache, dass die verschlüsselten Daten angegriffen werden können, vor allem wenn dies nicht nur durch eine Vielzahl von Nutzer, sondern auch durch organisiert arbeitende Straftätergruppen erfolgt. Selbst wenn eine perfekte Verschlüsselung der digitalen Güter möglich wäre, so würden die Originaldaten von Piraten jedoch gleichwohl in verwertbarer Weise „an der Verschlüsselung vorbei“ erlangt werden: Im Bereich der Software kann dies z.B. durch Insider in den Vertriebsfirmen erfolgen. Im Audiobereich können die für den Lautsprecher der Abspielgeräte in analoger Form ausgegebenen Daten abgegriffen, digitalisiert und dann unverschlüsselt verbreitet werden. Im Videobereich werden illegale Kopien und Mitschnitte regelmäßig

durch Beteiligte an der Produktion schon vor der offiziellen Filmfreigabe auf den illegalen Markt gebracht. Soweit digitale Güter für einen Massenmarkt produziert werden, kann der Urheber oder Vermarkter daher durch technische Maßnahmen auf Dauer nicht verhindern, dass zumindest einzelne Kopien der Werke in unverschlüsselter Form an Dritte gelangen.

- In der traditionellen nicht vernetzten Welt würden derartige einzelne Angriffe auf die betroffenen Güter nur zu begrenzten Schäden führen. In der digitalen Welt können über die weltweit zugänglichen und weitgehend anonymisierten Vertriebswege des Internets die einmal entschlüsselten und digitalisierten Güter heute jedoch sofort weltweit einem Massenpublikum angeboten werden. Die beliebige Kopierbarkeit und Übertragbarkeit der Daten im Internet macht eine – an sich nicht ins Gewicht fallende – einzelne Rechtsverletzung damit in kürzester Zeit zu einer Bedrohung des gesamten Marktes durch ein kostenfrei angebotenes und komfortabel abrufbares Angebot. Ein Raubkopierer formulierte dieses Phänomen anschaulich durch die Aussage im Nachrichtenmagazin „Focus“: „Ich bezahle doch nicht bei einer Tankstelle für Sprit, wenn ihn mir die Nachbartankstelle gratis offeriert“.[236]

3. Wirkungslosigkeit der rechtlichen Bekämpfung

Die vorstehende Analyse hat weiter deutlich gemacht, dass rechtliche Instrumentarien die Verbreitung der Raubkopien bisher ebenfalls nicht nennenswert verhindern. Das Ausmaß der in der Praxis festzustellenden Raubkopien steht in eklatantem Widerspruch zu den bisherigen rechtlichen Erfolgen. Hinzu kommt, dass die bisherigen rechtlichen Maßnahmen überwiegend auf dem eigenen (insb. auch zivilrechtlichen) Vorgehen der geschädigten Opfer und ihrer Verbände beruhen.

4. Neue Ansätze für rechtliche Bekämpfungsstrategien

Die Analyse der Angriffsformen und der Vertriebswege der Raubkopierer zeigt allerdings nicht nur die Wirkungslosigkeit der bisherigen technischen und rechtlichen Schutzmaßnahmen, sondern auch die verschiedenen Ansatzpunkte, mit denen Raubkopien zumindest erschwert werden können. Dabei ist entscheidend, dass rechtliche Maßnahmen nicht nur gegen die unbefugte Kopie von digitalen Gütern gerichtet werden können, sondern auch gegen Handlungen, die in der Praxis Voraussetzung für die Kopie sind und besser als das Verbot der Kopie durchsetzbar sind:

- Der klassische rechtliche Ansatz zur Verhinderung der Raubkopie von geistigen Gütern liegt im Verbot und in der Kriminalisierung des *Kopiervorgangs*, welcher die eigentlich schädigende Handlung ist. Dieser Ansatz ist jedoch – ohne dass damit der rechtlichen Analyse vorausgegriffen werden soll – aus zwei Gründen fragwürdig: Zum einen könnte ihm im Urheberrecht das Recht auf Erstellung einer privaten Kopie entgegenstehen. Selbst wenn dies nicht der Fall wäre, so beständen jedoch nur schlechte Chancen, den in der Privatsphäre erfolgenden Verletzungsakt dort zu entdecken und zu beweisen.

236. Vgl. http://www.focus.de/F/2002/15/Internet/hacker/hacker.htm (Stand: 12.8.2002).

- Im Ergebnis effektiver könnte dagegen das Verbot, die Kriminalisierung und vor allem die Verfolgung des *Anbietens der Raubkopien* sein, das – wie die obige Analyse gezeigt hat – unabdingbare Voraussetzung für das Entstehen der massenhaften Schädigung der Urheber ist. Diesem zweiten Ansatz steht im Urheberrecht nicht das Recht der Privatkopie entgegen. Auch wird die Verfolgung dieser – der eigentlichen Schädigung vorausgehenden – Tathandlung nicht durch ihre Lokalisation in der Privatsphäre der Nutzer verhindert, da die entsprechenden Angebote der Täter öffentlich erfolgen müssen.

- Ein dritter rechtlicher Ansatz könnte sich gegen die Angriffe auf die Verschlüsselung der digitalen Güter richten, die in vielen Fällen ebenfalls Voraussetzung für die illegale Kopie sind. Die vorangegangene Analyse macht allerdings deutlich, dass ein solcher Ansatz nur als ergänzende Maßnahme in Betracht kommt, da die digitalen Güter in den oben beschriebenen File-Sharing-Systemen unverschlüsselt angeboten werden. Das Verbot, die Kriminalisierung und die Verfolgung von Angriffen auf die Verschlüsselung digitaler Güter wirkt daher nur gegen den Teil der Raubkopierer, der die Verschlüsselung durch eigene Recherchemaßnahmen oder durch die Nutzung von fremden Tools bricht, nicht jedoch gegen diejenigen Personen, welche die – eventuell von anderen bereits dekodierten – Inhalte unverschlüsselt (z.B. in File-Sharing-Systemen) anbieten. Als ergänzende Maßnahme ist ein Verbot und eine Kriminalisierung der Umgehung von Sicherungsmechanismen jedoch von erheblicher Bedeutung, da dieser Ansatz sich speziell gegen diejenigen Personen richtet, die bei der Verbreitung von Raubkopien eine Schlüsselrolle einnehmen. Bei einem rechtlichen Vorgehen gegen die Dekodierung verschlüsselter digitaler Güter kann dabei wieder zwischen der eigentlichen Tathandlung des Dekodierens sowie der Verbreitung der entsprechenden Tools im Internet (sowie eventuell auch schon dem Besitz der entsprechenden Werkzeuge) unterschieden werden.

Die nachfolgende rechtliche Analyse soll untersuchen, inwieweit das geltende Recht diese drei möglichen Ansätze bereits verwirklicht oder ob insoweit Reformbedarf besteht.

III. Strafrechtliche Beurteilung

A. Überblick zu den relevanten Tatbeständen und Tathandlungen

1. Systematik des geltenden Rechts

Der strafrechtliche Schutz immaterieller Güter wird im geltenden Recht durch eine Vielzahl unterschiedlicher Strafvorschriften erreicht. Die Systematik der geltenden Strafvorschriften orientiert sich dabei nicht an den im Hinblick auf die Bekämpfung der Raubkopien relevanten Gesichtspunkten, sondern primär an den geschützten Rechtsgütern und sekundär an den unter Strafe gestellten Angriffsformen. Für die (insbesondere strafrechtliche) Erfassung der vorstehend dargestellten Erscheinungsformen sind dabei vor allem die folgenden Vorschriften zu unterscheiden:

- Das *Eigentum an materiellen Gütern* (einschließlich an Datenträgern) wird durch die Strafbestimmungen des Diebstahls, der Unterschlagung und der Hehlerei (§§ 242, 246, 259 StGB) in umfassender Weise geschützt.

- *Immaterielle Güter* erhalten einen der Art nach vergleichbaren *unmittelbaren und absoluten Schutz* nur in einigen wenigen – vom Gesetzgeber abschließend geregelten – Fällen. Ein derartiger unmittelbarer und absoluter Schutz der immateriellen Güter führt dazu, dass die Verwertung der geschützten Daten durch dritte Personen unabhängig davon rechtswidrig ist, wie diese Person die Daten erlangt haben, so dass ein „gutgläubiger Erwerb“ durch dritte Personen ausgeschlossen ist. Für die vorliegend interessierenden Software-, Audio- und Videodaten ist insoweit vor allem das Urheberrecht einschlägig, das die konkrete Formgestaltung dieser Güter schützt. Den – ebenfalls zu einem unmittelbaren und absoluten Schutz führenden – Regelungen des Patentrechts und des Halbleiterschutzrechts kommt dagegen im vorliegenden Zusammenhang keine wesentliche Bedeutung zu.

- Wegen des engen Kreises der absolut geschützten Immaterialgüter sowie der Ausnahmetatbestände der Immaterialgüterrechte (insbesondere im Bereich der privaten Nutzung) sind daneben Regelungen relevant, die Immaterialgüter zwar nicht als solche und auch nicht absolut schützen, die jedoch bestimmte *rechtswidrige Formen der Erlangung und teilweise auch der Verwertung der zugrunde liegenden Daten* strafrechtlich sanktionieren und den betroffenen Gütern dadurch einen *mittelbaren und relativen Schutz* geben. Die wichtigsten einschlägigen Strafbestimmungen im vorliegenden Zusammenhang sind

§ 17 UWG (der bestimmte Formen der sittenwidrigen Erlangung und Verwertung von Betriebsgeheimnissen erfasst), § 202a StGB (der bestimmte Formen der Erlangung von geschützten elektronisch gespeicherten Daten unter Strafe stellt), § 263a StGB (der vermögensschädigende Manipulationen von Datenverarbeitungsvorgängen kriminalisiert) sowie § 265a StGB (der die Erschleichung von Automatenleistungen und des Zutritts zu Veranstaltungen oder Einrichtungen bestraft). Die einschlägigen „Erlangungs- und Verwertungsverbote“ haben für die von ihnen geschützten Personen im Vergleich zu den absolut geschützten Immaterialgüterrechten allerdings den Nachteil, dass sie nur auf denjenigen Täter anwendbar sind, der die geschützten Informationen in der gesetzlich verbotenen Weise erlangt oder weiter verarbeitet, nicht jedoch z.B. auf den gutgläubigen Aufkäufer oder Verwender der – von einem „Vormann“ eventuell auch rechtswidrig erlangten – Daten.

Wegen dieses begrenzten Schutzes der relativen Erlangungs- und Verwertungsverbote stellt sich im Zusammenhang mit diesen Vorschriften noch die Frage, inwieweit entweder durch diese Vorschriften selbst oder aber durch weitere Strafvorschriften (wie den Tatbestand der Hehlerei gem. § 259 StGB) auch die entsprechende Verwertung der rechtswidrig erlangten Daten erfasst werden kann oder erfasst werden sollte.

- Da die rechtswidrige Nutzung von Informationen in vielen Fällen durch – vor allem im Internet angebotene – Werkzeuge (Tools), Anleitungen und Anpreisungen gefördert wird, entwickelt(e) die jüngste Reformgesetzgebung daneben *Vorfeldtatbestände*, welche bereits die Herstellung, den Vertrieb und teilweise auch den Besitz von *Tools oder Informationen* bestrafen, mit deren Hilfe *technische Schutzmaßnahmen für digitale Güter umgangen* werden können. Derartige Strafbestimmungen oder entsprechende Vorschläge sowie Empfehlungen finden sich insbesondere in § 4 und § 5 des Zugangskontrolldiensteschutz-Gesetzes (ZKDSG),[237] in § 108b i.V.m. § 95a Abs. 3 UrhG in der Fassung des Regierungsentwurfs für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 31.7.2002[238] sowie in Art. 6 (Misuse of Devices) i.V.m. Art. 10 (Offences Related to Infringements of Copyright and Related Rights) der Convention on Cybercrime des Europarats vom 23.11.2001.[239] Ansonsten wird die Anleitung und Aufforderung zu Straftaten durch die allgemeinen Vorschriften der Anstiftung gem. § 26 StGB oder unter dem Gesichtspunkt des öffentlichen Aufforderns zu Straftaten gem. § 111 StGB erfasst.

2. Systematik der vorliegenden Analyse und der zentralen Tathandlungen

Die Ausführungen im empirischen Teil dieses Gutachtens haben deutlich gemacht, dass für eine systematische Bewertung und Neukonzeption der rechtlichen Strategie zur Bekämpfung digitaler Raubkopien vier – für die Verbreitung von Raubkopien wesentliche – Sachverhalte unterschieden werden müssen. Ordnet man diese vier Sachverhalte nicht im Hinblick auf den oben analysierten Ablauf der typischen Missbrauchshandlungen, sondern im Hinblick auf ihre

237. Siehe oben Fn. 195.
238. Siehe oben Fn. 196.
239. Vgl. http://conventions.coe.int/treaty/en/Treaties/Html/185.htm (Stand: 12.8.2002).

Bedeutung für die Schädigung der digitalen Gütern, so sind für die rechtliche Beurteilung die folgenden vier Aspekte zu differenzieren:

- die Erstellung einer Raubkopie (als der eigentlich schädigenden Verletzungshandlung),
- das (insb. öffentliche) Angebot einer Raubkopie (das die Erstellung einer Raubkopie ermöglicht)

sowie – im Bereich der Kopierschutzmechanismen und DRM-Systeme –

- die Umgehung der technischen Schutzmechanismen und
- das öffentlichen Angebot von Tools zur Umgehung von technischen Schutzmechanismen.

Die nachfolgende Analyse orientiert sich deswegen zunächst an diesen unterschiedlichen Tathandlungen. Die vorgenannte Systematisierung des geltenden Rechts unter den Gesichtspunkten der betroffenen Rechtsgüter und der erfassten Angriffsformen findet sich dann auf der nachfolgenden Gliederungsebene.

B. Kopie der digitalen Güter

Die Kopie der digitalen Software-, Audio- und Videodaten stellt – wie die obigen Ausführungen zeigen – bei allen digitalen Gütern den *eigentlichen materiellen Verletzungs- und Schädigungsakt* von Raubkopien dar (der bei den durch technische Maßnahmen geschützten Gütern durch die Aushebelung der Schutzmechanismen ergänzt wird). Für die rechtliche Erfassung dieses Kopiervorgangs kommen neben klassischen Bestimmungen aus dem Kernstrafrecht des StGB (unten 1) vor allem die (Straf-)Vorschriften des Urheberrechts (unten 2) in Betracht.

1. Bestimmungen des StGB

a) Eigentumsdelikte (§§ 242, 246 StGB)

Der allgemeine Diebstahltatbestand (§ 242 StGB) und der Tatbestand der Unterschlagung (§ 246 StGB) erfassen die Erstellung von Raubkopien in der Regel nicht. Dies beruht zunächst darauf, dass das Eigentum durch diese Vorschriften nur im Hinblick auf körperliche Sachen geschützt ist. Unkörperliche Objekte – wie Forderungen, Rechte, Urheberrechte, Betriebsgeheimnisse und Know how – fallen dagegen nicht unter den Sachbegriff der §§ 242, 246 StGB.[240]

Eine Anwendbarkeit dieser Tatbestände kommt daher ernsthaft nur in denjenigen Fällen in Betracht, in denen körperliche Datenträger betroffen sind (so dass der gesamte Internet-Bereich von vornherein ausgeschlossen ist).[241] In der Praxis werden die §§ 242, 246 StGB daher vor allem in den Fällen relevant, in denen z.B. entsprechende Masterkopien von Ton-, Video- oder

240. Vgl. dazu OLG München JZ 1976, 411 ff. m. Anm. *Sieber*.
241. Vgl. Tröndle/*Fischer*, Kommentar zum StGB, 50. Aufl. 2001, § 242 Rn. 3.

Softwareträgern in den Produktionseinrichtungen der Hersteller – z.B. durch Mitarbeiter – entwendet oder unterschlagen werden. Falls der Täter in diesen Fällen einen von ihm weggenommenen oder in Besitz genommenen körperlichen Datenträger mit immateriellen Gütern auf Dauer behält, bereitet die Anwendbarkeit der §§ 242, 246 StGB keine Schwierigkeiten. Gibt der Täter den Datenträger nach seiner Kopie jedoch wieder zurück, so gestaltet sich die Anwendbarkeit der §§ 242, 246 StGB dagegen schwierig, weil es im Hinblick auf den Datenträger selbst an einer Zueignung(sabsicht) fehlt, die bekanntermaßen eine auf Dauer gerichtete Enteignung(sabsicht) erfordert. In diesen Fällen könnte zwar erwogen werden, die für die Zueignung(sabsicht) erforderlichen Komponenten der dauernden Enteignung(sabsicht) und der – zumindest vorübergehenden – Aneignung(sabsicht) nicht auf die Substanz des weggenommenen Datenträgers zu beziehen, sondern auf seinen immateriellen Sachwert. Da der Originaldatenträger seinen Sachwert durch die Kopie jedoch nicht eindeutig verliert, wären derartigen Konstruktionen jedoch sehr enge Grenzen gesetzt.[242] Die Anwendbarkeit der für körperliche Rechtsobjekte zugeschnittenen Diebstahls- und Unterschlagungstatbestände auf immaterielle Güter wurde deswegen von der deutschen – anders als von der angloamerikanischen – Rechtsprechung auch nicht ernsthaft in Erwägung gezogen. Dies ist im Ergebnis auch richtig, da immaterielle Güter sich (gerade bei ihrer Kopie) in so elementarer Weise von körperlichen Gütern unterscheiden, dass sie nicht durch die allgemeinen Straftatbestände, sondern durch spezielle Regelungen – wie sie sich im Urheberrecht und in den Bestimmungen des UWG gegen Geheimnisverrat finden – geschützt werden müssen.[243]

b) Hehlerei (§ 259 StGB)

Die Begrenzung des Tatobjekts durch den Sachbegriff ist auch eine wesentliche Ursache für die Unanwendbarkeit des in § 259 StGB normierten Hehlereitatbestand. Dieses „Anschlussdelikt“ kommt im vorliegenden Zusammenhang deswegen in Betracht, weil – wie die empirische Analyse gezeigt hat – bei der Erstellung der Raubkopien regelmäßig auf rechtswidrig angebotene Vorlagen – z.B. in Tauschbörsen oder auf speziellen Servern des Internets – zurückgegriffen wird. Insoweit stellt sich – sowohl de lege lata als auch de lege ferenda – die Frage, ob die Verwertung rechtswidrig angebotener Daten nach den gleichen Vorschriften – oder de lege ferenda aufgrund der gleichen Überlegungen – bestraft werden kann, wie das Sich-Verschaffen von rechtswidrig erlangten Sachen.

§ 259 StGB bedroht denjenigen mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe, der „eine Sache, die ein anderer gestohlen oder sonst durch eine gegen fremdes Vermögen gerichtete rechtswidrige Tat erlangt hat, ankauft oder sich oder einem Dritten verschafft, sie absetzt oder absetzen hilft, um sich oder einen Dritten zu bereichern“. Da Daten keine Sache i.S.d. § 259 StGB sind,[244] ist die Vorschrift in den – den Kernbereich der modernen Raubkopie bildenden – Fällen unanwendbar, in denen der Täter sich die als Vorlage benötigten Daten nicht auf einem körperlichen Datenträger verschafft, sondern sie in unkörperlicher Form aus dem Internet

242. Vgl. dazu unter strafrechtsdogmatischen Gesichtspunkten *Sieber*, Computerkriminalität und Strafrecht, 2. Aufl. 1980, S. 190.
243. Vgl. zu dieser grundsätzlichen Problemstellung des Informationsrechts – auch rechtsvergleichend – *Sieber*, Computerkriminalität und Strafrecht, 2. Aufl. 1980, S. 190; *Sieber*, The International Emergence of Criminal Information Law, 1992, S. 18 ff.
244. Vgl. nur Schönke/Schröder (Sch/Sch) / *Stree*, Kommentar zum StGB, 26. Aufl. 2001, § 259 Rn. 5.

herunterlädt.[245]

Aber auch in den Fällen der Verschaffung eines körperlichen Datenträger als Vorlage für eine Raubkopie greift die am Dogma des körperlichen Tatobjekts orientierte Vorschrift des § 259 StGB nach h.M. nicht ein.[246] Dies gilt nicht nur in den Fällen, in denen sich jemand eine Kopiervorlage rechtmäßig besorgt und in denen es deswegen schon am Merkmal einer rechtswidrigen Vortat fehlt. § 259 StGB ist darüber hinaus auch in denjenigen Fällen unanwendbar, in denen ein Datenträger mit einer rechtswidrig hergestellten oder verbreiteten (Raub-)Kopie als Vorlage benutzt wird. In diesen Fällen ist zwar eine gegen fremdes Vermögen gerichtete rechtswidrige Vortat gegeben. Jedoch fehlt es bei der Verletzung von Urheberrechten nach h.M. an der Aufrechterhaltung einer rechtswidrigen Besitzlage am Datenträger,[247] die erforderlich ist, weil § 259 StGB aufgrund der Beschränkung seines Tatobjekts auf körperliche Sachen die Perpetuierung einer rechtswidrigen Vermögenslage nur in der Form der Perpetuierung einer rechtswidrigen Besitzlage erfasst.[248] Dadurch, dass urheberrechtlich geschützte Daten rechtswidrig auf einen Datenträger des Kopierenden oder des Empfängers kopiert werden, erlangt der Urheber aber weder Besitz noch Eigentum an dem Datenträger selbst, so dass er auch keinen dinglichen Herausgabeanspruch hat.[249]

c) Geldwäsche (§ 261 StGB)

Der – erst im Jahr 1992 – durch das OrgKG[250] geschaffene und bisher im Zusammenhang mit der Bekämpfung von Raubkopien noch kaum diskutierte Straftatbestand des Geldwäsche (§ 261 StGB) ist demgegenüber als neuere Strafbestimmung nicht mehr am Sachdogma orientiert. Die Vorschrift betrifft vielmehr „Gegenstände“, deren Herkunft verschleiert wird (Abs. 1) oder – was im vorliegenden Zusammenhang von besonderem Interesse ist – die sich der Täter verschafft (Abs. 2). Der Begriff des „Gegenstandes“ ist dabei nicht auf Sachen i.S.d. § 90 BGB beschränkt, sondern erfasst auch Rechte,[251] unter die sich auch fremde Urheberrechte subsumieren lassen.[252] Eine Anwendbarkeit auf die Erlangung und Nutzung von rechtswidrigen Kopien zum Zwecke von deren Kopie scheitert allerdings daran, dass die von § 261 StGB erfassten Gegenstände aus bestimmten Vortaten herrühren müssen, die in dem Vortatenkatalog

245. Dagegen kann ein körperlicher Datenträger selbst Gegenstand einer Hehlerei sein, vgl. *Heinrich*, Die Entgegennahme von raubkopierter Software als Hehlerei?, JZ 1994, 938, 941; Sch/Sch/*Stree*, § 259 Rn. 5.
246. Vgl. KG, NStZ 1983, 561, 562; *Friedrich*, Strafbarkeit des Endabnehmers von Raubkopien, MDR 1985, 366 ff.; *Heinrich*, JZ 1994, 938; *Rupp*, Zur strafrechtlichen Verantwortung des „bösgläubigen“ Softwareerwerbers, wistra 1985, 137, 138; Sch/Sch/*Stree*, § 259 Rn. 9.
247. Das KG Berlin entschied daher auch, dass „der Erwerber eines rechtswidrig hergestellten Vervielfältigungsstücks von dem Hersteller oder Zwischenhändler rechtmäßig Eigentum und Besitz an einem Werkstück erhält“, vgl. KG, NStZ 1983, 561, 562 m. Anm. *Flechsig*, NStZ 1983, 562 f. Siehe auch *Heinrich*, JZ 1994, 938; *Sternberg-Lieben*, Musikdiebstahl, Köln 1985, S. 102 ff.; *Rupp*, wistra 1985, 137, 138; a.A. *Ganter*, Strafrechtliche Probleme im Urheberrecht, NJW 1986, 1479, 1480.
248. Vgl. *Heinrich*, JZ 1994, 938, 943 f.; Sch/Sch/*Stree*, § 259 Rn. 1.
249. Vgl. *Heinrich*, JZ 1994, 938, 944.
250. Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität v. 15.7.1992, BGBl. 1992 I, S. 1302 ff.
251. Vgl. Sch/Sch/*Stree*, § 261 Rdn. 3.
252. Vgl. auch *Cebulla*, Gegenstand der Geldwäsche, wistra 99, 281, der für einen funktionalen Gegenstandsbegriff plädiert und daher Computerprogramme, losgelöst von möglichen Urheberrechten, als tauglichen Gegenstand i.S.d. § 261 StGB ansieht.

des § 261 StGB ohne die Nennung von Urheberrechtsverletzungen abschließend umschrieben sind.

Die Anwendbarkeit von § 261 StGB im Bereich der Raubkopien kommt daher nur in speziellen Fallgestaltungen in Betracht, in denen sich jemand eine rechtswidrig erstellte Kopiervorlage (oder – in dem unten noch näher untersuchten Zusammenhang – ein Hackingtool) verschafft, die (bzw. das) aus einer Tat stammt, welche von einem Mitglied einer kriminellen Vereinigung (§ 129 StGB) begangen wurde. Da § 129 StGB an die Willensbildung einer kriminellen Vereinigung sehr viel höhere Anforderungen stellt als eine gewerbsmäßige oder bandenmäßige Begehung,[253] kann § 261 StGB zwar in speziellen Fallgestaltungen der organisierten Verbreitung von Raubkopien Anwendung finden, für eine flächendeckende Bekämpfung von Raubkopien hat er jedoch keine Bedeutung.

d) Zwischenbilanz

Die im Strafgesetzbuch enthaltenen Bestimmungen des sog. Kernstrafrechts bieten damit für die Erfassung der eigentlich schädigenden Handlung der Erstellung einer Raubkopie keine Grundlage.

2. Strafbestimmungen der §§ 106 ff. UrhG

a) Zivilrechtsakzessorietät der §§ 106 ff. UrhG

Die zentrale Strafvorschrift des Urheberstrafrechts, § 106 UrhG, bedroht denjenigen mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe, der in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt. Die Qualifikation des § 108a UrhG erhöht die Strafdrohung für Fälle des gewerbsmäßigen Handelns auf bis zu fünf Jahre.

Das Urheberstrafrecht ist damit in weitgehendem Maße zivilrechtsakzessorisch. Dies bedeutet, dass der Umfang der Strafvorschrift durch die zivilrechtlichen Regelungen bestimmt wird, wobei sich allerdings durch die unterschiedlichen Auslegungsgrundsätze des Zivilrechts und des Strafrechts unterschiedliche Verbotsbereiche oder Rückwirkungen der strafrechtlichen auf die zivilrechtliche Auslegung ergeben können.[254] Diese Zivilrechtsakzessorietät des Urheberstrafrechts vom Urheberzivilrecht besteht dabei sowohl im Hinblick auf das von § 106 UrhG geschützte Tatobjekt („ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes“) und die von der Vorschrift erfassten Tathandlungen („vervielfältigt, verbreitet oder öffentlich wiedergibt“) als auch für die Schranken des Urheberrechts („in anderen als den gesetzlich zugelassenen Fällen“).[255]

253. Vgl. *Sieber/Bögel*, Logistik der Organisierten Kriminalität, 1993, S. 360.
254. Vgl. zu diesen Problemen der „Normspaltung“ *Sieber*, in: Sieber/Hoeren, Handbuch Multimedia-Recht, Loseblattsammlung, 3. Ergänzungslieferung, Stand: Dezember 2001, Teil 19 Rn. 213.
255. Vgl. Schricker/*Haß*, Kommentar zum Urheberrecht, 2. Aufl. 1999, § 106 Rn. 7 ff.

b) Tatobjekt und Tathandlung der §§ 106, 108 UrhG

Im Hinblick auf Tatobjekt und Tathandlungen bereitet die Akzessorietät der §§ 106 ff. UrhG in dem vorliegend untersuchten Bereich keine besonderen Probleme:

- Die hier besonders interessierenden Software-, Video- und Audiodaten stellen regelmäßig urheberrechtlich geschützte Werke i.S.d. §§ 2, 4 UrhG dar. Der früher vehement geführte Streit über den Urheberrechtsschutz von Computerprogrammen hat seit der Einfügung der §§ 69a ff. UrhG viel von seiner Brisanz verloren.[256] Bei den heute weiter bestehenden Streitfragen – etwa nach der Schutzhöhe von Computerprogrammen (die eher niedrig angesetzt wird) und der Vollstreckbarkeit von Unterlassungsurteilen – handelt es sich um allgemeine Fragen, die im vorliegenden Kontext keine besondere Bedeutung haben. Nicht einschlägig sind die urheberrechtlichen Schutzvorschriften dagegen z.B. bei den oben erwähnten Daten mit Aktienkursen oder sonstigen Wirtschaftsdaten.[257]

- Die im vorliegenden Zusammenhang interessierende Kopie von Software-, Audio- und Videodaten verletzt auch regelmäßig das Vervielfältigungsrecht des Urhebers bzw. Nutzungsrechte der entsprechend Berechtigten: Eine Vervielfältigung ist „jede körperliche Festlegung eines Werkes, die geeignet ist, das Werk dem menschlichen Sinne auf irgendeine Weise unmittelbar oder mittelbar wahrnehmbar zu machen“.[258] Damit ist eine körperliche Fixierung des Werkes notwendig.[259] Diese liegt bei digitalen Werken dann vor, wenn sie auf einem Datenträger gespeichert werden, z.B. einer CD-ROM oder der Festplatte eines Computersystems. Die empirische Analyse zeigt, dass dies in den hier einschlägigen Piratefällen durch die Kopie auf CD-ROMs, DVD-R(W)s sowie auf Festplatten von Computersystemen – unabhängig ob es sich um einen privaten PC oder einen Internet-Server handelt – regelmäßig gegeben ist.

  Eine Vervielfältigung erfolgt insbesondere auch in dem besonders bedrohlichen Bereich der Verbreitung von Raubkopien über das Internet, da dabei regelmäßig Kopien auf Datenträgern abgespeichert werden. Dies gilt z.B. für die oben dargestellte Verbreitung von Raubkopien über Online-Tauschbörsen oder spezielle FTP-Server. Da die meisten Vorgänge der elektronischen Datenkommunikation aus technischen Gründen auch eine – zumindest zeitweise – Fixierung des digitalen Werkes während der Datenübertragung erfordern, war zwar lange Zeit umstritten, ob auch insoweit das ausschließliche Vervielfältigungsrecht des Urhebers betroffen ist.[260] Mit der Verabschiedung des Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft[261] wird dieser Meinungs-

256. Vgl. Schricker/*Loewenheim*, § 69a Rn. 2 ff.
257. Für diese Daten kann allerdings ein Datenbankschutz gem. den §§ 87a ff. UrhG in Betracht kommen, auf den in dem vorliegenden Gutachten wegen der unproblematischen Anwendbarkeit des Urheberrechts auf die hier vor allem interessierenden Software-, Video- und Audiodaten nicht eingegangen wird.
258. Vgl. BGH GRUR 1991, 449, 453; GRUR 1983, 28, 29; *Hänel*, Napster und Gnutella – Probleme bei der Übertragung von MP3-Dateien nach deutschem Urheberrecht, JurPC Web-Dok. 245/2000, Abs. 11, abrufbar unter http://www.jurpc.de/aufsatz/20000245.htm (Stand: 12.8.2002); *Kreutzer*, Napster, Gnuttella & Co.: Rechtsfragen zu Filesharing-Netzen aus Sicht des deutschen Urheberrechts de lege lata und de lege ferenda –Teil 1, GRUR 2001, 193, 199.
259. Vgl. Schricker/*Loewenheim*, § 16 Rn. 6.
260. Vgl. *Bosak*, Urheberrechtliche Zulässigkeit privaten Downloadings von Musikdateien, CR 2001, 176 f.; Schricker/*Loewenheim*, § 16 Rn. 19.
261. Siehe oben Fn. 196.

streit jedoch weitgehend obsolet werden, da nach dem geplanten § 44a UrhG-E „vorübergehende Vervielfältigungshandlungen, die flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen und deren alleiniger Zweck es ist 1. eine Übertragung in einem Netz zwischen Dritten und einen Dritten durch einen Vermittler oder 2. eine rechtmäßige Nutzung eines Werkes oder sonstigen Schutzgegenstandes zu ermöglichen“ vom Vervielfältigungsrecht ausgeschlossen sind, wenn sie „keine eigenständige wirtschaftliche Bedeutung haben“.[262] Alle anderen Vervielfältigungen werden jedoch erfasst.

Für die oben hervorgehobenen Online-Tauschbörsen bedeutet dies, dass sowohl die Kopie eines Spielfilms, die in einer Online-Tauschbörse angeboten wird, als auch die per Download von einem Nutzer auf seiner Festplatte abgespeicherte Kopie, eine Vervielfältigung darstellen; keine Vervielfältigungen wären demgegenüber nach der künftigen Rechtslage kurzzeitige Zwischenspeicherungen, die beispielsweise während des Datentransports in einem Router erfolgen; derartige Zwischenspeicherungen sind nicht nur integraler Bestandteil der Datenkommunikation im Internet, sondern auch flüchtig und begleitend im Sinne der neuen Vorschrift, weil die Zwischenspeicherung unter Umständen nur wenige Millisekunden dauert.[263] Für die Erfassung der vorgenannten Raubkopien ist dies jedoch im Ergebnis unschädlich.

c) Schranke des § 53 Abs. 1 UrhG n.F.

Gravierende Einschränkungen des Schutzes von digitalen Gütern resultieren im vorliegend untersuchten Bereich allerdings aus der Bezugnahme von §§ 106 ff. UrhG auf die gesetzlichen Schranken des Urheberrechts.[264] Von besonderer Bedeutung ist dabei im vorliegenden Kontext die Schranke des § 53 UrhG, wonach einzelne Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch zulässig sind. Besonders problematisch erweist sich dabei die Vervielfältigung zum privaten Gebrauch nach § 53 Abs. 1 S. 1 UrhG, wonach es zulässig ist, „einzelne Vervielfältigungsstücke eines Werkes zum privaten Gebrauch herzustellen“. Dabei stellt sich die Frage, ob hierunter nur analoge Kopien oder auch digitale Kopien fallen.[265] Insoweit wird jedoch in § 53 Abs. 1 S. 1 UrhG in der Fassung des Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft durch die Formulierung „Vervielfältigungen eines Werkes... auf

262. Siehe dazu auch *Linnenborn*, Europäisches Urheberrecht in der Informationsgesellschaft, K&R 2001, 394 f. und die „Stellungnahme der ARD und des ZDF zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“, S. 4 f., abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/ard_zdf1.pdf sowie Forum der Rechteinhaber, Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, S. 3, abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/ForumRechteinhaber.pdf (Stand: 12.8.2002).
263. Siehe dazu auch Schricker/*Loewenheim*, § 16 Rn. 19, wo bereits für die bestehende Rechtslage bezweifelt wird, ob extrem kurze Festlegungen eine Vervielfältigung darstellen.
264. Zu diesen Schranken zählt aufgrund der gesetzlichen Verortung aus dogmatischer Sicht auch die Vorschrift des geplanten § 44a UrhG.
265. Vgl. dazu *Bayreuther*, Beschränkungen des Urheberrechts nach der neuen EU-Urheberrechtsrichtlinie, ZUM 2001, 828, 831 sowie die „Stellungnahme der Filmwirtschaft zu dem Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 18. März 2002“, S. 5, abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/StellnahmeFiWi170402.pdf (Stand: 12.8.2002).

beliebigen Trägern“ klargestellt werden, dass sowohl analoge als auch digitale Kopien zum privaten Gebrauch hergestellt werden dürfen.[266]

Zentraler Begriff des § 53 Abs. 1 S. 1 UrhG ist damit der „private Gebrauch“. Darunter versteht die ganz h.M. den „Gebrauch in der Privatsphäre zur Befriedigung rein persönlicher Bedürfnisse durch die eigene Person oder die mit ihr durch ein persönliches Band verbundenen Personen“.[267] Damit ist z.B. die Kopie einer originalen Audio-CD zum Zwecke der Nutzung im Auto unproblematisch zulässig. Ebenso kann z.B. eine Vervielfältigung erfolgen, damit der Sohn oder die Tochter die Kopie auf eigenen Abspielgeräten benutzen können. Dabei ist zu beachten, dass das Gesetz nur einzelne Vervielfältigungen zulässt, wobei es sich nach verbreiteter Ansicht um maximal 7 Vervielfältigungen handeln darf.[268] Ein privater Gebrauch liegt weiterhin auch dann vor, wenn der Nutzer z.B. Musikstücke einer originalen Audio-CD oder einer rechtmäßig hergestellten Audio-CD-Kopie zunächst zum eigenen, privaten Gebrauch auf seinem Rechner speichert. Allerdings kann ein privater Gebrauch in dem Moment nicht mehr angenommen werden, in dem der Nutzer als Mitglied eines File-Sharing-Dienstes beliebigen Personen einen Zugriff auf die auf seiner Festplatte gespeicherten digitalen Inhalte gestattet.[269] Denn ab diesem Zeitpunkt werden die gespeicherten Inhalte nicht mehr im Privatbereich genutzt, sondern stehen einem Millionenpublikum zur Verfügung.

