Jg. 10 H.2 2010
€13,-

NAVIGATIONEN

Zeitschrift für Medien- und Kulturwissenschaften

Jens Schröter / Ludwig Andert / Carina Gerstengarbe /
Karoline Gollmer / Daniel Köhne / Katharina Lang /
Doris Ortinau / Anna Schneider / Xun Wang (Hrsg.)

KULTUREN DES KOPIERSCHUTZES II

Jg. 10 H.2 2010
NAVIGATIONEN
KULTUREN DES KOPIERSCHUTZES II

universi
universitätsverlag siegen

Jg. 10, H. 2, 2010

NAVIGATIONEN

Zeitschrift für Medien- und Kulturwissenschaften

Jens Schröter / Ludwig Andert / Carina Gerstengarbe / Karoline Gollmer /
Daniel Köhne / Katharina Lang / Doris Ortinau / Anna Schneider / Xun Wang (Hrsg.)

Kulturen des Kopierschutzes II

NAVIGATIONEN

Zeitschrift für Medien- und Kulturwissenschaften

IMPRESSUM

HERAUSGEBER:
Peter Gendolla
Sprecher des Kulturwissenschaftlichen
Forschungskollegs 615 Medienumbrüche

WISSENSCHAFTLICHER BEIRAT:
Knut Hickethier, Klaus Kreimeier,
Rainer Leschke, Joachim Paech

REDAKTION:
Nicola Glaubitz, Christoph Meibom,
Georg Rademacher

UMSCHLAGGESTALTUNG UND
LAYOUT:
Christoph Meibom, Susanne Pütz

TITELBILD:
Daniel Köhne

DRUCK:
UniPrint, Universität Siegen

REDAKTIONSADRESSE:
Universität Siegen
SFB/FK 615 Medienumbrüche
57068 Siegen
Tel.: 0271/740 49 32
Info@fk615.uni-siegen.de

universi - Universitätsverlag Siegen
Adolf-Reichwein-Str. 2
57076 Siegen

Erscheinungsweise zweimal jährlich

Preis des Einzelheftes: 13,-
Preis des Doppelheftes: 22,-
Jahresabonnement: 20,-
Jahresabonnement
für Studierende: 14,-

ISSN 1619-1641
ISBN 3-89472-544-3

Jens Schröter / Ludwig Andert / Carina Gerstengarbe /
Karoline Gollmer / Daniel Köhne / Katharina Lang / Doris Ortinau /
Anna Schneider / Xun Wang (Hrsg.)

KULTUREN DES KOPIERSCHUTZES II

INHALT

KULTUREN DES KOPIERSCHUTZES II

Ein Vorwort

VON JENS SCHRÖTER, LUDWIG ANDERT, CARINA GERSTENGARBE, KAROLINE GOLLMER, KATHARINA LANG, DANIEL KÖHNE, DORIS ORTINAU, ANNA SCHNEIDER UND XUN WANG

Spätestens seit den 1990er Jahren war viel die Rede von Kopie und Simulation, Reproduzierbarkeit und Serialität. Doch dass schon das eigene Portemonnaie Dinge wie Geld und Personalpapiere enthält, die nicht kopiert werden *sollen* und von Normalbürgern auch nicht kopiert werden *können*, wird oft vergessen. Wir leben (auch) in einer ›Kultur des Kopierschutzes‹, in der verschiedene technische, diskursive und juristische Verfahren zusammenwirken, um die gesteigerte ›technische Reproduzierbarkeit‹, um Benjamins berühmten Ausdruck zu bemühen, im Zaum zu halten. Besonders deutlich wird das auch in den manchmal aufgeregten Diskussionen um den Status des Urheberrechts im Feld der digitalen Medien.

Die beiden Hefte der Navigationen des Jahres 2010 sind das Ergebnis einer von Prof. Dr. Jens Schröter (Medienwissenschaft der Universität Siegen, Theorie und Praxis multimedialer Systeme) geleiteten Projektgruppe im Masterstudiengang ›Medienkultur‹. Die Studierenden haben im Rahmen des gesetzten Themas selbstständig Problemstellungen formuliert und diskutiert, die Ergebnisse dieser Arbeit sind in den beiden Heften publiziert – zusammen mit einer Reihe eingeladener Beiträge, die Aspekte abdecken, die in der Projektgruppe nicht bearbeitet werden konnten.

Erstens war es Ziel der Projektgruppe, den Studierenden vor dem Beginn der Abfassung ihrer Masterarbeit Erfahrung im Schreiben eigenständiger wissenschaftlicher Forschungsarbeiten zu vermitteln.

Daraus folgt *zweitens*, dass diese Hefte Resultat eines ernsthaften Versuches sind, die ›Einheit von Forschung und Lehre‹ in die Tat umzusetzen. In der Lehre wurde die Forschung an dem noch weitgehend unbearbeiteten Thema ›Kopierschutz‹ durchgeführt und in den hier publizierten Texten umgesetzt. Wir hoffen, dass die interessierten Leserinnen und Leser ebensoviel daraus lernen können, wie wir gelernt haben.

Das vorliegende Heft enthält fünf Beiträge, die das Thema speziell auf das Feld digitaler Medien beziehen – jenes Feld, in dem die Problematik gegenwärtig am virulentesten ist. Es beginnt mit einer umfangreichen Studie, in der die Geschichte des Wasserzeichens bis hin zu dem aktuellen Verfahren des ›Digital Watermarkings‹ rekonstruiert wird (Gerstengarbe/Lang/Schneider). Dann wird ein Überblick über die Verfahren des ›Digital Rights Management‹ und der damit verbundenen Probleme geliefert (Köhne). Weitere Texte behandeln spezielle Probleme wie die aktuelle Auseinandersetzung um Googles Projekt, eingescannte Bü-

cher online zur Verfügung zu stellen (Winston), die Schutzmechanismen von DVDs (Heilmann) und befassen sich schließlich mit der Rolle, die Kopierschutzverfahren in der Softwarenentwicklung spielen (Firyn).