Fraglich ist weiterhin, ob die private Kopie von urheberrechtlich geschützten Daten auch dann durch § 53 UrhG gerechtfertigt wird, wenn sie auf rechtswidrigen Vorlagen beruht, die beispielsweise im Internet öffentlich angeboten werden. Diese – im vorliegenden Kontext ganz zentrale – Problemstellung hängt davon ab, ob der Kopierende Eigentümer der Kopiervorlage

266. Vgl. *Flechsig*, Grundlagen des Europäischen Urheberrechts, ZUM 2002, 1, 9; *Goldmann*/*Liepe*, Vertrieb von kopiergeschützten Audio-CDs in Deutschland, ZUM 2002, 362, 369; *Kröger*, Die Urheberrechtsrichtlinie für die Informationsgesellschaft – Bestandaufnahme und kritische Bewertung, CR 2001, 316, 320; *Linnenborn*, K&R 2001, 394, 396 und auch die rechtspolitischen Überlegungen bei *Reinbothe*, Die Umsetzung der EU-Urheberrechtsrichtlinie in deutsches Recht, ZUM 2002, 43, 49 f. Die Klarstellung wird begrüßt in der „Stellungnahme der ARD und des ZDF zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“, oben Fn. 262, S. 6, sowie in der „Stellungnahme des Bundesverbandes Deutscher Zeitungsverleger e.V. (BDZV) zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“, S. 1, abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/BDZVStellungRefE-2002-04-18.pdf; ablehnend äußern sich dagegen der dmmv, Stellungnahme zur Umsetzung der EU-Urheberrechtsrichtlinie 2001/29/EG, S. 4, abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/stlgn_eu_rili_harmon_01.pdf, der BITKOM, Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, S. 4 f., abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/BITKOM-StellgRefE-2002-04-19.pdf, der Börsenverein des deutschen Buchhandels, Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, S. 1 f., abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/StellungBoevErg.pdf und die KirchMedia, Anmerkungen zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, S. 6, abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/KirchMedia.pdf (Stand: 12.8.2002).

267. Vgl. BGH GRUR 1978, 474 f.

268. Diese Zahl ergibt sich aus einer Entscheidung des Bundesgerichtshofs, der die Beklagte antragsgemäß verurteilte, 7 Vervielfältigungsstücke herstellen zu müssen. Vgl. BGH GRUR 1978, 474 ff. Dies darf allerdings nicht als absolutes „Dogma“ verstanden werden, sondern gibt lediglich einen Hinweis darauf, dass es sich auf jeden Fall um eine „überschaubare“ Anzahl von Privatkopien handeln muss. So wohl auch Schricker/*Loewenheim*, § 53 Rdnr. 14.

269. Vgl. *Hänel*, oben Fn. 258, Abs. 35.

sein muss, ob der Kopierende sich im rechtmäßigen Besitz der Kopiervorlage befinden muss und/oder ob der Kopierende auf eine rechtmäßig erstellte Vorlage zurückgreifen muss. Insoweit ist daher zu differenzieren.

Verzicht auf Eigentümerstellung

Die Vervielfältigung zum privaten Gebrauch setzt unstreitig nicht voraus, dass ein eigenes Werkstück benutzt wird, d.h. dass sich das Werkstück im Eigentum des Vervielfältigenden befinden muss.[270] Dies ergibt sich bereits aus dem Umkehrschluss zu § 53 Abs. 2 Nr. 2 UrhG (Aufnahme in ein eigenes Archiv), der explizit als Vorlage ein eigenes Werkstück fordert. Damit ist es z.B. erlaubt, von einer ausgeliehenen Original-Audio-CD eine Privatkopie zu erstellen.

Erfordernis des rechtmäßigen Besitzes

Ebenso unstreitig ist in der urheberrechtlichen Rechtsprechung und Literatur, dass als ungeschriebenes Tatbestandsmerkmal ein „rechtmäßiger Besitz“ an der Kopiervorlage bestehen muss.[271] Dies bedeutet allerdings nur, dass der Kopierende rechtmäßig in den Besitz der Kopiervorlage gekommen sein muss. Dies ist z.B. zu verneinen, wenn Audiodaten aus einem Tonstudio entwendet und zum eigenen Gebrauch vervielfältigt werden. Dagegen sagt dieses ungeschriebene Tatbestandsmerkmal im Hinblick auf die Online-Tauschbörsen nichts aus, da die Tauschbörsen nach einer Anmeldung von jedermann ohne weitere Einschränkung genutzt werden können.[272] Damit verschafft sich der Kopierende berechtigterweise „Besitz“ an den downgeloadeten Daten. Dasselbe gilt, wenn er die Dateien von den oben beschriebenen Servern im Internet abruft.

Problem des Erfordernisses einer rechtmäßigen Vorlage

Das eigentliche Problem bei der Vervielfältigung von digitalen Daten besteht somit darin, ob § 53 UrhG zusätzlich verlangt, dass eine rechtmäßig erstellte Kopiervorlage benutzt wird, d.h. z.B. ein entsprechendes Nutzungsrecht eingeräumt wurde. Diese Frage ist in der juristischen Literatur umstritten[273] und bisher – soweit ersichtlich – nicht gerichtlich geklärt.

Das Erfordernis einer rechtmäßigen Kopiervorlage wird dabei vor allem mit dem Argument abgelehnt, dass das „Recht der Allgemeinheit an dem ungehinderten Zugang zu den Kulturgütern“[274] nur durch explizit im Gesetzeswortlaut geregelte Tatbestandsmerkmale eingeschränkt werden dürfe.[275] Hiergegen kann man jedoch einwenden, dass der Gesetzgeber wohl kaum die

270. Vgl. BGH NJW 1997, 1363, 1366; NJW 1997, 1368, 1369; *Hänel*, oben Fn. 258, Abs. 17. Siehe dazu auch die Stellungnahme des Instituts für Rechtsfragen der freien und Open Source Software (ifrOSS) möglichen Neuregelung der Schrankenvorschrift § 53 UrhG und damit zusammenhängender Normen im Zuge der Neuordnung des deutschen UrhG bei der Einarbeitung der Richtlinie 2001/29/EG“, S. 3, abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/ifross/art13.pdf (Stand: 12.8.2002).
271. Vgl. KG GRUR 1992, 168 f.; *Bosak*, CR 2001, 176, 180; *Hänel*, oben Fn. 258, Abs. 19; *Kreutzer*, GRUR 2001, 193, 200; Schricker/*Loewenheim*, § 53 Rdnr. 13; ifrOSS, oben Fn. 270, S. 3.
272. Vgl. *Bosak*, CR 2001, 176, 180; *Kreutzer*, GRUR 2001, 193, 200.
273. Für die Voraussetzung einer legalen Quelle sind *Braun*, GRUR 2001, 1106, 1107 f.; *Leupold*/*Demisch*, Bereithalten von Musikwerken zum Abruf in digitalen Netzen, ZUM 2000, 379, 385; Weinknecht, http://www.weinknecht.de/mp3.htm (Stand: 12.8.2002). Ablehnend stehen dieser Einschränkung gegenüber *Bosak*, CR 2001, 176, 180; ifrOSS, oben Fn. 270, S. 3; *Kreutzer*, GRUR 2001, 193, 200; *Mönkemöller*, Moderne Freibeuter unter uns? – Internet, MP3, CD-R als GAU für die Musikindustrie!, GRUR 2000, 663, 667 f.
274. Vgl. BT-Drucks. 10/837.
275. So *Bosak*, CR 2001, 176, 181.

Verbreitung von Raubkopien in diesem Bereich legalisieren wollte, zumal der Schutz der Urheber überhaupt erst sicherstellt, dass es auch zukünftig Kulturgüter für die Allgemeinheit gibt. Zudem ergibt sich aus § 96 Abs. 1 UrhG, dass rechtswidrig hergestellte Vervielfältigungsstücke nicht verbreitet oder zu öffentlichen Wiedergaben verwendet werden dürfen. Außerdem dürfen nach § 96 Abs. 2 UrhG rechtswidrig veranstaltete Funksendungen nicht auf Bild- oder Tonträger aufgenommen werden. Es liegt damit nahe, diese Vorschriften auch auf das Herunterladen von rechtswidrigen Ton- und Bilddateien anzuwenden.[276] Der Gesetzgeber hat es bisher allerdings versäumt, das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft[277] auch zu einer Erweiterung des § 96 Abs. 2 UrhG zu nutzen, so dass insoweit nur schwerlich von einer planwidrigen Gesetzeslücke gesprochen werden kann.[278] Gleichwohl zeigt § 96 UrhG bereits heute, dass der Gesetzgeber sehr wohl zwischen rechtmäßigen und rechtswidrigen Werken unterscheidet.

Gegen ein Tatbestandsmerkmal der rechtmäßigen Kopie wird weiter vorgebracht, dass der Nutzer – also der Kopierende – nicht dadurch unangemessen benachteiligt werden dürfe, dass ihm eine Prüfungspflicht im Hinblick auf die Rechtmäßigkeit der Kopie auferlegt werde.[279] Dieses Argument greift jedoch zumindest für das Problem der über das Internet bezogenen Raubkopien zu kurz, weil jedem Nutzer einer Online-Tauschbörse oder eines speziellen Servers bewusst ist, dass die dort abrufbaren Dateien nahezu vollständig ohne Einwilligung der Rechteinhaber angeboten werden.[280]

Weiterhin wird von den Gegnern des Tatbestandmerkmals einer rechtmäßigen Kopiervorlage darauf verwiesen, dass § 53 UrhG als gesetzliche Lizenz das urheberrechtliche Ausschließlichkeitsrecht auf einen (mittelbaren) Vergütungsanspruch reduziert.[281] Dabei ist allerdings zu beachten, dass der Interessenausgleich zwischen Urhebern und Nutzern heute im Bereich der neuen Medien empfindlich gestört ist, da die §§ 54 ff. UrhG den Urhebern keinen adäquaten Vergütungsanspruch mehr geben. Dies beruht darauf, dass die Vergütungspflicht entweder an den zum Kopieren verwendeten Geräten oder an den Trägermedien ansetzt. Die empirischen Ausführungen haben jedoch gezeigt, dass sehr viele Raubkopien heute direkt über das Internet erfolgen und auf den Festplatten der Computer abgelegt werden. Daher müssten konsequenterweise nicht nur spezielle Kopiervorrichtungen, wie CD-Brenner, mit einer Abgabe belegt werden, sondern auch die Computersysteme in ihrer Gesamtheit. Letzteres ist aber rechtspolitisch umstritten. Hinzu kommt, dass auch mit der Abgabe auf einzelne Trägermedien, wie CD-R(W)s, kein interessengerechter Ausgleich mehr zu erreichen ist: Auf CD-Rohlinge können nicht nur Audio-CDs 1:1 kopiert werden, sondern z.B. bis zu 250 Audiodateien im MP3-Format, was den Anteil der Abgabe auf das einzelne Musikstück massiv schmälert. Dies zeigt, dass der überkommene Ansatz der Vergütungspflicht im Bereich der PCs und des Internets überholt ist und bisher durch kein adäquates neues System ersetzt wurde. Solange dies nicht der Fall ist, sollten Privatkopien nur von rechtmäßigen Vorlagen erstellt werden dürfen. Dies fordert – zumindest indirekt – auch der EU-Gesetzgeber, der in Art. 5 Abs. 5 der EU-Richtlinie „zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte

276. So *Braun*, GRUR 2001, 1106, 1107 f.
277. Siehe oben Fn. 196.
278. Daher wir auch immer wieder gefordert, § 96 Abs. 1 UrhG dahingehend zu ergänzen, dass rechtswidrig hergestellte oder verbreitete Vervielfältigungsstücke nicht vervielfältigt werden dürfen, vgl. zum Ganzen ifrOSS, oben Fn. 270, S. 5 ff.
279. Vgl. *Kreutzer*, GRUR 2001, 193, 200; ifrOSS, oben Fn. 270, S. 6.
280. So auch Braun, GRUR 2001, 1106, 1108.
281. So *Kreutzer*, GRUR 2001, 193, 200.

in der Informationsgesellschaft“[282] klarstellt, dass im Falle der Implementierung von Schranken die berechtigten Interessen des Rechtsinhabers nicht ungebührlich verletzt werden dürfen. Ein Ausschluss der Privatkopie bei der Verwendung von rechtswidrigen Vorlagen wird vor allem auch durch die unten näher ausgeführten verfassungsrechtlichen Überlegungen gestützt. Solange die Urheber für die massenhafte Kopie von Software, Audiodaten und Videodaten im Internet keine adäquate Vergütung erhalten, sprechen daher bei der zivilrechtlichen Beurteilung die besseren Gründe dafür, die Kopie von (z.B. in Tauschbörsen oder auf speziellen Servern des Internets) rechtswidrig angebotenen urheberrechtlich geschützten Werken nicht durch § 53 UrhG zu rechtfertigen, sondern als rechtswidrig zu beurteilen.[283]

Allerdings ist fraglich, ob dieses Ergebnis auch im Strafrecht gelten kann. Art. 103 Abs. 2 GG verlangt, dass Strafvorschriften „gesetzlich bestimmt“ sein müssen. Diese verfassungsrechtliche Verbürgung für Strafvorschriften beruht dabei nicht nur auf den staatsrechtlichen Gesichtspunkten der Gewaltenteilung (nach dem das Parlament und nicht der Richter über die Grundlagen der Strafbarkeit entscheiden muss) und des Willkürverbots (das der richterlichen Auslegung Grenzen setzt). Entscheidend sind vielmehr auch die strafrechtlichen Gesichtspunkte der Verhaltenssteuerung der Bürger (die durch Strafvorschriften nur dann erfolgen kann, wenn der Bürger genau weiß, was er zu tun oder zu unterlassen hat) sowie der Schuldgrundsatz (der ebenfalls voraussetzt, dass der strafrechtliche Normbefehl für den Bürger erkennbar ist). Die Grenze der Auslegung wird deswegen nach h.M. stets durch den Wortlaut einer Strafvorschrift gezogen.

Für zivil- und verwaltungsakzessorische Strafvorschriften ist dabei allerdings erörterungsbedürftig, ob das Bestimmtheitsgebot von Art. 103 Abs. 2 GG nur für die eigentliche Strafnorm gilt oder auch für die von ihr in Bezug genommenen Ausfüllungsnormen. Soweit die eigentliche Strafnorm – auch ohne Heranziehung der akzessorischen Ausfüllungsnormen – den Verbots- oder Gebotsbereich für den Bürger hinreichend genau umschreibt, lässt sich im Einzelfall durchaus vertreten, die außerstrafrechtlichen Ausfüllungsnormen nur als – dem strafrechtlichen Bestimmtheitsgebot nicht unterliegende – „zusätzliche“ Erläuterungen der Strafnorm zu sehen. Soweit die – neben der Sanktionsnorm bestehende – Bestimmungsnorm einer Strafvorschrift dagegen lediglich in einer Verweisung auf außerstrafrechtliche Normen besteht, ist dies dagegen nicht mehr möglich, da ansonsten das grundgesetzlich garantierte Bestimmtheitsgebot des Art. 103 Abs. 2 GG durch eine entsprechende Gesetzgebungstechnik leer laufen und leicht umgangen werden könnte.

Die Strafvorschrift des § 106 UrhG gehört insbesondere im Hinblick auf ihr Tatbestandsmerkmal der „anderen gesetzlich zugelassenen Fälle“ zu dieser letzten Fallgruppe.[284] Denn die Bestimmungsnorm des § 106 UrhG enthält ihre Kontur und umschreibt ihren Verbotsbereich erst durch die Einbeziehung der zivilrechtlichen Normen über das geschützte Tatobjekt, die verbotenen Tathandlungen und die Schranken des Urheberrechts. Insbesondere die Verweisung auf die „gesetzlich zugelassenen Fälle“ ist ohne Heranziehung der akzessorischen zivilrechtlichen Schrankenbestimmungen inhaltsleer. Die Garantiefunktion von Art. 103 Abs. 2 GG muss daher auch auf die bezuggenommenen Schrankenbestimmungen erstreckt werden.

Dies führt dazu, dass im Rahmen der strafrechtlichen Beurteilung eine Beschränkung von § 53 UrhG auf Fälle der Verwendung einer rechtmäßigen Vorlage nicht möglich ist. Der Wortlaut

282. Vgl. ABl. L 167/17 vom 22.6.2001.
283. In diesem Sinne auch der BITKOM, oben Fn. 266, S. 5; *Hänel*, oben Fn. 258, Abs. 23 und das Forum der Rechteinhaber, oben Fn. 262, S. 5. Siehe auch *Goldmann*/*Liepe*, ZUM 2002, 362, 369.
284. Siehe dazu Schricker/*Haß*, § 106 Rn. 7 ff.

von § 53 Abs. 1 UrhG garantiert – über den Tatbestandsausschluss von § 106 UrhG – Straflosigkeit, indem er es als zulässig erklärt, „einzelne Vervielfältigungsstücke eines Werkes zum privaten Gebrauch herzustellen“. Die Beschränkung dieser Regelung auf Fälle der Benutzung einer rechtmäßigen Vorlage lässt sich dem Wortlaut der Vorschrift nicht entnehmen. Eine derartig grundlegende Entscheidung wie die Beschränkung von § 53 UrhG auf rechtmäßige Kopiervorlagen kann daher auch nicht vom Strafrichter getroffen werden, sondern nur vom demokratisch legitimierten Gesetzgeber, der sich im übrigen bisher bei den Beratungen des Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft[285] um diese Entscheidung gerade „gedrückt“ hat. Angesichts dieser Regelungsabstinenz des Gesetzgebers ist es zwar geboten, dass die Judikative im Bereich des Zivilrechts eine Entscheidung trifft. Die – massiv in Grundrechte der Bürger eingreifende – Strafbarkeit der entsprechenden Handlungen kann auf diese Weise und ohne gesetzliche Entscheidung jedoch nicht begründet werden.

Damit tritt allerdings das Problem auf, wie diese engere strafrechtliche Auslegung mit der oben als vorzugswürdig beurteilten zivilrechtlichen Auslegung zu vereinbaren ist. Soweit die Literatur diese Problematik einer möglichen „Normspaltung“ sieht, werden zwei unterschiedliche Lösungsmöglichkeiten vorgeschlagen: [286] Zum einen kommt in Betracht, unter dem Gesichtspunkt der „Einheit der Rechtsordnung“ die strafrechtliche Auslegung auch auf die zivilrechtliche Auslegung zurückwirken zu lassen. Dies hätte den Vorteil, dass § 53 UrhG sowohl für die zivilrechtliche Beurteilung als auch für die strafrechtliche Beurteilung den gleichen Inhalt hätte. Bei Gesetzen, die (wie z.B. das Urheberrechtsgesetz oder das Bundesdatenschutzgesetz) umfassende akzessorische Strafnormen aufweisen, hätte eine solche Auslegung allerdings zur Folge, dass weite Teile der zivilrechtlichen und der verwaltungsrechtlichen Bestimmungen den strafrechtlichen Auslegungsgrundsätzen unterworfen würden. Aus diesem Grunde ist es zumindest für primär zivilrechtliche oder verwaltungsrechtliche Gesetze mit weitreichenden akzessorischen Strafbestimmungen vorzugswürdig, die bezuggenommenen Normen nur für ihre strafrechtliche und nicht auch für ihre zivilrechtliche und verwaltungsrechtliche Funktion den strengeren Auslegungsgrundsätzen des Strafrechts zu unterwerfen. Diese „Normspaltung“ hat auch den Vorteil, dass das Strafrecht dadurch seine Funktion als ultima ratio des Rechtsgüterschutzes gerade in Rechtsgebieten entfaltet, in denen durch umfassende akzessorische Strafbestimmungen eine weitreichende Strafbewehrung aller zivil- und verwaltungsrechtlichen Verbote und Gebote erfolgt. In dem vorliegend untersuchten Bereich ermöglicht dieses Vorgehen auch, dass trotz der fehlender Strafbarkeit der Fertigung einer Privatkopie von einer rechtswidrig hergestellten Vorlage die so erstellte Kopie eine rechtswidrige Vervielfältigung bleibt, gegen die mit zivilrechtlichen (insb. Vernichtungs-)Ansprüchen vorgegangen werden kann. Die Beurteilung der Privatkopie als rechtswidrig schließt dabei de lege ferenda die Statuierung von Pauschalvergütungen für die Rechteinhaber (vor allem aufgrund eines Erst-Recht-Schlusses) nicht zwingend aus; bei einer eventuellen Konzeption entsprechender Vergütungssysteme sollte jedoch ein Nebeneinander von Individualvergütungssystemen und Pauschalvergütungen angestrebt werden.

3. Ergebnis

Die empirische Analyse in Teil 2 hat gezeigt, dass bei allen digitalen Gütern die den Urheber und Verwertungsberechtigten primär schädigende Handlung in der *Erstellung der Kopie* durch den

285. Siehe oben Fn. 238.

286. Vgl. dazu m.w. Nachw. *Sieber*, in: Hoeren/Sieber, Handbuch Multimedia-Rechts, Teil 19 Rn. 213; *Tiedemann*, Datenübermittlung als Straftatbestand, NJW 1981, 945.

Endnutzer liegt, der für diese Kopie keine Vergütung entrichtet. Die rechtliche Untersuchung erbringt hierzu das Ergebnis, dass diese eigentlich schädigende Handlung in einem Großteil der Fälle strafrechtlich nicht erfasst wird.

- Für den Bereich des Kernstrafrechts beruht diese weitgehend fehlende Strafbarkeit der eigentlich schädigenden Kopierhandlung darauf, dass die Eigentumsdelikte (§§ 242, 246 StGB) sowie der Tatbestand der Hehlerei (§ 259) am Tatobjekt der körperlichen Sache orientiert sind und die Kopie unkörperlicher digitaler Werte deswegen nur in einigen wenigen Einzelfällen über Hilfskonstruktionen erfassen können; die „Verschaffensalternative“ des Tatbestandes der Geldwäsche (§ 261 Abs. 2 StGB) erstreckt sich zwar weitergehend auf „Gegenstände“, jedoch stellen Urheberrechtsverletzungen keine geeignete Vortaten für die Geldwäsche dar.

- Die Anwendbarkeit des Urheberstrafrechts (§§ 106 ff. UrhG) ist dagegen aufgrund des Rechts auf Privatkopien (§ 53 UrhG) problematisch, da umstritten ist, ob dieses Recht auch dann gegeben ist, wenn die Kopie – wie in der großen Masse der hier einschlägigen Fälle – von einer rechtswidrig hergestellten Vorlage gemacht wird. Die besseren und deswegen auch für die zivilrechtliche Auslegung von § 53 UrhG durchschlagenden Gründe sprechen zwar dafür, das Recht auf Privatkopie nur bei Benutzung einer rechtmäßigen Vorlage anzuerkennen. Da dieses Erfordernis jedoch im Gesetzeswortlaut von § 53 Abs. 1 UrhG keinen Niederschlag gefunden hat, lässt sich eine entsprechende Forderung im Anwendungsbereich der zivilrechtsakzessorischen Strafbestimmungen der §§ 106 ff. UrhG nicht mit dem Bestimmtheitsgebot von Art.103 Abs. 2 GG vereinbaren.

Die damit festzustellende weitgehende Straflosigkeit der primär schädigenden Kopierhandlungen hat unter anderem auch zur Folge, dass das *Angebot von entsprechenden Kopiervorlagen* z.B. im Internet nicht unter den Gesichtspunkten der Anstiftung zu einer Straftat oder des öffentlichen Aufforderns zu einer Straftat erfasst werden kann, da es insoweit an der von § 26 StGB und von § 111 StGB geforderten rechtswidrigen Haupttat fehlt. Die zweite, für die Verbreitung von Raubkopien zentrale Tathandlung des (eine massenhafte Herstellung von Kopien erst ermöglichenden) Angebots von Kopiervorlagen kann daher nur durch im folgenden näher zu prüfende eigenständige Verbote des Urheberrechts erfasst werden.

C. Zurverfügungstellung der Vorlagen

Die empirische Analyse dieses Gutachtens hat gezeigt, dass die Kopie digitaler Güter durch den „Endverbraucher“ durch zwei unterschiedliche Arten der Zurverfügungstellung von Vorlagen ermöglicht wird: Zum einen werden *körperliche Datenträger* (bei denen es sich um Originaldatenträger des Nutzungsberechtigten oder aber um rechtmäßig oder rechtswidrig hergestellte Kopien handeln kann) zur Verfügung gestellt, die entweder ungeschützt oder aber mit einem Kopierschutz versehen sind (unten 1). Zum anderen werden die Dateien *in unkörperlicher Form* über öffentlich zugängliche Online-Tauschbörsen oder auf speziellen Internet-Servern zum Zwecke des Kopierens angeboten (unten2).

1. Weitergabe körperlicher Datenträger

Die Weitergabe von körperlichen Datenträgern bietet – wie oben gezeigt – nur in einem kleineren Teil der Fälle die Grundlage für die Kopie digitaler Güter. Entsprechende Sachverhaltskonstellationen liegen insb. in den Fällen vor, in denen Schüler Datenträger mit Audiodaten, Filmen oder Software ihren Schulkameraden zum Zwecke der Kopie weitergeben.

Diese Weitergabe von Originalen und rechtmäßig hergestellten Vervielfältigungsstücken von Audiodaten und Filmen ist dabei aufgrund der gesetzlichen Regelung des § 17 UrhG in weitreichendem Umfang rechtmäßig. Das in § 17 UrhG geregelte Verbreitungsrecht betrifft das Recht des Urhebers, das Original oder Vervielfältigungsstücke des Werkes der Öffentlichkeit anzubieten oder in Verkehr zu bringen.[287] Das Anbieten bzw. das Inverkehrbringen kann sich dabei nicht nur auf eine Veräußerung des Werkstückes beziehen, sondern auch auf Vermietung, Verleih oder sonstige entgeltliche oder unentgeltliche Überlassung, d.h. auch die schlichte Besitzüberlassung.[288] Nach der – auch für § 17 UrhG entsprechend heranziehbaren – Legaldefinition des § 15 Abs. 3 UrhG finden entsprechende Handlungen gegenüber der Öffentlichkeit statt, wenn sie gegenüber einer nicht bestimmt abgegrenzten oder durch keine persönlichen Beziehungen miteinander verbundenen Mehrheit von Personen erfolgen.[289] Ein Angebot an die Öffentlichkeit kann damit auch schon bei einem Angebot an eine – mit dem Anbieter nicht persönlich verbundene – Einzelperson vorliegen.[290]

Das Verbreitungsrecht wird dabei jedoch durch den in § 17 Abs. 2 UrhG normierten Erschöpfungsgrundsatz eingeschränkt.[291] Danach ist die Weiterverbreitung mit Ausnahme der Vermietung gem. § 17 UrhG zulässig, wenn das Original oder Vervielfältigungsstücke des Werkes mit Zustimmung des zur Verbreitung Berechtigten – d.h. des Urhebers oder entsprechend autorisierter Nutzungsberechtigter – im Wege der Veräußerung in Verkehr gebracht worden ist. Der Begriff der Veräußerung erfasst dabei jede Form der Übereignung; auf das zugrundeliegende Kausalgeschäft kommt es dagegen nicht an.[292]

Aufgrund des Erschöpfungsgrundsatzes ohne weiteres zulässig ist damit zunächst die Verbreitung und damit die Weitergabe von Originalen – auch soweit dies gegenüber der Öffentlichkeit geschieht.[293] So dürfen etwa Originale auch an jedermann verkauft oder über eine Internetauktion versteigert werden; für Software gilt dies allerdings aufgrund der einschränkenden Sonderregelungen der §§ 69c Abs. 1 S. 1 Nr. 1 i.V.m. 69a Abs. 4 nur, wenn der Verkäufer bzw. Versteigerer keine Kopie der auf dem Datenträger befindlichen Daten für sich behält und damit das Vervielfältigungsrecht des Urhebers nicht verletzt. Aufgrund der Einschränkung des Erschöpfungsgrundsatzes generell nicht zulässig ist lediglich die Vermietung; da diese jedoch unmittelbar oder mittelbar Erwerbszwecken dienen muss, liegt bei der bloßen Weitergabe von Werkstücken keine Vermietung vor.

Nicht verbreitet werden dürfen allerdings nach § 53 Abs. 1 bis 3 UrhG hergestellte Vervielfältigungsstücke. Dabei handelt es sich zwar um rechtmäßig hergestellte Vervielfältigungsstücke;[294]

287. Vgl. Schricker/*Loewenheim*, § 17 Rn. 1 ff.
288. Vgl. BGH GRUR 1987, 37, 38.
289. Vgl. BGH GRUR 1991, 316, 317.
290. Vgl. BGH GRUR 1991, 316, 317.
291. Vgl. dazu den Überblick bei Schricker/*Loewenheim*, § 17 Rn. 35 ff.
292. Vgl. Schricker/*Loewenheim*, § 17 Rn. 39.
293. Vgl. Schricker/*Loewenheim*, § 17 Rn. 56.
294. Vgl. dazu oben III. B. 2. c).

diese dürfen jedoch aufgrund der einschränkenden Regelung des § 53 Abs. 6 UrhG nicht verbreitet werden. Entsprechende (insb. Privat-)Kopien dürfen damit z.B. nicht verkauft oder im Rahmen von Internetauktionen angeboten werden. Da – wie vorstehend ausgeführt – ein Verbreiten voraussetzt, dass sich die entsprechende Handlung an die Öffentlichkeit richtet, können entsprechend rechtmäßig hergestellt Vervielfältigungsstücke jedoch an ein Familienmitglied, einen Freund oder einen Bekannten weitergegeben werden.

Etwas anderes gilt allerdings in den oben dargestellten weit verbreiteten Fällen, in denen nicht das Original oder rechtmäßig hergestellte Vervielfältigungsstücke weitergegeben werden, sondern Datenträger mit rechtswidrig hergestellten Kopien gegenüber Personen angeboten werden, die mit dem Verbreiter persönlich nicht verbunden sind. In diesen Fällen liegt neben dem Verstoß gegen das Vervielfältigungsrecht dann auch ein Verstoß gegen das Verbreitungsrecht vor; der Erschöpfungsgrundsatz des § 17 Abs. 2 UrhG rechtfertigt das Angebot des Datenträgers in diesen Fällen ebenfalls nicht, da nicht das mit Zustimmung des zur Verbreitung Berechtigten in Verkehr gekommene Original oder Vervielfältigungsstück, sondern eine rechtswidrige Kopie weiterverbreitet wird.

Zusammenfassend ist damit festzustellen, dass bei dem oben dargestellten „Vertrieb“ über körperliche Datenträger die Zurverfügungstellung der Vorlage in einer Reihe von Fällen nicht rechtswidrig ist. Dies betrifft allerdings überwiegend Fallkonstellationen, die zur Verbreitung von Kopien und zur Schädigung der Rechteinhaber nicht in wesentlichem Umfang beitragen. Bei der Verbreitung von körperlichen Datenträgern durch – insbesondere gewerbsmäßig handelnde – Täter, die eine Vielzahl von kopierten Datenträgern an eine Vielzahl von mit ihnen persönlich nicht verbundene Personen weitergeben, verletzt die Weitergabe der Vorlage jedoch das Verbreitungsrecht und häufig auch das Vervielfältigungsrecht des UrhG.

2. Veröffentlichung von Vorlagen im Internet

Die empirische Analyse hat gezeigt, dass eine der wichtigsten „Vertriebsschienen“ für Raubkopien nicht die körperliche Weitergabe von Datenträgern, sondern das immaterielle Angebot der digitalen Güter in Online-Tauschbörsen und auf speziellen Servern des Internet ist. Diese Angebote sind grundsätzlich rechtswidrig. Dabei ist allerdings umstritten, welches Recht des Urhebers verletzt wird. In Betracht kommt zunächst wiederum ein Verstoß gegen das Verbreitungsrecht des § 17 UrhG. Allerdings geht die h.M. davon, dass nur die Verbreitung körperlicher Werkstücke unter § 17 UrhG fällt.[295] Dies ist allerdings nicht unproblematisch, da insbesondere der Verkauf von Werkstücken heutzutage nicht selten rein elektronisch, z.B. über das Internet, erfolgt. Letztlich ist es daher oft nur eine technische Zufälligkeit, ob der Kunde einen Datenträger oder nur die Daten selbst erhält. Es sprechen daher gute Gründe dafür, in diesem Fall auch den Erschöpfungsgrundsatz des § 17 Abs. 2 UrhG eingreifen zu lassen.[296] D.h.: Wird ein Werkstück auf elektronischem Wege käuflich erworben, so darf es durch den Käufer – von der Vermietung abgesehen – auch elektronisch weiterverbreitet werden.[297] Dies führt allerdings nicht dazu, dass der ursprüngliche Käufer eine Kopie der Daten behalten darf. Es muss den Besitz

295. Vgl. BGHZ 11, 135, 144; 33, 38, 41; 38, 356, 362; BGH GRUR 1995, 673, 676. Siehe auch *Flechsig*, ZUM 2002, 1, 7f.
296. Vgl. *Kröger*, CR 2001, 316, 318. Siehe auch *Spindler*, Europäisches Urheberrecht in der Informationsgesellschaft, GRUR 2002, 105, 110.
297. Vgl. *Berger*, Urheberrechtliche Erschöpfungslehre und digitale Informationstechnologie, GRUR 2002, 198, 199. Ablehnend hierzu aber Schricker/*Loewenheim*, § 17 Rn. 37.

an den Daten vielmehr vollständig aufgeben.[298] Im Bereich vor allem der Online-Tauschbörsen stellt sich die Situation aber so dar, dass die Anbieter insbesondere von Musikstücken nicht den eigenen Besitz an diesen Stücken aufgibt, sondern zumindest eine Kopie behält. Damit wäre aber auch bei einer analogen Anwendung des § 17 UrhG ein Verstoß gegen das Verbreitungsrecht zu bejahen. Gleichwohl ist darauf hinzuweisen, dass die entsprechende Anwendung des Erschöpfungsgrundsatzes auf andere Verwertungsrechte als das Verbreitungsrecht höchst strittig ist. Der BGH hat zwar in mehreren Entscheidungen ausgeführt, dass alle Verwertungsrechte durch den Erschöpfungsgrundsatz beschränkt seien; dies stieß innerhalb der Literatur allerdings nahezu einhellig auf Ablehnung.[299] Auch die Online-Übertragung soll nach der Literatur folglich nicht dem Erschöpfungsgrundsatz unterliegen.[300]

Unabhängig von der Frage, welcher Auffassung man sich hinsichtlich des Erschöpfungsgrundsatzes anschließt und welche Folgerungen man daraus zieht, liegt nach h.M. jedenfalls (auch) ein Verstoß gegen das Recht auf die öffentliche Wiedergabe nach § 15 Abs. 2 UrhG vor.[301] Auch wenn die unkörperliche Weiterverbreitung im Internet dabei nicht ausdrücklich im Gesetz erwähnt wird, kann eine analoge bzw. direkte Anwendung des Senderechts oder ein unbenanntes Verwertungsrecht i.S.d. § 15 Abs. 2 UrhG angenommen werden, da die Aufzählung in § 15 Abs. 2 UrhG nicht abschließend ist.[302] Probleme ergeben sich allerdings daraus, dass es sich hierbei um eine *öffentliche* Wiedergabe handeln muss. Dabei ist umstritten, ob eine öffentliche Wiedergabe nur vorliegt, wenn eine Mehrzahl von Personen gleichzeitig erreicht wird oder ob eine wiederholte gleichförmige Wiedergabe (sukzessive Wiedergabe) ausreicht.[303] Dies ist für den Bereich der Online-Tauschbörsen von zentraler Bedeutung, weil dort die Dateien von den Nutzern nicht gleichzeitig, sondern nacheinander abgerufen werden. Gleichwohl anerkennen auch diejenigen, die eine sukzessive Öffentlichkeit nicht ausreichen lassen, dass eine Regelungslücke besteht und daher § 15 Abs. 2 UrhG zumindest analog angewendet werden muss.[304] Eine vertiefte Auseinandersetzung mit der Problematik erübrigt sich aber, da der Gesetzgeber mit dem neuen Gesetz zur Regelungen des Urheberrechts in der Informationsgesellschaft in §§ 15 Abs. Nr. 2, 19a UrhG ausdrücklich ein ausschließliches Recht der öffentlichen Zugänglichmachung – das insbesondere das Anbieten im Internet erfasst – normieren und zudem § 15 Abs. 3 UrhG so verstanden wissen will, dass eine sukzessive Öffentlichkeit ausreichend ist.[305] Die grundsätzliche Rechtswidrigkeit des Anbietens urheberrechtlich geschützter Werke im Internet ist damit nicht nur bereits heute zu bejahen, sondern wird durch die zukünftige Gesetzgebung noch einmal untermauert werden.