Das Heft »Kulturen des Kopierschutzes I«, welches parallel mit diesem Heft erschienen ist, enthält sechs Beiträge, die das Problem in allgemeinerer Hinsicht behandeln. Es geht um die Verortung des Problem des Kopierschutzes (und damit des Urheberrechts) in der medienwissenschaftlichen Diskussion (Schröter), aus Sicht einer kritischen, am Werk von Marx orientierten Perspektive (Meretz), im Rahmen einer allgemeineren Betrachtung von ›Barriere-Infrastrukturen‹ (Andert/Ortinau), aus juristischer (Senftleben) und interkultureller (Wang) Perspektive. Abgeschlossen wird jenes Heft mit einer Studie zur Geschichte des Begriffs der »Raubkopie« (Gollmer).

Wir danken dem Forschungskolleg 615 ›Medienumbrüche‹ und seiner Koordination für die ideelle, finanzielle und logistische Unterstützung. Wir danken Georg Rademacher für seine Briefings bezüglich der Formatierung. Wir danken Sebastian Abresch und Benjamin Beil für die Unterstützung bei der Fertigstellung der Texte. Wir danken Holger Steinmann für die Übersetzung des Textes von Brian Winston. Es seien Ludwig Andert und Daniel Köhne für ihre Bemühungen zur Erstellung der Heftcover gedankt.

Siegen, 2010

WASSERZEICHEN

Vom 13. Jahrhundert bis zum Digital Watermarking

VON CARINA GERSTENGARBE, KATHARINA LANG UND ANNA SCHNEIDER

Nichts geht häufiger durch unsere Hände als Geld – rund 330 Millionen Menschen bezahlen täglich mit Euro-Banknoten, welche nicht zuletzt aufgrund der eingefügten Wasserzeichen zu den sichersten der Welt zählen. Im Gegenlicht betrachtet weist dieses in 16 EU-Mitgliedsstaaten[1] eingeführte Papiergeld im unbedruckten Bereich beidseitig das jeweilige Architekturmotiv des Geldscheins sowie die entsprechende Wertzahl als Wasserzeichen auf. Diese aktuell bekannteste Verwendung von Wasserzeichen dient, wie allgemein bei Wertpapieren, in erster Linie dem Nachweis von Authentizität und damit maßgeblich der Fälschungssicherheit. Noch heute täglich im Einsatz, blicken Wasserzeichen dabei auf eine mehr als 700 Jahre alte Geschichte zurück (vgl. Weiss 1986).

Erstmals treten Wasserzeichen im 13. Jahrhundert in Verbindung mit Papier in Italien auf. Als schwächere Hintergrundbilder sind sie bei der zeitgenössischen Papierherstellung als Herkunfts- bzw. Qualitätsmerkmale ins Papier eingebracht. Somit kennzeichnen sie seit den Anfängen der Papierproduktion in Europa, die vermutlich bis ins 12. Jahrhundert zurückreicht, durch das zusätzliche Anbringen von Namen, Initialen und Monogrammen Herstellungsort sowie Produktionsbetrieb des jeweiligen Papiers. Modern formuliert könnte hier von Firmenlogos gesprochen werden. Im Laufe der Zeit dienen ebendiese auch als Sorten- und Formatbezeichnung, signalisieren gehobene Schreibpapierqualitäten und legen Zeugnis über die Echtheit von Wertpapieren und Urkunden ab.

Mit Beginn industriell hergestellter Maschinenpapiere verschwinden die Wasserzeichen zunächst vom Papier, da es aufgrund der raschen technologischen Entwicklung der Papiermaschine immer schwieriger wurde, Wasserzeichen makellos und preisgünstig zu fertigen. Die Bedeutung des Wasserzeichens als Informationsträger im Papier wurde aus seinem bisherigen traditionellen Verwendungszusammenhang gelöst und seit Anfang des 19. Jahrhunderts bis auf die Verwendung als Kopierschutz bei Banknoten weitgehend marginalisiert.

Der Grundgedanke der Sicherung der Urheberschaft von Papiererzeugnissen durch Wasserzeichen nimmt in der modernen digitalen Welt gleichermaßen Einfluss auf den Kopierschutz von Datenmaterial. Sog. *Digitale Wasserzeichen* werden direkt in Mediendateien eingefügt und dienen somit dem Nachweis der Fäl-

1 Mit dem Beitritt der Slowakei zur europäischen Gemeinschaftswährung im Januar 2009 umfasst der Euro-Raum 16 Mitgliedsstaaten; somit ist der Euro derzeit für rund 330 Millionen Menschen in Europa einheitliches Zahlungsmittel (vgl. Schöberl 2009).

schungssicherheit der Ursprungsdaten. Im Gegensatz zu papierbasierten Wasserzeichen geschieht dies normalerweise für den Benutzer in nicht wahrnehmbarer Weise. Das Interesse am Einsatz digitaler Wasserzeichen ist hierbei kommerziellen Ursprungs und soll der Verhinderung bzw. Identifikation illegaler Kopien zuträglich sein.