Hieran ändert sich – zumindest in der Zukunft – auch nichts durch die Schranke des § 52 Abs. 1 S. 1 UrhG-E, wonach die öffentliche Wiedergabe eines veröffentlichten Werkes zulässig ist, wenn die Wiedergabe keinem Erwerbszweck des Veranstalters dient, die Teilnehmer ohne Entgelt zugelassen werden und im Falle des Vortrages oder der Aufführung des Werkes keiner der

298. Vgl. *Berger*, GRUR 2002, 198, 201.
299. Vgl. die Ausführungen bei Schricker/*v. Ungern-Sternberg*, § 15 Rn. 31 ff.
300. Vgl. Schricker/*v. Ungern-Sternberg*, § 15 Rn. 34.
301. Vgl. *Hänel*, oben Fn. 258, Abs. 13, Abs. 46.
302. Vgl. Schricker/*v. Ungern-Sternberg*, § 15 Rn. 22 ff
303. Sieh dazu *Dreier*, Die Umsetzung der Urheberrechtsrichtlinie 2001/29/EG in deutsches Recht, ZUM 2002, 28, 31; *Hänel*, oben Fn. 258, Abs. 47; Schricker/*v. Ungern-Sternberg*, § 15 Rn. 59 f
304. Siehe *Hänel*, oben Fn. 258, Abs. 48; Schricker/*v. Ungern-Sternberg*, § 15 Rn. 24, 27.
305. Vgl. die Gesetzesbegründung auf S. 39 f. zum Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, oben Fn. 196; siehe auch *Kröger*, CR 2001, 316, 318; *Spindler*, GRUR 2002, 105, 108.

ausübenden Künstler eine besondere Vergütung erhält. Zwar lässt sich aufgrund des oben Gesagten de lege lata das Anbieten von urheberrechtlich geschützten Werken – insbesondere in Online-Tauschbörsen – als eine öffentliche Wiedergabe ansehen.[306] Diese erfolgt auch unentgeltlich, da die Dateien in der Regel kostenlos angeboten werden. Jedoch wird § 52 Abs. 3 UrhG durch das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft neu gefasst, indem klargestellt wird, dass öffentliche Zugänglichmachungen von Werken nur mit Einwilligung des Berechtigten zulässig sind.[307] Gerade bei den heute aktiven Online-Tauschbörsen fehlt es aber regelmäßig an entsprechenden Einwilligungen der Rechteinhaber.

Etwas anderes gilt daher nur in den Fällen, in denen im nicht öffentlichen Bereich auf elektronischem Wege urheberrechtlich geschützte Werke zugänglich gemacht werden. Dies ist z.B. dann der Fall, wenn jemand einem Freund per E-Mail ein Musikstück zuschickt oder wenn eine WWW-Seite, auf der urheberrechtlich geschützte Werke zum Abruf bereit stehen, mit einem Passwortschutz eingerichtet wird und dieses nur Familienmitgliedern bekannt ist. Ein solches Verhalten ist im Einzelfall nach § 53 Abs. 1 S. 1 UrhG zulässig, da mangels Öffentlichkeit ein Verbreiten oder eine öffentliche Wiedergabe im Sinne des § 53 Abs. 6 UrhG nicht vorliegt. Im Hinblick auf ihre praktische Bedeutung und die Schädigung der Rechteinhaber sind diese Fälle jedoch vernachlässigbar.

Unabhängig von einem möglichen Verstoß gegen § 17 UrhG oder § 15 Abs. 2 UrhG, berührt das Anbieten einer Kopie urheberrechtlich geschützter Werke insbesondere über File-Sharing-Systeme auch das Vervielfältigungsrecht nach § 16 UrhG. Dieser Vervielfältigungsvorgang könnte allerdings nach § 53 Abs. 1 UrhG zulässig sein. Wie oben bereits dargestellt,[308] scheitert die Anwendung von § 53 Abs. 1 S. 1 UrhG zugunsten des Anbieters daran, dass bei einer weltweiten Abrufbarkeit in einem File-Sharing-System bereits kein privater Gebrauch mehr angenommen werden kann. Zwar bestimmt § 53 Abs. 1 S. 2 UrhG, dass der zur Vervielfältigung Befugte die Vervielfältigungsstücke – welche sich nicht in seinem Eigentum befinden müssen[309] – auch durch einen Dritten herstellen lassen kann, wobei dies nach der aktuellen Gesetzeslage im Falle von Bild- und Tonträgern sowie von Werken der bildenden Künste unentgeltlich geschehen muss.[310] Im übrigen beseitigt der Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft die Beschränkung auf Bild- und Tonträger sowie Werke der bildenden Künste und fordert entweder eine generelle Unentgeltlichkeit oder, dass es sich um Vervielfältigungen auf Papier oder einen ähnlichen Träger mittels beliebiger photomechanischer Verfahren oder andere Verfahren mit ähnlicher Wirkung handelt.[311] Eine solche Unentgeltlichkeit ist bei einer Vervielfältigung in einem File-Sharing-System durchaus gegeben, da der Anbieter (= der Dritte) dort einzelne Werke für einen Nutzer (= den Befugten) kostenlos zum Abruf bereitstellt.[312] Allerdings verlangt die Rechtsprechung, dass sich die Tätigkeit des Dritten im Rahmen einer konkreten Anweisung zur Herstellung eines bestimm-

306. Vgl. *Kreutzer*, GRUR 2001, 193, 202 ff., der sich auch mit dem Verhältnis von § 53 Abs. 6 UrhG zu § 52 UrhG auseinandersetzt.
307. Siehe oben Fn. 196.
308. Siehe oben III. B. 2. c).
309. Vgl. BGH NJW 1997, 1363, 1366.
310. Unentgeltlich bedeutet insoweit, dass für die Herstellung der Vervielfältigungsstücke keine Gegenleistung erbracht werden darf. Ob die Erstattung der reinen Materialkosten – z.B. für einen zur Verfügung gestellten CD-Rohling – zulässig ist, ist fraglich. Es wird jedoch überwiegend als zulässig angesehen und insoweit nicht als Entgelt eingestuft; vgl. *Schwenzer*, Werden Träume wahr in der CD-Kopier-Bar?, ZUM 1997, 478, 480; Schricker/*Loewenheim*, § 53 Rn. 16.
311. Vgl. Fn. 196.
312. Deswegen sprechen sich für eine Streichung der Vorschrift des § 53 Abs. 1 S, 2 UrhG aus – vor

ten Vervielfältigungsstücks für den vom Gesetz begünstigten Nutzer hält.[313] Dies ist bei File-Sharing-Systemen schon fraglich, da der Anbieter von sich aus aktiv wird und festlegt, welche Werke abrufbar sind und welche nicht. Hinzu kommt, dass die Vorschrift des § 53 Abs. 1 S. 2 UrhG eng auszulegen ist[314] und von ihrem Normzweck nur denjenigen privilegieren möchte, der sich kein Vervielfältigungsgerät – z.B. einen CD-Brenner – leisten kann.[315] Der Dritte muss damit an die Stelle des Vervielfältigungsgeräts des berechtigten Nutzers treten.[316] Bei den File-Sharing-Systemen ist der Anbieter aber nicht nur die Kopierstelle des Begünstigten. Vielmehr bestimmt der Anbieter z.B., welche Inhalte überhaupt zum Abruf bereitstehen oder wann bzw. in welcher Form diese zur Verfügung stehen. Das Anbieten eines Servicepakets überschreitet aber nach der Rechtsprechung den „gesetzlich zugelassenen Rahmen, der einer Hilfsperson bei der Vervielfältigung von Werkstücken für einen privilegierten Nutzer zugute kommen kann."[317] Schließlich ist zu berücksichtigen, dass Ausnahmetatbestände nicht zu einer Aushöhlung der Urheberrechte führen dürfen.[318] Genau dies würde aber geschehen, wenn das massenhafte Tauschen über File-Sharing-Systeme nach § 53 Abs. 1 S. 2 UrhG zulässig wäre. Daher kann diese Vorschrift nicht zugunsten des Anbieters eingreifen.

3. Ergebnis

Anders als die – zur eigentlichen Schädigung der Rechteinhaber führende – Kopie digitaler Güter können die diese Handlung vorbereitenden Angebote von Kopiervorlagen – vor allem wenn sie öffentlich im Internet erfolgen – in fast allen für die Erstellung von Raubkopien relevanten Fallgestaltungen durch das Urheberrecht bereits heute erfasst werden. Der Verstoß gegen das zivilrechtliche Verbreitungs- und teilweise auch das Vervielfältigungsverbot des Urheberrechtsgesetzes führt dabei dazu, dass die einschlägigen Handlungen auch gegen die oben genannten akzessorischen Strafbestimmungen der §§ 106, 108 UrhG verstoßen und dadurch mit Freiheitsstrafe von bis zu drei – bzw. bei gewerbsmäßigem Handeln bis zu fünf – Jahren bedroht sind.

D. Umgehung der Schutzmechanismen

Die bisherige Untersuchung der Strafbarkeit des Kopierens von digitalen Gütern und des Angebots von entsprechenden Kopiervorlagen betraf die beiden für die Erstellung von Raubkopien zentralen Tathandlungen bei unverschlüsselten und ungeschützten digitalen Gütern. Soweit

allem bezüglich digitaler Kopien – der BITKOM, oben Fn. 266, der BDZV, oben Fn. 266, S. 1 f., der Börsenverein des deutschen Buchhandels, oben Fn. 266, S. 2, die KirchMedia, oben Fn. 266, S. 7, der Verband Deutscher Zeitschriftenverleger (VDZ), Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, S. 4, abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/Stellungnahme_VDZ_180302.pdf, und der Verband privater Rundfunk und Telekommunikation e.V. (VPRT), Stellungnahme zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, S. 2, abrufbar unter http://www.urheberrecht.org/topic/Info-RiLi/st/VPRTStellungRefE-2002-04-18.pdf (Stand: 12.8.2002).

313. Vgl. BGH NJW 1997, 1363, 1366.
314. Vgl. BGH NJW 1997, 1363, 1367.
315. Vgl. BGH NJW 1997, 1363, 1367.
316. Vgl. BGH NJW 1997, 1363, 1366.
317. Vgl. BGH NJW 1997, 1363, 1367.
318. Vgl. BGH NJW 1997, 1363, 1368.

digitale Güter durch Schutzmechanismen, insbesondere Digital Rights Management (DRM) Systeme, geschützt werden, kommen aufgrund der oben dargestellten empirischen Analyse zusätzliche strafbare Tathandlungen in Betracht, die Voraussetzung für die Kopie digitaler Güter und damit auch für eine Schädigung der Rechteinhaber sind: Für die durch bestimmte Verfahren geschützten digitalen Güter ist deswegen im folgenden zusätzlich zu untersuchen, inwieweit

- die Umgehung von Schutzmechanismen (insbesondere die Überwindung von Kopierschutzmechanismen und DRM-Systemen) sowie
- das öffentliche Angebot und der Besitz von Entschlüsselungsinformationen sowie sonstiger Tools zur Begehung einschlägiger Rechtsverletzungen strafrechtlich relevant sind.

Die damit zunächst interessierende Strafbarkeit der *Überwindung von Schutzmechanismen* kann sich dabei zunächst unter dem Gesichtspunkt der Verschaffung geheimer oder geschützter Daten ergeben; einschlägig sind insoweit vor allem die Vorschriften gegen den Verrat von Wirtschaftsgeheimnissen (§ 17 UWG) und gegen das Ausspähen von Daten (§ 202a StGB). Die Strafbarkeit der Überwindung von Schutzmechanismen kann jedoch auch aus der dabei erfolgenden Verletzung von Vermögensrechten sowie von Integritäts- und Beweisinteressen resultieren; insoweit kommen vor allem die Strafvorschriften gegen Computerbetrug (§ 263a StGB), gegen Leistungserschleichung (§ 265a StGB), gegen Datenveränderung (§§ 303a und 303b StGB) sowie gegen die Fälschung beweiserheblicher Daten (§ 269 StGB) in Betracht. Soweit diese allgemeinen Strafvorschriften nicht eingreifen, hängt die Strafbarkeit der Überwindens von Schutzmechanismen von den neu geschaffenen nebenstrafrechtlichen Spezialtatbeständen des Zugangskontrolldiensteschutz-Gesetzes (ZKDSG)[319] sowie de lege ferenda von den entsprechenden Vorschlägen des Regierungsentwurfs für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft[320] und der Umsetzung der Empfehlungen der Convention on Cybercrime des Europarats ab.[321]

1. § 17 UWG

a) Übersicht

Die Vorschrift des § 17 UWG über den „Verrat von Geschäfts- und Betriebgeheimnissen“ enthält in ihren beiden ersten Absätzen zwei unterschiedliche Tatbestände. Von diesen kommt im vorliegenden Zusammenhang lediglich eine Strafbarkeit nach § 17 Abs. 2 UWG in Betracht, da Abs. 1 der Vorschrift nur den Geheimnisverrat im Rahmen von Arbeitsverhältnissen oder ähnlichen Sonderrechtsverhältnissen erfasst. Nach § 17 Abs. 2 UWG wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, „wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, 1. sich ein Geschäfts- oder Betriebsgeheimnis durch a) Anwendung technischer Mittel, b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert oder 2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.“

319. Vgl. Fn. 237.
320. Siehe oben Fn. 196.
321. Siehe oben Fn. 239.

b) Kritische Tatbestandsmerkmale im Hinblick auf die Umgehung von Schutzmechanismen

Im Hinblick auf die oben dargestellte Umgehung von Schutzmechanismen ist § 17 Abs. 2 UWG in mehrfacher Hinsicht problematisch:

- Der Tatbestand erfordert zunächst, dass die verwendeten geheimen elektronischen Schutzmechanismen ein *Geschäfts- oder Betriebsgeheimnis* darstellen. Nach h.M. ist ein Geschäfts- oder Betriebsgeheimnis jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem Willen des Betriebsinhabers aufgrund eines berechtigten wirtschaftlichen Interesses geheimgehalten werden soll.[322] Der Zusammenhang mit dem Betrieb kann dabei aber auch dann noch vorliegen, wenn das Geheimnis innerhalb eines Produktes veräußert wird.[323] Allerdings darf das Geheimnis in diesem Fall nicht offenkundig sein.[324] Das Reichsgericht verneinte die Offenkundigkeit in einer entsprechenden Sachverhaltsgestaltung in einem Fall, in welchem die Bauart einer höherwertigen Maschine nur durch eine mit größeren Opfern und Schwierigkeiten verbundene Zerlegung festgestellt werden konnte.[325] Das Bayerische Oberste Landesgericht ließ es ausreichen, dass Daten durch ein verschlossenes Behältnis geschützt wurden.[326] Literatur und Rechtsprechung nehmen eine Offenkundigkeit daher nur dann an, wenn eine Tatsache allgemein bekannt ist oder für einen Interessierten die Möglichkeit besteht, sich mit lauteren Mittel ohne größere Schwierigkeiten von ihr Kenntnis zu verschaffen.[327] Die zum Schutz digitaler Güter verwendeten Mechanismen stellen daher dann Geschäfts- und Betriebsgeheimnisse dar, wenn es schwierig ist, herauszufinden, wie diese funktionieren, weil beispielsweise verschlüsselte Daten zum Einsatz kommen.[328]

- Die Qualifizierung von bestimmten Informationen als Geschäfts- und Betriebsgeheimnisse kann allerdings dadurch *aufgehoben* werden, dass die geheimen Informationen für die Allgemeinheit offenkundig werden.[329] Zur Beurteilung der *Offenkundigkeit* fragte das Bayerische Oberste Landesgericht München bei einem Glücksspielautomaten-Programm

322. Vgl. LG Stuttgart NJW 1991, 441, 442; Baumbach/*Hefermehl*, Kommentar zum Wettbewerbsrecht, 22. Aufl. 2001, § 17 UWG, Rn. 2; Erbs/Kohlhaas/*Diemer*, Strafrechtliche Nebengesetze, Band 4, 136. Ergänzungslieferung, Stand: März 2000, § 17 UWG Rn. 5; *Etter*, Noch einmal: Systematisches Entleeren von Glücksspielautomaten, CR 1988, 1021, 1024. *Harte-Bavendamm*, Wettberwerbsrechtliche Aspekte des Reverse Engineering von Computerprogrammen, GRUR 1990, 657, 660; *Raubenheimer*, Softwareschutz nach den Vorschriften des UWG, CR 1994, 264, 266; *Taeger*, Softwareschutz durch Geheimnisschutz, CR 1991, 449, 455; *Wiebe*, Reverse Engineering und Geheimnisschutz von Computerprogrammen, CR 1992, 134, 135.
323. Vgl. BayObLG NJW 1991, 438, 439 und *Harte-Bavendamm*, GRUR 1990, 657, 660.
324. Vgl. *Wiebe*, Reverse Engineering und Geheimnisschutz von Computerprogrammen, CR 1992, 134, 135.
325. Vgl. RG GRUR 1936, 573, 576; GRUR 1942, 352, 355.
326. Vgl. BayObLG NJW 1991, 438, 439; siehe insoweit auch LG Stuttgart NJW 1991, 441, 442.
327. Vgl. BayObLG NJW 1991, 438, 439; Baumbach/*Hefermehl*, § 17 UWG, Rn. 7; Erbs/Kohlhaas/*Diemer*, § 17 UWG Rn. 6; *Taeger*, CR 1991, 449, 456; siehe auch AG Augsburg CR 1989, 1004, 1006 m. Anm. *Etter*, CR 1989, 1006 f.
328. Vgl. *Beucher*/*Engels*, Harmonisierung des Rechtsschutzes verschlüsselter Pay-TV-Dienste gegen Piraterieakte, CR 1998, S. 101, 102
329. Vgl. BayObLG NJW 1991, 438, 439 und *Etter*, CR 1988, 1021, 1025; *Harte-Bavendamm*, GRUR 1990, 657, 660; *Taeger*, CR 1991, 449, 453.

danach, wie groß die Zahl derjenigen Personen war, die das Geheimnis kannten. Allerdings ließ das Gericht die Frage dann offen und verwies darauf, dass dies stets am konkreten Einzelfall zu bestimmen sei.[330] Werden daher geheime Schlüsselinformationen oder Funktionsweisen von Kopierschutzverfahren z.B. durch Hacker im Internet bekannt gemacht, so verlieren sie nach kurzer Zeit aufgrund ihrer Offenkundigkeit den Status als Geschäfts- oder Betriebsgeheimnisse.[331] Aus diesem Grund zweifelte das OLG Frankfurt bei einer SmartCard auch am Bestehen eines Geschäfts- und Betriebsgeheimnisses, wenn das verwendete Verschlüsselungsverfahren veraltet und die Softwaretools zur Entschlüsselung allgemein zugänglich sind.[332] Dies hat zur Folge, dass zwar der die Informationen erstmals bekannt gebende Hacker sich nach § 17 Abs. 2 UWG strafbar macht, die nachfolgende Verbreitung der Entschlüsselungsinformationen und sonstigen Zugangsinformationen z.B. im Internet jedoch nicht mehr unter § 17 Abs. 2 UWG fällt.

- Die von § 17 Abs. 2 UWG erfassten *Tathandlungen des Verschaffens, Sicherns, Verwertens und Mitteilens* erfassen nicht nur das Hacking geheimer Schutzmechanismen, sondern – mit der Tathandlung des Mitteilens und des Verwertens – auch die Bekanntgabe des Geheimnisses durch den Hacker. Die in § 17 Abs. 2 Nr. 2 UWG enthaltene Alternative der Geheimniserlangung durch eine *fremde Handlung* in Verbindung mit der Tathandlung der unbefugten Geheimnisverwertung macht den Tatbestand darüber hinaus auch auf die Nutzung der entschlüsselten Geheimnisse durch Personen anwendbar, welche die Geheimnisse nicht selbst entschlüsseln, sondern das Geheimnis nutzende Tools – z.B. nach deren Veröffentlichung im Internet – einsetzen.[333] Die Nutzung eines derartigen „Forward Programming“[334] ist nach § 17 UWG allerdings nur dann strafbar, wenn die Geheimniseigenschaft in diesen Fällen durch die Veröffentlichung noch nicht verloren gegangen ist.

- Die Tathandlungen des § 17 Abs. 2 UWG führen allerdings in einigen Fällen deswegen zu Problemen, weil das Verschaffen, Sichern, Verwerten und Mitteilen sich *auf das Geschäfts- oder Betriebsgeheimnis beziehen* müssen. Der Tatbestand greift deswegen nicht ein, wenn der Täter das Geheimnis „umgeht“, d.h. wenn er die geschützten digitalen Gütern „am Geheimnis vorbei“ (d.h. unter Umgehung der das Geheimnis schützenden Sicherungsmechanismen) kopiert. Dies ist insbesondere der Fall, wenn von einem kopiergeschützten Datenträger eine exakte 1:1 Kopie erstellt und damit das Geheimnis einfach mitkopiert wird.

- Erhebliche Anwendungsschwierigkeiten von § 17 UWG resultieren schließlich auch aus den geforderten Motiven und Gründen des Handelns. Der Tatbestand verlangt insoweit ein Handeln „zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen“.

  Ein *Handeln zu Zwecken des Wettbewerbs* liegt dabei unproblematisch in denjenigen Fälle vor, in denen die Hacker das Ziel haben, die digitalen Güter in Konkurrenz zu den

330. Vgl. BayObLG NJW 1991, 438, 439; so auch Erbs/Kohlhaas/*Diemer*, § 17 UWG Rn. 6.
331. Vgl. OLG Frankfurt NJW 1996, 264 (Veröffentlichung in Mailboxen). Parallel hierzu wird in der Literatur auch die Ansicht vertreten, dass durch eine Veröffentlichung eines Geheimnisses in einer Fachzeitschrift Offenkundigkeit eintritt, vgl. Erbs/Kohlhaas/*Diemer*, § 17 UWG Rn. 6; *Harte-Bavendamm*, GRUR 1990, 657, 661.
332. Vgl. OLG Frankfurt NJW 1996, 264.
333. Siehe dazu LG Stuttgart NJW 1997, 441, 442.
334. Vgl. *Wiebe*, CR 1992, 134, 136.

Rechteinhabern zu vertreiben.[335] Soweit Angriffe auf Programme und deren Schutzmechanismen dagegen aus „sportlichem Ehrgeiz“, aus wissenschaftlichem Interesse oder zur Feststellung von Schwachstellen erfolgen, ist dieses Merkmal nicht gegeben.

In diesen Fällen scheidet auch ein *Handeln in Schädigungsabsicht* aus, da hierfür direkter Vorsatz in der Form des Wollens erforderlich ist.[336] Eine derartige Absicht in der Form des dolus directus ersten Grades dürfte jedoch in vielen Fällen des Hackings von Schutzmaßnahmen nicht nachweisbar sein.

Das gleiche Ergebnis gilt beim Hacken „aus sportlichem Ehrgeiz“ oder persönlicher Neugier[337] auch im Hinblick auf ein *Handeln aus Eigennutz*. Dieses Merkmal liegt zwar in den Fällen vor, in denen die gehackten Betriebsgeheimnisse gegen Entgelt vertrieben werden oder die Täter sonst zur Gewinnerzielung tätig werden.[338] Da Eigennutz kein Erstreben materieller Vorteile verlangt, sondern auch bei der Erlangung ideeller Vorteile gegeben sein kann,[339] ist dieses Merkmal möglicherweise auch dann anwendbar, wenn ein Hacker sich durch die Veröffentlichung der entschlüsselten Geheimnisse „einen Namen“ in der Hackerszene machen will oder die Geheimnisse für eigene private Zwecke nutzen möchte.[340] In dem – wie die empirische Analyse gezeigt hat häufigsten – Fall der anonymen Veröffentlichung der gehackten Geheimnisse lässt sich ein Handeln aus Eigennutz dagegen nicht mehr begründen. Die mögliche „Freude“ des Hackers über den Erfolg der Entschlüsselung reicht insoweit nicht aus.[341]

In den – in der Praxis häufigen – Fällen des Hackens aus „sportlichem“ Ehrgeiz ist damit entscheidend, ob ein *Handeln zugunsten eines Dritten* angenommen werden kann. Dies hängt zunächst von der Rechtsfrage ab, ob hierfür Absicht im Sinne des dolus directus zu fordern ist oder aber auch ein Eventualvorsatz ausreicht. Der Kontext der anderen genannten Motive könnte insoweit zwar für die Forderung eines dolus directus sprechen; der Wortlaut des Gesetzes verlangt eine solche Absicht jedoch gerade nicht; der Gesetzgeber hat z.B. *keine „Absicht* der Begünstigung eines Dritten“ gefordert. Gleichwohl verlangt die Literatur, dass der Täter mit dem Ziel handelt, einen Dritten zu begünstigen.[342] Dies dürfte in der Praxis allerdings nur schwer zu beweisen sein. Auf der Grundlage dieser Auslegung stellt sich dann die weitere Frage nach der Zahl und der Konkretisierung der begünstigten Personen. Ein Handeln zugunsten eines Dritten liegt insoweit unzweifelhaft vor, wenn die entschlüsselten Geheimnisse einer anderen konkret bestimmten Person oder mehreren anderen konkret bestimmten Personen mit dem Ziel mitgeteilt werden, diesen Personen Vorteile (z.B. durch eine kostenlose Nutzung digitaler Güter) zu verschaffen. Fraglich ist jedoch, ob ein solches Handeln auch dann noch gegeben ist, wenn die gesamte „Internet-Community“ oder alle erreichbaren Personen begünstigt werden sollen. Dem könnte entgegen gehalten werden, dass bei einer entsprechend weiten Auslegung das Motiv des Handelns zugunsten eines Dritten letztlich mit der Mitteilung an den Dritten gleichgesetzt wird. Dies stellt allerdings kein überzeugendes Argument dar,

335. Vgl. Erbs/Kohlhaas/*Diemer*, § 17 UWG Rn. 25.
336. Vgl. Baumbach/*Hefermehl*, § 17 UWG, Rn. 22.
337. Vgl. *Harte-Bavendamm*, GRUR 1990, 657, 659, zu weiteren Handlungsmotiven im Bereich des Reverse Engineering.
338. Vgl. OLG Celle CR 1989, 1002, 1003.
339. Vgl. Erbs/Kohlhaas/*Diemer*, § 17 UWG Rn. 26; *Raubenheimer*, CR 1994, 264, 266.
340. Vgl. *Raubenheimer*, CR 1994, 264, 268.
341. Vgl. *Harte-Bavendamm*, GRUR 1990, 657, 663.
342. Vgl. Erbs/Kohlhaas/*Diemer*, § 17 UWG Rn. 27.

da die Frage des Vorliegens einer Begünstigung von der Zahl der begünstigten Personen zu trennen ist und es durchaus Fälle gibt, in denen die Mitteilung des Geheimnisses an einen bestimmten Empfänger (der z.B. nur neugierig ist, von der Geheimnismitteilung jedoch nicht profitiert) noch zu keiner Begünstigung dieses Empfängers führt. Eine Drittbegünstigung könnte daher nur mit dem Argument verneint werden, dass der (oder die) Dritte(n) zum Zeitpunkt der Tathandlung bereits in ähnlicher Weise konkretisiert sein müssen, wie der „andere" im Bereich der Anstiftung und der Beihilfe, und dass es in § 17 Abs. 2 UWG an einem – § 111 StGB entsprechenden – Tatbestand des Handelns zugunsten einer Vielzahl von Personen oder zugunsten der „Allgemeinheit" fehlt. Eine derartige Konkretisierung der dritten Person ist vom Wortlaut der Vorschrift her jedoch nicht geboten und widerspricht dem kriminalpolitischen Zweck des § 17 UWG. Da und soweit die Hacker bei der Veröffentlichung von Betriebsgeheimnisses eine Begünstigung der Empfänger zumindest billigend in Kauf nehmen, ist eine Drittbegünstigung damit auch dann – und sogar erst recht – zu bejahen, wenn alle potentiellen Empfänger eines bestimmten Internetdienstes begünstigt werden sollen. § 17 UWG scheidet dagegen aus, wenn der Hacker nur seinen persönlichen Ehrgeiz befriedigen will.

c) Analyse der Einzelfälle

Inwieweit die vorstehend in allgemeiner Form erörterten Merkmale zur Erfassung oder Nichterfassung der Umgehung von geheimen Schutzmechanismen führen, kann nur aufgrund einer Einzelanalyse der oben im empirischen Teil der Untersuchung dargestellten Fallkonstellationen und Manipulationstechniken bestimmt werden. Dabei ist insbesondere zwischen den folgenden oben näher dargestellten Fallgruppen zu unterscheiden:

- *Umgehung der Zwangsaktivierung bei Software*

  Bei der – im Bereich der Softwarepiraterie nicht unbedeutenden Fallgruppe – der Umgehung der Zwangsaktivierung von Software geht es – wie oben näher dargestellt – im Kern um die Ermöglichung beliebig vieler Installationsvorgänge einer bestimmten Software, wobei der Täter die vorgesehene Bindung einer installierten Software an ein bestimmtes Computersystem zu umgehen versucht. In diesen Fällen verschafft der Täter sich ein Betriebsgeheimnis dann, wenn zur Umgehung der Zwangsaktivierung auf Know-how innerhalb der Software zurückgegriffen werden muss, welches dem Nutzer nur im Maschinencode (Object-Code) – und nicht auch im Quellcode (Source-Code) – zur Verfügung steht.[343] In diesem Fall kann die Struktur und die Funktionsweise eines Programms überhaupt erst dann nachvollzogen werden, wenn der Object-Code z.B. wieder mittels Disassemblierung oder Dekompilierung in den Quellcode rückübersetzt wird[344] (sog. „Reverse Engineering").[345] Zu beachten ist dabei jedoch, dass es eine Vielzahl von Programmen und auch Betriebssysteme gibt, bei denen der Source-Code nicht geheim gehalten wird, sondern für jedermann frei zugänglich ist.[346] Zudem scheidet ein Verschaffen eines Betriebsgeheimnisses aus, wenn es zur Umgehung der Zwangsaktivierung ausreicht, dass

343. Vgl. Baumbach/*Hefermehl*, § 17 UWG, Rn. 9; *Harte-Bavendamm*, GRUR 1990, 657, 661; *Raubenheimer*, CR 1994, 264, 266; *Taeger*, CR 1991, 449, 453, 456; *Wiebe*, CR 1992, 134, 136.
344. Vgl. *Raubenheimer*, CR 1994, 264, 266.
345. Siehe dazu *Harte-Bavendamm*, GRUR 1990, 657, 658; *Raubenheimer*, CR 1994, 264, 266; *Taeger*, CR 1991, 449, 456; *Wiebe*, CR 1992, 134 f.
346. Vgl. *Wiebe*, CR 1992, 134, 136.

die vom Hersteller veröffentlichen Informationen bezüglich der Zwangsaktivierung ausgenutzt werden oder sonstige Schwachstellen aufgrund einer Funktionsanalyse gefunden werden und daher kein Eingriff in den Object-Code nötig wird. Das selbe gilt, wenn das Geheimnis durch die Hacker veröffentlicht wird und damit eine Vielzahl von potentiellen Nutzern zur Verfügung steht, was insbesondere dann der Fall ist, wenn Tools oder Patches erstellt werden, die im Internet abgerufen werden können.

Die Tathandlung des unbefugten Verschaffens liegt nur dann vor, wenn insbesondere technische Mittel zur Ausspähung der Funktionsweise einer Zwangsaktivierung verwendet werden, wie z.B. spezielle Editoren oder sonstige Softwareprogramme, die eine Auswertung des Object-Code ermöglichen.[347] Sofern bloße Beobachtungen oder „Erfahrungen" gesammelt werden, die einen Eingriff in ein bestimmtes Programm erlauben, fehlt es dagegen an der Verwendung technischer Mittel.

Soweit der Täter auch zugunsten eines Dritten handelt, ist in dieser Fallkonstellation § 17 UWG Abs. 2 häufig erfüllt. Da Angriffe auf Zwangsaktivierungen häufig aus „sportlichem Ehrgeiz", aus wissenschaftlichem Interesse oder nur zur Feststellung von Schwachstellen erfolgen, liegt dagegen regelmäßig keine Schädigungs*absicht* vor, zumal bedingter Vorsatz insoweit nicht ausreichend ist. In Betracht kommt zwar noch das subjektive Tatbestandsmerkmal des Eigennutzes – hierbei genügt jedes Streben nach irgendeinem Vorteil[348] –, wenn auch die Anerkennung in der Hackerszene erstrebt wird. Gleichwohl wird Handeln aus Eigennutz nur relativ schwer nachweisbar sein. Gleiches gilt für ein Handeln zugunsten Dritter, wenn es an einer Mitteilung des Geheimnisses fehlt.

- *Umgehung von Schutzmechanismen bei Daten- und Audio-CDs*

  Soweit bei Daten- und Audio-CDs Kopierschutzmechanismen umgangen werden, die ein Auslesen und Kopieren der gespeicherten Informationen verhindern sollen, scheitert eine Anwendbarkeit des § 17 UWG häufig schon daran, dass nicht das Geheimnis selbst beschafft wird, sondern ein Weg gesucht und auch gefunden wird, um die Auswirkungen des Kopierschutzes umgehen zu können. Dies gilt insbesondere beim 1:1 Kopieren der Daten auf einen anderen Datenträger. Dies kann z.B. dadurch geschehen, dass ein Datenträger im so genannten RAW-Modus kopiert wird, d.h. die Daten werden – inklusive des Schutzmechanismus – Bit für Bit auf den Datenrohling übertragen. Ein solches Verhalten wird aber nicht von § 17 UWG erfasst, da die Vorschrift nicht das Anfertigen von 1:1 Raubkopien unterbinden will, sondern den Zugang zu geheimem Know-how schützen.[349] Hinzu kommt, dass die Funktionsweise gerade der gebräuchlichen Kopierschutzmechanismen bei Datenträgern inzwischen allgemein bekannt und teilweise sogar dokumentiert ist, so dass schon nicht mehr von einem Geschäfts- und Betriebsgeheimnis ausgegangen werden kann.

  Auf der anderen Seite werden bei kopiergeschützten Daten-CDs teilweise auch verschlüsselte Dateien auf dem Datenträger abgelegt, an denen die Hacker Modifikationen vornehmen. Hierzu werden z.B. bestimmte verschlüsselte Dateien decodiert, modifiziert und anschließend durch die modifizierte Variante ersetzt. Dies erfüllt wiederum den Tatbestand

347. Der Begriff der „technischen Mittel" wird dabei sehr weit verstanden und erfasst alle Vorrichtungen mit deren Hilfe man sich fremde Geheimnisse verschaffen kann, vgl. *Harte-Bavendamm*, GRUR 1990, 657, 662; *Raubenheimer*, CR 1994, 264, 266.
348. Vgl. Baumbach/*Hefermehl*, § 17 UWG, Rn. 20; *Raubenheimer*, CR 1994, 264, 266.
349. So *Taeger*, CR 1991, 449, 453; siehe auch *Beucher*/*Engels*, CR 1998, S. 101, 102.

des § 17 Abs. 2 UWG, wenn die Daten auf dem Datenträger im Object-Code vorliegen und es daher eines erheblichen Aufwandes bedarf, um hierfür einen „Patch“ oder „Crack“ zu entwickeln. Jedoch liegt auch insoweit ein Handeln zu Zwecken des Wettbewerbs, aus Eigennutz oder zugunsten eines Dritten nur in den bereits oben bei der Umgehung von Zwangsaktivierungen bei Software erwähnten Fallkonstellationen vor, wobei der Nachweis der subjektiven Tatbestandsmerkmale besondere Schwierigkeiten bereiten dürfte.

- *Umgehung von Schutzmechanismen bei Video-DVDs*

  Bei Video-DVDs kommen – wie dargestellt – unterschiedliche Schutzmechanismen zum Einsatz. Zum einen soll durch die Verwendung von Ländercodes eine Beschränkung der Abspielbarkeit der DVD innerhalb einer bestimmten Region sichergestellt werden. Zum anderen werden die Video-Daten auf der DVD verschlüsselt abgelegt, damit diese nicht ohne weiteres ausgelesen und auf andere Datenträger kopiert werden können. Soweit eine Umgehung von Ländercodes bei Video-DVDs vorgenommen wird, kommt § 17 Abs. 2 UWG nicht in Betracht, da es sich bei diesen Codes nicht um Geheimnisse handelt, sondern um eine Vorgabe, welche die Hersteller von DVD-Hardware und entsprechender Software zu beachten haben. Dass dies nicht geschieht, weil sich z.B. Stand-alone DVD-Player oder DVD-Laufwerke code-free schaltet lassen, beruht daher nur auf der Missachtung der entsprechenden Vorgaben durch die DVD-Produzenten. Dagegen greift der Tatbestand des § 17 Abs. 2 UWG ein, wenn die zur Entschlüsselung von DVD-Inhalten verwendeten geheimen Schlüsselinformationen beschafft werden. Diese Schlüsselinformationen befinden sich z.B. vor Zugriffen gesichert in der Hardware eines stand-alone DVD-Players und stellen damit ein Geschäfts- und Betriebsgeheimnis dar. Werden diese „Informationen“ mit Hilfe technischer Mittel durch einen Dritten beschafft, so geschieht dies zweifellos unbefugt, da sie von ihrer Konzeption her die Hardware nicht verlassen sollen. Bei der Verwertung derartiger Informationen ergibt sich auch hier das Problem, dass nach Veröffentlichung der Informationen insbesondere im Internet nicht mehr von einem Geschäfts- und Betriebsgeheimnis ausgegangen werden kann, so dass entsprechende Folgeverwertungen, etwa in Softwaretools, nicht mehr von § 17 Abs. 2 UWG erfasst werden. Der subjektive Tatbestand des § 17 Abs. 2 UWG ist wiederum erfüllt, wenn zugunsten Dritter die Schlüsselinformationen besorgt werden oder wenn der Täter aus Eigennutz handelt, weil er die Informationen z.B. für die Herstellung eines Software-DVD-Players für ein bestimmtes Betriebssystem benötigt. Der Tatbestand ist dagegen unanwendbar, wenn der Täter aus dem „sportlichen“ Motiv der Überwindung von Sicherungsmechanismen handelt.

- Umgehung von Schutzmechanismen bei softwarebasierten DRM-Systemen

  Angriffe auf die Schutzmechanismen von softwarebasierten DRM-Systemen, die eine vom Inhaltsanbieter vorgegebene Nutzung digitaler Inhalte steuern, betreffen die dort verwendeten Authentifizierungs- und Entschlüsselungsmechanismen. Dies gilt z.B. auch für den bereits oben näher erörterten Angriff auf das DRM-System von Windows Media.[350] Soweit bei diesen Angriffen der Object-Code der DRM-Software wieder in Source-Code rückgewandelt wird, ist der Tatbestand des unbefugten Ausspähens mittels technischer Mittel gemäß § 17 Abs. 2 Nr. 1a UWG in gleichem Umfang wie bei der Umgehung von Zwangsaktivierungen erfüllt. Erfolgt der Angriff lediglich durch Ausprobieren und

350. Siehe oben II. B. 2. c).

Entdecken von Schwachstellen, fehlt es dagegen am Ausspähen eines Geheimnisses. Bezüglich des subjektiven Tatbestandes kann auf die Ausführungen oben zur Umgehung von Zwangsaktivierungen und Kopierschutzmechanismen von Datenträgern verwiesen werden.

- *Einsatz von Piraten-SmartCards beim digitalen TV*

  Beim Einsatz von Piraten-SmartCards – bei denen es sich um SmartCards handelt, die zwar Original-SmartCards entsprechen, aber ohne Genehmigung der die SmartCard ausgebenden Stelle nachgebaut oder modifiziert wurden – müssen im Hinblick auf § 17 Abs. 2 UWG zwei von einander getrennt zu sehende Vorgänge unterschieden werden.[351] Damit überhaupt eine Piraten-SmartCard verwendet werden kann, ist es zunächst notwendig, dass die benötigten Informationen – vor allem Betriebsprogramme und Entschlüsselungscodes – von einer Original-SmartCard erlangt werden. In einem weiteren Schritt geht es dann darum, die gewonnenen Informationen zum Bau einer Piraten-SmartCard zu verwenden. Die Verschaffung der Informationen von einer Original-SmartCard erfüllt den Tatbestand des § 17 Abs. 2 Nr. 1 UWG, da ein Geheimnis – d.h. die auf der SmartCard befindlichen Informationen – unbefugt verschafft und gesichert wird.[352] Auch wenn sich eine hierzu verwendete SmartCard im Besitz des Täters befindet, ändert dies nichts an dem Vorliegen eines Geschäfts- und Betriebsgeheimnisses, da die SmartCards gegen unerwünschte Zugriffe geschützt werden.[353] Dem steht auch nicht die oben genannte Entscheidung des OLG Frankfurt entgegen, in der das Bestehen eines Geschäfts- und Betriebsgeheimnis bei einer SmartCard angezweifelt wurde.[354] Denn diese Entscheidung beruhte darauf, dass das verwendete Verschlüsselungsverfahren zum Zeitpunkt der Entscheidung veraltet war und die Softwaretools zur Entschlüsselung allgemein zugänglich waren, mithin also schon einer Offenkundigkeit des Geheimnisses ausgegangen werden konnte. Gerade im Bereich des digitalen TV werden heutzutage aber sehr aufwändig geschützte SmartCards verwendet, so dass die dort gesicherten Informationen nur mit professionellem Equipment und mit dem nötigen physikalischen Wissen ausgelesen werden können. Insofern kann nicht ernsthaft behauptet werden, die in der SmartCard verborgenen Informationen seinen wegen ihrer Offenheit nicht durch § 17 UWG geschützt. Etwas anderes kann sich aber – worauf *Beucher*/*Engel* zurecht hinweisen – insbesondere dann ergeben, wenn nicht die Daten der SmartCards ausgelesen werden, sondern gleich der gesamte Mikrochip auf der SmartCard kopiert wird, da in diesem Fall keine Kenntnis vom Betriebsgeheimnis vorliegt.[355] Dieses wird quasi nur von einem Datenträger auf einen anderen übertragen. Im übrigen entspricht dies auch dem bereits oben zum Ausspähen von Programmen Gesagten, da auch die bloße 1:1 Kopie eines Programms nicht von § 17 UWG erfasst wird. Der subjektive Tatbestand in Form des Handelns zu Zwecken des Wettbewerbs liegt insoweit vor, wenn die SmartCard-Informationen ausgelesen werden, um selbst Piraten-SmartCards herstellen und verkaufen zu können. Soweit das Ausspähen der Daten wiederum durch Hacker aus rein „sportlichem Ehrgeiz“ erfolgt, ergeben sich wiederum Schwierigkeiten beim Nachweis eines Eigennutzes. Weiterhin ist

351. Zum Begriff der Piraten-SmartCard vgl. oben II. B. 3 c).
352. Vgl. *Beucher*/*Engels*, CR 1998, 101, 102; *Dressel*, Strafbarkeit von Piraterie-Angriffen gegen Zugangsberechtigungssysteme von Pay-TV-Anbietern, MMR 1999, 390, 391.
353. So auch *Beucher*/*Engels*, CR 1998, S. 101, 102.
354. Vgl. OLG Frankfurt, NJW 1996, 264.
355. Vgl. *Beucher*/*Engels*, CR 1998, S. 101, 102.

eine Strafbarkeit nach § 17 Abs. 2 Nr. 2 UWG wegen Verwertung eine Geschäfts- und Betriebsgeheimnis bei der Herstellung von Piraten-SmartCards tatbestandlich nur gegeben, wenn feststeht, dass die SmartCard-Informationen insbesondere nicht aus dem Internet oder sonstigen öffentlich zugänglichen Quellen stammen, da es in diesem Fall aufgrund der Offenheit an einem Geschäfts- und Betriebsgeheimnis mangelt.

Ob eine Strafbarkeit privater Nutzer einer Piraten-SmartCard wegen unbefugter Verwertung eines Geschäfts- und Betriebsgeheimnis nach § 17 Abs. 2 Nr. 2 UWG in Betracht kommt, hängt insbesondere vom Begriff der Verwertung ab. Eine Verwertung setzt allerdings eine wirtschaftliche Ausschlachtung voraussetzt.[356] Auch wenn hierunter jede Nutzung des Geheimnisses verstanden wird, gibt es doch Stimmen in der Literatur, die einen über den Privatgebrauch hinausgehenden Gebrauch fordern.[357] Soweit Softwaretools zum Entschlüsseln digitaler Pay-TV Angebote hergestellt und verwendet werden, kommen auch dort Entschlüsselungsinformationen zur Anwendung, die von Original-SmartCards stammen dürften. Wenn dies der Fall ist, gilt im Hinblick auf § 17 Abs. 2 UWG das oben zum Auslesen von SmartCard-Informationen und deren Verwendung Gesagte entsprechend.[358]

2. § 202a StGB

a) Übersicht

§ 202a Abs. 1 StGB bedroht denjenigen mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe, der „unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugriff besonders gesichert sind, sich oder einem anderen verschafft". § 202a Abs. 2 StGB definiert dazu die Daten im Sinne des Abs. 1 als „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden".

b) Kritische Tatbestandsmerkmale im Hinblick auf die Umgehung von Schutzmechanismen

Soweit das Tatobjekt von § 202a StGB die in Abs. 2 näher definierten *Daten* verlangt, bereitet die Anwendbarkeit des Tatbestandes auf die hier interessierenden Raubkopien keine Probleme. Elektronisch gespeicherte Daten sind der Prototyp des Tatobjekts von § 202a StGB.[359] Im Gegensatz zu § 17 UWG müssen die Daten dabei auch nicht geheim sein, da § 202a nur eine formelle Verfügungssphäre und nicht die Geheimsphäre schützt.[360]

Die Daten sind für den Täter dann *nicht bestimmt*, wenn sie ihm nach dem Willen des Berechtigten im Zeitpunkt der Tathandlung nicht zur Verfügung stehen sollen.[361] Die Überlassung

356. Vgl. Baumbach/*Hefermehl*, § 17 UWG, Rn. 37.
357. Vgl. *Beucher*/*Engels*, CR 1998, S. 101, 103.
358. Siehe oben bei Fn. 351.
359. Vgl. Leipziger Kommentar (LK) / *Schünemann*, Kommentar zum StGB, 11. Aufl. 2001, § 202a Rn. 3 und *Bandekow*, Strafbarer Missbrauch des elektronischen Zahlungsverkehrs, Lübeck 1989, S. 27.
360. Vgl. LK/*Schünemann*, § 202a Rn. 2.
361. Vgl. LK/*Schünemann*, § 202a Rn. 9.

von Daten zum Zwecke ihrer Nutzung ist dabei nicht automatisch und immer mit ihrem Zugänglichmachen und damit ihrem Zurverfügungstellen verbunden.[362] Dies hat nicht nur für verschlüsselte Daten auf dem Magnetstreifen einer Bankomatenkarte Bedeutung sondern auch für verschlüsselte Daten im Bereich von DRM-Systemen und bei Kopierschutzmechanismen. Bei der Erlangung von Daten zur Umgehung von Sicherungsmaßnahmen zwecks Erstellung von Raubkopien ist daher zu differenzieren: Kann der Täter (wie in den Fällen der Kopierschutzsperren) mit Daten zwar arbeiten, diese jedoch nicht kopieren, so sind die Daten für ihn bestimmt und damit nicht durch § 202a StGB geschützt.[363] Verhindern Schutzmechanismen dagegen den Zugriff auf die Daten oder auf die vom Täter gehackten Schlüsselinformationen, so verschafft sich der Täter für ihn nicht bestimmte Daten auch dann, wenn er die Daten aufgrund einer Entscheidung des Verfügungsbefugten auf seinem Rechner gespeichert hat.

Schwieriger zu beurteilen ist die gesetzliche Forderung, dass die Daten *gegen unbefugten Zugriff besonders gesichert* sein müssen. Dieses Merkmal erfordert, dass die Daten gegenüber denjenigen Personen, für die sie nicht bestimmt sind, durch Vorkehrungen gesichert sind, die einen Datenzugriff verhindern oder nicht unerheblich erschweren. Dabei spielt es wiederum keine Rolle, dass sich die Daten in der räumlichen Sphäre des Täters befinden, solange sie ihm gegenüber gegen Zugriff besonders gesichert sind. Der Tatbestand erfasst daher z.B. die vor einem Zugriff gesicherten Entschlüsselungsinformationen oder verschlüsselte digitale Inhalte.[364] Kopierschutzmechanismen von Datenträgern verhindern dagegen nicht den Zugriff als solchen auf die Daten, sondern nur deren Kopie; sie fallen daher – was allerdings umstritten ist – nicht unter § 202a StGB.[365] Ob der Vertrieb eines Programms nur im Objektcode eine Zugangssicherung im Hinblick auf den Quellcode darstellt ist fraglich und wurde bisher noch kaum untersucht. *Meier* sieht den Objektcode zwar nicht per se als eine Zugangssicherung an, differenziert aber danach, welche Länge und Komplexität das Programm aufweist und bejaht bei aufwändig in den Quellcode zurück zu übersetzenden Programmen eine besondere Sicherung i.S.d. § 202a StGB.[366] Diese Differenzierung erscheint aber problematisch, da der Aufwand einer Rückübersetzung wesentlich vom Know-how des Täters abhängt und damit den besonders geschickten Täter besser stellen würde.

Der Täter *verschafft* sich die Daten, wenn er von ihnen tatsächlich Kenntnis nimmt oder wenn er sie – z.B. auf einem Datenträger – in seine Verfügungsgewalt bringt.[367] Bei verschlüsselten Daten ist im letztgenannten Fall allerdings erforderlich, dass der Täter die Daten entschlüsseln kann oder wenigstens den vor einem Zugriff geschützten Schlüssel in seine Verfügungsgewalt bringt.[368] Dies liegt beispielsweise vor, wenn er die auf einer Original-SmartCard abgespeicherten Informationen ausliest oder verschlüsselte Videoinhalte hackt. Einen Grenzfall stellt es dagegen dar, wenn der Täter sich die geschützten Zugangsdaten – z.B. Entschlüsselungsinformationen – in einem Softwaretool verschafft. In diesem Fall kann er zwar nicht auf die

362. So auch Vgl. LK/*Schünemann*, § 202a Rn. 12.
363. So auch LK/*Schünemann*, § 202a Rn. 10.
364. Siehe *Bandekow*, S. 258.
365. Gegen eine Anerkennung von Kopierschutzmechanismen als Zugangssicherungen sind LK/*Schünemann*, § 202a Rn. 15; *Kuhlmann*, Kein Rechtsschutz für den Kopierschutz, CR 1989, 177, 185; dagegen sprechen sich aus Sch/Sch/*Lenckner*, § 202a Rn. 8 und *Meier*, Softwarepiraterie – eine Straftat?, JZ 1992, 657, 662.
366. Vgl. *Meier*, JZ 1992, 657, 662.
367. LK/*Schünemann*, § 202a Rn. 6, spricht insoweit vom „Erwerb der Herrschaft über die Daten“. Vgl. auch *Bandekow*, S. 260.
368. In diesem Sinne wohl auch LK/*Schünemann*, § 202a Rn. 6.

Zugangsdaten selbst zugreifen, aber er kann das Softwaretool zum Auslesen und Kopieren von geschützten Daten verwenden. Da der Täter die Daten in diesen Fällen nicht nur in seiner räumlichen Verfügungsgewalt hat, sondern sie auch funktionell einsetzt, sollte dies jedoch für ein Verschaffen ausreichen. In vielen Fällen kommt es auf diese Frage allerdings letztlich nicht an, da der Täter beim späteren Einsatz des Softwaretool Zugangssperren beseitigt und sich Daten i.S.d. § 202a StGB verschafft.

c) Analyse der Einzelfälle

Wendet man die vorgenannten Grundsätze auf die in der empirischen Analyse festgestellten Fallgruppen an, so ergeben sich folgende Ergebnisse:

- Bei der Umgehung von Zwangsaktivierungen bei Softwareprodukten greift § 202a StGB ein, wenn Veränderungen am Object-Code vorgenommen werden und man mit *Meier* davon ausgeht, dass dies bereits eine ausreichende Zugangssicherung im Sinne der Vorschrift darstellt.[369] Dagegen ist § 202a StGB nicht einschlägig, wenn die Zwangsaktivierung dadurch manipuliert wird, dass bestimmte frei zugängliche Daten und Dateien einer Software ausgetauscht oder gelöscht werden.

- Bei der Umgehung der Kopierschutzmechanismen von Datenträgern ist danach zu differenzieren, ob nur Kopien erstellt werden oder ob bestimmte verschlüsselte Daten entschlüsselt werden. Soweit exakte 1:1 Kopien erstellt werden, wie z.B. bei Software- oder auch Audio-CDs, ergibt sich eine Strafbarkeit, wenn man es für ein unbefugtes Verschaffen von Daten ausreichen lässt, dass der Täter diese anderes verwendet als vom Hersteller des Datenträgers gewollt. Müssen dagegen auch bestimmte verschlüsselte Daten erst entschlüsselt werden, damit ein Kopiervorgang möglich wird, so greift § 202a StGB ein. Dies gilt z.B. für die digitale Kopie von Video-DVDs, bei denen insoweit zwar die verschlüsselten, nicht aber die unverschlüsselten Videodaten für den Nutzer bestimmt sind.

- Soweit ein Angriff auf softwarebasierte DRM-Systeme erfolgt, liegt § 202a StGB vor, wenn der Täter Zugangssicherungen umgeht oder verschlüsselte Daten mit unlauteren Mitteln entschlüsselt. Dies ist z.B. der Fall, wenn die verschlüsselten Inhalte nur über einen bestimmten Zeitraum benutzt werden dürfen, der Täter die Verschlüsselung aber hackt, um einen dauernden Zugriff auf den Inhalt zu erhalten. Das selbe gilt, wenn sich der Täter vor einem Zugriff gesicherte Zugangsschlüssel für geschützte digitale Inhalte rechtswidrig besorgt oder wenn er Veränderungen am Object-Code einer Abspielsoftware vornimmt, vorausgesetzt man sieht diesen schon als eine Zugangssicherung an.[370]

- Weiterhin ist der Tatbestand des § 202a StGB erfüllt, wenn sich der Täter die auf einer Original-SmartCard abgelegten und üblicherweise sogar sehr stark vor Zugriffen geschützten Informationen verschafft. Bereits aus dem Wortlaut des § 202a StGB ergibt sich aber auch, dass die Vorschrift weder die Herstellung noch den Vertrieb von Piraten-SmartCards erfasst, denn insoweit liegt nur ein Benutzen der ausgespähten Daten vor.[371]

369. Vgl. *Meier*, JZ 1992, 657, 662.
370. Vgl. *Meier*, JZ 1992, 657, 662.
371. Vgl. *Beucher/Engels*, CR 1998, S. 101, 104.

Wird dagegen eine Piraten-SmartCard benutzt, so kann ein Verschaffen der dort enthalten Informationen mit der oben vertretenen funktionalen Sichtweise durchaus vertreten werden.[372] Allerdings hat dies keine praktische Auswirkung, da der Nutzer die Piraten-SmartCard zur Entschlüsselung der digitalen Videodaten verwendet und sich durch diese Handlung ohnehin unbefugt Daten verschafft, die nicht für ihn bestimmt und besonders vor einem Zugriff gesichert sind.

3. § 263a StGB

a) Übersicht

Während die vorstehend erörterten §§ 17 UWG, 202a StGB die Umgehung von Schutzmechanismen unter dem Gesichtspunkt der dabei erfolgenden Verschaffung geheimer oder besonders gesicherter Daten erfassen, zielt § 263a StGB auf einen anderen Aspekt der Tat: Für die Anwendung von § 263a StGB ist entscheidend, ob durch die Manipulation der Schutzmechanismen unberechtigte Leistungen in Anspruch genommen und das Vermögen eines anderen geschädigt wird.

§ 263a StGB bedroht denjenigen mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe, der „in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst."

b) Kritische Merkmale im Hinblick auf die Umgehung von Schutzmechanismen

Die Erfassung der Umgehung von Schutzmechanismen durch § 263a StGB ist im Hinblick auf mehrere Merkmale des Tatbestandes problematisch:

- Ein in der bisherigen Literatur noch nicht erörtertes grundsätzliches Problem ergibt sich zunächst im Hinblick auf das Erfordernis der *Beeinflussung eines Datenverarbeitungsvorgangs*. Dieses Problem resultiert aus der Tatsache, dass § 263a StGB zur Schaffung der Lücken des Betrugstatbestandes von § 263 StGB geschaffen wurde und deswegen strukturell ähnlich konstruiert und auszulegen ist wie dieser Tatbestand.[373] Die Bedeutung dieser Strukturgleichheit und der daraus resultierenden betrugsähnlichen Auslegung von § 263a StGB hat der BGH erst jüngst in einer Entscheidung zur abredewidrigen Verwendung einer Geldautomatenkarte durch den berechtigten Kontoinhaber betont.[374] Dies bedeutet: So wie § 263 StGB die täuschungs- und irrtumsbedingt erfolgende vermögensschädigende Vermögensverfügung des Tatopfers erfasst, richtet sich § 263a StGB gegen die durch eine Computermanipulation und einen Datenverarbeitungsvorgang erfolgende Vermögensverfügung des Opfers. Auf der Grundlage dieser Parallele von § 263 und § 263a StGB ist offensichtlich, dass bei § 263a StGB im Grundsatz ebenso wie bei §

372. Siehe oben III. D. 2. b).
373. Siehe insoweit auch LK/*Tiedemann*, § 263a Rn. 13 ff.
374. Vgl. BGH CR 2002, 413 ff.

263 StGB eine durch die Datenverarbeitungsanlage erfolgende Verfügung des Opfers erfolgen muss. Da die Vermögensverfügung dem Opfer zugerechnet werden und durch die Datenverarbeitungsanlage erfolgen muss, ist ein Datenverarbeitungsvorgang erforderlich, der ebenfalls dem Opfer zugerechnet werden muss. § 263a StGB erfasst daher z.B. nicht den Fall, dass der Täter mit Hilfe seiner eigenen Datenverarbeitungsanlage Missbräuche begeht und durch die Nutzung dieser Ergebnisse das Opfer schädigt.

Im Normalfall des § 263a StGB erfolgt die Vermögensverfügung des Opfers deswegen durch dessen eigene Datenverarbeitungsanlage, die vom Täter manipuliert wird. Für die insoweit erfolgende Zuordnung der im Eigentum des Opfers stehenden Datenverarbeitungslage zum Opfer ist es dabei unschädlich, wenn sich die Datenverarbeitungsanlage in der räumlichen Sphäre des Täters befindet, wie z.B. in dem Fall eines vom Opfer dem Täter mietweise überlassenen Digital Receivers mit einem Conditional Access Module (CAM).[375] Da es für die Zuordnungsfrage nicht auf das Sacheigentum des Opfers an der Datenverarbeitungsanlage ankommt, sondern die Verfügung nach dem Gesetzeswortlaut durch einen „Datenverarbeitungs*vorgang*“ (des Opfers) erfolgen muss, ist beim Auseinanderfallen der Zuordnung von Hardware und Software auf die *Zuordnung des konkreten Datenverarbeitungsvorgangs* abzustellen. Hieraus resultiert die Möglichkeit, einen Datenverarbeitungsvorgang des Opfers nicht nur dann anzunehmen, wenn das Opfer eine Verfügungsbefugnis über die Hardware hat, sondern auch in denjenigen Fällen, in denen das Opfer den Datenverarbeitungsvorgang aufgrund der eingesetzten Software in rechtlich anerkannter Weise bestimmen kann. Dies bedeutet, dass ein Datenverarbeitungsvorgang des Opfers auch in den Fällen bejaht werden kann, in denen – z.B. beim Einsatz eines softwarebasierten DRM-Systems – ein von diesem System gesteuerter Datenverarbeitungsvorgang auf dem PC eines Nutzers erfolgt. Kein Datenverarbeitungsvorgang des Rechteinhabers liegt allerdings mehr vor, wenn der Täter nicht das – den Datenverarbeitungsvorgang festlegende und damit dem Rechteinhaber zuordnende – DRM-System manipuliert, sondern mit Hilfe eines von ihm bestimmten missbräuchlichen Datenverarbeitungsvorgangs auf die geschützten Daten zugreift. Das gleiche gilt, wenn bei der Entschlüsselung von Daten auf einer CD nicht ein darauf gespeichertes Schutzsystem manipuliert wird, sondern ein – vom Verfügungsberechtigten an den Daten unerwünschter – sonstiger Datenverarbeitungsvorgang erfolgt.

- Die Manipulation des Datenverarbeitungsvorgangs muss sodann durch die unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch die unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf erfolgen. Vor allem im Hinblick auf die unrichtige Programmgestaltung als auch im Hinblick auf die unbefugte Datenverwendung ist dabei streitig, wie die Merkmale der „Unrichtigkeit“ und der „Unbefugtheit“ zu bestimmen sind. Die Unrichtigkeit eines Programms liegt nach einer – subjektiv beurteilenden – Ansicht vor, wenn das Programm nicht dem Willen des Berechtigten entspricht.[376] Vorherrschend ist allerdings die objek-

375. Dies deckt sich mit der Ansicht *Zahns*, Die Betrugsähnlichkeit des Computerbetrugs (§ 263a StGB), Aachen 2000, S. 106, wonach auch im Falle des Betreibens eines Glücksspielautomatens auf Kosten eines Gastwirtes dennoch der Hersteller des Glücksspielautomaten Berechtigter der in dem Automaten verwendeten Daten bleibt.

376. Vgl. LK/*Tiedemann*, § 263a Rn 29; *Scheffler*, Das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität unter besonderer Berücksichtigung des Tatbestandes des Computerbetrugs (§ 263a StGB) und des Tatbestandes des Missbrauchs von Scheck- und Kreditkarten (§ 266b StGB), Kiel 1998, S. 163 ff.; *Zahn*, S. 92 ff.

tive Betrachtungsweise, die danach fragt, ob durch das Programm ein dem Zweck der jeweiligen Datenverarbeitung entsprechendes objektiv zutreffendes Ergebnis entsteht.[377] Das Merkmal der Unbefugtheit im Rahmen der dritten Tatalternative wird nach der „subjektivierenden“ Auslegung danach bestimmt, ob eine vertragswidrige, dem tatsächlichen oder mutmaßlichen Willen des Rechtsinhabers widersprechende, Datenverarbeitung vorgenommen wird.[378] Die „computerspezifische“ Auslegung will bei diesem Merkmal darauf abstellen, ob sich der der Datenverarbeitung entgegenstehende Wille des Betreibers im Computerprogramm niedergeschlagen hat.[379] Dagegen fragt die von der herrschenden Meinung vertretene „betrugsspezifische“ Auslegung bei der Unbefugtheit danach, ob der Einsatz der Daten und Informationen gegenüber einer natürlichen Person eine zumindest konkludente Täuschung darstellen würde.[380]

Bei der ersten Tatalternative des § 263a StGB ist insb. auch der Begriff der „Gestaltung“ klärungsbedürftig. Er wird üblicherweise sehr weit verstanden. Hierunter fällt daher nicht nur die Neuprogrammierung und das Hinzufügen von Programmteilen, sondern auch das Veränderung und Löschen einzelner Programmteile oder der Einbau sonstiger falscher Funktionen sowie auch die Verwendung von zusätzlichen Programmen.[381] *Tiedemann* erwähnt insoweit ActiveX-Controls, welche die Finanzsoftware des Nutzers so manipulieren, dass es zu ungewollten Banküberweisungen kommt.[382] Diese Situation ist mit den Angriffen auf DRM-Systeme und Zwangsaktivierungen vergleichbar, da auch hier „Ergänzungen“ zu bestimmten Softwareprodukten vorgenommen werden, damit die verwendeten Mechanismen ausgehebelt werden können.

- Weitere Probleme resultieren aus dem Erfordernis, dass die vermögensschädigende Verfügung den Vermögensschaden des Opfers unmittelbar verursachen muss.[383] An dieser „Unmittelbarkeit“ fehlt es, wenn der Vermögensschaden erst durch weitere Handlungen des Täters verursacht wird.[384] Bei der Umgehung von Schutzmechanismen und der Entschlüsselung geschützter Inhalte stellt sich deswegen in dem zu beurteilenden Einzelfall jeweils die Frage, ob ein Vermögensschaden bereits durch die Umgehung eines Sicherungsmechanismus (insb. durch die Entschlüsselung von Daten) erfolgt oder aber durch – für § 263a StGB nicht mehr zu berücksichtigende – spätere Handlungen des Täters (wie z.B. den Vertrieb der gehackten Daten). Besonders problematisch ist dies immer dann, wenn sich der Täter unberechtigterweise die Nutzungsmöglichkeit digitaler Güter verschafft, also z.B. die Aktivierungsroutine einer Software beeinflusst oder Inhalte entschlüsselt, da der Vermögensschaden hier erst dadurch entsteht, dass der Täter die Nutzung nicht „anmeldet“, also z.B. keine Softwarelizenz erwirbt oder kein Abonnement für ein digitales Pay-TV Angebot abschließt.[385] Gleichwohl erscheint eine solche Aufspaltung künstlich, weil z.B. bei der Entschlüsselung mittels einer Piraten-SmartCard prak-

377. Vgl. LK/*Tiedemann*, § 236a Rn. 30.
378. Vgl. LK/*Tiedemann*, § 236a Rn 42 f.; *Scheffler*/*Dressel*, Unbefugtes Verwenden von Daten beim Computerbetrug, NJW 2000, 2645. Siehe auch *Bandekow*, S. 237 ff.; *Scheffler*, S. 184 ff., 272 ff.; *Zahn*, S. 102 ff.
379. Vgl. LK/*Tiedemann*, § 236a Rn 45.
380. Vgl. BGH CR 2002, 413 f.; Sch/Sch/*Tiedemann*, § 236a Rn 44 f.; *Scheffler*, S. 185.
381. Vgl. LK/*Tiedemann*, § 263a Rn. 28; *Scheffler*, S. 164 ff.; *Zahn*, S. 90 f.
382. Vgl. LK/*Tiedemann*, § 263a Rn. 28.
383. Siehe auch *Bandekow*, S. 245 f.; *Scheffler*, S. 221 f.
384. Vgl. LK/*Tiedemann*, § 263a Rn. 65; *Zahn*, S. 154 ff.
385. Vgl. *Beucher*/*Engels*, CR 1998, 101, 104.

tisch gleichzeitig auch gegenüber dem Digital-Receiver die Nichtanmeldung der Nutzung erklärt wird.[386] Genauso erklärt der Täter mit der unberechtigten Freischaltung einer zu aktivierenden Software, dass er die Nutzung ohne Bezahlung vornehmen möchte.

- Schließlich ist im vorliegenden Kontext zu klären, worin überhaupt der Vermögensschaden des Rechteinhabers zu sehen ist. Der Vermögensschaden in § 263a StGB entspricht dabei demjenigen in § 263 StGB. Voraussetzung ist damit ganz allgemein eine Vermögensminderung, also der Unterschied zwischen dem Wert des Vermögens vor und nach der Vermögensverfügung.[387] In Betracht kommt dabei vor allem ein entgangener Gewinn des Rechteinhabers, da er für die in Anspruch genommene Leistung oder das unberechtigterweise verwendete Programm kein Entgelt erhält.[388] Hierbei ergibt sich aber das Problem, dass ein reiner Vergleich der Vermögenslage vor und nach dem schädigenden Ereignis – also z.B. der unberechtigten Entschlüsselung von Inhalten oder der unberechtigten Verwendung von Software – keine Vermögensminderung auf Seiten des Anbieters oder Softwareherstellers ergibt. Dies liegt daran, dass dem Raubkopierer oder unberechtigten Nutzer nicht unterstellt werden kann, er hätte für die unberechtigt in Anspruch genommene Leistung oder das rechtswidrig erlangte Softwareprodukt auch tatsächlich bezahlt, wenn nur ein legaler Zugang zu den Informationen möglich gewesen wäre. Vielmehr ist davon auszugehen, dass der Nutzer in diesem Fall die Software nie verwendet oder die entsprechenden Inhalte nie genutzt hätte. Auf der anderen Seite ist aber im Offline-Bereich anerkannt, dass ein Vermögensschaden auch dann vorliegt, wenn eine Kontrollperson in den Glauben versetzt wird, der Täter habe eine ordnungsgemäße Eintrittskarte und so eine bestimmte Leistung in Anspruch nimmt.[389] Überträgt man dies auf die Anbieter digitaler Güter, so müsste auch insoweit ein Vermögensschaden bejaht werden, da diese Leistungen nur gegen Entgelt erbracht werden.

c) Analyse der Einzelfälle

Aufgrund der Vielzahl der praktisch relevanten und im empirischen Teil näher herausgearbeiteten Formen der Umgehung von Sicherungsmechanismen setzt eine Beurteilung der Anwendbarkeit von § 263a StGB wiederum eine differenzierende Einzelanalyse voraus. Dabei sind – ebenso wie im Hinblick auf die Anwendbarkeit der §§ 17 UWG, 202a StGB – wiederum die folgenden Handlungen zu unterscheiden:

- *Umgehung der Zwangsaktivierung bei Software*

  Bei der Umgehung der Zwangsaktivierung von Software liegt ein Datenverarbeitungsvorgang i.S.d. § 263a StGB vor, da die Ermittlung der notwendigen Aktivierungsinformationen sowie die anschließende Aktivierung vom Opfer, d.h. dem Softwarehersteller, gesteuert wird. Dies gilt sowohl für den Fall, dass bestimmte Daten ausgetauscht werden, um die Aktivierungsprozedur zu manipulieren, als auch für den Fall, dass ein Aktivierungsschlüssel bei einer Programmversion angewendet wird, für die er eigentlich nicht

386. In diesem Sinne wohl auch *Scheffler*, CR 2002, 151, 154 f.; zweifelnd aber *Beucher*/*Engels*, CR 1998, 101, 104.
387. Vgl. Tröndle/*Fischer*, § 263 Rn. 30.
388. Vgl. *Scheffler*, CR 2002, 151, 153.
389. Vgl. *Scheffler*, Einsatz einer Pay-TV Piraten-SmartCard – strafrechtliche Würdigung, CR 2002, S. 151, 153; Tröndle/*Fischer*, § 263 Rn. 37.

vorgesehen ist. In beiden Fällen greift der Täter damit in einen Programmablauf ein, der zwar auf seinem Computersystem abläuft, der aber gleichwohl vom Hersteller der Software automatisch nach der Installation der Software gestartet wird und daher seiner Sphäre zuzuordnen ist.

Sofern unmittelbar Manipulationen am Programm vorgenommen werden, damit dieses eine Aktivierung der installierten Software vornimmt, erfolgt auch eine unrichtige Gestaltung des Programms, da in der Form der Aktivierung ein Ergebnis erzielt wird, welches mangels ordnungsgemäßer Aktivierungsdaten objektiv nicht hätte eintreten dürfen. Soweit ein Master-Key bei einer Programmversion angewendet wird, für die er nicht bestimmt ist, handelt es sich nach allen Ansichten um eine unbefugte Verwendung dieser Daten. Die Unbefugtheit folgt dabei daraus, dass der Master-Key nur durch den Berechtigten bei bestimmten Programmversionen verwendet werden darf und zudem gegenüber dem Aktivierungsprozess „erklärt“ wird, man sei zur Verwendung dieser Daten berechtigt.

Soweit der Täter nicht im Besitz einer ordnungsgemäß erworbenen Lizenz für die entsprechende Software ist, entsteht dadurch auch ein Vermögensschaden i.S. eines entgangenen Gewinns, wobei sich die Unmittelbarkeit des Schadens daraus ergibt, dass mit der Überlistung der Zwangsaktivierung auch gleich eine unberechtigte Nutzung der Software erfolgt. Etwas anderes gilt insoweit nur, wenn der Käufer einer entsprechenden Softwarelizenz die Zwangsaktivierung umgeht, da es insoweit an einem Vermögensschaden fehlt.

- *Umgehung von Kopierschutzmechanismen bei Daten-CDs*

  Soweit bei Daten-CDs Kopien unter Umgehung der Kopierschutzmechanismen hergestellt werden, liegt schon kein Datenverarbeitungsvorgang des Opfers i.S.d. § 263a StGB vor, weil dieser Vorgang nicht vom Opfer (also dem Datenträgerproduzenten), sondern vom Nutzer selbst gesteuert wird und es sich damit nicht um einen fremden Datenverarbeitungsvorgang handelt. Vielmehr findet bei der Kopie von Datenträgern ein Datenverarbeitungsvorgang statt, der erst durch den Nutzer selbst initiiert wurde.
  Selbst wenn man aber einen Datenverarbeitungsvorgang i.S.d. § 263a StGB annehmen würde, müsste § 263a StGB zumindest deshalb regelmäßig abgelehnt werden, weil beim Einsatz von speziellen Kopierprogrammen keine unbefugte Verwendung von Daten vorliegt. Kopierprogramme, welche Schutzmechanismen z.B. bei Audio-CDs erkennen und umgehen können, analysieren „nur“, welche Veränderungen im Vergleich zum Audio-CD-Standard vorgenommen wurden. M.a.W.: Es ist überhaupt nicht notwendig, dass irgendwelche “unbefugten” Daten verwendet werden, damit das gewünschte Ergebnis erzielt werden kann, denn es muss nur herausgefunden werden, welche von dem Audio-CD-Standard abweichenden Daten sich auf der Audio-CD befinden und diese müssen dann „ausgeblendet“ werden. Schließlich kommt § 263a StGB bei Software-CDs auch deshalb nicht in Betracht, weil die Kopie dieser Datenträger noch keinen unmittelbaren Vermögensschaden darstellt. Dieser tritt immer erst dann ein, wenn die kopierte Software oder das kopierte Spiel – ohne dass eine Lizenz erworben wurde – auf einem Computersystem unberechtigterweise installiert und verwendet wird.

- *Umgehung von Schutzmechanismen bei Video-DVDs*

  Bei der bloßen Umgehung von Ländercodes bei Video-DVDs (ohne Verwendung einer Raubkopie), scheitert § 263a StGB schon daran, dass sich der geforderte Vermögensschaden bei einer Umgehung der Ländercodes nicht feststellen lässt. Der Ländercode soll

nur verhindern, dass DVDs einer bestimmten Region in einer anderen abgespielt werden können. Wird aber z.B. durch eine Person in Deutschland eine DVD der Region 1 (Nordamerika) käuflich erworben, so mag dies unerwünscht sein, führt aber nicht nur zu keiner Vermögensminderung, sondern im konkreten Fall sogar zu einer Vermögensmehrung des DVD-Produzenten. Mögliche mittelbare Schäden, die von den Produzenten befürchtet werden, wenn DVDs weltweit zur gleichen Zeit auf den Markt kommen – wie ein Rückgang bei den Kinobesuchen – spielen für § 263a StGB keine Rolle, denn der Vermögensschaden muss unmittelbar auf der Manipulation des Datenverarbeitungsvorgangs beruhen.

Werden dagegen die verschlüsselten Videodaten mittels Softwaretools entschlüsselt und ausgelesen, so liegt eine Beeinflussung eines fremden Datenverarbeitungsvorgangs i.S.d. § 263a StGB durch die unbefugte Verwendung von Daten vor, weil hierdurch zum einen ein DRM-System manipuliert wird, welches vom Datenträgerproduzenten zum Schutz der Videodaten verwendet wird. Dieses System stellt – im Zusammenspiel mit der Hardware – sicher, dass Video-DVDs weder ausgelesen noch kopiert, sondern lediglich angeschaut werden können. Zum anderen werden vom Täter Tools verwendet, die notwendigen Entschlüsselungsinformationen zur Umgehung dieses DRM-Systems enthalten; dies geschieht auch unbefugt, weil die entsprechenden Informationen nur in lizenzierten Softwareprogrammen und Geräten und nur zum Anschauen von Video-DVDs verwendet werden dürfen. Zudem wird man die Unmittelbarkeit eines Vermögensschadens – hier eines entgangenen Gewinns – dann annehmen können, wenn eine Video-DVD ausgelesen oder kopiert wird, denn damit erspart sich der Täter die Kosten für einen Kauf.