Vor dem Hintergrund eines wirtschafts- und technikgeschichtlichen Ansatzes ist es das Ziel dieses Textes, Grundlagen, Verfahren und Anwendungen von Wasserzeichen in verschiedenen historischen Kontexten aufzuzeigen. Zu diesem Zweck ist der Text in drei Teile gegliedert: In einem *ersten Teil* soll die Entstehung und Herstellung von Wasserzeichen in der Papiergeschichte nachgezeichnet werden. Um das ursprüngliche Aufkommen, die Arten und Verwendungszwecke des Wasserzeichenpapiers und der Wasserzeichen zu klären, werden Papiermarken nicht nur technikgeschichtlich, sondern auch hinsichtlich ihrer ästhetischen bzw. gestalterischen Wandlung untersucht.

Daran anschließend wird im *zweiten Teil* auf die wohl bekannteste Anwendung von Wasserzeichen, nämlich auf Banknoten, eingegangen. Hierzu wird zunächst ein historischer Abriss erfolgen, um die Entwicklungsgeschichte der Wasserzeichen auf Banknoten darzustellen. Nachfolgend wird zum einen die Herstellung der Euro-Banknote allgemein, zum anderen die Herstellung des Wasserzeichens als sicherstes aller fälschungshemmenden Sicherheitsmerkmale explizit zum Thema gemacht.

Im *dritten Teil* folgt schließlich eine Auseinandersetzung mit der wohl modernsten Form von Wasserzeichen. Einleitend sollen hier die Grundlagen des *Digital Watermarking* herausgearbeitet werden, um im Anschluss auf verschiedene Anwendungsmöglichkeiten für digitale Wasserzeichen unter Berücksichtigung der unterschiedlichen Medienarten digitaler Güter eingehen und deren Vor- und Nachteile skizzieren zu können. Zum Abschluss der Arbeit wird resümierend der aktuelle Forschungsstand aufgezeigt sowie ein Blick in die Zukunft unternommen.

1 ENTSTEHUNG UND HERSTELLUNG VON WASSERZEICHEN IM HISTORISCHEN KONTEXT DER PAPIERGESCHICHTE

»Beim Betrachten von Papier, vornehmlich handgeschöpftem, scheint [...] plötzlich eine eigene Welt auf, hell sichtbar treten Zeichen hervor, in jedem einzelnen Blatt. Papier in seiner Leichtigkeit und Zerstörbarkeit, in seiner Allgegenwärtigkeit und scheinbaren Belanglosigkeit hat das enorme Potential der Wasserzeichen in sich, einer Wahrnehmungsebene und Informationsplattform im Material selbst.«
Gangolf Ulbricht (2000: 39)

1.1 WASSERZEICHEN DES MITTELALTERS

Die Beschäftigung mit Wasserzeichen im geschichtlichen Kontext muss bei einer Auseinandersetzung mit dem interdisziplinären Forschungsfeld der Papiergeschichte[2] ansetzen. Der chinesische Hofbeamte Tsai Lun, der im Jahr 105 unserer Zeitrechnung erstmals ein Verfahren zur Papierherstellung aus Lumpen- und Pflanzenfasern beschrieb, gilt nach Überlieferungen der chinesischen Kaiserchronik als Erfinder des Papiers im heutigen Sinne. Erst über tausend Jahre später diffundierte die Kunst der Papierherstellung über den Orient und Nordafrika in den europäischen Kulturkreis, wo für diesen bedeutenden Schriftträger der Name »Papier«[3] geprägt wurde. Die älteste bekannte europäische Papierhandschrift entstand im spanischen Kloster Silos noch auf importiertem arabischem Papier und kann aufgrund von Nachforschungen des Papierhistorikers Peter F. Tschudin noch vor 1036 datiert werden. Schon kurze Zeit später – laut Tschudin wohl bereits vor 1150 – wurde in Spanien und in den Jahren vor 1230 auch in Italien die Papierherstellung im eigenen Land aufgenommen (vgl. Tschudin 2002: 98ff.). Als ältester nördlich der Alpen erhaltener Papierkodex gilt das ab 1246 geführte Registerbuch Albert Behaims aus dem bayerischen Kloster Aldersbach, verfasst auf importiertem südeuropäischen Papier. Die Produktion von Papier wurde im damals deutschsprachigen Raum erstmals 1390 in der »Gleismühl«, einer umgebauten alten Kornmühle des Handelsherrn Ulman Stromer in Nürnberg, aufgenommen. Weitere Papiermühlengründungen folgten 1391 in Ravensburg, 1468 in Augsburg, 1477 in Kempten, 1481 in Memmingen, 1482 in Ettlingen, 1486 in Reutlingen und 1489 in Landshut (vgl. Kämmerer 2009a: 12).

Seit diesem Siegeszug der Papierherstellung[4] im Mitteleuropa des 15. Jahrhunderts sollte Papier als bedeutendster Schriftträger bis in unsere Zeit fungieren. Die Erfindung des Buchdrucks 1445 durch Johannes Gutenberg und das folgende Zeitalter der Aufklärung ließen den Bedarf an Papier weiter stark ansteigen – oder, wie Gertraude Spoer festhält:

> »Seitdem begleitet Papier die Menschheit in guten und in bösen Zeiten; es ist Mittler ihres Geistes, Träger ihrer Gedanken, auch ihrer Hoffnungen, Verbreiter ihrer Erfindungen und revolutionären Ideen und des Traumes vom dauerhaften Frieden.« (Spoer 1987: 7)

---

2 Die Wasserzeichenforschung hat sich in den vergangenen 55 Jahren zu einer eigenständigen Disziplin der Papiergeschichte entwickelt, was sich in der zahlreich vorhandenen Literatur zu diesem Thema seit den 1950er Jahren widerspiegelt.