- *Umgehung von Schutzmechanismen bei softwarebasierten DRM-Systemen*

  Ansatzpunkt derartiger Angriffe sind üblicherweise nicht die digitalen Inhalte selbst, sondern das zum Abspielen des Inhalts verwendete Softwareprogramm, welches auch das Rechte Management System beinhaltet. Damit ist die Tathandlung der unrichtigen Gestaltung des Programms, mithin also eine Programmmanipulation, gegeben. Werden derartige Manipulationen vorgenommen, um unberechtigterweise digitale Inhalte – z.B. Filme oder Musik – nutzen zu können, so liegt in diesem Zeitpunkt noch kein unmittelbarer Vermögensschaden vor. Dieser tritt erst ein, wenn der Täter die manipulierte Software zur unberechtigten Nutzung von digitalen Inhalten verwendet.

- *Einsatz von Piraten-SmartCards beim digitalen TV*

  In Betracht kommt § 263a StGB auch beim Einsatz – nicht jedoch bei der Erstellung, dem Nachbau oder dem Vertrieb – von so genannten Piraten-SmartCards zur Entschlüsselung des digitalen Pay-TV.[390] Piraten-SmartCards sind – wie oben erläutert – entweder modifizierte Original-SmartCards, die weitergehende Berechtigungen enthalten als das Vertragsverhältnis zwischen Kunde und Programmanbieter vorsieht[391] oder aber so genannte Digital Pirate SmartCards, also Nachbauten von Originalkarten. Werden Piraten-SmartCards zur Entschlüsselung der Videodaten eines Programmanbieters in einem Digital-Receiver verwendet, so liegt eine unbefugte Verwendung von Daten vor, die einen Datenverarbeitungsvorgang beeinflusst.[392] Dabei handelt es sich um einen frem-

390. Vgl. *Beucher*/*Engels*, CR 1998, 101, 104.
391. Vgl. *Scheffler*, CR 2002, S. 151.
392. Vgl. BGH CR 2002, 413 zum Fall einer gefälschten EC-Karte. Siehe auch *Beucher*/*Engels*, CR 1998, 101, 104; *Dressel*, MMR 1999, 390, 392; *Scheffler*, CR 2002, 151, 152.

den Datenverarbeitungsvorgang, weil dieser mittels des im Digital Receiver eingebauten CAMs und mittels der SmartCard vom Opfer gesteuert wird. Die Unbefugtheit ergibt sich daraus, dass eine entsprechende SmartCard zur Entschlüsselung nur von zahlenden Kunden des Programmanbieters verwendet werden darf und mit der Benutzung einer Piraten-SmartCard die Software des CAM darüber getäuscht wird, dass eine Berechtigung zur Entschlüsselung nicht vorliegt. Auch ein unmittelbarer Vermögensschaden kann bejaht werden, wenn man davon ausgeht, dass unmittelbar durch die unberechtigte Entschlüsselung der Videodaten dem Programmanbieter Gewinn entgeht.[393] Soweit ein softwarebasiertes Zusatzmodul – welches gehackte Entschlüsselungsinformationen enthält – eingesetzt wird, um an einem Computersystem die verschlüsselten Programme der Pay-TV Anbieter anschauen zu können, ergeben sich hinsichtlich § 263a StGB keine Abweichungen zu dem zur Verwendung von Piraten-SmartCards Gesagten. Dies beruht darauf, dass die technischen Abläufe vom Prinzip her identisch sind. Das Zusatzmodul entspricht in seiner Funktion einer SmartCard. Die entsprechenden Handlungen werden damit durch § 263a StGB erfasst.

4. § 265a StGB

a) Überblick

§ 265a StGB bedroht denjenigen mit einer Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe, „der die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Fernmeldenetzes, die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht erschleicht, das Entgelt nicht zu entrichten“. Die Tatbestandsalternative der Erschleichung des Zutritts zu einer Veranstaltung ist dabei im vorliegend untersuchten Bereich nicht anwendbar, da für diese Tatbestandsalternative eine körperliche Anwesenheit des Täters in der Veranstaltung erforderlich ist.[394] Auch die Erschleichung der Leistungen eines öffentlichen Zwecken dienenden Telekommunikationsnetzes liegt in den Fällen der Nutzung einer Piraten-SmartCard zur Entschlüsselung eines Pay-TV Angebotes nicht vor, da insoweit schon nicht die von einem öffentlichen Telekommunikationsnetz erbrachte Dienstleistung betroffen ist.[395] Vorliegend kommt daher nur die Erschleichung einer Automatenleistung in Betracht, die im folgenden näher untersucht werden soll.

b) Erschleichen einer Automatenleistung

Eine Automatenleistung im Sinne von § 265a StGB liegt immer dann vor, wenn eine selbsttätige und zwangsläufige Erbringung einer Leistung durch ein technisches Gerät erfolgt, „welches über ein mechanisches oder elektronisches Steuersystem verfügt und durch Entrichtung des vorgeschriebenen Entgelts oder mittels einer Code- oder Wertkarte in Funktion gesetzt wird.[396] Im

393. In diesem Sinne wohl auch *Dressel*, MMR 1999, 390, 392; *Scheffler*, CR 2002, 151, 154 f.; siehe aber auch *Beucher*/*Engels*, CR 1998, 101, 104.
394. Vgl. LK/*Tiedemann*, § 265a Rn. 32.
395. Vgl. Sch/Sch-*Lenckner*/*Perron*, § 265a Rn. 10 a.E. A.A. *Ory*, Rechtsfragen des Abonnementfernsehens, ZUM 1988, 225, 229, der auch bei einer unberechtigten Entschlüsselung von Pay-TV Angeboten annimmt, dass die Leistung eines Fernmeldenetzes erschlichen wird; siehe auch LK/*Tiedemann*, § 265a Rn. 44, 58.
396. Vgl. LK/*Tiedemann*, § 265a Rn. 20.

Hinblick auf die erfassten Leistungen wird der Tatbestand des § 265a StGB dabei aus historischen Gründen und wegen seiner Konkurrenz zu § 242 StGB auf Leistungsautomaten, d.h. die Erbringung unkörperlicher Leistungen, beschränkt.[397] Aufgrund dieser Vorgaben kommt § 265a StGB vorliegend in Betracht, wenn mittels einer Piraten-SmartCard und einem Digital-Receiver ein Pay-TV Angebot vom Täter genutzt wird, da in diesem Fall eine Codekarte eingesetzt wird, die das technische Gerät – insbesondere das CAM – dazu veranlasst, die verschlüsselten Daten zu entschlüsseln.[398] Gegen eine solche Anwendung des § 265a StGB könnte zwar vorgebracht werden, dass in den klassischen Fällen der Leistungserschleichung – z.B. bei Spiel- oder Musikautomaten – der Automat nicht im Eigentum des Täters steht, während der verwendete Digital-Receiver häufig vom Täter käuflich erworben sein dürfte. Wie bereits bei § 263a StGB dargestellt, kommt es jedoch auch hier nicht auf das Eigentum an der Hardware an, sondern auf die Zuordnung des konkreten Datenverarbeitungsvorgangs bzw. der konkreten Leistungserbringung. Der im CAM ablaufende Datenverarbeitungsvorgang der Entschlüsselung ist jedoch dem Diensteanbieter – also dem Pay-TV Anbieter – zugeordnet, der nur berechtigten Inhabern einer SmartCard den Zugang zu den verschlüsselten Informationen gestatten will.[399] Das Erschleichen der Leistung – also die Betrachtung des entschlüsselten Fernsehprogramms – erfolgt in diesen Fällen im übrigen auch unbefugt, da die eingesetzten Piraten-SmartCards vom Pay-TV Anbieter nicht zur Erbringung einer Leistung bestimmt sind.[400]

Die Anwendbarkeit von § 265a StGB im Bereich der Umgehung von Schutzmechanismen kann letztlich allerdings in den meisten hier relevanten Fällen dahinstehen, da diese Vorschrift dann nicht eingreift, wenn die Tat in einer anderen vermögensschützenden Vorschrift mit einer schweren Strafe bedroht ist.[401] Wie oben bereits dargestellt, ergibt sich bei der Verwendung einer Piraten-SmartCard regelmäßig eine Strafbarkeit nach dem schwereren Delikt des § 263a StGB.

5. § 303a StGB

a) Übersicht

Während die Umgehung von Schutzmechanismen bei den §§ 17 UWG, 202a StGB unter dem Gesichtspunkt der Verschaffung geheimer oder gesicherter Daten und bei § 263a StGB unter dem Gesichtspunkt der vermögensschädigenden Beeinflussung eines Datenverarbeitungsvorgangs beurteilt wird, stellen die §§ 303a, b StGB auf einen hiervon zu unterscheidenden anderen Gesichtspunkt ab, nämlich die bei der Umgehung von Schutzmechanismen erfolgende Datenveränderung oder Datenlöschung.

§ 303a StGB bedroht denjenigen mit Freiheitsstrafe bis zu zwei Jahren, der „rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert“. In den von § 303b StGB qualifizierten Fällen beträgt die Freiheitsstrafe bis zu fünf Jahren. Nach § 303c StGB wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

397. Vgl. LK/*Tiedemann*, § 265a Rn. 21.
398. So im Ergebnis *Beucher*/*Engels*, CR 1998, 101, 104 f.
399. Vgl. auch *Beucher*/*Engels*, CR 1998, 101, 105.
400. So auch *Beucher*/*Engels*, CR 1998, 105.
401. Vgl. LK/*Tiedemann*, § 265a Rn. 57.

b) Begrenzung des Tatbestandes auf „fremde Daten“

Für die Beurteilung der Umgehung von Schutzmechanismen ist bei § 303a StGB vor allem die Frage relevant, inwieweit der Tatbestand im Hinblick auf die Verfügungsbefugnis an den das Tatobjekt bildenden Daten einzugrenzen ist. Damit der Tatbestand von § 303a StGB seine Funktion der Umschreibung von typischem Unrecht erfüllt, muss sein Tatobjekt auf Daten beschränkt werden, an denen ein anderer ein bestimmtes Interesse besitzt. Aufgrund der systematischen Stellung von § 303a StGB im Bereich der Sachbeschädigungsdelikte muss dieses Interesse allerdings in einer eigentümerähnlichen Stellung bestehen. Wegen der immateriellen Natur des Tatobjekts von § 303a StGB kommt es für diese Verfügungsbefugnis jedoch nicht auf das Sacheigentum am Datenträger an, sondern auf eine Verfügungsberechtigung an den Daten selbst.[402]

Eine derartige Verfügungsbefugnis kann sich nach der Literatur z.B. aus einem Besitz- oder Nutzungsrecht ergeben; persönlichkeitsrechtliche Befugnisse im Hinblick auf die Daten reichen dagegen nicht aus. Eine Verfügungsberechtigung an den Daten setzt damit jedenfalls nicht voraus, dass sich die Daten im Besitz des Verfügungsberechtigten befinden.

Im Hinblick auf die Anlehnung von § 303a StGB an den das Sacheigentum schützenden § 303 StGB ist jedoch eine umfassende Verfügungsbefugnis erforderlich, die dem Volleigentum an Sachen entspricht. Diese Position des Volleigentums ist nach § 903 BGB durch die beiden Befugnisse geprägt, mit der Sache nach Belieben zu verfahren und andere Personen von der Nutzung auszuschließen. Einzelne Ansprüche zur Einwirkung auf die Daten – wie die oben erwähnten persönlichkeitsrechtlichen Befugnisse – sind damit nicht vergleichbar. Befugnisse des Rechteinhabers an einem DRM-System oder des Verwenders eines Kopierschutzmechanismus gegen Personen, die diese Schutzmechanismen auf eigenen Datenträgern manipulieren, stellen – anders als bei der vergleichbaren Fragestellung im Rahmen von § 263a StGB – insoweit keine umfassende Befugnis über den jeweiligen Datenbestand dar, welche die Daten für ihren Besitzer zu „fremden“ Daten machen. Eine derartig weitreichende Ausdehnung des § 303a StGB auf die Beeinträchtigung von Einzelansprüchen im Hinblick auf Daten kann nicht im Wege der Ausdehnung von § 303a StGB durch die Rechtsprechung, sondern nur durch den Gesetzgeber erfolgen. Dies zeigt sich für den vorliegend interessierenden Bereich auch sehr deutlich in dem Vorschlag der neuen §§ 95a, 108b UrhG in der Fassung des Referentenentwurfs für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft,[403] welche die Umgehung von bestimmten Sicherungsmaßnahmen nur unter bestimmten Voraussetzungen verbieten und kriminalisieren. Würde man § 303a StGB durch eine weite Ausdehnung der „fremden“ Daten zu einer „Supernorm“ bei der Erfassung von Interessenverletzungen an gespeicherten Daten machen, würden die Neuregelungen und Differenzierungen der §§ 95a, 108b UrhG-E überflüssig bzw. eingeebnet.

Hinzu kommt, dass auch die in § 303a StGB vorgesehenen Tathandlungen des Löschens, Unterdrückens, Unbrauchbarmachens oder Veränderns die hier relevanten Vorgänge weitestgehend nicht erfassen können.[404] Denn bei der Entschlüsselung von Inhalten und sogar beim Auslesen von Informationen, z.B. aus einer Original-SmartCard werden Daten zwar regelmäßig gespeichert und später verwendet, aber nicht verändert oder sonst beeinträchtigt.

402. So auch *Bandekow*, S. 263 f.
403. Siehe oben Fn. 196.
404. Siehe auch *Beucher*/*Engels*, CR 1998, 101, 105.

6. § 269 StGB

a) Übersicht

§ 269 StGB schützt die Zuverlässigkeit des Rechts- und Beweisverkehrs. Er bedroht denjenigen mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe, der „zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht." Gem. § 270 StGB steht der Täuschung im Rechtsverkehr die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich.

b) Kritische Merkmale im Hinblick auf die Umgehung von Schutzmechanismen

Die strafrechtliche Beurteilung der Umgehung von Schutzmechanismen unter dem Gesichtspunkt des § 269 StGB hängt zunächst entscheidend davon ab, wann *beweiserhebliche Daten* vorliegen. Nach dem Willen des Gesetzgebers sollen dies solche Daten sein, die dazu bestimmt sind, bei einer Verarbeitung im Rechtsverkehr als Beweisdaten für rechtlich erhebliche Tatsachen benutzt zu werden. [405] Gemeint sind damit insbesondere Daten, die verwendet werden, um gegenüber einer Maschine eine Berechtigung nachzuweisen. Dies gilt klassischerweise bei der Benutzung einer EC-Karte, da hier der Verwender durch Eingabe der PIN gegenüber dem Bankautomaten (der die Bank repräsentiert) erklärt, er sei zur Vornahme von Bankgeschäften berechtigt. In Betracht kommt § 269 StGB damit im vorliegenden Kontext allenfalls im Hinblick auf die Verwendung von Zugangscodes zur Entschlüsselung digitaler Inhalte und von Piraten-SmartCards zur Entschlüsselung digitaler Pay-TV Angebote. Allerdings dienen die Entschlüsselungscodes und SmartCards insoweit nicht der Kontrolle der Berechtigung (sie müssen nur angewendet werden), sondern stellen unmittelbar den Zugang zu den Informationen her.[406] Sie sind damit letztlich nur Teil des Entschlüsselungsprozesses.[407] Gleichwohl halten *Beucher*/*Engel* ein Vorliegen von beweiserheblichen Daten zumindest bei der Verwendung von SmartCards nicht von vornherein für ausgeschlossen, weil der Verwender mit ihrem Einsatz konkludent auch erklären soll, er sei zur Entschlüsselung berechtigt.[408] Entsprechend kommt daher auch bei der Zwangsaktivierung von Softwareprodukten § 269 StGB in Betracht, weil beweiserhebliche Daten gespeichert oder verändert werden, wenn durch die Eingabe falscher Informationen eine Berechtigung zur dauerhaften Freischaltung der betreffenden Software nachgewiesen wird.

Wenn man insbesondere bei der unberechtigten Entschlüsselung von digitalen Inhalten vom Vorliegen beweiserheblicher Daten ausgeht, so stellt sich weiter die Frage, ob der Täter dadurch auch eine Täuschung im Rechtsverkehr bzw. eine fälschliche Beeinflussung einer Datenverarbeitung (§ 270 StGB) vornehmen möchte. Auch dies wird man nicht von vornherein ablehnen können, da die Entschlüsselung deshalb erfolgt, weil z.B. der den Programmanbieter repräsentierende Digital Receiver aufgrund der „richtigen" Daten auf der SmartCard von einer Berechtigung des Verwenders ausgeht. Auch hier handelt der Täter, um eine fälschliche Beeinflussung einer Datenverarbeitung vorzunehmen.

405. Siehe LK/Gribbohm, § 269 Rn. 9.
406. Vgl. Vgl. *Beucher*/*Engels*, CR 1998, 101, 105.
407. Vgl. *Beucher*/*Engels*, CR 1998, 101, 105.
408. vgl. Vgl. *Beucher*/*Engels*, CR 1998, 101, 105.

Gleichwohl scheidet § 269 StGB in diesen und anderen Fällen der Umgehung von Sicherungsmaßnahmen aus, weil die das Tatobjekt bildenden Daten nach dem Gesetz bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde darstellen müssten: Das bei dieser hypothetischen Betrachtung geforderte Merkmal der Urkunde verlangt unter anderem, dass die Daten eine bestimmte Erklärung enthalten, die ihren Aussteller erkennen lässt. Das Erfordernis der unechten oder verfälschten Urkunde ist darüber hinaus nur erfüllt, wenn durch die Umgehung der Schutzmechanismen über den Aussteller getäuscht wird. Diese Anforderungen sind – wie der empirische Teil oben zeigt – bei der Umgehung von Sicherungsmechanismen von digitalen Gütern in der Regel nicht erfüllt: Im Bereich der Daten von Sicherungsmechanismen ist es schon schwierig, irgendwelche Erklärungen zu finden oder zu konstruieren, die einem bestimmten Aussteller zugerechnet werden können. Bei den entsprechenden Manipulationen wird jedoch vor allem auch nicht über den Aussteller irgendwelcher Erklärungen getäuscht, vielmehr werden unbefugte Dateneingaben sowie Umgehungen von Kopierschutzmechanismen vorgenommen. Dies zeigt sich z.B. bei den oben genannten Piraten-SmartCards: Werden die dort abgelegten Informationen zur Entschlüsselung von Videodaten verwendet, so spielt es für den technischen Vorgang der Entschlüsselung keine Rolle, von wem die SmartCard bzw. die darauf befindlichen Informationen stammen. Es kommt darauf an, ob es sich um Schlüsselinformationen handelt, die zur Entschlüsselung zugelassenen sind. M.a.W.: Für diesen Vorgang ist es bedeutungslos, wer Aussteller der Informationen ist, wichtig ist alleine dass die Integrität der Entschlüsselungsinformationen gewahrt ist. Die Vorschrift des § 269 StGB hat daher im vorliegenden Zusammenhang keine wesentliche Bedeutung.

7. §§ 4, 5 ZKDSG

Das unten im Zusammenhang mit der Verbreitung von Umgehungseinrichtungen näher erörterte „Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (Zugangskontrolldiensteschutz-Gesetz – ZKDSG) vom 19. März 2002[409] bedroht in §§ 4 und 5 die Herstellung, die Einfuhr und die Verbreitung von Umgehungseinrichtungen für bestimmte zugangskontrollierte Dienste zu gewerblichen Zwecken mit Freiheitsstrafe von bis zu einem Jahr oder mit Geldstrafe. Es enthält jedoch keine Strafvorschrift gegen das eigentliche Umgehen eines Zugangskontrolldienstes. Dies dürfte zum einen auf der – durch Gründe der Gesetzgebungskompetenz bedingten – begrenzten Reichweite der zugrunde liegenden EG-Richtlinie beruhen,[410] zum anderen auf der Annahme des Gesetzgebers, dass die entsprechenden Umgehungshandlungen bereits strafrechtlich (z. B. durch § 265a StGB) erfasst werden.

409. BGBl 2002 I, S. 1090 f.

410. Vgl. Richtlinie des Europäischen Parlaments und des Rates über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten vom 20. November 1998, ABl. L 20/54 v. 18.11.1998. Die (im Hinblick auf allgemeine Strafvorschriften) begrenzte Reichweite der Richtlinie beruht darauf, dass der Europäische Gesetzgeber keine originäre Kompetenz zum Erlass von Strafnormen hat, sondern (strafrechtliche) Schutznormen nur auf der Grundlage einer Annexkompetenz in Bereichen fordern kann, in denen er eine durch den EG-Vertrag zugewiesene anderweitige Sachkompetenz besitzt. Vgl. dazu und zu den Fragen der demokratischen Legitimation des europäischen Gesetzgebers bei der Strafrechtsharmonisierung durch Verordnungen und Richtlinien *Sieber*, Europäische Einigung und Europäisches Strafrecht, ZStW Bd. 103 (1991), S. 957 ff.

8. § 108b Abs. 1 i.V.m §§ 95a Abs. 1, 2, 95c UrhG-E

a) Allgemeine Problematik

Im Hinblick auf die Umgehung von Schutzmechanismen kann zukünftig auch dem vom Gesetzentwurf zur Regelung des Urheberrechts in der Informationsgesellschaft[411] vorgeschlagenen §§ 95a Abs. 1, 2, 95c UrhG-E i.V.m. § 108b Abs. 1 UrhG-E Bedeutung zukommen.[412] Der Inhalt des strafrechtlichen Verbotsbereichs dieser Vorschriften ist allerdings schwierig zu erfassen, da er sich nur durch ein kompliziertes Zusammenlesen von mehreren Tatbeständen ergibt, die teilweise ähnliche Merkmale enthalten. Die Komplexität der dadurch entstehenden Verbotsnorm zeigt sich beispielsweise darin, dass der durch das Zusammenlesen entstehende Tatbestand der §§ 108b Abs. 1, 95a Abs. 1 UrhG-E neben den normalen Vorsatzanforderungen insgesamt vier (!) weitere spezielle subjektive Merkmale verlangt (Absicht der Zugangserlangung bzw. Nutzungsermöglichung, wenigstens leichtfertige Verletzung von Urheberrechten, kein Handeln zum persönlichen Gebrauch in § 108b Abs. 1 UrhG-E sowie Kenntnis oder Kennenmüssen der Zugangs- oder Nutzungsermöglichung in § 95a Abs. 1 UrhG-E). Nicht nur für den juristischen Laien, sondern auch für viele Juristen dürfte der Inhalt der neuen Strafbestimmungen dadurch nur schwer verständlich sein. Hinzu kommt, dass die subjektiven Anforderungen an die in den §§ 108a Abs. 1, 95a Abs. 1 UrhG-E normierte eigentliche Verbotshandlung (d.h. an die Umgehung technischer Schutzmaßnahmen) sehr viel strenger sind als an die in den §§ 108b Abs. 2, 95a Abs. 3 UrhG-E verbotenen Vorbereitungshandlungen (d.h. an die Herstellung, Einfuhr oder Verbreitung von hierzu geeigneten Hilfsmitteln). Da dieser Wertungswiderspruch – auch in der Begründung des Regierungsentwurfs – nicht erklärt oder irgendwie plausibel gemacht wird, kann nicht ausgeschlossen werden, dass möglicherweise auch die Verfasser des Gesetzentwurfs Opfer der Komplexität ihrer Verweisungstechniken und Differenzierungen wurden. Ein entsprechender Wertungswiderspruch zwischen der eigentlichen Tathandlung der Umgehung von Sicherungsmechanismen und ihren Vorfeldtatbeständen besteht im übrigen auch im Hinblick auf die Privilegierung des persönlichen Gebrauchs, die sich bei der Umgehung der Schutzmechanismen findet, nicht jedoch bei den entsprechenden Vorbereitungshandlungen: Die Umgehung der technischen Schutzmaßnahmen zum persönlichen Gebrauch soll daher nach dem Regierungsentwurf straflos bleiben, die Herstellung oder die Einfuhr der hierfür erforderlichen Tools zum privaten Gebrauch soll dagegen mit Freiheitsstrafe bis zu einem Jahr bestraft werden. Zur Erklärung des Regierungsentwurfs lässt sich daher nur anführen, dass dieser sich teilweise am Wortlaut der einschlägigen EG-Richtlinie orientiert, in der diese Widersprüche bereits angelegt sind. Die – durch die EG-Richtlinie allerdings nicht geforderte – Begrenzung des Vorfeldschutzes von § 108b Abs. 2 UrhG-E auf gewerbliches Handeln kann die Wertungswidersprüche jedenfalls nicht begründen, da gewerbliches Handeln bei objektiv neutralen Verhaltensweisen (wie dem Handel mit Dual-use-Produkten) keinen Unrechtgehalt aufweist.

411. Siehe oben Fn. 238.

412. Die Bestimmungen beruhen auf Art. 6 Abs. 1 – 4, und Art. 7 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft vom 22. Mai 2001, ABl. L 167/10 ff. v. 22.6.2001.

b) §§ 108b Abs. 1 Nr. 1, 95a Abs. 1 UrhG-E

Der Inhalt der wichtigsten gesetzlichen Regelung von §§ 108b Abs. 1 Nr. 1, 95a Abs. 1 UrhG-E wird aufgrund der vorgenannten Probleme am besten verständlich, wenn zunächst das zivilrechtliche Verbot des § 95a Abs. 1 und 2 UrhG-E und dann die zusätzlichen Merkmale des § 108b Abs. 1 UrhG-E betrachtet werden: Nach § 95a Abs. 1 UrhG-E dürfen ohne Zustimmung des Rechtsinhabers *wirksame technische* Maßnahmen zum Schutz eines nach dem Urheberrechtsgesetz geschützten Werkes oder eines anderen nach diesem Gesetz geschützten Schutzgegenstandes nicht umgangen werden, soweit dem Handelnden bekannt ist oder den Umständen nach bekannt sein muss, dass die Umgehung erfolgt, um den Zugang zu einem solchen Werk oder Schutzgegenstand oder deren Nutzung zu ermöglichen.

Nach § 95a Abs. 2 S. 1 UrhG-E sind technische Maßnahmen im Sinne des Gesetzes Technologien, Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, geschützte Werke und andere (nach dem Urheberrechtsgesetz geschützte Schutzgegenstände betreffende) Handlungen, die nicht vom Rechtsinhaber genehmigt sind, zu verhindern oder zu beschränken. Für deren Wirksamkeit verlangt § 95a Abs. 2 S. 2, dass durch die technischen Maßnahmen die Nutzung des geschützten Werks oder eines sonstigen Schutzgegenstandes von dem Rechtsinhaber unter Kontrolle gehalten wird und zwar entweder durch eine Zugangskontrolle oder einen Schutzmechanismus wie Verschlüsselung, Verzerrung sowie sonstige Umwandlung oder einen Mechanismus zur Kontrolle der Vervielfältigung, der die Erreichung des Schutzziels sicherstellt. Gemeint ist damit z.B. die Umgehung eines Schutzmechanismus, der verhindern soll, dass ein Werk kopiert oder auf eine bestimmte Art und Weise genutzt werden kann.[413]

Nimmt man den Wortlaut hinsichtlich der Voraussetzungen für eine wirksame technische Maßnahmen Ernst, so hätte es der Verbotsnorm des § 95a Abs. 1 UrhG-E überhaupt nicht bedurft: Würden hierunter nur Schutzmechanismen fallen, welche eine Erreichung des Schutzziels *sicherstellen*, so bedeutete dies im Umkehrschluss, dass gehackte Schutzmechanismen schon gar nicht vom Tatbestand erfasst würden.[414] Dies macht aber offensichtlich keinen Sinn. Daher muss der Begriff der wirksamen technischen Maßnahme anders ausgelegt werden. Die Gesetzesbegründung zum Regierungsentwurf für ein Gesetz zur Regelung der Urheberrechte in der Informationsgesellschaft geht deswegen davon aus, dass „technische Maßnahmen grundsätzlich auch dann wirksam sein können, wenn ihre Umgehung möglich ist".[415] Wirksame Schutzmechanismen dürften daher solche sein, die zwar nicht absolut sicher sind, jedoch in der Praxis eine so hohe Hürde darstellen, dass es eines erheblichen Aufwandes bedarf, um sie umgehen zu können. Der Schutzmechanismus muss somit gegenüber einem Durchschnittsnutzer wirken.[416]

Liegt eine Umgehung wirksamer technischer Maßnahmen vor, so ist die handelnde Person gleichwohl nach § 108b Abs. 1 Nr. 1 UrhG-E nicht strafbar, wenn die Tat ausschließlich zum eigenen privaten Gebrauch des Handelnden oder mit ihm persönlich verbundener Personen erfolgt oder wenn sich die Tat auf einen derartigen Gebrauch bezieht. Diese Privilegierung erweist sich vor allem dann als fragwürdig, wenn man den Verbotsbereich dieser Norm mit dem – diese Privilegierung nicht enthaltenden – Verbotsbereich der bereits erwähnten Vorbereitungshandlungen vergleicht. Auch aus weiteren Gründen ist die Privilegierung problematisch. Hierauf

413. Vgl. *Bayreuther*, ZUM 2001, 828, 838.
414. Vgl. *Spindler*, GRUR 2002, 105, 116; *Linnenborn*, K&R 2001, 394, 397.
415. Siehe oben Fn. 196.
416. So ifrOSS, oben Fn. 270, S. 5; KirchMedia, oben Fn. 266, S. 10; *Kröger*, CR 2001, 316, 322; *Linnenborn*, K&R 2001, 394, 397; *Spindler*, GRUR 2002, 105, 116; VPRT, oben Fn. 312, S. 4

wird bei der rechtspolitischen Analyse zurückzukommen sein.

Erfolgt die Tat gewerbsmäßig, so sieht das Gesetz – statt der ansonsten vorgesehenen Freiheitsstrafe von bis zu einem Jahr oder Geldstrafe – eine Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe vor. Eine Strafbarkeit erfordert dabei allerdings stets, dass der Täter in der Absicht handelt, sich oder einem Dritten den Zugang zu einem nach dem Urheberrechtsgesetz geschützten Werk oder einem anderen nach diesem Gesetz geschützten Schutzgegenstand oder deren Nutzung zu ermöglichen. Damit wird der Anwendungsbereich der Strafvorschrift schon deshalb stark eingeengt, weil eine entsprechende Absicht in vielen Fällen nur schwer zu beweisen sein wird. Auch wenn der Gesetzgeber nach der Gesetzesbegründung vor allem Umgehungshandlungen aus dem Anwendungsbereich des § 95a Abs. 1 UrhG-E herausnehmen möchte, die ausschließlich wissenschaftlichen Zwecken dienen, so stellt sich die Frage, wie zukünftig Handlungen von Hackern zu bewerten sein sollen, die sich aus sportlichem Ergeiz oder Neugier mit den technischen Maßnahmen beschäftigen und anschließend häufig ihre Ergebnisse z.B. im Internet veröffentlichen. Die vom Gesetzentwurf bezweckte Privilegierung der Forschung und der notwendigen öffentlichen Auseinandersetzung mit Sicherheitsfragen sollte deswegen besser durch die positive Normierung einer Rechtfertigungsnorm erfolgen als durch ein für alle Fälle geltendes und erhebliche Nachweisschwierigkeiten verursachendes allgemeines Absichtsmerkmal.

Durch die Tathandlung muss sodann wenigstens leichtfertig die Verletzung von Urheberrechten veranlasst, ermöglicht, erleichtert oder verschleiert werden. Für eine Strafbarkeit reicht es damit nicht aus, dass der Täter nur einfach fahrlässig in Bezug auf die Ermöglichung einer Verletzung von Urheberrechten handelt. Auch dies schränkt den Anwendungsbereich der Strafvorschrift ebenfalls stark ein, da leichtfertiges Handeln der groben Fahrlässigkeit im bürgerlichen Recht entspricht

Werke und andere Schutzgegenstände, die mit technischen Maßnahmen geschützt werden, sind nach § 95d Abs. 1 UrhG-E deutlich sichtbar mit Angaben über die Eigenschaften der technischen Maßnahmen zu kennzeichnen. Diese Kenzeichnungspflicht ist nach der Gesetzesbegründung notwendig, da technische Schutzmechanismen der Konsumentererwartung widersprechen und damit die Kaufentscheidung des Kunden beeinflussen können. Nach der Gesetzesbegründung soll es deswegen der Verbraucherschutz und die Lauterkeit des Wettbewerbs gebieten, dass ein Hinweis auf die verwendeten Schutzmechanismen erfolgt. Dabei darf allerdings nicht übersehen werden, dass die Erfüllung der Kennzeichnungspflicht für die Rechteinhaber unter Umständen einen erheblichen Kostenmehraufwand bedeutet, wenn der Kennzeichnungspflicht nur mit aufwändigen Verfahren entsprochen werden kann.

An der Strafbarkeit ändert sich dabei nichts, wenn ein Schrankenberechtigter – z.B. i.S.d. § 53 Abs. 2 S. 1 Nr. 1 UrhG – zur Selbsthilfe greift und den Schutzmechanismus entfernt: § 95b Abs. 2 UrhG-E und §§ 2a, 3 Unterlassungsklagengesetz-E bestimmen insoweit eindeutig, dass eine Durchsetzung von Schrankenbestimmungen notfalls auf dem Klageweg zu erfolgen hat. Ein Selbsthilferecht des Schrankenberechtigten besteht daher nicht.[417] In diesem Zusammenhang ist auch relevant, dass eine Durchsetzungsmöglichkeit für die Schranke des § 53 Abs. 1 UrhG (Privatkopie) nur für den Fall vorgesehen ist, dass es sich um eine Vervielfältigung auf Papier oder einen ähnlichen Träger mittels beliebiger photomechanischer Verfahren oder andere Verfahren mit ähnlicher Wirkung handelt. D.h.: Für den hier interessierenden Fälle digitaler

417. Vgl. *Dreier*, ZUM 2002, 28, 39; *Goldmann*/*Liepe*, ZUM 2002, 362, 370; *Metzger*/*Kreutzer*, Richtlinie zum Urheberrecht in der Informationsgesellschaft, MMR 2002, 139, 140 f; *Spindler*, GRUR 2002, 105, 117.

Privatkopien besteht gerade keine Durchsetzungsmöglichkeit.[418] Zudem kommt nach § 95b Abs. 3 UrhG-E von vornherein keine Durchsetzung der Schrankenbestimmungen in Betracht, wenn „Werke und sonstige Schutzgegenstände der Öffentlichkeit aufgrund einer vertraglichen Vereinbarung in einer Weise zugänglich gemacht werden, dass sie Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich sind." Dies erfasst vor allem Werke, die im Wege der Online-Nutzung auf vertraglicher Basis zugänglich gemacht werden.[419] Auch hier ist zu beachten, dass nach § 95d Abs. 2 UrhG-E die Werke und anderen Schutzgegenstände zur Geltendmachung der Ansprüche nach § 95b Abs. 2 UrhG-E mit dem Namen oder der Firma sowie einer ladungsfähigen Anschrift des Verwenders technischer Maßnahmen zu versehen sind, wobei sich ebenfalls die oben geäußerten Kostenbedenken ergeben können.

c) §§ 108b Abs. 1 Nr. 2 UrhG-E

Die oben im empirischen Teil erwähnten Watermarks und Fingerprints werden zukünftig durch § 95c UrhG-E vor Entfernung und Veränderung geschützt.[420] Hierzu bestimmt § 95c Abs. 1 UrhG-E, dass vom Rechtsinhaber stammende Informationen für die Rechtewahrnehmung nicht entfernet oder verändert werden dürfen, wenn irgendeine der betreffenden Informationen an einem Vervielfältigungsstück eines Werks oder eines sonstigen Schutzgegenstandes angebracht ist oder im Zusammenhang mit der öffentlichen Wiedergabe eines solchen Werkes oder Schutzgegenstandes erscheint. Hinzu kommen muss allerdings, dass die Entfernung oder Veränderung wissentlich unbefugt erfolgt und dem Handelnden bekannt ist oder den Umständen nach bekannt sein muss, dass er dadurch die Verletzung von Urheber- oder verwandten Schutzrechten veranlasst, ermöglicht, erleichtert oder verschleiert. Was unter Informationen für die Rechtwahrnehmung zu verstehen ist, definiert § 95c Abs. 2 UrhG-E: Es handelt sich dabei um elektronische Informationen, die Werke oder andere Schutzgegenstände, den Urheber oder jeden anderen Rechtsinhaber identifizieren, um Informationen über die Modalitäten und Bedingungen für die Nutzung der Werke oder Schutzgegenstände sowie um Zahlen und Codes, durch die derartige Informationen ausgedrückt werden. Hierunter fallen z.B. die bei DRM-Systemen verwendeten Informationen, die festlegen, wie lange oder in welchem Umfang ein bestimmter Inhalt genutzt werden darf.