3 Das lateinische Wort *papyrus*, abgeleitet vom Griechischen *pápyros*, die ägyptische Papyrusstaude, wird im Französischen und somit im europäischen Sprachgebrauch zu *papier*, im Englischen sowie Schwedischen zu *paper* (vgl. Schwenck 1934: 462).

4 Ab dem 13. Jahrhundert hatte die Verbreitung der Papierproduktion in Europa die allmähliche Verdrängung des zuvor gebräuchlichen, teureren Schriftträgers, des Pergaments, zur Folge. Die Gründung von Papiermühlen trieb diesen Prozess schließlich wesentlich voran.

Im Zuge der Industrialisierung hat sich die Papierproduktion Ende des 19. Jahrhunderts grundlegend verändert, und die Bedeutung der in Papier eingebrachten Wasserzeichen – bis auf eben jene in Banknoten – weitgehend marginalisiert (vgl. Rückert 2009: 9). Aufgrund der aktuellen Veränderungen der Kommunikationsstrukturen durch die Einführung elektronischer Medien wird die Bedeutung des Papiers zwar zunehmend geringer, Wasserzeichen hingegen erleben – wie bereits eingangs erläutert – gerade seit den letzten Jahren wieder ein regelrechtes *Revival* im digitalen Bereich. Die traditionellen analogen Sicherungsmedien wie Papier und Film werden zunehmend von einer elektronischen Speicherung auf unterschiedlichen Datenträgern ersetzt, obwohl für diese keine Erfahrungswerte hinsichtlich ihrer Haltbarkeit bestehen. Die im Mittelalter gefertigten Papiere und ihre Wasserzeichen stellen dagegen »bei professioneller Aufbewahrung und adäquatem Umgang normalerweise keine konservatorischen Probleme dar« (Rückert 2009: 9)[5], was auch die entsprechend lange Tradition der international betriebenen Papier- und Wasserzeichenforschung erklärt.

Bereits im Mittelalter war der Einsatz von Wasserzeichen bei der Papierproduktion im Bewusstsein der Menschen verankert, wie schon früh der *Tractatus de insignis et armis*[6] des seinerzeit großen Rechtsgelehrten Bartolo da Sassoferrato deutlich macht. In dieser Schrift von 1350 erwähnt Sassoferrato Wasserzeichen erstmals in der Literatur und betrachtet diese »unter rechtlichen Gesichtspunkten als Geschäftsmarken, die an die Werkstätte gebunden und vor Nachahmung zu schützen sind« (Ulbricht 2000: 40). Dabei bezieht er sich in seinen Ausführungen auf die italienische Stadt Fabriano, in der jedes Blatt Papier sein Zeichen habe, an dem die jeweilige Werkstätte erkannt werden könne (vgl. Renker 1950: 113). Das Wasserzeichen wurde also nicht zu rein dekorativen Zwecken in das Papier eingebracht, sondern um – ähnlich wie auch Steinmetze oder Goldschmiede ihre Werke signierten – ein Markenzeichen zu schaffen. Das Außergewöhnliche an Wasserzeichen ist dabei die Tatsache, dass die Zeichen nicht auf den ersten Blick sichtbar auf dem erzeugten Stoff angebracht wurden, sondern sich dem Betrachter erst durch genaues Hinsehen erschlossen.

5 Dagegen wurden ab Mitte des 19. Jahrhunderts säurehaltige Papiere hergestellt, die einem langsamen, aber irreversiblen Alterungsprozess unterliegen; die Zellulosefasern werden mit der Zeit zersetzt, das Papier spröde und brüchig und zerfällt schließlich zu Staub. Erst 1962 gelang es, eine neutrale Leimung in der Massenproduktion von Papier einzusetzen (vgl. Will 2002: 260f.).

6 In dem Traktat über die Insignien/Zeichen/Marken und Wappen schildert der italienische Rechtsgelehrte Bartolus da Sassoferrato (1314-1357) die Papiermacherei in Fabriano und führt aus: »Et ut videamus, hic quodlibet folium chartae habet suum signum, per quod significatur, cujus aedificii aut molendini est charta. Dic ergo quod isto casu apud illum remanebit signum, apud quem remanebit aedificium ipsum. (Und so sehen wir, dass jedes Blatt Papier hier sein Zeichen hat, durch das angegeben wird, aus welcher Werkstätte oder Papiermühle es stammt. Nach dem Recht verbleibt daher in jedem Fall das Zeichen dem, bei dem auch die Mühle verbleibt)« (Ulbricht 2000: 40).

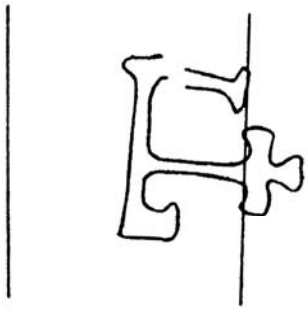

Abb. 1: Buchstabe F – ältestes bekanntes Papierzeichen der Welt, Cremona 1271. Aufgenommen von Theodor Gerardy (1975: 51).

Das älteste bekannte Wasserzeichen wird von der Forschung heute auf das Jahr 1271 datiert. Es wurde in Cremona (Italien) verwendet und stellt den Buchstaben F dar (vgl. Abb. 1). Die Publikation des erst 1954 in drei auf 1271 datierten Blättern gefundenen Papierzeichens erfolgte in einer Festschrift der Papierfabrik *BURGO*, die aus Anlass ihres 50jährigen Firmenbestehens 1955 in Mailand gedruckt wurde (vgl. Gerardy 1975: 51).

Zuvor war der Schweizer Papierhändler Charles-Moïse Briquet von einem griechischen Kreuz aus dem Jahr 1282[7], das in Bologna angewendet wurde, als ältestes Wasserzeichen ausgegangen. Ob nun ein Buchstabe oder ein Kreuz, Fakt ist, dass am Beginn seiner Geschichte ein Wasserzeichen aus Oberitalien und somit aus Europa steht und nicht etwa – wie zunächst angenommen werden könnte – aus China, wo auch die Papierherstellung ihren Ursprung hat (vgl. Gerardy 1975: 51f.). Die Tatsache, dass kein älteres Papier aus dem fernöstlichen Kulturkreis Wasserzeichen aufweist, ist einerseits auf religiöse Motive und andererseits auf seine Herstellungstechnik zurückzuführen (vgl. Beyerling 1940: 16). Seit seiner Erfindung spielt Papier in China eine herausragende Rolle – es wird als Geschenk der Götter, als heiliges Gut angesehen (vgl. Exner 1889: 155). Somit verbietet dieses Sakrileg die Identifizierung des »einfachen Papiermachers« mit seinem Erzeugnis durch das Anbringen von Wasserzeichen. Daneben machte die in China angewandte Technik der Papierherstellung das Einbringen von Wasserzeichen schlichtweg unmöglich:

7 Dieses Kreuz aus dem Jahr 1282 wird auch heute noch in zahlreichen literarischen Quellen als erstes Wasserzeichen genannt. Dies mag vielleicht daran liegen, dass das von 1271 aus Cremona stammende Papier mit dem Wasserzeichen, das den Buchstaben »F« darstellt, erst im Jahr 1954 gefunden wurde und daher von einigen Forschern angezweifelt wird bzw. in früheren, zum Teil noch vor diesem Datum entstandenen Sammlungen bekannter Wasserzeichenforscher, wie Karl Theodor Weiss, Wisso Weiss, Theodor Gerardy und Gerhard Piccard nicht auftritt, deren Arbeiten zur gegenwärtigen wissenschaftlichen Auseinandersetzung mit diesem Thema aber hauptsächlich herangezogen werden.

> »Aus Seidenabfällen einerseits, der Rinde des Maulbeerbaums, Chinagras (Ramie), Hanf, Lumpen und alten Fischernetzen andererseits wurde Papiermasse gewonnen. Durch Einweichen und Schlagen der zerkleinerten Pflanzenbestandteile oder Textilabfälle erhielt man eine mit Wasser versetzte Fasersuspension, die über eine Bambusmatte gestrichen nach dem Trocknen an der Luft ein dünnes, dabei aber zähes Vlies ergab. Die Papierherstellung wurde regional unterschiedlich gehandhabt und änderte sich nach und nach. So lernte man ein Sieb einzutauchen und aus dem dünnen Papierbrei heraus zu schöpfen, und man lernte das noch nasse Vlies vom Sieb abzuziehen, so daß die Siebe schneller wieder verfügbar wurden.« (Hanebutt-Benz 1999: 390)

Trotz der Innovation der Siebtechnik waren auf den Bambusgeflechten keine erhabenen Teile haltbar anzubringen, die der gesamten Abrollung[8] des Papiers vom Sieb auf ein Brett oder Tuch standgehalten hätten (vgl. Renker 1950: 106). Daher ließen sich bei dieser Art der Papierherstellung keine Wasserzeichen im heutigen Sinne hervorbringen.

Im Europa des 13. Jahrhunderts standen zur Papierherstellung dagegen keine Bambuspflanzen zur Verfügung, weshalb das zeitgenössische Handwerk dazu überging, für die Produktion von Papier das vertraute Erzeugnis Kupferdraht zu verwenden.[9] Statt flexibler Bambusmatten, wie sie zum Schöpfen in Asien Verwendung fanden, wurden starre Holzrahmen fest mit »Metallsieben« bezogen, was die Haltbarkeit der Schöpfsiebe wesentlich erhöhte und das Anbringen von Drahtfiguren zur Herstellung von Wasserzeichen ermöglichte (vgl. Ulbricht 2000: 39f.). Aufgrund dieser technischen Voraussetzung treten Wasserzeichen im europäischen Mittelalter also erst recht spät auf.

Über die Frage, zu welchem Zweck das Wasserzeichen eingeführt wurde, sind die Fachleute bis heute geteilter Meinung.

> »Daß die Anbringung aber – nach einem vielleicht einzigen Zufall und anregendem Beispiel – als nützlich und vorteilhaft befunden worden sein muß, ergibt sich aus der schnellen und allgemeinen Einbürgerung dieser Handwerks- oder Kunstgepflogenheit, die unter veränderten Verhältnissen in der Zeit des Maschinenpapiers imitiert wurde und in der gesamten Kulturwelt teilweise bis heute fortbesteht.« (Weiss/Weiss 1962: 3)

8 Das Siebgeflecht, wie es in Asien Verwendung fand, bestand aus flexiblen Bambusstäben, die durch Seidenfäden miteinander verbunden waren. Nach dem Schöpfvorgang wurde die Form mit dem Papierblatt nach unten auf eine Unterlage gelegt und das biegsame Bambusgeflecht vom Papierblatt abgerollt.

9 Zudem galt Papier im Westen keinesfalls als heiliges Gut, wie das rund 1000 Jahre zuvor in China der Fall war. In Europa wurde Papier schnell zum Artikel des täglichen Gebrauchs. Es diente vorwiegend zum Beschriften, Bedrucken und Verpacken.