Um hierüber hinausgehend auch im „Nachfeld" einer Tat i.S.d. § 95c Abs. 1 UrhG-E einen Schutz zu erreichen, dürfen nach § 95c Abs. 3 UrhG-E Werke und sonstige Schutzgegenstände, bei denen die genannten Informationen unbefugt entfernt oder verändert wurden, nicht wissentlich unbefugt verbreitet, zur Verbreitung eingeführt, gesendet, öffentlich wiedergegeben oder öffentlich zugänglich gemacht werden. Auch insoweit ist aber wiederum Voraussetzung, dass dem Täter bekannt ist oder den Umständen nach bekannt sein muss, dass er dadurch die Verletzung von Urheberrechten oder verwandten Schutzrechten veranlasst, ermöglicht, erleichtert

418. Zwar sieht die EU-Richtlinie 2001/29/EG zum Urheberrecht in der Informationsgesellschaft in Art. 5 Abs. 2 lit. b fakultativ einen Ausnahmetatbestand auch für digitale Privatkopien vor. Der deutsche Gesetzgeber will hiervon aber zunächst keinen Gebrauch machen; vgl. *Bayreuther*, ZUM 2001, 828, 838 f.; *Goldmann/Liepe*, ZUM 2002, 362, 369 f.; *Reinbothe*, ZUM 2002, 43, 49 f.; *Spindler*, GRUR 2002, 105, 118.

419. Vgl. dazu *Dreier*, ZUM 2002, 28, 37; *Flechsig*, ZUM 2001, 1, 16; ifrOSS, oben Fn. 270, S. 8 ff.; *Linnenborn*, K&R 2001, 394, 400 f.; *Metzger/Kreutzer*, MMR 2002, 139, 141 f.; *Spindler*, GRUR 2002, 105, 118 f.

420. Vgl. *Dreier*, ZUM 2002, 28, 39; *Flechsig*, ZUM 2001, 1, 16 f.; *Reinbothe*, ZUM 2002, 43, 51; *Spindler*, GRUR 2002, 105, 119.

oder verschleiert.

Liegt ein Verstoß gegen § 95c Abs. 1 oder Abs. 3 UrhG-E vor, so macht sich der Täter gemäß § 108b Abs. 1 Nrn. 2, 3 UrhG-E strafbar, es sei denn dass die Tat ausschließlich zum eigenen privaten Gebrauch oder mit ihm persönlich verbundener Personen erfolgt oder sich auf einen derartigen Gebrauch bezieht. Auf die obigen kritischen Anmerkungen zu diesem Merkmal kann insoweit verwiesen werden. Erfolgt die Tat gewerbsmäßig, so sieht das Gesetz – statt der ansonsten vorgesehenen Freiheitsstrafe von bis zu einem Jahr oder Geldstrafe – eine Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe vor. Auch hier sind wiederum die oben bei §§ 95a Abs. 1, 108b Abs. 1 Nr. 1 erwähnten Einschränkungen im subjektiven Tatbestand zu beachten.

9. Ergebnis

Fasst man die vorliegenden Prüfungen zusammen, so ist festzustellen, dass die strafrechtliche Erfassung der Umgehung von Schutzmechanismen in vielen Fällen möglich, jedoch nicht umfassend gesichert ist: § 17 UWG greift insbesondere ein, wenn der Täter – wie häufig bei der Umgehung von DRM-Systemen – sich bei der Umgehung der Sicherungsmechanismen Geschäftsgeheimnisse verschafft; der Tatbestand kommt jedoch nicht zur Anwendung, wenn die Betriebsgeheimnisse durch ein massenhaftes Hacking bereits offenkundig geworden sind oder wenn der Täter sich die Betriebsgeheimnisse nur aus „sportlichem Ehrgeiz“ verschafft. Die in den letztgenannten Fallkonstellationen auftreten Strafbarkeitslücken lassen sich allerdings in erheblichem Umfang durch § 202a StGB schließen, dessen Tatobjekt keine Betriebsgeheimnisse, sondern nur gesicherte Daten verlangt und der darüber hinaus auch nicht durch subjektive Absichtsmerkmale eingeschränkt ist. Daneben erfasst § 263a StGB diejenigen Umgehungen von Sicherheitsmechanismen, in denen es – wie häufig beim Einsatz von SmartCards – zu einer unmittelbaren Vermögensverfügung durch einen dem Opfer zurechenbaren Datenverarbeitungsvorgang (auch auf der Hardware des Täters) kommt. Die – bereits gesetzestechnisch missglückte – Neuregelung des § 108b UrhG in der Fassung des Regierungsentwurfs für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft enthält darüber hinaus zwar das Verbot der Umgehung wirksamer technischer Maßnahmen sowie das Verbot der Entfernung oder Veränderung von Fingerprints und Watermarks; diese Verbote greifen jedoch in einer großen Zahl der vorliegend analysierten Fälle nicht, da die vorgeschlagene Strafnorm bei einem Handeln zum eigenen persönlichen Gebrauch ausscheiden soll. Strafbarkeitslücken bleiben damit insbesondere bei der 1:1 Kopie von Datenträgern, auch wenn diese mit einem Kopierschutzmechanismus versehen sind.

Die strafrechtliche Erfassung der Umgehung von Schutzmechanismen erfordert damit in vielen Fällen komplizierte rechtliche Konstruktionen und wirft auch schwierige Rechtsfragen auf. Für eine strafrechtliche Erfassung ist auch häufig eine detaillierte Analyse komplizierter technischer Sachverhalte erforderlich, wie sie in der obigen empirischen Analyse erarbeitet wurde. Eine strafrechtliche Verfolgung der Umgehung von Sicherungsmechanismen wird dem Rechtsanwender und insbesondere den Strafverfolgungsbehörden daher nicht leicht gemacht. Der im Gesetzentwurf zur Regelung des Urheberrechts in der Informationsgesellschaft vorgeschlagene neue § 108b Abs. 1 UrhG-E nutzt aufgrund seiner missglückten Gesetzgebungstechnik und falschen Grundentscheidungen die Chance nicht, hier zu klaren und effektiven Regelungen zu kommen.

E. Öffentliches Angebot und Besitz von Tools zur Umgehung von Schutzmechanismen

1. Problemstellung

Die vorstehend im Hinblick auf ihre strafrechtliche Relevanz untersuchte Umgehung von Schutzmechanismen führt zwar zu einer Gefährdung der Rechte der Nutzungsberechtigten, jedoch noch nicht zur eigentlichen materiellen Schädigung. Zu dieser Schädigung kommt es – wie die empirische Analyse gezeigt hat – erst durch weitere Handlungen, bei denen zwei unterschiedliche Vorgehensweisen der Raubkopierer zu unterscheiden sind:

- Zum einen werden die entschlüsselten digitalen Inhalte – ebenso wie die oben untersuchten ungeschützten Werke – in entschlüsselter Form über Tauschbörsen oder spezielle Server des Internets anderen Nutzern angeboten. Für diese Vertriebsform der ursprünglich durch Schutzmechanismen geschützten Werke gelten die obigen Ausführungen über das öffentliche Angebot von urheberrechtlich geschützten Werken entsprechend. Sie werden deswegen nach den oben dargestellten Grundsätzen insbesondere durch die §§ 106, 108 UrhG i.V.m. § 17 UrhG strafrechtlich erfasst. Diese Vertriebsschiene der Verbreitung der entschlüsselten digitalen Werke braucht daher im folgenden nicht näher untersucht zu werden.

- Die §§ 106, 108 UrhG greifen dagegen bei der zweiten oben herausgearbeiteten Vertriebstechnik der Raubkopierer nicht ein, bei der nicht die urheberrechtlich geschützten Werke verbreitet werden, sondern nur die Entschlüsselungsinformationen und andere Hackingtools, die dann den Empfängern dieser Daten die Möglichkeit geben, die durch Schutzmechanismen geschützten Inhalte auf ihrem eigenen Rechner zu entschlüsseln und entgegen den Vorgaben zu verwerten. Bei dieser „Vertriebsschiene“ hängt ein strafrechtliches Vorgehen entscheidend davon ab, inwieweit das öffentliche Angebot, die (auch: nichtöffentliche) Weitergabe und eventuell sogar schon der Besitz der Entschlüsselungsinformationen strafrechtlich erfasst werden, soweit nicht im Einzelfall – wie oben erwähnt – § 17 UWG unter dem Gesichtspunkt eingreift, dass dem Empfänger in dem Tool ein Betriebsgeheimnis verschafft wird.

Für die damit entscheidende Frage nach der Strafbarkeit des öffentlichen Anbietens, der Weitergabe und des Besitzes von fremden Entschlüsselungsinformationen und von sonstigen Hackingwerkzeugen sind insbes. die folgenden Strafvorschriften in Betracht zu ziehen:

- Da und soweit der Einsatz der Entschlüsselungsinformationen und der sonstigen Hackingwerkzeuge nach den vorgenannten Ausführungen strafbar ist, kommt zunächst eine Anstiftung zu den entsprechenden Entschlüsselungs- und Missbrauchshandlungen der Empfänger bzw. ein öffentliches Auffordern zu den insoweit begangenen Straftaten in Betracht.

- Daneben sind deliktsspezifische Vorfeldtatbestände über die Verbreitung und den Besitz von Umgehungseinrichtungen zu berücksichtigen, wie sie sich de lege lata in den §§ 4, 5 des „Gesetzes über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (Zugangskontrolldiensteschutz-Gesetz – ZKDSG)[421] finden und wie sie de

421. Siehe oben Fn. 237.

lege ferenda von § 108b i.V.m. § 95a Abs. 3 UrhG-E in der Fassung des Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft[422] und von Art. 6 der Convention on Cybercrime[423] vorgeschlagen bzw. empfohlen werden.

Diese Bestimmungen und Lösungsansätze sind im folgenden näher zu untersuchen.

2. Klassische Ansätze der Anstiftung und der Aufforderung zu Straftaten

a) Anstiftung und Beihilfe

Erfordernis der rechtswidrigen Haupttat

Die Vorschriften der Anstiftung (§ 26 StGB) und der Beihilfe (§ 27 StGB) setzen zunächst eine *rechtswidrige Tat (sog. Haupttat)* eines anderen voraus. Wie bereits oben bei der Untersuchung der Strafbarkeit des Kopiervorganges ausgeführt, kann diese Haupttat in der Mehrzahl der Fälle nicht in der Vervielfältigung der digitalen Güter durch den Nutzer gesehen werden, da und soweit dieser unter dem Gesichtspunkt der Herstellung einer Privatkopie gem. § 53 UrhG straflos ist. Die Vorschriften der Anstiftung und Beihilfe kommen daher von vornherein nur in den Fällen in Betracht, in denen sich die Strafbarkeit des Nutzers unter dem vorstehend erörterten Gesichtspunkt der Umgehung von Schutzmechanismen ergibt. Dies sind insbesondere die Fälle, in denen oben eine Anwendbarkeit der §§ 17 UWG und § 263a StGB bejaht wurde.

Aber auch in diesen Fällen des Vorliegens einer strafbaren Haupttat scheitert die Konstruktion einer Anstiftung oder Beihilfe in der Regel an der fehlenden Konkretisierung des Anstifter- oder Gehilfenvorsatzes. Denn sowohl bei der Anstiftung als auch bei der Beihilfe ist es erforderlich, dass der Vorsatz des Anstifters bzw. Gehilfen als „Doppelvorsatz“ nicht nur auf die von ihm begangene Anstiftungs- oder Beihilfehandlung gerichtet sein muss, sondern jeweils auch auf eine konkret bestimmte Haupttat.

Konkretisierung des Anstiftervorsatzes

Für eine Anstiftungshandlung i.S.d. § 26 StGB genügt zwar jede Verursachung des Tatentschlusses,[424] gleich durch welches Mittel,[425] so dass insbesondere auch das Bereitstellen einer Anleitung oder eines technischen Mittels (wie einer Hacking-Software oder einer Piraten-SmartCard) ausreichen kann, wenn der Täter zumindest mit der ernsthaften Möglichkeit rechnet (dolus eventualis), dass ein anderer dadurch motiviert wird, eine strafbare Tat zu begehen.

Auf eine Haupttat hinreichend konkretisiert ist der Anstiftervorsatz aber nur dann, wenn ihm die Vorstellung einer in ihren Grundzügen, namentlich ihrem wesentlichen Unrechtsgehalt und ihrer Angriffsrichtung, umrissenen Tat zugrunde liegt.[426] Insbesondere genügt es nicht, dass die Haupttat nur nach dem gesetzlichen Tatbestand oder abstrakten Tattyp oder nach abstrakten

422. Siehe oben Fn. 196.
423. Siehe oben Fn. 239.
424. Auch bloße Mitursächlichkeit genügt, BGHSt 45, 373, 374; BGH NStZ 2000, 421.
425. BGHSt 2, 279; BGH NStZ 2000, 421. Soweit in der Literatur einschränkend gefordert wird, es müsse sich um eine „kommunikative Beeinflussung“ handeln, würde das für das Bereitstellung von Anleitungen zur Umgehung von Schutzmechanismen im Ergebnis nichts ändern.
426. St. Rspr., vgl. etwa BGHSt 42, 332 m.w.N.

Tatobjekten umschrieben ist. Erforderlich ist darüber hinaus vielmehr mindestens die Vorstellung der „wesentlichen Dimension“ des Haupttatunrechts[427] oder eines zeitlichen und örtlichen Rahmens, innerhalb dessen sich die Haupttat abspielen soll.[428] Als in dieser Hinsicht hinreichend konkretisiert wäre daher unter Umständen eine Anleitung, welche die Umgehung eines ganz bestimmten, von einem bestimmten Inhalteanbieter verwendeten Schutzmechanismus für ein bestimmtes Produkt betrifft; in den meisten Fällen wird aber auch schon insoweit keine hinreichend konkrete Vorstellung einer Haupttat vorliegen.

Die Haupttat muss darüber hinaus zudem auch in Bezug auf die Person des Haupttäters konkretisiert sein. Daher genügt es nicht, dass sich die Aufforderung zu bestimmten Taten an einen individuell unbestimmten Personenkreis richtet.[429] Aus diesem Grund fehlt es daher in der Praxis gerade in den besonders gefährlichen und strafwürdigen Fällen der öffentlichen Verbreitung von Anleitungen an einer ausreichenden Konkretisierung der Person des Haupttäters, da sich Anleitungen zur Umgehung von Schutzmechanismen zunächst an jedermann richten.

Eine Strafbarkeit wegen Anstiftung kommt daher nur in Betracht, wenn einer bestimmten Person eine Anleitung oder ein technisches Mittel zur Verfügung gestellt wird und der Täter eine hinreichend konkrete Vorstellung von der Haupttat im oben beschriebenen Sinne hat. Der Nachweis des zumindest bedingten Vorsatzes, dass dieser damit die Haupttat begehen werde, bereitet dann keine Schwierigkeiten. Die empirische Analyse hat insoweit jedoch gezeigt, dass derartige Fälle für die Praxis des Raubkopierens keine wesentliche Rolle spielen.

Konkretisierung des Gehilfenvorsatzes

Ähnliche Anforderungen an die Konkretisierung des Vorsatzes gelten auch für die Beihilfe. Das Bereitstellen von Anleitungen oder technischen Mitteln ist unproblematisch als Hilfeleistung i.S.d. § 27 StGB zu werten, soweit nicht schon eine Anstiftung vorliegt, die als stärkere Form der Beteiligung vorrangig ist. Jedoch ist eine Strafbarkeit wegen Beihilfe nur dann möglich, wenn sich die Hilfeleistung an eine bestimmte Person richtet, also etwa beim individuellen Verkauf einer kopierten SmartCard oder von Hacking-Software. Beim Verbreiten von jedermann zugänglichen Anleitungen oder von Hacking-Software über das Internet fehlt es dagegen an der notwendigen Konkretisierung der Person des Haupttäters.

b) Öffentliche Aufforderung zu Straftaten

Auch die Strafbestimmung des § 111 StGB über die öffentliche Aufforderung zu Straftaten kann die im Internet verbreiteten „Angebote“ zur Umgehung von Schutzmechanismen rechtlich geschützter Güter bisher nicht erfassen. Der Tatbestand setzt zunächst voraus, dass insbesondere durch die Verbreitung von – auch elektronischen – Schriften (§ 11 Abs. 3 StGB), d.h. z.B. mit (erfolgreichem) Abruf der Daten aus dem Internet,[430] zu einer rechtswidrigen Tat aufgefordert wird. Ebenso wie bei der Anstiftung und der Beihilfe ist daher auch hier zunächst eine strafbare Haupttat erforderlich. Insoweit gilt das Gleiche wie oben zu Anstiftung und Beihilfe ausgeführt wurde.

427. So *Roxin*, in: Küper/Welp (Hrsg.), FS für Walter Stree und Johannes Wessels, Heidelberg 1993, S. 365.
428. BGHSt 34, 63, 66.
429. H.M., vgl. Sch/Sch/*Cramer/Heine*, § 26 Rn. 513.
430. So jetzt BGH, Urt. v. 27.6.2001 – StR 66/01, JZ 2002, 308, 309, gegen die bisher wohl h.L., vgl. Sch/Sch-*Lenckner/Perron*, § 184 Rn. 57 m.w.N.

Die Aufforderung i.S.d. § 111 StGB muss sich dabei allerdings aufgrund des Normzwecks der Vorschrift (vor allem wegen der besonderen Gefährlichkeit der Äußerung, deren Wirkung sich vom Täter nicht kontrollieren lässt) anders als eine Anstiftung i.S.d. § 26 StGB an einen nicht individualisierten unbestimmten Adressatenkreis richten. Dies ist bei der typischen Verbreitung von Anleitungen über eine Internetseite oder in Zeitschriften stets der Fall. Dagegen würde § 111 StGB ausscheiden, wenn der Äußernde z.B. bei Übermittlung durch eine E-Mail die Anleitung nur an einen bestimmten Adressatenkreis richtet. Der Tatbestand des § 111 StGB hat daher insoweit einen sehr viel weiter gehenden Anwendungsbereich als die Bestimmungen der Anstiftung und der Beihilfe.

Der Tatbestand des § 111 StGB unterscheidet sich von den Vorschriften der Anstiftung und der Beihilfe darüber hinaus jedoch vor allem auch dadurch, dass der Begriff des Aufforderns mit dem der Anstiftung nicht deckungsgleich ist, da er teilweise weiter und teilweise enger ist. Zum einen wird für § 111 StGB anders als für die Anstiftung nicht vorausgesetzt, dass der Tatentschluss erst durch den Auffordernden geweckt wird;[431] andererseits genügt aber nicht eine nur allgemeine Befürwortung bestimmter Taten,[432] also erst recht nicht eine bloße Anleitung dazu, auch wenn sie mittelbar dazu führt, dass ein entsprechender Tatentschluss hervorgerufen wird. Denn die bloße Befürwortung oder Anleitung ist keine Kundgabe des Willens, dass vom Adressaten der Äußerung strafbare Handlungen begangen werden sollen.[433] Dass der Begriff des „Aufforderns“ insoweit enger auszulegen ist als der Begriff der Anstiftung, zeigt auch der Vergleich von § 111 StGB mit § 130a StGB (Anleitung zu Straftaten), der nur im Hinblick auf bestimmte schwere Straftaten des Katalogs von § 126 Abs. 1 StGB (Gewaltdelikte und gemeingefährliche Straftaten) schon das Anleiten unter Strafe stellt, mit § 53 Abs. 1 S. 1 Nr. 5 WaffG (Anleiten zur Herstellung von Waffen) sowie mit dem inzwischen aufgehobenen § 88a StGB (Verfassungsfeindliche Befürwortung von Straftaten)[434]. Im Ergebnis scheidet daher eine Strafbarkeit nach § 111 StGB in den vorliegend interessierenden Fällen regelmäßig aus, weil sich eine öffentlich oder durch Schriften verbreitete Anleitung zur Umgehung von Schutzmechanismen für digitale Inhalte ohne weiteres „neutral“ formulieren lässt oder durch den ausdrücklichen Zusatz „entschärft“ werden kann, dass nur informiert und nicht zur Begehung von Straftaten aufgefordert werden soll.

3. Deliktsspezifische Ansätze

a) Ansatz, Probleme und Überblick

Aufgrund dieser Probleme der allgemeinen strafrechtlichen Regelungen der Anstiftung, der Beihilfe und des öffentlichen Aufforderns zu Straftaten versucht der Gesetzgeber in zunehmendem Maß, die Problematik der vorbereitenden Förderhandlungen durch spezielle Vorfeldtatbestände zu lösen, die für bestimmte Deliktsbereiche spezielle Vorbereitungs- und Förderhandlungen unter Strafe stellen.

- Ein klassisches Beispiel für derartige Vorfeldtatbestände ist § 149 StGB über die Vorbereitung der Fälschung von Geld und Wertzeichen. Der Tatbestand bedroht denjenigen

431. Sch/Sch-*Eser*, § 111 Rn. 3. Insoweit käme keine vollendete, sondern nur eine versuchte Anstiftung nach § 30 Abs. 1 StGB in Betracht.
432. BGHSt 32, 310, 311 im Anschluss an RGSt 63, 170, 173.
433. OLG Köln, MDR 1983, 339.
434. BGHSt 32, 310, 311.

mit Freiheitsstrafe nicht unter einem Jahr, der eine Fälschung von Geld oder Wertzeichen vorbereitet, indem er z.B. Platten, Druckstöcke, Negative oder spezielles Papier, das zur Fälschung von Geld besonders geeignet ist, herstellt, sich verschafft oder einem anderen überlässt.

- Die gleiche Gesetzgebungstechnik liegt dem 1986 durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität[435] geschaffenen § 152a StGB über die Fälschung von Zahlungskarten und Vordrucken für Euroschecks zugrunde. Die Strafvorschrift bedroht denjenigen mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, der zur Täuschung im Rechtsverkehr z.B. Zahlungskarten oder Euroscheckvordrucke nachmacht oder solche falschen Karten oder Vordrucke sich oder einem anderen verschafft, feilhält, einem anderen überlässt oder gebraucht.

Diese beiden klassischen Beispiele machen die Probleme der Vorfeldkriminalisierung von vorbereitenden Förderhandlungen deutlich: Um den grundrechtlich garantierten Freiraum des Bürgers nicht übermäßig zu beeinträchtigen, versucht der Gesetzgeber bei diesen speziellen Vorfeldtatbeständen, bereits im objektiven Tatbestand die unter Strafe gestellten Handlungen auf solche Verhaltensweisen zu beschränken, die stets oder typischerweise oder zumindest häufig der Vorbereitung einer Straftat dienen. Darüber hinaus begrenzt der Gesetzgeber den Tatbestand durch subjektive Erfordernisse: So muss der Täter bei § 146 StGB in der Absicht handeln, Geld nachzumachen, und auch § 152a StGB verlangt ein absichtliches Handeln „zur Täuschung im Rechtsverkehr oder, um eine solche Täuschung zu ermöglichen“.[436] Auch im Bereich der Tathandlungen wird sorgfältig differenziert, welche Handlungen strafrechtlich verboten sind, wobei die Strafbarkeit des bloßen Besitzes den Strafschutz gegenüber der Strafbarkeit des Überlassens in besonders weitgehender Weise ins Vorfeld (und auch in den Bereich der Privatsphäre) verlagert.

Im Hinblick auf diese bereits bestehenden Straftatbestände war und ist es daher konsequent, dass der Gesetzgeber versucht(e), die hier bereits erprobte Technik der Erfassung von typischen Förderhandlungen im Vorfeld der eigentlichen Tatbestandsverwirklichung auch für den Schutz digitaler Güter zu nutzen. Entsprechende Vorfeldtatbestände liegen hier sogar besonders nahe, weil die empirische Analyse gezeigt hat, dass diese Güter in großem Umfang durch typische und in der Praxis weit verbreitete Förderhandlungen gefährdet werden. Entsprechende Ansätze finden sich deswegen im Zugangskontrolldiensteschutz-Gesetz (ZKDSG)[437] aus dem Jahre 2002, im Referentenentwurf zur Neuregelung der Urheberrechte in der Informationsgesellschaft[438] sowie in der 2001 vom Europarat beschlossenen Convention on Cybercrime, die in der Bundesrepublik Deutschland noch umgesetzt werden muss.[439] Die entsprechenden Ansätze in diesen Gesetzen, Gesetzentwürfen und internationalen Vereinbarungen sollen im folgenden näher untersucht werden.

435. BGBl. 1986 I, S. 721 ff.
436. Vgl. Sch/Sch-*Stree/Sternberg-Lieben,* § 146 Rn. 7 und § 152a Rn. 6-9.
437. Siehe oben Fn. 237.
438. Siehe oben Fn. 238.
439. Siehe oben Fn. 239.

b) §§ 4, 5 ZKDSG

Das „Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (Zugangskontrolldiensteschutz-Gesetz – ZKDSG) vom 19. März 2002[440] beruht auf der bereits oben erwähnten Richtlinie des Europäischen Parlaments[441] und des Rates über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten vom 20. November 1998.[442] Das Gesetz hat das „Ziel, die gewerbsmäßige Verbreitung von „Vorrichtungen“ zu verhindern (einschließlich Wartung und Werbung), mit denen sich der Zugangsschutz von Fernseh- und Radiosendungen sowie von Diensten der Informationsgesellschaft unbefugt überwinden lässt“.[443]

Der in § 2 mit dem Begriff der „zugangskontrollierten Dienste“ umschriebene dienstespezifische Schutzbereich des Gesetzes erfasst Rundfunkdarbietungen im Sinne von § 2 des Rundfunkstaatsvertrages, Teledienste im Sinne von § 2 des Teledienstegesetzes sowie Mediendienste im Sinne von § 2 des Mediendienste-Staatsvertrages, die unter der Voraussetzung eines Entgelts erbracht werden und nur unter Verwendung eines Zugangskontrolldienstes genutzt werden können. „Zugangskontrolldienste“ werden dabei definiert als „technische Verfahren oder Vorrichtungen, die die erlaubte Nutzung eines zugangskontrollierten Dienstes ermöglichen.“

Der technisch-gegenständliche Verbotsbereich des Zugangskontrolldiensteschutz-Gesetzes betrifft unter der Bezeichnung der „Umgehungsvorrichtungen“ „technische Verfahren oder Vorrichtungen, die dazu bestimmt oder entsprechend angepasst sind, die unerlaubte Nutzung eines zugangskontrollierten Dienstes zu ermöglichen. Damit werden insbesondere Computerprogramme, die Manipulation von Set-Top-Boxen zur Nutzungserweiterung oder der Bau von neuen Geräten erfasst. Es genügt dabei, wenn Vorrichtungen unter anderem der Umgehung dienen, da ansonsten die Vorschrift durch Geräte oder Software mit gemischten Funktionen leicht umgangen werden könnte“.[444] Nicht einbezogen werden damit insbesondere Tools zur Umgehung von Kopierschutzmechanismen bei Datenträgern, denn diese stellen weder einen Teledienst noch einen Mediendienst dar.

Bei den im Hinblick auf diese Umgehungsvorrichtungen einschlägigen verbotenen Tathandlungen ist die Reichweite des allgemeinen (nicht unmittelbar strafbewehrten) Verbots sowie der Straf- und Ordnungswidrigkeitstatbestände der §§ 4 und 5 zu unterscheiden.

- Das allgemeine zivilrechtliche Verbot des § 3 erfasst (1) die Herstellung, die Einfuhr und die Verbreitung von Umgehungsvorrichtungen zu gewerblichen Zwecken, (2) den Besitz, die technische Einrichtung, die Wartung und den Austausch von Umgehungsvorrichtungen zu gewerblichen Zwecken sowie (3) die Absatzförderung von Umgehungsmaßnahmen.

- Die Strafvorschrift des § 4 begrenzt die Androhung einer Freiheitsstrafe bis zu einem Jahr dagegen auf die von § 3 Nr. 1 erfasste Herstellung, das Einführen und die Verbreitung einer Umgehungseinrichtung zu gewerblichen Zwecken.

440. Siehe oben Fn. 237.
441. Siehe oben Fn. 410.
442. ABl. L 320/54 v. 18.11.1998. Siehe auch *Wand*, oben Fn. 227, S. 77 ff.
443. Vgl. BT-Drucks 14/7229 v. 24.10.2001.
444. Vgl. BT-Drucks 14/7229 v. 24.10.2001, S. 7.

- Die von § 3 Nr. 2 erfassten Tathandlungen des Besitzes, der technischen Einrichtung, der Wartung und des Austausches einer Umgehungsvorrichtung werden von § 5 lediglich als Ordnungswidrigkeit mit einer Geldbuße von bis zu 50.000 Euro bedroht.

- Die – noch weiter im Vorfeld der eigentlichen Verletzungshandlung liegende – Absatzförderung nach § 3 Nr. 3 – ist dagegen weder straf- noch ordnungswidrigkeitenrechtlich bewehrt.

Im Vergleich zu den bisher bekannten Vorfeldtatbeständen der §§ 146, 152a StGB fällt bei diesen Regelungen vor allem zweierlei auf: Einerseits werden die straf- und bußgeldrechtlich bewehrten Verbote dadurch erheblich eingeschränkt, dass sie ein Handeln zu gewerbsmäßigen Zwecken verlangen. Andererseits verlangen die Tatbestände keine Absicht, eine bestimmte Straftat zu begehen oder zu fördern. Die Forderung nach einem Handeln zu gewerbsmäßigen Zwecken scheidet die in der empirischen Analyse ermittelten Fälle aus, in denen die entsprechenden Anleitungen und Tools von Hackern und Privatleuten ohne finanzielle Interessen verbreitet werden. Der Verzicht auf die Absicht der Straftatbegehung führt dagegen zu Abgrenzungsschwierigkeiten bei Dual-use-Produkten und zur Gefahr einer Behinderung der Entwicklung von Schutzmechanismen, da die Aufdeckung von Schwachstellen bei Schutzmechanismen auch der Verbesserung dieser Produkte dienen kann. Dualuse-Produkte zeichnen sich dadurch aus, dass sie zumindest auch für legale Zwecke entwickelt wurden oder anwendbar sind, jedoch in identischer Art und Weise sowohl zu legalen als auch zu illegalen Zwecken eingesetzt werden können. Auf diese Punkte wird im Rahmen der Reformüberlegungen zurückzukommen sein.

c) §§ 108b Abs. 2, 111a i.V.m. § 95a Abs. 3 UrhG-E

Auch für den Bereich der Urheberrechte beabsichtigt der Gesetzgeber, mit den §§ 108b Abs. 2, 95a Abs. 3 UrhG (in der Fassung des bereits genannten Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft[445]) die Schaffung eines Straftatbestandes im Vorfeld von Umgehungsmaßnahmen.[446] Im Hinblick auf die Komplexität der vorgeschlagenen Strafbestimmung und ihre Wertungswidersprüche zu dem in den §§ 108b Abs. 1, 95a Abs. 1 UrhG-E enthaltenen Verbot der Umgehung von Sicherungsmaßnahmen kann auf die obigen Ausführungen verwiesen werden.[447] Während die eigentlich schädigende Tathandlung der Umgehung von technischen Schutzmaßnahmen in § 108b Abs. 1 UrhG-E jedoch zu restriktiv bestimmt wird, ist der Verbotsbereich der einschlägigen Vorfeldtatbestände des § 108b Abs. 2 UrhG-E teilweise zu weit gefasst.

Nach der – zum besseren Verständnis zunächst analysierten – zivilrechtlichen Verbotsnorm des § 95a Abs. 3 UrhG-E sollen zukünftig die Herstellung, die Einfuhr, die Verbreitung, der Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung sowie der gewerblichen Zwecken dienende Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen verboten sein, die entweder

445. Siehe oben Fn. 196.

446. § 95a Abs. 2 UrhG-E beruht auf Art. 6 Abs. 2 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft vom 22. Mai 2001, ABl. L 167/10 ff. v. 22.6.2001. Siehe auch *Flechsig*, ZUM 2002, 1, 14 f.; *Spindler*, GRUR 2002, 105, 116 f.

447. Siehe oben III. D. 8. a).

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

Damit wird auf den ersten Blick ein sehr umfassender Vorfeldschutz im Hinblick auf die Umgehung von Schutzmaßnahmen normiert, der insbesondere nicht nur explizit für das Hacken von Schutzmaßnahmen entworfene Tools erfasst, sondern auch Dual-use-Produkte, sofern diese primär dem verbotenen Zweck dienen. Ob hierdurch allerdings auch Softwareprodukte – wie z.B. CloneCD – erfasst werden, die ganz allgemein zum Kopieren von (auch kopiergeschützten) Datenträgern verwendet werden können, ist fraglich, da deren Hauptzweck sich nur schwer bestimmen lässt. Die Hersteller von derartigen Programmen werden argumentieren, die Software sei völlig neutral und die Nutzer seien zur Respektierung der Urheberrechte angehalten. Faktisch werden Kopierprogramme, die auch kopiergeschützte Datenträger kopieren, allerdings ganz überwiegend wegen dieser speziellen Funktion eingesetzt. Dies ist den Herstellern entsprechender Produkte auch bekannt.

Weiterhin müssen die Vorrichtungen, Erzeugnisse und Bestandteile sowie die Erbringung von Dienstleistungen nach dem Wortlaut der Vorschrift auch hier der Umgehung *wirksamer* technischer Maßnahmen dienen, so dass sich das bereits oben diskutierte Problem stellt, wie diese Formulierung des Gesetzes zu verstehen ist. Insoweit kann deshalb auf die obigen Ausführungen verwiesen werden.[448]

Nach dem Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 18. März 2002 war zudem bezüglich des geplanten § 95a Abs. 3 UrhG-E (damals § 95a Abs. 2 UrhG-E) problematisch, dass sich der Begriff des „gewerblichen Zwecks“ sprachlich nicht zwingend nur auf den Besitz, sondern auch auf die sonstigen im Gesetz genannten Tathandlungen beziehen konnte. Wäre dies so gewollt gewesen, so würde die Vorschrift in weiten Bereichen leer laufen, da gerade im Hinblick auf Hackingtools zur Umgehung von Schutzmaßnahmen dem Handeln zu nicht gewerblichen Zwecken das gleiche Gefahrenpotential wie dem Handeln zu gewerblichen Zwecken zukommt. Dies liegt – wie oben dargestellt – daran, dass die Angriffe auf Schutzmaßnahmen und die Erstellung entsprechender Tools häufig aus „sportlichen“, ideellen oder sogar wissenschaftlichen Gründen erfolgen. Daher werden viele Tools in diesem Bereich sogar kostenlos über das Internet abgegeben. Auch werben Privatleute auf ihren Homepages insbesondere für einen Verkauf dieser Tools. Der Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft stellt deswegen in § 95a Abs. 3 UrhG-E nunmehr klar, dass sich die gewerbliche Zwecksetzung ausschließlich auf den Besitz bezieht.

Weiterhin können sich Schwierigkeiten daraus ergeben, dass § 95a Abs. 3 UrhGE nur von einer „Verbreitung“ von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie Dienstleistungen spricht. Versteht man aber den Begriff des Verbreitens so, wie er auch in anderen Vorschriften des UrhG – z.B. bei § 17 UrhG – verwendet wird, dann wäre eine körperliche Fixierung dieser Tools erforderlich. Dies würde im Ergebnis aber bedeuten, dass gerade die besonders

448. Siehe oben III. D. 7.

gefährliche „Verbreitung“ entsprechender Vorrichtungen, Erzeugnisse oder Bestandteile über das Internet mangels körperlicher Fixierung nicht von der Vorschrift erfasst wäre. Dies entspricht aber nicht der Intention der Bundesregierung, die sich der „Internetproblematik“ bei Abfassung der Vorschrift bewusst war und deshalb – anders als noch beim Referentenentwurf – in der Gesetzesbegründung des Regierungsentwurfs für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft darauf hinweist, dass der hier verwendete Begriff der Verbreitung von dem auf körperliche Werkstücke beschränkten Verbreitungsbegriff des § 17 UrhG zu unterscheiden ist.[449] Verbreiten i.S.d. § 95a UrhG-E muss daher allgemeiner als Zugänglichmachen gelesen werden. Eine solche unterschiedliche Verwendung eines identischen Begriffs in dem selben Gesetz ist jedoch unschön und im übrigen auch leicht vermeidbar. Um Auslegungsschwierigkeiten zu vermeiden, sollte der Gesetzgeber deswegen auch das öffentliche Zugänglichmachen mit in den Tatbestand aufnehmen.[450] Schließlich scheint der Wortlaut des § 95a Abs. 3 UrhG-E die bloße Information über Umgehungsmöglichkeiten von Schutzmechanismen nicht zu erfassen. Damit würde § 95a Abs. 3 UrhG-E aber in weiten Bereichen leer laufen, da gerade die Hinweise auf Hackertools im Internet durch Private – aber auch zu gewerblichen Zwecken – in erheblichem Maß die Urheberrechte bedrohen.[451]

Verstöße gegen § 95a Abs. 3 UrhG-E werden nach dem Willen des Gesetzgebers entweder als Straftat nach § 108b Abs. 2 UrhG-E oder als Ordnungswidrigkeit nach § 111a Abs. 1 UrhG-E geahndet:

- Eine Straftat nach § 108b Abs. 2 UrhG-E begeht allerdings nur, wer eine Vorrichtung, ein Erzeugnis oder einen Bestandteil nach § 95a Abs. 3 UrhG-E zu *gewerblichen* Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet. Die Strafvorschrift ist damit einerseits zu weit und andererseits zu eng geraten. Sie ist insoweit zu weit gefasst, als sie im Hinblick auf „Dualuse-Produkte“ keine einschränkenden Absichtsmerkmale fordert (das Handeln zu gewerblichen Zwecken hat bei neutralen Verhaltensweisen keinen zusätzlichen Unrechtsgehalt). Die Strafnorm ist dagegen insoweit zu eng formuliert, als ihre Beschränkung auf gewerbliches Handeln sie in den – wie die empirische Analyse gezeigt hat – häufigen Fällen unanwendbar macht, in denen Hackingtools aus „sportlichem Ehrgeiz“ im Internet verbreitet werden. Hierauf wird unten im Rahmen der Reformmaßnahmen näher einzugehen sein.