Abb. 2: Schöpfer, Gautscher und Leger bei der Arbeit; im Hintergrund das Lumpenstampfwerk. Nach einem Holzschnitt von 1689 (Weiss/Weiss 1962: 28).

Auch wenn an dieser Stelle nicht alle Deutungen zur Entstehung des Wasserzeichens, die innerhalb der letzten Jahrhunderte gemacht wurden, besprochen werden sollen, ist dennoch auf die Ansicht des Paläographen Rudolf Forrer hinzuweisen. Dieser geht nämlich davon aus, dass die Wasserzeichen mit großer Wahrscheinlichkeit heraldische Zeichen bzw. Embleme ersetzten, die vor allem in Frankreich neben dem Namenszug zur besonderen Beglaubigung von wichtigen Schriftstücken Verwendung fanden:

> »Die fürstlichen bzw. geistlichen Personen ließen ihren Bedarf an Kanzleipapier in bestimmten Papierfabriken herstellen und setzten ihre Embleme als Kennzeichen ihrer Spezialmarken fest. Nur so ist das gleichzeitige Verschwinden jener die Unterschrift vertretenden ›Handmale‹ und das Aufkommen der Wasserzeichen zu erklären.« (Wolbe 1923: 146f.)

Neben der Einführung der mit Drahtgeflechten bespannten Schöpfsiebe erleichterte eine weitere technische Neuerung das Handwerk der europäischen Papiermacher: Das Zerstampfen der in Europa verwendeten Leinenlumpen oder Hadern wurde nicht mehr wie rund tausend Jahre zuvor im asiatischen Raum von Hand in Steinmörsern besorgt, sondern in einem vom Wasserrad der Papiermühle betriebenen »Stampfgeschirr«. Das Stampfwerk bestand aus einem ausgehöhlten Baumstamm, der durch Eisenplatten unterteilt war und von Wasserkraft, in

seltenen Fällen auch von Windkraft angetrieben wurde. Messerartige Schienen sorgten im Stampfgeschirr – das sich aufgrund des Lärms meist gut abgeschirmt von der Mühle in einem sog. Stampfkeller befand – dafür, dass die Lumpen immer weiter zerkleinert wurden. Der so entstandene Faserbrei wurde unter starker Wasserverdünnung in sog. »Bütten«, große Stein- oder Holzwannen gefüllt, aus denen mit drahtbespannten Holzrahmen eine dünne Schicht des Papierbreies herausschöpft wurde (vgl. Schwieger 1973: 14). Dieses zur Papiergewinnung genutzte Siebgeflecht bestand aus eng und parallel verlaufenden Bodendrähten (Rippdrähte), die mit rechtwinklig angeordneten Querdrähten, den sog. Bind- oder Kettdrähten vernäht waren. Während das Wasser beim Schöpfvorgang zurück in die Bütte abfloss, setzten sich die Fasern in einem dünnen Film auf der engmaschigen Anordnung der Drähte ab. Durch geschicktes Hin- und Herbewegen der Schöpfform entstand durch Verfilzung der aufgelösten Fasern ein Papierbogen. Nach dem Trocknungsvorgang[10] blieb auf dem Papier ein sichtbarer Abdruck der Siebdrähte zurück, an denen sich weniger Papiermasse absetzen konnte als in deren Zwischenräumen – bei Durchsicht der Papiere ließ sich eine vertikale und horizontale Rippung erkennen (vgl. Abb. 3). Nach demselben Prinzip entstanden die ersten Wasserzeichen. Das Aufnähen von zusätzlichen Drähten auf der Siebinnenseite in Form von Zeichen, Bildern oder Buchstaben bewirkte an den betreffenden Stellen eine Erhebung des Siebes und somit eine höhere Transparenz im Papier – das Wasserzeichen war geboren (vgl. Kämmerer 2009a: 12f., siehe hierzu auch Abb. 4). Es ist davon auszugehen, dass sich die Papiermacher diese Gepflogenheit von anderen Handwerkern, wie den Zinngießern oder Steinmetzen, abgeschaut hatten, die ihre Produkte zum Herstellernachweis ebenfalls mit Zeichen versahen (vgl. Spoer 1987: 9).

Die Qualität der europäischen Büttenpapiere erlangte im 15./16. Jahrhundert ihren Höhepunkt. Besonders großer Beliebtheit erfreute sich auf den Märkten Papier aus Fabriano, das aufgrund seines hohen Qualitätsstandards schon bald über die Grenzen der Stadt hinaus bekannt wurde. Die Funktion der ins Papier eingebrachten Wasserzeichen änderte sich vom reinen Herstellernachweis bzw. Herkunftsmerkmal hin zum Gütesiegel – so stand z.B. das Ochsenkopfzeichen für besonders wertvolles, feines Papier; in manchen Fällen wurde den Papierherstellern das Einfügen von Wasserzeichen von den Händlern sogar vorgeschrieben, um vor Fälschungen zu schützen (vgl. Mariani/Pelligrini 2009: 15f.).

10 Bei der Papierherstellung wurde der Schöpfer vom Gautscher und Leger unterstützt (vgl. Abb. 2). Dem Gautscher kam dabei die Aufgabe zu, die nassen Bögen durch Umdrehen der Form auf ein Filztuch abzudrücken (gautschen). Daraufhin stapelte der Leger diese Filzstücke mit den darauf abgelegten Papierbögen zu einem Stapel, aus dem mit einer handbetriebenen Presse überschüssiges Wasser ausgepresst wurde, bevor die Papierbögen von den Filzen gelöst wurden und zum Trocknen gelegt wurden (vgl. Keim 1956: 14).

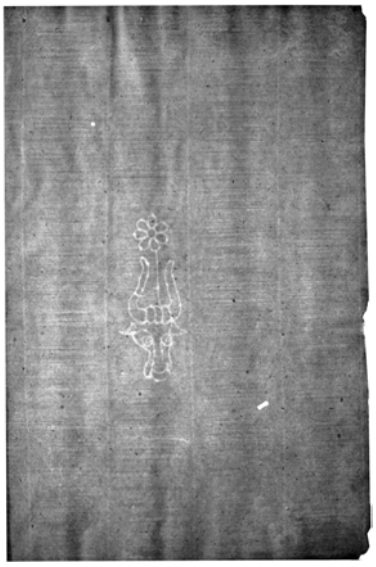

Abb. 3: Wasserzeichen »Ochsenkopf«; deutlich erkennbar ist hier auch die Rippstruktur im Papier (Kämmerer 2009b: 55).

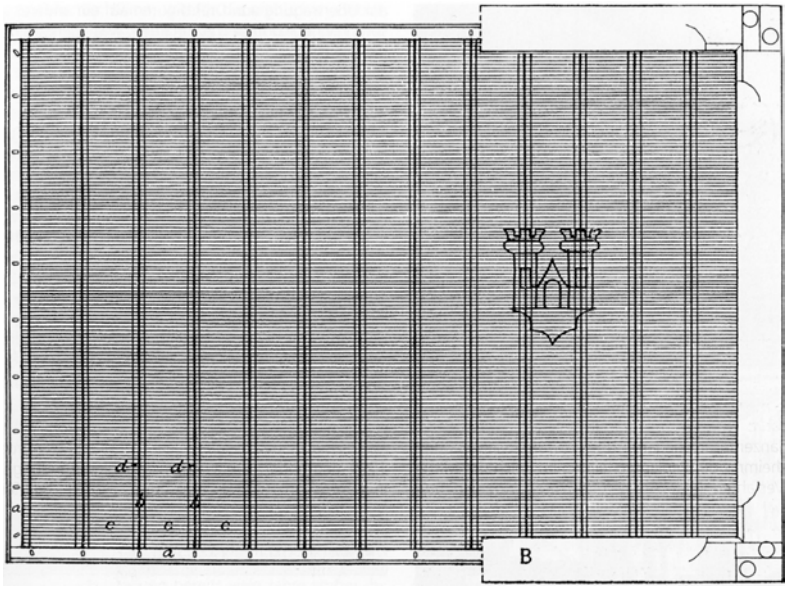

Abb. 4: Schematische Darstellung eines Schöpfsiebes für die Papierherstellung; deutlich zu erkennen der starre Holzrahmen, die Kett- und Rippdrähte sowie eine im Schöpfsieb angebrachte Drahtfigur/Turmfigur (Piccard 1956: 67).

Im weitesten Sinne können Wasserzeichen in dieser Verwendung erstmals mit Kopierschutz in Verbindung gebracht werden.

1.1.1 WASSERZEICHENFORSCHUNG ALS HISTORISCHE HILFSWISSENSCHAFT

Für die spätere wissenschaftliche Auseinandersetzung mit Wasserzeichen sind es aber nicht ausschließlich die eingebrachten Papiermarken, die wertvolle Datierungsmöglichkeiten liefern, wie auch Gerhard Piccard in seinen Schriften erläutert.

Piccard, der Mitte des 20. Jahrhunderts für seine Wasserzeichenforschung bekannt wurde, spricht in seinen wissenschaftlichen Arbeiten davon, dass genau genommen von zwei Wasserzeichen, die bei einem Schöpfprozess entstehen, auszugehen ist:

> »Er meint zum einen die technisch bedingten Abdrucke der Boden- und Binddrähte der Schöpfform, die gleichzeitig auch die zentralen Charakteristika des handgeschöpften Papiers darstellen, und zum zweiten die Transparenzen, die durch gezielt angebrachte Drahtfiguren zur Erzeugung von Wasserzeichen im eigentlichen Sinne (Piccard spricht von ›Papiermarken‹) dienten.« (Kämmerer 2009a: 13)

Darüber hinaus konnte von Piccard und Tschudin historisch nachgewiesen werden, dass die Gebrauchsdauer für ein Schöpfsieb bei höchstens zwei Jahren lag – völlig identische Wasserzeichen konnten also lediglich auf Papieren auftreten, die innerhalb eines Zeitraums weniger Jahre hergestellt worden waren (vgl. Piccard 1954 sowie Tschudin 1996a).