- Dagegen liegt eine Ordnungswidrigkeit nach § 111a Abs. 1 Nr. 1a UrhG-E vor, wenn der Täter eine Vorrichtung, ein Erzeugnis oder einen Bestandteil nach § 95a Abs. 3 UrhG-E verkauft, vermietet oder über den Kreis der mit dem Täter persönlich verbundenen Personen hinaus verbreitet – also insoweit nicht gewerblich handelt – oder gemäß § 111a Abs. 1 Nr. 1b UrhG-E wiederum zu gewerblichen Zwecken eine Vorrichtung, ein Erzeugnis oder einen Bestandteil besitzt, für deren Verkauf oder Vermietung wirbt oder eine Dienstleistung erbringt.

- Daraus folgt, dass der Täter nach den Plänen des Gesetzgebers dann straflos bleibt und auch keine Ordnungswidrigkeit begeht, wenn er Vorrichtungen, Erzeugnisse oder Be-

449. Vgl. oben Fn. 196, S. 63.
450. So auch BDZV, oben Fn. 266, S. 4; Forum der Rechteinhaber, oben Fn. 262, S. 6; VDZ, oben Fn. 312, S. 8.
451. So auch Forum der Rechteinhaber, oben Fn. 262, S. 7; KirchMedia, oben Fn. 266, S. 11 f.; SPIO/Film20, oben Fn. 265, S. 10; *Spindler*, GRUR 2002, 105, 117.

standteile nach § 95a Abs. 3 UrhG-E zu nicht gewerblichen Zwecken besitzt oder einführt sowie an Personen verbreitet, die mit ihm persönlich verbunden sind.

d) Art. 6 der Convention on Cybercrime

Die „Convention on Cybercrime“ des Europarats vom 23.1. 2001[452] wählt demgegenüber einen anderen Ansatz zur Kriminalisierung der Verbreitung von Hackingtools. Bei der objektiven Beschreibung der erfassten Werkzeuge stellt die Convention darauf ab, dass das Werkzeug *hauptsächlich* zur Begehung von bestimmten computerspezifischen Straftaten entwickelt oder angepasst ist. Darüber hinaus wird im subjektiven Tatbestand gefordert, dass der Täter in der *Absicht* handelt, der Empfänger werde das Werkzeug zum Zwecke der Begehung einer der genannten Straftaten begehen, zu denen „illegal access“, „illegal interception“ und „data interference“ gehören. Die in Art. 10 der Convention genannten „offences related to infringements of copyright and related rights” gehören dazu allerdings nicht. Art. 6 der Europaratskonvention hat in dem vorliegend interessierenden Bereich daher keine unmittelbare, sondern nur eine mittelbare Bedeutung (z.B. wenn Angriffe auf digitale Güter mit Hilfe von Hacking erfolgen). Art. 6 ist jedoch vor allem auch im Hinblick auf seine Tatbestandstechnik mit ihren subjektiven Absichtsmerkmalen von Interesse.

Die Empfehlung des Europarats lautet:

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

   a. the production, sale, procurement for use, import, distribution or otherwise making available of:

      i. a device, including a computer program, *designed or adapted primarily for the purpose of committing any of the offences* established in accordance with Article 2 – 5;

      ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed
      with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5; and

   b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with *intent that it be used for the purpose of committing any of the offences* established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

452. Siehe oben Fn. 239.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Art. 6 der Convention on Cybercrime bewältigt die "Dual-use-Problematik" daher wesentlich besser als § 5 ZKDSG oder § 108b Abs. 2 des Gesetzentwurfs zur Regelung des Urheberrechts in der Informationsgesellschaft. Er enthält insbesondere nicht die – im Kontext der hier analysierten Deliktsformen zur Strafbarkeitsbegründung untaugliche – Begrenzung des Handelns zu gewerbsmäßigen Zwecken. Die Begrenzung der erfassten Tools auf „hauptsächlich" strafbaren Zwecken dienende Produkte stellt demgegenüber im objektiven Tatbestand einen – im einzelnen sicherlich noch diskussionsbedürftigen, aber im Grundsatz sinnvollen – Vorfilter zur Begrenzung der erfassten Produkte dar. Die darüber hinaus geforderte Absicht zur Begehung bestimmter Straftaten nimmt dann die entscheidende und auch trennscharfe Ausgrenzung der nicht strafbaren Fallgestaltungen vor. Wünschenswert wäre daher nur gewesen, dass insoweit noch die Absicht zur Begehung von Urheberrechtsverletzungen in Art. 6 der Konvention mit aufgenommen worden wäre.

4. Ergebnis

Die im Bereich der Raubkopien eine bedeutende Rolle spielende Veröffentlichung von Anleitungen und Hilfestelllungen zur Begehung von Rechtsverletzungen und das Anbieten entsprechender Tools im Internet werden von den *klassischen Strafvorschriften der Anstiftung, der Beihilfe und des öffentlichen Aufforderns zu Straftaten* in den meisten Fällen nicht erfasst.

Die Strafvorschriften des *Gesetzes über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten* (Zugangskontrolldiensteschutz-Gesetz – ZKDSG) vom 19. März 2002 beschränken sich auf den Teilbereich der zugangskontrollierten Dienste (der z.B. Kopierschutzmechanismen bei Datenträgern nicht erfasst). Sie gehen dabei durch ihre Forderung nach einem gewerbsmäßigen Handeln an dem – in der empirischen Analyse dargestellten – Großteil der einschlägigen Fälle vorbei, in denen die entsprechenden Tools von Hackern ohne eine gewerbsmäßige Absicht quasi „als Sport" ins Internet gestellt werden.

Die geplanten Neuregelungen des *Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft* sind demgegenüber in der Beschreibung der verbotenen Tools und sonstigen Hilfestellungen sehr viel weiter. Sie können aufgrund unklarer gesetzlicher Formulierungen allerdings nicht garantieren, dass die entscheidenden Tathandlungen eindeutig kriminalisiert werden. Die nichtgewerbliche Verbreitung der Tools wird zudem nur mit einer Ordnungswidrigkeit sanktioniert. Einige Tathandlungen – wie die private Einfuhr entsprechender Tools – werden überhaupt nicht strafrechtlich oder ordnungswidrigkeitenrechtlich sanktioniert.

IV. Reformbedarf und Lösungsvorschläge

A. Verfassungsrechtliche Vorgaben

1. Empirischer Ausgangspunkt

Die empirisch Analyse hat gezeigt, dass digitale Güter heute aufgrund der technischen Veränderungen bei PCs und des rasanten Wachstum des Internets massiv gefährdet sind. Diese Entwicklung wird aufgrund fortschreitender Leistungs- und Kapazitätssteigerungen der Computerkomponenten und mit der Verbreiterung der Übertragungsbandbreiten im Internet weitergehen und ohne eine Veränderung grundsätzlicher Parameter nicht nur zu einer empfindlichen Schädigung der Urheber und sonstigen Rechteinhaber führen, sondern auch zur Gefährdung der Software-, Audio- und Videoindustrie.

Bereits heute hat die Entwicklung der Raubkopien ein Ausmaß erreicht, dass die Frage gestellt werden muss, ob der Gesetzgeber nicht zu einem Einschreiten verpflichtet ist. In dem vorliegenden strafrechtlichen Gutachtens ist es zwar nicht möglich, diese Frage im Detail zu untersuchen und abschließend zu beantworten. Gleichwohl soll kurz auf die tragenden Gesichtpunkte einer Verpflichtung des Gesetzgebers zu einem wirksamen Schutz digitaler Güter hingewiesen werden.

2. Allgemeine Schutzpflichten im Hinblick auf das geistige Eigentum

Es ist unstreitig, dass das Urheberrecht als Nutzungsrecht „Eigentum“ im Sinne des Art. 14 Abs. 1 S. 1 GG ist. Art. 14 Abs. 1 S. 1 GG gebietet deswegen die grundsätzliche Zuordnung des wirtschaftlichen Wertes eines geschützten Werkes an den Urheber. Da es keinen absoluten und vorgegebenen Begriff des Eigentums gibt, hat die Verfassung dem Gesetzgeber die Aufgabe übertragen, den Inhalt und die Schranken des Eigentums zu bestimmen. Art. 14 Abs. 1 S. 1 GG sichert damit nicht jede denkbare Verwertungsmöglichkeit des Eigentums verfassungsrechtlich ab. Im Hinblick auf Vergütungsregelungen ist der Gesetzgeber von Verfassungs wegen vielmehr nur gehalten, eine angemessene Verwertung sicherzustellen, die der Natur und der sozialen Bedeutung des Rechts entspricht. Es ist daher z.B. Aufgabe des Gesetzgebers, das Interessenviereck Urheber – Geräteindustrie – Trägermedienproduzenten – Werknutzer sachgerecht und praktikabel auszugestalten.

Der Gesetzgeber hat bei der ihm hierbei obliegenden Aufgabe der Bestimmung von Inhalt und Schranken des Eigentums allerdings den grundgesetzlich geschützten Kern des Urheberrechts zu berücksichtigen. Zu den konstituierenden Merkmalen des Urheberrechts als Eigentum im

Sinne der Verfassung gehört dabei die grundsätzliche Zuordnung des vermögenswerten Ergebnisses der schöpferischen Leistung an den Urheber im Wege privatrechtlicher Normierung und seine Freiheit, in eigener Verantwortung darüber verfügen zu können.[453] Eine weitgehende Entwertung z.B. des Rechts der unkörperlichen Wiedergabe verstößt daher gegen Art. 14 GG.[454] Auf dem Hintergrund der oben dargestellten Bedrohung für digitale Güter würde deswegen auch eine gesetzgeberische Formulierung oder eine Auslegung von § 53 Abs. 1 UrhG gegen Art. 14 GG verstoßen, wenn sie eine massenhafte Privatkopie im Internet auf der Basis rechtswidrig genutzter Vorlagen erlauben würde.

Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts enthalten die Grundrechtsnormen dabei nicht nur subjektive Abwehrrechte des Einzelnen gegen den Staat, sondern sie verkörpern zugleich auch eine objektive Wertordnung, die als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gilt und Richtlinien und Impulse für Gesetzgebung, Verwaltung und Rechtsprechung gibt.[455] Aus den Grundrechten folgt damit auch, ob und in welchem Ausmaß der Staat zu rechtlichem Schutz verpflichtet ist. Aufgrund der im empirischen Teil analysierten Bedrohung digitaler Güter ergibt sich daher im vorliegenden Bereich nicht nur das Verbot von die Rechtsinhaber übermäßig treffenden zivilrechtlichen Schranken, sondern auch eine allgemeine Pflicht zu einem Schutz der Urheber digitaler Güter. Dies gilt vor allem auch deshalb, weil –wie das technische Gutachten von *Pfitzmann*/*Federrath*/*Kuhn* zeigt – ein technischer Schutz durch die Urheber selbst nur in begrenztem Umfang möglich ist, und diese Situation sich auch nicht ändern wird.

3. Pflicht zum strafrechtlichen Schutz

Der vorstehend bereits in allgemeiner Form angesprochene Ermessensspielraum des Gesetzgebers bei der Erfüllung seiner Aufgaben führt dazu, dass eine Verpflichtung des Gesetzgebers speziell zur Schaffung eines strafrechtlichen Schutzes nur in Ausnahmefällen in Betracht kommt. Nur im äußersten Falle, wenn der von der Verfassung gebotene Schutz auf keine andere Weise erreicht werden kann, ist der Gesetzgeber verpflichtet, zur Sicherung besonders bedeutender Rechtsgüter das Mittel des Strafrechts einzusetzen. Dies erfordert nach der Rechtsprechung des BVerfG eine Gesamtbetrachtung, die einerseits den Wert des verletzten Rechtsguts und das Maß der Sozialschädlichkeit der Verletzungshandlung in den Blick nimmt, andererseits aber auch die Vorstellungen in der modernen Gesellschaft über die Rolle des Strafrechts berücksichtigt sowie die praktische Wirksamkeit von Strafdrohungen und die Möglichkeit ihres Ersatzes durch andere rechtliche Sanktionen nicht außer acht lässt.[456]

In dem vorliegend untersuchten Bereich lässt sich daher eine unmittelbare Verpflichtung des Staates zu strafrechtlichen Schutzmaßnahmen nur schwer begründen. Soweit alternative Schutzmaßnahmen jedoch nicht Erfolg versprechend sind oder (wie z.B. eine erweiterte Geräteabgabe) vom Gesetzgeber nicht gewählt werden, läuft die allgemeine Schutzpflicht des Staates im Bereich der Verletzung der Rechte an digitalen Gütern faktisch auf einen strafrechtlichen Schutz hinaus. Die verfassungsrechtlichen Überlegungen streiten daher vor allem für einen allgemeinen Schutz der vorliegend bedrohten Urheberrechte, der – falls vom Gesetzgeber keine anderen

453. Vgl. z.B. BVerfGE 31, 229, 240 ff.; 31, 248, 250 ff.; 31, 270, 272 ff.; 49,382, 392 ff.; 77, 264, 270 ff.; 79, 1, 25.
454. Vgl. BVerfGE 49, 382, 399.
455. Vgl. BVerfGE 49, 89, 141; 56, 54, 73.
456. Vgl. BVerfGE 1, 1, 45.

Lösungsmöglichkeiten ergriffen werden – jedoch in der Sache rasch zu einem strafrechtlichen Schutz wird.

Vor diesem Hintergrund ist es im folgenden erforderlich, zunächst Strategien und dann konkrete Möglichkeiten eines strafrechtlichen Schutzes zu entwickeln, dabei jedoch gleichzeitig auch alternative (z.B. zivilrechtliche) Schutzmöglichkeiten einzubeziehen. Diese Entwicklung der entsprechenden Lösungsmöglichkeiten und Vorschläge erfolgt dabei nicht primär unter dem Gesichtspunkt, entsprechende Schutzpflichten des Gesetzgebers einzufordern, sondern dem Gesetzgeber ein effektives und attraktives Schutzmodell anzubieten, das auch Aussicht auf einen gesellschaftlichen Konsens und damit eine Umsetzung hat.

B. Strategien eines effektiven strafrechtlichen Schutzsystems

1. Erfordernis eines differenzierenden Schutzsystems

Die empirische Analyse der Rechtswirklichkeit hat gezeigt, dass für den (insbesondere straf-)rechtlichen Schutz digitaler Güter zwei unterschiedliche Sachverhaltskonstellationen unterschieden werden müssen: (a) der rechtliche Schutz der (insb. auch ungeschützten) *digitalen Güter* sowie (b) der rechtliche Schutz ihrer *technischen Schutzmechanismen*. Die zweitgenannte Fallgruppe des Schutzes technischer Schutzmaßnahmen macht den erstgenannten rechtlichen Schutz ungeschützter digitaler Güter dabei nicht obsolet, da nicht alle digitalen Güter durch entsprechende Mechanismen geschützt werden können; auch stehen nicht allen Rechtsinhaber technische Schutzmechanismen zur Verfügung. Zudem werden Schutzmechanismen umgangen und die zugrunde liegenden digitalen Güter dann häufig in ungeschützter – z.B. entschlüsselter – Form im Internet angeboten. Ein effektiver Schutz digitaler Güter und die oben dargestellten verfassungsrechtlichen Vorgaben erfordern deswegen ein *doppeltes Schutzsystem*, das sowohl die ungeschützten digitalen Güter als auch die entsprechenden technischen Schutzmechanismen absichert. Der Gesetzgeber muss daher sowohl einen allgemeinen Schutz der digitalen Güter als auch spezielle Schutzvorschriften für technische Schutzmechanismen schaffen.

2. Schutzstrategien für (insb. ungeschützte) digitale Güter

Gegen die unberechtigte Nutzung aller (insbesondere: technisch ungeschützter) *digitalen Güter* im Bereich der neuen Medien gibt es zwei Schutzstrategien, die – im Sinne eines effektiven Schutzes – auch miteinander kombiniert werden können:

- Die erste Schutzstrategie zielt auf den Endnutzer und die von ihm vorgenommene *Kopierhandlung*. Das für diese Strategie im Bereich des materiellen Rechts ausreichende Verbot der Kopie digitaler Güter (d.h. Vervielfältigungsverbot) hat den Vorzug, dass es aufgrund seines möglichen Gesetzeswortlauts die den Rechteinhaber schädigenden Handlungen in weitgehendem Umfang (z.B. durch eine Beschränkung der Privatkopie auf rechtmäßig erlangte Vorlagen) erfassen kann. In materiell-rechtlicher Hinsicht ist ein solches Verbot

– vor allem bei der zunächst gebotenen zivilrechtlichen Beurteilung – auch zu rechtfertigen. Es weist jedoch zumindest derzeit den Nachteil auf, dass es in der Praxis nicht durchsetzbar ist, weil die entsprechenden Kopierhandlungen weitgehend in der Privatsphäre erfolgen und sich dadurch faktisch dem Zugriff der Strafverfolgungsbehörden entziehen.[457] Inwieweit neue Techniken des „Monitoring“ und des „Watermarking“ in der Zukunft zu einer besseren Verfolgbarkeit der entsprechenden Handlungen – auch ohne ein Eindringen in die Privatsphäre – führen werden, bleibt dabei abzuwarten.

- Die zweite Schutzstrategie knüpft an der für die Kopiererstellung notwendigen Vorlage an und versucht, die – vor allem öffentliche – *Verbreitung* und *Zugänglichmachung der Vorlagen* (insb. im Internet) zu unterbinden. Diese Strategie hat zwar den Nachteil, dass sie gesetzlich nicht alle Möglichkeiten der „Verbreitung“ von Vorlagen erfassen kann (da z.B. die Weitergabe rechtmäßig erworbener Datenträger zulässig bleiben muss). Sie hat dafür allerdings den Vorzug, dass sie nicht an eine unkontrollierbare Handlung in der Privatsphäre anknüpft, sondern an ein häufig öffentliches Anbieten der digitalen Güter, das von den Rechteinhabern und den Strafverfolgungsbehörden kontrollierbar ist. Eine solche Strategie bietet daher in der Praxis sehr viel bessere Erfolgsaussichten als ein (dadurch nicht ausgeschlossenes) bloßes Verbot der eigentlich schädigenden Kopierhandlung. Die oben dargestellte empirische Analyse macht insoweit eindrucksvoll deutlich, dass die Raubkopie digitaler Güter ganz wesentlich bekämpft werden könnte, wenn vor allem das öffentliche Angebot von digitalen Gütern im Internet zurückgedrängt werden würde. Ein zukünftiger Schwerpunkt der Bekämpfung von Raubkopien muss daher in diesem zweiten Bereich liegen, vor allem auch um die erwähnten Defizite bei der Durchsetzung der Verbotsnormen gegen unbefugtes Kopieren im erstgenannten Bereich zu kompensieren.

3. Schutzstrategien für technische Schutzmechanismen

Gegen die Angriffe auf *technische Schutzmechanismen* für digitale Güter kommen – wie die vorangegangene Analyse bereits deutlich gemacht hat – ebenfalls zwei verschiedene rechtliche Strategien in Betracht, die miteinander kombiniert werden können:

- Zum einen kann durch rechtliche Vorschriften die *Umgehung der Schutzmechanismen* und insbesondere die Manipulation von DRM-Systemen – z.B. in Form der unberechtigten Entschlüsselung – verboten werden. Diese Strategie ist im Hinblick auf ihre Rechtfertigung weitgehend unproblematisch, da der Unrechtsgehalt der entsprechenden Tathandlungen (z.B. auch im Hinblick auf die strukturelle Ähnlichkeit mit § 17 UWG und § 202a StGB) klar zu Tage liegt. Die praktische Umsetzung dieser Strategie ist allerdings wiederum dadurch erschwert, dass die einschlägigen Tathandlungen regelmäßig in der

457. Dies kann – ungeachtet der zivilrechtlichen Rechtswidrigkeit der entsprechenden Handlungen – auch Probleme für die Strafbewehrung dieser Handlungen aufwerfen. Denn wie oben dargestellt, verlangt die Rechtsprechung des BVerfG für die Frage der Strafbewehrung eine Gesamtbetrachtung, die einerseits den Wert des verletzten Rechtsguts und das Maß der Sozialschädlichkeit der Verletzungshandlung in den Blick nimmt, andererseits aber auch die Vorstellungen in der modernen Gesellschaft über die Rolle des Strafrechts berücksichtigt sowie die *praktische Wirksamkeit von Strafdrohungen* und die Möglichkeit ihres Ersatzes durch andere rechtliche Sanktionen nicht außer acht lässt; vgl. BVerfGE 1, 1, 45.

Privatsphäre erfolgen und dadurch schwer zu entdecken und zu verfolgen sind. Dies belegen auch die oben angeführten Schadenshöhen, bei denen es sich stets um Schätzungen handelt, die z.B. auf der Anzahl der verkauften Datenrohlinge beruhen.

- Zum andern kann auf die *Verbreitung und Zugänglichmachung von* Tools, Patches, Anleitungen und anderer Hilfsmittel zur Umgehung von Schutzmechanismen abgestellt werden. Da die Handlungsform des Verbreitens und Zugänglichmachens dieser Hilfsmittel meistens öffentlich erfolgt, ist die Verfolgung dieses zweiten Ansatze wiederum nicht dadurch erschwert, dass die Tathandlung sich in der Privatsphäre abspielt. Ein Verbot und insbesondere eine Bestrafung der Verbreitung diesbezüglicher Tools und Programme ist jedoch vor allem im Hinblick auf Dual-use-Produkte gesetzestechnisch schwierig begrenzbar und erfordert einen besonderen rechtspolitischen Begründungsbedarf.

Auch in diesem zweiten Bereich des Schutzes von technischen Sicherungsmechanismen geht es somit darum, eine effektive und angemessene rechtliche Gesamtstrategie zu entwickeln.

C. Einzelne Lösungsvorschläge

Aufgrund der vorangegangenen Überlegungen ist für eine systematische Entwicklung konkreter Reformvorschläge – ähnlich wie für die Analyse de lege lata – damit zwischen den folgenden vier Aspekte zu differenzieren:

- der Kopie der digitalen Güter (als der eigentlich schädigenden Verletzungshandlung),
- dem (insb. öffentlichen) Angebot von Vorlagen zum Kopieren (die das Erstellen der Raubkopien erst ermöglichen und häufig selbst Raubkopien sind)

sowie – im Bereich der Schutzmechanismen (insb. Kopierschutzverfahren, DRM-Systeme) –

- der Umgehung der technischen Schutzmechanismen und
- dem öffentlichen Angebot von Tools und anderer Hilfsmittel zur Umgehung von technischen Schutzmechanismen.

Ein – aus der Sicht der Rechteinhaber – ideales Schutzsystem müsste dabei alle vier genannten Handlungen strafrechtlich bewehren und verfolgen. Jedoch ist es möglich, bestimmte Defizite bei der Strafbewehrung der einen Handlung durch eine stärkere Strafbewehrung einer anderen Handlung (die eine zur Tatdurchführung essentielle Vorbereitungshandlung darstellt) auszugleichen. Die Wirksamkeit des strafrechtlichen Schutzsystems ergibt sich dadurch erst durch die Addition und das Zusammenspiel der Strafbewehrung der genannten Einzelhandlungen, die daher zunächst getrennt zu untersuchen sind.

1. Kopie der digitalen Güter

Die Analyse des geltenden Rechts in Kapitel 3 hat gezeigt, dass die rechtliche Erfassung der Kopie digitaler Güter in der hier interessierenden Masse der Fälle deswegen problematisch ist, weil nach wie vor ungeklärt ist, ob eine rechtmäßige Privatkopie auch dann vorliegt, wenn eine rechtswidrig angebotene Vorlage genutzt wird.

- Bei der zivilrechtlichen Beurteilung sprachen die besseren Gründe bereits de lege lata für eine Rechtswidrigkeit dieser Handlungen.[458] Vor allem solange der Gesetzgeber nicht durch entsprechende Vergütungsregelungen für die Möglichkeit einer Kompensation der Rechteinhaber sorgt, muss diese Beurteilung schon aus verfassungsrechtlichen Überlegungen auch de lege ferenda gelten. Die zivilrechtliche Gesetzeslage muss daher insoweit – auch aus verfassungsrechtlichen Überlegungen – in dem hier dargestellten Sinn klargestellt werden. Wenn der Gesetzgeber sich zur Entwicklung von Pauschalvergütungslösungen entschließt, so sollte es dabei zu einem Nebeneinander zwischen Individualvergütungssystemen und Pauschalvergütungen kommen.

- Für die strafrechtliche Beurteilung ist dagegen aus den oben näher ausgeführten Gründen[459] eine entsprechende Auslegung de lege lata wegen des (auch für akzessorische Strafvorschriften geltenden) strafrechtlichen Bestimmtheitsgebots von Art. 103 Abs. 2 GG nicht möglich. De lege ferenda spricht zwar der Wert des verletzten Rechtsguts und das Maß der Sozialschädlichkeit der massenhaft erfolgenden Verletzungshandlung für eine Strafbewehrung. Allerdings ist auch zu berücksichtigen, dass die private Kopie ungeschützter digitaler Güter von rechtwidrig hergestellten Vorlagen – anders als die Umgehung von Sicherungsmechanismen – keine wesentliche kriminelle Energie erfordert und auch nur einen geringeren Handlungsunwert aufweist. Nach den oben dargestellten Vorgaben des Bundesverfassungsgerichts sind für die Frage der Kriminalisierung von Verhaltensweisen darüber hinaus auch die Vorstellungen in der modernen Gesellschaft über die Rolle des Strafrechts sowie die praktische Wirksamkeit von Strafdrohungen und die Möglichkeit ihres Ersatzes durch andere rechtliche Sanktionen nicht außer Acht zu lassen. Die moderne Kriminalpolitik ist deswegen aufgrund der ultima ratio Funktion des Strafrechts bei massenhaften Delikten mit kleineren Einzelschäden nicht auf eine Kriminalisierung, sondern eher auf eine Entkriminalisierung gerichtet. Dies gilt vor allem in Fällen, in denen die Kriminalisierung in der Praxis aufgrund der faktischen Nichtverfolgbarkeit in der Privatsphäre nicht durchgesetzt werden kann.[460] Selbst bei Aufdeckung einschlägiger Fälle würden die – erheblich überlasteten Strafverfolgungsbehörden – die einschlägigen Fälle nicht schwerpunktmäßig verfolgen. Eine Kriminalisierung der privaten Kopie von einer rechtswidrig angebotenen Vorlage würde daher zwar die Rechtswidrigkeit und Sozialschädlichkeit dieses Verhaltens plakativ deutlich machen und insoweit ein richtiges Signal zur Rechtswidrigkeit dieser Handlungen aussenden, jedoch im Ergebnis keinen großen praktischen Gewinn bringen und damit auf ein nur symbolisches Strafrecht hinauslaufen. Ein Verzicht auf die *Strafbarkeit* der Erstellung privater Kopien von rechtswidrig erstellten Vorlagen wäre daher für den Schutz digitaler Güter nicht nur

458. Siehe oben III. B. 2. c).
459. Siehe oben III. B. 2. c).
460. Siehe insoweit auch die Begründung zum Referentenentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, oben Fn. 196, S. 34.

> wenig schädlich, insb. wenn auf andere Weise die *Rechtswidrigkeit* der entsprechenden Kopierhandlungen eindeutig klargestellt würde. Eine solche Klarstellung der Rechtswidrigkeit der Erstellung privater Kopien mit Hilfe von rechtswidrig erstellten Vorlagen würde durch einen Verzicht auf eine Kriminalisierung der entsprechenden Handlungen sogar erleichtert: Bei der Diskussion der aktuellen Urheberrechtsnovelle zur Regelung des Urheberrechts in der Informationsgesellschaft wurde deutlich, dass die Widerstände gegen eine klare Etikettierung dieser Privatkopien als rechtswidrig zu einem erheblichen Teil darauf beruhen, dass mit der Bewertung dieser Handlungen als rechtswidrig auch eine Kriminalisierung von Vorgängen in der Privatsphäre einherginge.[461]

Ein sinnvolles kriminalpolitisches Konzept sollte deswegen nach einem Weg suchen, die private Kopie von rechtswidrig hergestellten Vorlagen nicht zu kriminalisieren, jedoch klar als rechtswidrig zu beurteilen. Darüber hinaus könnten auch angemessene zivilrechtliche oder ordnungswidrigkeitenrechtliche Sanktionen entwickelt werden, die nicht den gleichen kriminalpolitischen Bedenken und Vollzugsproblemen wie Kriminalstrafen ausgesetzt sind.

Als angemessene Lösungsmöglichkeiten kämen damit in Betracht:

- die Beurteilung der privaten Kopie von rechtswidrig erstellten Vorlagen als rechtmäßig unter gleichzeitiger Schaffung einer angemessenen Geräteabgabepflicht (was für den Internetbereich aber kaum praktikabel ist),

- die Beurteilung der privaten Kopie von rechtswidrig erstellten Vorlagen als rechtswidrig unter Ausschluss der Strafvorschrift des § 106 UrhG,

- die Beurteilung der privaten Kopie von rechtswidrig erstellten Vorlagen als rechtswidrig unter Ausschluss der Strafvorschrift des § 106 UrhG, jedoch bei gleichzeitiger Erfassung durch eine Ordnungswidrigkeit (die z.B. lex specialis zu § 106 UrhG sein könnte),

- die Beurteilung der privaten Kopie von rechtswidrig erstellten Vorlagen als rechtswidrig unter Ausschluss der Strafvorschrift des § 106 UrhG, jedoch unter Schaffung von wirksamen zivilrechtlichen Sanktionen.

Die zuletzt genannte Entwicklung eines effektiven zivilrechtlichen Sanktionensystems hätte dabei – auch für andere Bereiche des Urheberrechts – den Vorzug, dass die Rechtsdurchsetzung nicht von den – ohnehin überlasteten und an der Strafverfolgung von (auch massenhaft auftretenden) Einzelbagatelldelikten grundsätzlich wenig interessierten – Strafverfolgungsbehörden vorgenommen werden müsste, sondern dass den Verbänden und Vereinigungen der Rechteinhaber wirksame Maßnahmen der Selbsthilfe an die Hand gegeben würden. Für ein derartiges zivilrechtliches Sanktionensystem wären neben den materiell-rechtlichen Sanktionstatbeständen (z.B. in Anlehnung an die deutsche Rechtsprechung zum Schadensersatz nach den Grundsätzen

461. Vgl. dazu im Hinblick auf die Umgehung von Schutzmaßnahmen z.B. S. 49 f. der Begründung des Referentenentwurfs, oben Fn. 196: „Vor dem Hintergrund der Offizialmaxime wird damit zugleich der Zwang zu umfangreichem Tätigwerden der Strafverfolgungsbehörden vermieden, das weitgehend wenig erfolgversprechend bliebe und im Hinblick der sich häufig ergebenden Notwendigkeit von Hausdurchsuchungen in der Verhältnismäßigkeit nicht unproblematisch wäre."

der Lizenzanalogie bei Urheberrechtsverletzungen, an die treble-damage-Klagen des angloamerikanischen Rechts oder an die neuen verwaltungsrechtlichen und zivilrechtlichen Sanktionstatbestände des EG-Rechts[462]) vor allem auch angemessene Auskunftsansprüche (z.B. gegen die Internet-Provider) erforderlich, um eine effektive Rechtsverfolgung zu ermöglichen. Bei der Ausgestaltung der Auskunftsansprüche wäre dabei vor allem entscheidend, dass nicht nur – wie bisher im deutschen Recht vorherrschend – bei nachgewiesener Schadensverursachung ein Auskunftsanspruch über die Schadenshöhe gewährt wird, sondern auch ein Auskunftsanspruch über das „Ob“ der Schädigung in bloßen Verdachtsfällen. Ein derartiges zivilrechtliches Sanktionensystem könnte in dem hier diskutierten Bereich sehr viel wirksamer als eine in der Praxis nicht durchgesetzte Kriminalisierung sein. Soweit der Gesetzgeber kein angemessenes System der Geräteabgabe schafft oder ein solches aufgrund der tatsächlichen Gegebenheiten die Wirklichkeit nicht zutreffend abbilden kann, stellt ein effektives System zivilrechtlicher Sanktionen deswegen die effektivste Möglichkeit zur Verhinderung der massenhaften Privatkopien von rechtswidrig angebotenen Vorlagen dar.

2. Angebot der Vorlagen

Die Analyse des geltenden Rechts in Kapitel III hat gezeigt, dass das – im Mittelpunkt der schadensverursachenden Kopie digitaler Güter (vor allem im Internet) stehende – Angebot der Kopiervorlagen durch die *materiell-rechtlichen Strafvorschriften* der §§ 106 ff. UrhG in weitgehendem Umfang erfasst wird.

Nach der Neuregelung des UrhG durch das geplante Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft[463] wird dieses Ergebnis noch eindeutiger sein, da mit den §§ 15 Abs. 2 Nr. 2, 19a UrhG-E ein ausschließliches Recht der öffentlichen Zugänglichmachung – das insbesondere das Anbieten im Internet erfasst – aufgenommen werden soll und zudem § 15 Abs. 3 UrhG-E zukünftig keine Anhaltspunkte mehr dafür liefert, dass eine sukzessive Öffentlichkeit nicht ausreichend ist. Diese Änderung ist daher zur Bekämpfung der vorliegend untersuchten Missbräuche empfehlenswert.

Im Hinblick auf die dargestellten Missbräuche in File-Sharing-Systemen ist auch die vom Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vorgeschlagene Änderung von § 52 Abs. 3 UrhG-E erforderlich, dass die öffentliche Zugänglichmachung von Werken nur mit Einwilligung des Rechteinhabers zulässig ist.[464] Hierdurch wird klargestellt, dass das weltweite Angebot digitaler Güter in File-Sharing-Systemen aufgrund dieser Ausnahmebestimmungen nicht zulässig ist.

Zivilrechtliche Änderungen sind über diese Vorschläge des Regierungsentwurfs hinausgehend aber auch im Hinblick auf § 53 Abs. 1 S. 2 UrhG erforderlich. Wie oben dargestellt,[465] besteht beim Abruf von urheberrechtlich geschützten Werke über File-Sharing-Systeme die Gefahr, dass die Kopie des Werkes damit gerechtfertigt wird, hier werde eine Privatkopie gem. § 53

462. Vgl. dazu *Sieber*, Das strafrechtliche Sanktionensystem zum Schutz der europäischen Gemeinschaftsinteressen, in: Ellen Schlüchter (Hrsg.), Festschrift für Friedrich Geerds, Verlag Schmidt-Römhild, Lübeck, 1995, S. 113 ff. (auch abgedruckt in dem Tagungsband: van Gerven/Zuleeg (Hrsg.), Sanktionen als Mittel zur Durchsetzung des Gemeinschaftsrechts, Schriftenreihe der Europäischen Rechtsakademie Trier, Band 12, 1996, S. 71 ff.).
463. Siehe oben Fn. 198.
464. Siehe oben Fn. 196.
465. Siehe oben III. C. 2.

Abs. 1 S. 2 UrhG durch einen anderen hergestellt. Diese Argumentation ist – wie dargestellt – zwar aufgrund der Rechtsprechung des BGH nicht überzeugend.[466] Vorsorglich sollten entsprechende Auslegungsprobleme jedoch durch eine gesetzliche Klarstellung vermieden werden. Falls der Gesetzgeber sich nicht dazu entschließen kann, die Privatkopie durch einen anderen ganz aus dem Gesetz zu streichen, so sollte für deren Zulässigkeit wenigstens verlangt werden, dass die Privatkopie durch einen anderen nur dann gestattet ist, wenn der begünstigte Nutzer ihm hierfür eine rechtmäßig erlangte Vorlage zur Verfügung stellt.[467]

Die empirische Analyse der Rechtswirklichkeit hat im Hinblick auf das Angebot der Vorlagen allerdings ein *praktisches Vollzugsdefizit* deutlich gemacht: Das Problem bei der Bekämpfung der – vor allem im Internet – angebotenen Vorlagen besteht darin, dass diese Delikte von den Strafverfolgungsbehörden in der Praxis, wenn überhaupt, nur in ganz selten Ausnahmefällen verfolgt werden. Der Grund hierfür liegt zum einen in den Kapazitätsengpässen und der Überlastung der Strafverfolgungsbehörden, zum anderen in den Schwierigkeiten der Identifizierung und der Verfolgung der Anbieter der Vorlagen im Internet, vor allem in Fällen mit Auslandsbezug.[468] Angesichts der oben dargestellten empirischen Situation, aber auch der bekannten Überlastung der Strafverfolgungsbehörden, ist der Appell an eine stärkere Verfolgung der Angriffe auf digitale Güter berechtigt; er sollte vor allem durch eine verbesserte Ausbildung der Ermittlungsbehörden und ihre Sensibilisierung für den Schutz geistiger Güter unterstützt werden. Vor allem im Hinblick auf die möglichen Verbesserungen beim Zusammenwirken von staatlicher Strafverfolgung und privaten Schutzmaßnahmen der Industrie im Bereich des Internets kann auf einschlägige Vorschläge des Verfassers für die Bertelsmann-Stiftung verwiesen werden.[469] Bei realistischer Einschätzung der Situation werden derartige Maßnahmen in dem hier untersuchten Bereich jedoch angesichts der Mittelknappheit der öffentlichen Hand nur teilweise in der Lage sein, die Situation im Bereich der Strafverfolgung zu ändern.

Die gegenwärtige Situation und diese Perspektiven sind vor allem deswegen unbefriedigend, weil angesichts der in der Öffentlichkeit leicht feststellbaren rechtswidrigen Angebote (z.B. in den File-Sharing-Systemen des Internets) eine rechtliche Strategie gegen die entsprechenden Angebote durchaus erfolgreich sein könnte. Die im empirischen Teil dieses Gutachtens dargestellten privaten Verfolgungsmaßnahmen der betroffenen Rechteinhaber – z.B. gegen Softwarepiraterie – machen dies anschaulich deutlich. Aus diesem Grund sollte auch im Bereich der illegalen Angebote – hier allerdings *neben* die strafrechtliche Verfolgungsschiene – eine wirksame zivilrechtliche Strategie zur Bekämpfung der illegalen Angebote etabliert werden. Außer geeigneten abschreckenden zivilrechtlichen Sanktionstatbeständen (z.B. in Anlehnung an die angloamerikanischen treble-damage-Klagen) sind hier vor allem wieder zivilrechtliche Auskunftspflichten (z.B. gegen die Internet-Provider) erforderlich.[470] Durch eine internationale Koordination des zivilrechtlichen Verfolgungsansatzes müsste dabei sichergestellt werden, dass diese zivilrechtliche Verfolgungsschiene auch gegen die im Ausland aktiven Anbieter wirksam ist. Aufgrund der bestehenden weitreichenden Harmonisierung des Urheberrechts durch die bestehenden internationalen Abkommen könnte die internationale Koordinierung der zivilrechtlichen Verfolgungsschiene jedoch leichter sein, als die entsprechende Durchsetzung der –

466. Siehe oben III. C. 2.
467. Siehe auch KirchMedia, oben Fn. 266, S. 7.
468. Vgl. dazu *Sieber*, Hass im Internet, ZRP 2001, 97, 98 f.
469. Vgl. *Sieber*, Legal Regulation, Law Enforcement and Self-Regulation: A new Alliance for Preventing Illegal Content on the Internet, in: Waltermann/Machill (eds.), Protecting our children on the Internet, Gütersloh 2000, S. 319 ff.
470. Vgl. dazu oben bei Fn. 462.

gerade im Bereich von kleineren Delikten notorisch uneffektiven – strafrechtlichen Amts- und Rechthilfe.

3. Umgehung der Schutzmechanismen

Die rechtliche Analyse hat weiter gezeigt, dass die Umgehung von Schutzmechanismen digitaler Güter bereits heute in vielen Fällen strafbar, jedoch nicht durchgehend gewährleistet und stets vom Einzelfall abhängig ist: § 17 UWG greift insbesondere ein, wenn der Ersttäter – wie häufig bei der Umgehung von DRM-Systemen – sich bei der Umgehung der Sicherungsmechanismen Geschäftsgeheimnisse verschafft und diese verwertet; der Tatbestand kommt jedoch nicht zur Anwendung, wenn die Betriebsgeheimnisse durch eine Veröffentlichung insbesondere im Internet bereits offenkundig geworden sind oder wenn der Täter sich die Betriebsgeheimnisse nur aus „sportlichem Ehrgeiz“ verschafft. Die in den letztgenannten Fallkonstellationen auftretenden Strafbarkeitslücken lassen sich allerdings in erheblichem Umfang durch § 202a StGB schließen, dessen Tatobjekt keine Betriebsgeheimnisse, sondern nur gesicherte Daten verlangt und der darüber hinaus auch nicht durch subjektive Absichtsmerkmale eingeschränkt ist. Daneben erfasst § 263a StGB diejenigen Umgehungen von Schutzmechanismen, in denen es – wie häufig beim Einsatz von SmartCards – zu einer unmittelbaren Vermögensverfügung durch einen dem Opfer zurechenbaren Datenverarbeitungsvorgang (auch auf der Hardware des Täters) kommt. Die Neuregelung des § 108b UrhG in der Fassung des Regierungsentwurfs für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft enthält darüber hinaus zwar das strafrechtlich bewehrte Verbot der Umgehung wirksamer technischer Maßnahmen sowie das Verbot der Entfernung oder Veränderung von Informationen, die der Rechtewahrung dienen (z.B. Fingerprints und Watermarks); er ist jedoch bei einer großen Zahl der vorliegend analysierten Fälle nicht anwendbar, da die vorgeschlagene Strafnorm bei einem Handeln zum eigenen persönlichen Gebrauch ausscheidet. Hinzu kommt, dass § 108b UrhG-E einen unbefugten Eingriff in eine *wirksame* technische Maßnahme fordert und trotz der Gesetzesbegründung zum Regierungsentwurfs für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft ungeklärt ist, wann diese vorliegt. Problematisch ist dies z.B. bei den verwendeten Kopierschutzmechanismen für Datenträger, die mit Hilfe entsprechender Programme häufig leicht umgangen werden können. Strafbarkeitslücken bestehen damit insbesondere bei der 1:1 Kopie von Datenträgern, auch wenn diese mit einem Kopierschutzmechanismus versehen sind. Die strafrechtliche Erfassung der Umgehung von Schutzmechanismen erfordert dabei in vielen Fällen komplizierte und schwierige rechtliche Konstruktionen. Eine strafrechtliche Verfolgung der Umgehung von Schutzmechanismen wird dem Rechtsanwender und insbesondere den Strafverfolgungsbehörden daher nicht leicht gemacht.

De lege ferenda wirft diese Feststellung zunächst die Frage auf, ob es bei der Umgehung von Schutzmechanismen bei dem gegenwärtigen „Einzelansatz“ unterschiedlicher Strafbestimmungen bleiben soll, ob eine allgemeine Vorschrift über die Umgehung von Schutzmechanismen digitaler Güter erforderlich ist oder ob insoweit ein vermittelnder Ansatz verfolgt werden sollte: Ein Verzicht auf die vorgenannten Strafbestimmungen kommt dabei nicht in Betracht, da diese Strafbestimmungen den spezifischen Unrechtsgehalt spezieller Formen der Umgehung von Schutzmechanismen erfassen und dieser spezifische Unrechtsgehalt im Falle seines Vorliegens auch durch eine entsprechende Verurteilung zum Ausdruck gebracht werden sollte. Eine – z.B. durch Umgestaltung der oben diskutierten Vorschrift des § 303a StGB – zu schaffende

allgemeine „Generalnorm“ zur Erfassung aller Verletzungen von Integritätsinteressen an Daten ist gleichermaßen abzulehnen, da eine solche Norm aufgrund der ultima ratio Funktion des Strafrechts nicht zu rechtfertigen und im übrigen auch kaum abzugrenzen wäre. Damit stellt sich die Frage, inwieweit die vorgenannten Einzelvorschriften des StGB und des UWG sowie der neue Ansatz der §§ 95a, 108b UrhG-E berechtigt und/oder reformbedürftig sind.

- Die vorangegangene empirische Analyse zeigt, dass der Ansatz von §§ 95a, 108b Abs. 1 Nr. 1 UrhG-E im Bereich der Umgehung von Schutzmechanismen nicht nur berechtigt, sondern grundsätzlich auch geboten ist. Die Umgehung von Schutzmaßnahmen stellt im Bereich der geschützten digitalen Güter die zentrale Angriffsform dar, die zu existenziellen Schäden der Software-, Audio- und Videoindustrie führt. Der Bereich der technischen Maßnahmen wird dabei in der Vorschrift zwar grundsätzlich weit gefasst, dies ist durch die Begrenzung auf wirksame technischen Maßnahmen jedoch berechtigt. Zur Vermeidung von Missverständnissen und Auslegungsschwierigkeiten wäre allerdings eine Modifikation der Vorschrift dahingehend wünschenswert, dass für eine wirksame technische Maßnahme nur ein bestimmtes (noch näher zu konkretisierendes) technisches Schutzniveau erforderlich ist. Immerhin zeigt der Hinweis in der Gesetzesbegründung zum Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, dass der Gesetzgeber auch dann von wirksamen technische Maßnahmen ausgeht, wenn eine Umgehung möglich ist.[471]

  Die Strafbestimmung geht auch nicht dadurch zu weit, dass sie die wissenschaftliche und sonstige gebotene Auseinandersetzung mit Schutzmaßnahmen erschwert: Der Regierungsentwurf weist insoweit darauf hin, dass die Vorschrift eine auf Werkzugang oder Werkverwertung gerichtete Umgehungsabsicht voraussetzt und Umgehungshandlungen, die ausschließlich wissenschaftlichen Zwecken dienen, nicht erfasst werden.[472] Da allerdings nicht zweifelsfrei ist, ob beim Test von Schutzmechanismen nicht doch der Zugang zum Werk ermöglicht werden soll oder gar muss, sollte das in der Sache berechtigte Anliegen der Bundesregierung besser umgesetzt werden. Dies könnte z.B. über eine Privilegierung erreicht werden, die auf ein Handeln abstellt, das ausschließlich auf den Gewinn von Erkenntnissen über Schutzmechanismen abstellt.

  Anders als die zivilrechtliche Vorschrift des § 95a Abs. 1 UrhG-E erfasst die Strafvorschrift des § 108b Abs. 1 UrhG-E die Tat nicht, wenn sie „ausschließlich zum eigenen privaten Gebrauch des Täters oder mit dem Täter persönlich verbundener Personen erfolgt oder sich auf einen derartigen persönlichen Gebrauch bezieht.“ Der Regierungsentwurf ermöglicht es dadurch jedermann, zum persönlichen Gebrauch Schutzmaßnahmen zu umgehen, soweit dies nicht gegen andere Strafvorschriften (z.B. §§ 17 UWG, § 202a StGB, § 263a StGB) verstößt. Die Begründung des Regierungsentwurfs zum Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft rechtfertigt dies damit, dass die Nutzung zum eigenen privaten Gebrauch des Täters oder mit dem Täter persönlich verbundener Personen der Regelung des § 15 Abs. 3 UrhG entspreche und eine Kriminalisierung des Nutzers in der Privatsphäre verhindern wolle.[473] Die Fragwürdigkeit der erstgenannten Begründung wird jedoch deutlich, wenn man die oben dargestellten Gesichtspunkte berücksichtigt, welche die Begrenzung der privaten Kopie auf rechtmäßig

471. Vgl. Fn. 196.
472. Vgl. oben Fn. 196, S. 62.
473. Vgl. oben Fn. 196, S. 68.

erlangte Vorlagen fordern, da bei der Umgehung von Schutzmechanismen im Regelfall gerade *keine* rechtmäßig erlangte Kopie eingesetzt wird. Als Begründung für die Privilegierung bleibt damit lediglich der Hinweis auf die unerwünschte Kriminalisierung von Handlungen in der Privatsphäre, der allerdings – anders als bei der privaten Kopie von rechtswidrigen (ungeschützten) Vorlagen – hier deswegen weniger überzeugend ist, weil der Unrechtsgehalt der Umgehung von technischen Schutzmechanismen sehr viel größer ist als der Unrechtsgehalt der „bloßen" Kopie von rechtswidrig erlangten Vorlagen ungeschützter Daten. Dies zeigt sich auch daran, dass das Argument der Kriminalisierung von Handlungen in der Privatsphäre bei den oben analysierten Straftaten der §§ 202a, 263a StGB, § 17 UWG ebenfalls nicht zum Tragen kommt. Da diese Vorschriften weiter anwendbar bleiben, dürfte die Privilegierung des eigenen Gebrauchs durch § 108b Abs. 1 UrhG-E in der Praxis auch nur eine begrenzte Relevanz haben, im Hinblick auf die schwierige Anwendbarkeit der §§ 202a, 263a StGB, § 17 UWG für die hier untersuchten Fallkonstellationen jedoch zu erheblicher Rechtsunsicherheit führen. Hinzu kommt der weitere Wertungswiderspruch, dass auch bei den neuen Vorfeldtatbeständen des § 108b Abs. 2, 95a Abs. 3 UrhG-E das Handeln zum privaten Gebrauch nicht privilegiert wird. Auch ist überaus fraglich, ob die Privilegierung der Umgehung von Sicherungsmaßnahmen zum eigenen Gebrauch sich noch mit Art. 6 Abs. 1 der zugrunde liegenden EG-Richtlinie zur Harmonisierung bestimmter Aspekte der Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft vereinbaren lässt.[474] Art. 6 Abs. 1 verlangt von den Mitgliedstaaten „einen angemessenen Rechtsschutz gegen die Umgehung wirksamer technischer Maßnahmen durch eine Person, der bekannt ist oder den Umständen nach bekannt sein muss, dass sie dieses Ziel verfolgt". Damit sprechen insgesamt die besseren Gründe dafür, die durch die Privilegierung des privaten Handelns entstehenden Wertungswidersprüche des § 108b Abs. 1 UrhG-E sowohl mit den §§ 202a StGB, 17 UWG als auch mit den neuen Vorfeldtatbeständen des § 108b Abs. 2 UrhG-E dadurch aufzulösen, dass bei Angriffen auf Schutzmechanismen die Privilegierung des Handelns zum persönlichen Gebrauch in Wegfall kommen sollte.

- Die Strafvorschrift des § 4 ZKDSG[475] begrenzt die Androhung einer Freiheitsstrafe bis zu einem Jahr auf die von § 3 Nr. 1 ZKDSG erfasste Herstellung, das Einführen und die Verbreitung einer Umgehungseinrichtung zu gewerblichen Zwecken. § 4 ZKDSG sollte allerdings nicht nur diese genannten Vorfeldtatbestände erfassen, sondern auch die im Mittelpunkt ihrer Zielsetzung stehende eigentliche Tathandlung der Umgehung der einschlägigen Schutzmechanismen. Die mögliche Konkurrenz dieser Tathandlung mit § 263a StGB oder § 265a StGB ist kein überzeugender Grund, auf sie zu verzichten, da den zuletzt genannten Vorschriften ein anderes Rechtsgut und ein anderer Unrechtsgehalt zugrunde liegt. Die Aufnahme der eigentlich interessierenden Tathandlung des Umgehens des Zugangskontrolldienstes ist um so mehr geboten, als die obige rechtliche Analyse gezeigt hat, dass § 263a StGB im Einzelfall schwierig anzuwenden ist.

  Die §§ 4, 5 ZKDSG sollten die Umgehung eines Zugangskontrolldienstes – d.h. von technischen Verfahren oder von Vorrichtungen, welche die erlaubte Nutzung eines zugangskontrollierten Dienstes ermöglichen – dabei auch in den Fällen einschließen, in denen der Nutzer nicht zu gewerblichen Zwecken handelt. Die empirische Analyse hat deutlich gezeigt, dass die von Zugangskontrolldiensten geschützten digitalen Güter nicht nur von

474. Vgl. dazu oben Fn. 446.
475. Siehe oben Fn. 195.

organisiert handelnden Straftäter, sondern in massenhafter Form auch von Endnutzern umgangen werden. Hinzu kommt, dass dem „Conditional Access“ in Zukunft eine große Bedeutung zukommen wird, weil vor allem im Internet vermehrt digitale Inhalte nur noch gegen entsprechende Bezahlung und Registrierung angeboten werden. Der „Conditional Access“ kann daher das Geschäftsmodell der Zukunft für die Distribution digitaler Inhalte sein.

- Bei § 17 UWG sollte zumindest für die Tathandlungen des Mitteilens und Verwertens auf die subjektiven Tatbestandsmerkmale des Handelns „zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen“, verzichtet werden, da der Verrat fremder Wirtschaftsgeheimnisse auch ohne derartige Absichten strafwürdig ist, die Merkmale bei zutreffender Auslegung ohnehin keine nennenswerte Eingrenzungsfunktion haben und (z.B. beim Handeln aus „sportlichen Gründen“) zu überflüssigen Abgrenzungsschwierigkeiten führen.

  Aufgrund der zentralen Bedeutung immaterieller Wirtschaftsgüter für die moderne Informationsgesellschaft sollte § 17 UWG auch in das StGB eingefügt werden, damit ihm – schon bei der Ausbildung der Juristen – eine größere Beachtung zukommt und er dadurch bei der praktischen Strafverfolgung stärker beachtet wird. Durch eine derartige Lozierung im StGB könnte der Gesetzgeber ein Signal für einen besseren Schutz immaterieller Güter setzen, die für die Volkswirtschaft in der Informationsgesellschaft von zentraler Bedeutung sind.

4. Öffentliches Angebot und Besitz von Tools zur Umgehung von Schutzmechanismen

Die empirische Analyse und die strategischen Überlegungen zur Entwicklung eines effektiven rechtlichen Präventionskonzepts zum Schutz digitaler Güter haben gezeigt, dass die Strafbarkeit des öffentlichen Anbietens von Tools und anderer Hilfsmittel zur Umgehung von Schutzmechanismen für den Schutz digitaler Güter von besonderer Bedeutung ist. Denn die öffentliche Verbreitung und Zugänglichmachung dieser Hilfsmittel ist zusammen mit der öffentlichen Verbreitung und Zugänglichmachung von Kopiervorlagen eine unabdingbare Voraussetzung für die massenhafte Erstellung der Raubkopien von digitalen Gütern.

Ebenso wie das öffentliche Anbieten von Kopiervorlagen ist das öffentliche Anbieten insbesondere von Hackingtools in der Öffentlichkeit auch feststellbar und damit verfolgbar. Die Verfolgung des öffentlichen Anbietens der Tools zur Umgehung von Schutzmechanismen ist deswegen auch sehr viel leichter möglich als die Umgehung der Schutzmaßnahmen selbst, die sich meist in der Privatsphäre abspielt. Anders als diese Handlung ist die Strafbarkeit des öffentlichen Anbietens von entsprechenden Tools und anderen Hilfsmitteln deswegen auch nicht dem – in der Begründung des Regierungsentwurfs der Urheberrechtsnovelle formulierten – Bedenken ausgesetzt, dass die Ermittlungsbehörden zur Verfolgung mit Hausdurchsuchungen und ähnlichen Maßnahmen in die Privatsphäre eindringen müssen.[476]

Die Schwierigkeit eines entsprechenden Verfolgungsansatzes liegt jedoch insbesondere in der genauen Beschreibung der strafbaren Tools, vor allem im Hinblick auf die oben genannten

476. Vgl. oben Fn. 196, S. 68 f.

Dual-use-Produkte. Diese Problematik der Produkteingrenzung hängt eng mit der Fragestellung zusammen, inwieweit der Tatbestand durch bestimmte Absichtsmerkmale des Täters einzuschränken ist (die auch eine zu weit gehende Produktbeschreibung wieder kompensieren können). Schließlich stellt sich das Problem, inwieweit nicht nur die Tathandlung des öffentlichen Verbreitens entsprechender Tools erfasst werden soll, sondern auch schon im Vorfeld dieser – den materiellen Unrechtskern bildenden – Tathandlung auch die Herstellung, die Verschaffung, die Einfuhr oder der Besitz sowie die Bewerbung dieser Werkzeuge. Zu denken ist zudem an eine Pönalisierung von Informationen und Anleitungen betreffend der Tools zur Umgehung von Schutzmechanismen.

Die vorausgegangene rechtliche Analyse macht deutlich, dass die bisher vorliegenden Strafvorschriften und Gesetzentwürfe diese Herausforderungen nicht bewältigt und noch keine stimmigen Konzepte vorgelegt haben, die sowohl einen effektiven strafrechtlichen Schutz der digitalen Güter ermöglichen als auch die Freiheit der Forschung im Bereich der Umgehung von Schutzmaßnahmen und einen sinnvollen Einsatz der Dual-use-Produkte nicht tangieren. Die bisherigen Regelungen der §§ 4, 5 ZKDSG und der geplanten §§ 95a Abs. 3, 108b UrhG-E machen diese Schwierigkeiten deutlich und lassen insbesondere auch kein schlüssiges Gesamtkonzept erkennen:

- § 2 ZKDSG definiert „Umgehungseinrichtungen“ als „technische Verfahren oder Vorrichtungen, die *dazu bestimmt sind oder entsprechend angepasst sind*, die unerlaubte Nutzung eines zugangskontrollierten Dienstes zu ermöglichen. Für die Auslegung ist völlig unklar, wer diese Bestimmung vornimmt und wie bei Dual-use-Produkten zu entscheiden ist. Würde man für die Gebrauchsbestimmung auf den Willen des Entwicklers abstellen, so wäre Schutzbehauptungen Tür und Tor geöffnet.

  § 95a Abs. 3 UrhG-E betrifft demgegenüber „Vorrichtungen, Erzeugnisse oder Bestandteile 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.“ Während die Ziff. 1 durch ihr Absichtsmerkmal klare Konturen hat, sind die in Nr. 2 und 3 enthaltenen Merkmale des begrenzten wirtschaftlichen Zwecks bzw. die „hauptsächlich“ zur Umgehung technischer Maßnahmen dienende Herstellung usw. bei isolierter Betrachtung unbestimmt und zur Abgrenzung von Dualuse-Produkten untauglich. Zudem scheinen vom Wortlaut der Vorschrift Informationen und Anleitungen zum Umgehen von Schutzmechanismen zumindest nicht zwingend erfasst. Dies stellt aber eine bedeutende Gesetzeslücke dar, da gerade dem technisch weniger versierten Nutzer wird eine Umgehung von Schutzmechanismen erst dadurch ermöglicht, dass ihm entsprechende Informationen an die Hand gegeben werden. Dabei werden diese Informationen – vor allem in Fachzeitschriften – häufig in einer Form präsentiert, die beim Nutzer gerade erst den Wunsch erweckt, entsprechende Umgehungen von Schutzmechanismen vorzunehmen.

- § 4 i.V.m. § 3 Nr. 1 ZKDSG versucht dann ähnlich wie § 108b Abs. 2 UrhG-E die zu unbestimmte und zu weite objektive Eingrenzung des Tatobjekts dadurch auszugleichen, dass der Tatbestand auf ein Handeln „zu gewerbsmäßigen Zwecken“ bzw. bei § 108b Abs. 2 UrhG-E „zu gewerblichen Zwecken“ begrenzt wird (wobei § 111a Abs. 1 Nr. 1

UrhG-E für bestimmte Fälle des nicht-gewerblichen Handelns eine Ordnungswidrigkeit schafft). Die Begrenzung des Straftatbestandes auf ein Handeln zu gewerblichen Zwecken löst die Problematik der Dual-use-Produkte jedoch in keiner Weise, sondern verschlimmert den Tatbestand derart krass, dass er für die in der empirischen Analyse dargestellten jugendlichen Hacker unanwendbar wird, sich aber gleichzeitig für die im Bereich der Schutzmechanismen forschenden Unternehmen zu einer realen Gefahr entwickelt. Diese unsinnige Folge beruht darauf, dass die im Bereich von Schutzmechanismen forschende Industrie sowie die gutgläubigen Vertreiber von echten Dual-use-Produkten in der Regel gewerbsmäßig und gewerblich handeln, die mit der Verbesserung der Schutzmechanismen von digitalen Gütern dagegen eher seltener befassten jugendlichen Hacker dagegen meist nicht gewerbsmäßig oder gewerblich tätig sind. Die Merkmale des gewerbsmäßigen oder gewerblichen Handelns zielen daher nur teilweise auf den richtigen Adressaten. Der Gesetzgeber hat hier nicht erkannt, dass die Gewerbsmäßigkeit oder Gewerblichkeit des Handelns bei neutralen oder ambivalenten Verhaltensweise nichts über deren Unrechtsgehalt aussagt. Zu einer Eingrenzung der Verwendung von DualuseProdukten sind diese Merkmale daher auch völlig untauglich.

- Die Begrenzung der Tathandlungen auf gewerbsmäßiges oder gewerbliches Handeln wäre im übrigen auch dann unzutreffend, wenn es dem Gesetzgeber gelungen wäre, die Tatbestände auf ansonsten strafwürdige Fälle einzugrenzen. Die empirische Analyse dieses Gutachtens hat deutlich gemacht, dass die – für die massenhafte Verbreitung von Raubkopien geschützter digitaler Güter verantwortliche – Verbreitung von Hackingtools gerade nicht von gewerblich oder gewerbsmäßig handelnden Tätern verbreitet werden, sondern von Personen, die aus „sportlichem Ehrgeiz“ handeln. Eine Eingrenzung der Verbreitung von Hackingtools auf das gewerbliche oder gewerbsmäßige Handeln würde daher den neuen Bekämpfungsansatz völlig leer laufen lassen, zumal die gewerblich angebotenen Tools zumindest teilweise auf den „Vorarbeiten“ der Hacker beruhen. Die bereits erwähnte Ordnungswidrigkeit des § 111a Abs. 1 Nr. 1 UrhG-E stellt insoweit keinen wirksamen Ausgleich dar.

  Überzeugende Gründe für die Eingrenzung der Strafnorm auf gewerbliches oder gewerbsmäßiges Handeln gibt es im übrigen nicht: Während man beim Kopieren digitaler Güter zu privaten Zwecken und beim Umgehen von Schutzmechanismen zu privaten Zwecken an der Strafwürdigkeit der Tathandlung und am Erfolg der die Privatsphäre betreffenden Strafverfolgung noch zweifeln kann, kommt Entsprechendes beim öffentlichen Verbreiten der kriminellen Zwecken dienenden Tools und sonstigen Hilfsmittel nicht in Betracht. Die öffentliche Verbreitung dieser Tools ist für große Schäden verantwortlich und spielt sich auch nicht in der Privatsphäre ab.

Die Vorschriften über die öffentliche Verbreitung von Tools und Dienstleistungen zur Umgehung von zugangskontrollierten Diensten und von Schutzmechanismen müssen daher – unter besonderer Berücksichtigung der Dual-use-Problematik – völlig neu konzipiert werden. Im Rahmen des vorliegenden Gutachtens ist es zwar nicht möglich, ausformulierte einschlägige Gesetzesvorschläge zu entwickeln. Gleichwohl sollen einige konkrete Hinweise darauf gegeben werden, mit welchen Gesetzgebungstechniken die Problematik zu lösen ist.

Die wichtigsten Gesichtspunkte hierfür sind:

- Die Frage nach den Möglichkeiten einer objektiven Eingrenzung von nur kriminellen Zwecken dienenden Tools kann nicht von Rechtspolitikern und Juristen allein entschieden

werden, sondern nur in der gemeinsamen Diskussion mit den damit befassten Technikern und Wirtschaftsvertretern. Der entsprechende Dialog hat bisher noch nicht stattgefunden und muss erst noch geführt werden. Dabei ist allerdings nicht zu erwarten, dass eine überzeugende Möglichkeit für eine ausschließlich objektive Begrenzung auf kriminelle Tools gefunden wird. Diese beruht – wie die Problematik der (Computer-)Virenforschung zeigt – darauf, dass jedes entsprechende Tool analysiert werden muss, wenn man sich dagegen schützen will. Die objektive Tatbestandsbeschreibung der einschlägigen Delikte kann daher zwar eine sinnvolle Vorselektion übernehmen, die Tatbestände jedoch nicht auf strafwürdige Fälle begrenzen. Sieht man die Funktion der objektiven Beschreibung des Tatobjekts nur in einer – den Unrechtsgehalt nicht prägenden – Vorselektion, so sind die oben erörterten Begrenzungen auf „hauptsächlich“ oder „ganz überwiegend“ kriminellen Zwecken dienende Tools durchaus in Betracht zu ziehen. Weitere objektive Merkmale können darüber hinaus von der Rechtsprechung als Indizien für bestimmte Absichten der Straftatbegehung oder –unterstützung herangezogen und möglicherweise auch zu einem entsprechenden Kriterienkatalog weiterentwickelt werden.

- Die entscheidende Abgrenzung der strafbaren von den nicht strafwürdigen Fällen der Verbreitung von Dual-use-Produkten kann daher nicht im Bereich des objektiven Tatbestandes gefunden werden, sondern nur im Bereich des Tätervorsatzes und insbesondere der Täterabsichten. Das Spektrum der Lösungsmöglichkeiten ist dabei sehr viel weiter als die bisher vertretenen Lösungsansätze. Für die subjektiven Tatbestandseingrenzungen kommen z.B. nicht nur die bisher diskutierten Positivmerkmale, sondern auch Negativmerkmale in Betracht. Durch ein Positivmerkmal kann die Strafbarkeit z.B. auf Fälle beschränkt werden, in denen der Täter in der Absicht handelt, bestimmte Straftaten zu begehen (wie dies von Art. 6 der Convention on Cybercrime des Europarats gefordert wird).[477] Da derartige Absichten schwer nachweisbar sind und im übrigen auch das Verbreiten und Zugänglichmachen von überwiegend strafbaren Zwecken dienenden Tools bei einem Handeln des Täters aus „sportlichen Gründen“ oder aus Gleichgültigkeit strafwürdig sein kann, sollten insb. für die Tathandlung des Verbreitens jedoch auch Negativmerkmale in Betracht gezogen werden. Wenn die Tatobjekte auf Tools eingegrenzt werden, die ganz überwiegend kriminellen Zwecken dienen, dann kann es durchaus gerechtfertigt sein, die Tat zu bestrafen, wenn der Täter *nicht* zum Zwecke der Entwicklung von Schutzmechanismen oder anderer berechtigter Interessen handelt.

- Diese subjektiven Tatbestandsvoraussetzungen können auch im Hinblick auf die unter Strafe gestellten Tathandlungen differenzieren: Beim öffentlichen Verbreiten der Tools können z.B. strengere Anforderungen gestellt werden als beim bloßen Herstellen und Besitzen dieser Werkzeuge, das nur unter strengeren Einschränkungen und in besonderen Konstellationen bestraft werden sollte, um die Forschungs- und Informationsfreiheit nicht zu gefährden.

- Zudem sollte geprüft werden, inwieweit auch Anleitungen und Informationen zu Tools und anderen Hilfsmittel für die Umgehung von Schutzmechanismen zu verbieten sind. Damit würde für viele Nutzer die Verwendung entsprechender Hilfsmittel zumindest erschwert. Bei der Konzeption der entsprechenden Verbote ist jedoch vor allem auch die Forschungsfreiheit sowie die Informations- und Pressefreiheit zu berücksichtigen. Ein

477. Siehe oben Fn. 239.

kritischer Dialog über die Funktionsfähigkeit von Schutzmechanismen darf – gerade auch in deren langfristigem Interesse – nicht unterdrückt werden.

Bevor der Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft in der nächsten Legislaturperiode neu eingebracht wird, sollten auf der Grundlage dieser Überlegungen neue Strafbestimmungen entwickelt werden, die nicht nur wesentlich effektiver als die bisherigen Vorschläge sind, sondern dabei auch sehr viel weniger in die Freiheitssphäre der Bürger und der Industrie eingreifen als die bisherigen Vorschläge.

V. Zusammenfassung

Das vorliegende Gutachtens hat es aufgrund seiner empirischen Grundlage und der darauf aufbauenden Systematik erstmals in Deutschland ermöglicht, einen umfassenden und systematischen Überblick über die strafrechtliche Erfassung der Kopie digitaler Güter und der heute in der Praxis erfolgenden Manipulation ihrer technischen Schutzmechanismen zu geben. Dieser Überblick hat gezeigt, dass viele der einschlägigen Handlungen durch das geltende Strafrecht erfasst werden. Er hat allerdings auch deutlich gemacht, dass für einen wirksamen strafrechtlichen Schutz der digitalen Güter noch einige wenige, aber ganz entscheidende Bausteine fehlen (wie z.B. die Ausdehnung der Strafbarkeit einer Verbreitung von Hackingtools auch auf nichtgewerbliches Handeln). Auf der Grundlage der vorgelegten systematischen Analyse konnten daher nicht nur einzelne strafrechtliche Reformvorschläge entwickelt werden, sondern war eine schlüssige strafrechtliche Gesamtstrategie für die wirksame Bekämpfung von digitalen Raubkopien möglich.

Das Gutachten hat dabei anschaulich gemacht, dass die neuen Kopiertechniken von Personal Computern und die Distributionstechniken des Internets vor allem für die Software-, Audio- und Videoindustrie existenzbedrohend sind und dass der Gesetzgeber aus verfassungsrechtlichen Gründen zu einem Schutz der Rechteinhaber verpflichtet ist. Jedoch obliegt es dem Gesetzgeber, wie er diese Schutzverpflichtung erfüllen will, d.h. insbesondere, ob er den Schutz der Rechteinhaber durch eine erweiterte Geräteabgabepflicht, durch strafrechtliche Sanktionen oder durch andere Maßnahmen vornimmt. Falls der Gesetzgeber den verfassungsrechtlich geschützten Interessen der Rechteinhaber nicht durch ein neues System der Geräteabgabe Rechnung trägt, dürften die hier entwickelten zivilrechtlichen und strafrechtlichen Maßnahmen jedoch weitgehend unverzichtbar sein, da alternative Schutzkonzepte bisher nicht erkennbar sind und das Gutachten von *Pfitzmann*/*Federrath*/*Kuhn* auch die Grenzen zukünftiger technischer Schutzmöglichkeiten deutlich gemacht hat.

Bei der Entwicklung der Vorschläge des Gutachtens für die Bekämpfung der Raubkopien wurde darauf geachtet, dass die vorgeschlagenen Maßnahmen nicht nur zu einem effektiven Schutz führen, sondern nach Möglichkeit auch eine – in der Praxis ohnehin nicht durchsetzbare und damit im Ergebnis unergiebige – Kriminalisierung von geringfügigeren Massenhandlungen in der Privatsphäre der PC-Nutzer vermeiden. In die Beurteilung einbezogen wurden auch die – aufgrund der akzessorischen Strafvorschriften der Urheberstrafrechts wichtigen – zivilrechtlichen Vorfragen sowie alternative zivilrechtliche Maßnahmen.

Für einen Ausbau der bisherigen Strafvorschriften und der Reformvorschläge der Urheberrechtsnovelle zu einem wirksamen Schutzkonzept sind dabei insbesondere die folgenden ergänzenden Bausteine erforderlich:

- die – über die zivilrechtlichen Änderungen der §§ 15 Abs. 2 Nr. 2, 19a, 52 Abs. 1 S. 1 UrhG-E hinausgehende – Beschränkung der zulässigen Privatkopien nach § 53 Abs. 1 UrhG auf die Fälle der Nutzung rechtmäßiger Vorlagen (unter Beschränkung der einschlägigen Sanktionen auf zivilrechtliche Maßnahmen),

- die Beschränkung der Erstellung von Privatkopien gem. § 53 Abs. 1 S. 2 UrhG durch andere Personen auf Fälle, in denen der Auftraggeber dem Auftragnehmer eine rechtmäßige Kopiervorlage liefert,

- die Verbesserungen der Möglichkeiten der Rechteinhaber zum zivilrechtlichen Vorgehen gegen Raubkopierer (insb. durch Auskunftsansprüche im Hinblick auf das „Ob“ einer Rechtsverletzung und pauschalierte Schadensersatzklagen),

- die vollständige redaktionelle und inhaltliche Überarbeitung der durch ihre Verweisungstechnik komplizierten und insgesamt missglückten Strafnormen des § 108b UrhG-E einschließlich der Klarstellung, dass wirksame technische Maßnahme i.S. dieses Tatbestandes nur ein bestimmtes technisches Schutzniveau erfordern,

- die Abschaffung der Privilegierung des Handelns „zum eigenen privaten Gebrauch des Täters oder mit dem Täter persönlich verbundener Personen“ in § 108b Abs. 1 Nr. 1 i.V.m. § 95a Abs. 1 UrhG-E und ihre Ersetzung durch die Privilegierung z.B. von Handlungen, die ausschließlich auf den Gewinn von Erkenntnissen über Schutzmechanismen zielen und nicht auf die Verbreitung oder Nutzung der geschützten Inhalte,

- die Ergänzung der Vorfeldtatbestände von § 4 ZKDSG um die im Mittelpunkt ihrer Zielsetzung stehende Tathandlung der Umgehung der einschlägigen Schutzmechanismen, wobei das Erfordernis der geltenden §§ 4, 5 ZGKDSG, dass der Nutzer zu gewerblichen Zwecken handeln muss, ebenfalls durch eine Privilegierung zu ersetzen ist, die z.B. auf Handlungen abstellt, die ausschließlich auf den Gewinn von Erkenntnissen über Schutzmechanismen zielen und nicht auf die Verbreitung oder Nutzung der geschützten Inhalte,

- den Verzicht von § 17 UWG auf die den Tatbestand eingrenzenden Handlungsmotive bei den Tathandlungen des Mitteilens und des Verwertens sowie die Lozierung von § 17 UWG im Strafgesetzbuch,

- die völlige Neukonzeption der gesetzestechnisch missglückten und im Ansatz verfehlten Vorschriften über die Verbreitung von Tools, anderen Hilfsmitteln und Dienstleistungen zur Umgehung von Schutzmechanismen im ZKDSG *und* im Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft[478] unter Verzicht auf das Erfordernis des gewerblichen oder gewerbsmäßigen Handelns und unter besonderer Berücksichtigung der „Dual-use-Problematik“ mit Hilfe von subjektiven Absichtsmerkmalen.

Es bietet sich an, diese Reformvorschläge zusammen mit einem neuen Regierungsentwurf für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft in der im Herbst neu beginnenden Legislaturperiode des Bundestags einzubringen.

478. Siehe oben Fn. 196.