Damit steht der Nutzen der Filigranologie für die zeitliche Einordnung undatierter Schriftstücke durch Vergleich der Zeichen außer Zweifel, was gerade für die frühen Stücke des 14. bis 16. Jahrhunderts von einschlägiger wissenschaftlicher Bedeutung ist. In der entsprechenden Literatur lassen sich mehrere methodisch orientierte Beiträge finden, die sich mit der Wasserzeichenforschung als Hilfswissenschaft für Handschriften- und Inkunabelforschung, für Kunstgeschichte (Zeichnungen, Graphiken), Musikwissenschaft (Notenblätter) und für Kartographie beschäftigen.[11] Um Wasserzeichen als Instrumentarium für das Forschungsfeld der Handschriftenkatalogisierung überhaupt einsetzen zu können, ist die Vergleichsmöglichkeit vieler gleichartiger datierter Typen und Varianten notwendig. Neben

11 Nachfolgend eine Auswahl einschlägiger Literatur, die sich der Wasserzeichenforschung als Hilfswissenschaft für weitere Forschungsfelder/Wissenschaften bedient: Wasserzeichenforschung als Hilfswissenschaft für Handschriften- und Inkunabelforschung (vgl. hierzu Gerardy 1964, Haidinger 2004 sowie Piccard 1956); Wasserzeichenforschung als Hilfswissenschaft für Kunstgeschichte (vgl. hierzu Ash/Fletcher 1998 und Griffiths/Hartley 1997); Wasserzeichenforschung als Hilfswissenschaft für Musikwissenschaft (vgl. hierzu Duda 2000, Hudson 1987 sowie La Rue 1961); Wasserzeichenforschung als Hilfswissenschaft für Kartographie (vgl. hierzu Gerardy 1974 und Woodward 1987).

den auf Papier festgehaltenen, überlieferten Sammlungen hat vor allem die Digitalisierung und Präsentation großer Bestände bedeutender Wasserzeichensammler im Internet seit den letzten Jahren das Interesse der Historiker an der Wasserzeichenforschung erkennbar belebt. Zu den weltweit bedeutendsten Wasserzeichendatenbanken zählen derzeit die digitalisierte Sammlung »Piccard Online« des Hauptstaatsarchivs Stuttgart mit etwa 92.000 Belegen, »Wasserzeichen des Mittelalters (WZMA)« der Wiener Akademie der Wissenschaften sowie »Watermarks in Incunabula printed in the Low Countries (WILZ)« in Den Haag. In dem seit 2006 von der Europäischen Kommission geförderten Projekt *Bernstein – The Memory of Paper* werden diese existierenden Datenbanken in einem gemeinsamen Internetportal[12] zusammengeführt und im Kontext der Papierforschung und –geschichte präsentiert. Wie diese Bestände zeigen, haben die Wasserzeichen des alten Handbüttenpapiers im Verlauf von über 700 Jahren in mehrfacher Beziehung eine Wandlung durchgemacht.

1.2 PAPIERPRODUKTION IM ÜBERGANG ZUR INDUSTRIELLEN HERSTELLUNG

> »Seit dem ausgehenden 18. Jahrhundert setzte auf dem Gebiet der Papierherstellung eine tiefgreifende Umbruchsphase ein, an deren Ende bis zur Mitte des 19. Jahrhunderts die meisten in handwerklich-traditionsverbundener Manufakturfertigung tätigen Papiermühlen aufgegeben wurden, da sich die industrielle Großproduktion als leistungsfähigere Fertigungsweise durchgesetzt hatte. Hierzu hatte eine Reihe bahnbrechender Innovationen beigetragen.«
> Georg Dietz/Frieder Schmidt (2009: 20)

Mitte des 18. Jahrhunderts treten in England erstmals handgeschöpfte Papiere auf, die aufgrund gewebter Siebe eine ungerippte Struktur aufweisen. Die Entwicklung immer dünnerer Drähte machte die Herstellung engmaschigerer Siebe und damit die Erzeugung von Papier mit nahezu strukturloser Oberfläche möglich. Dieses sog. Velin-Papier wurde in Deutschland erstmals durch den Papiermacher Ebart in Spechthausen produziert (vgl. Keim 1956: 47). Da die Wasserzeichen in ihrer Bildwirkung auf diesem »neuen« Papier weder durch Rippen noch durch Stege beeinträchtigt werden, kommen die verschiedenen Darstellungen hier voll zur Geltung. Die veränderte Siebtechnologie brachte ebenfalls neuartige Formen der Wasserzeichen hervor – Grundlage der *Vollwasserzeichen* waren nicht mehr jene aufgenähten Drahtfiguren, sondern auf dem Papiersieb angebrachte Blechschablonen, die im Papier vollflächige helle Flächen hinterlassen (vgl. hierzu Abb. 5).

12 Website des Projekts *Bernstein – The Memory of Paper* online verfügbar unter: http://www.memoryofpaper.eu, 01.03.2010.

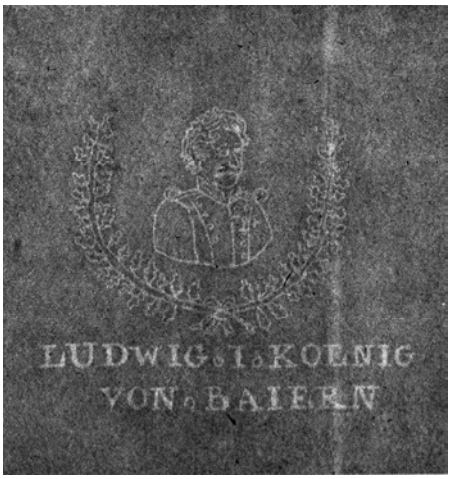

Abb. 5: Wasserzeichen aus einem Velinpapier der Papiermühle Mindelheim. Der Schriftzug »LUDWIG.I.KOENIG VON.BAIERN« wurde um 1835 von dem Papiermacher Joseph Hundegger als Vollwasserzeichen ausgeführt (Dietz/Schmidt 2009: 21).

Dieselbe Wirkung konnte allerdings auch aufgrund von Erhöhungen im feinmaschigen Sieb erreicht werden, die durch starke Einpressung untergelegter Blechschablonen hervorgerufen wurden. Auf diese Weise wurden erhöhte Stellen im Sieb geschaffen, an denen sich lediglich eine dünnere Faserschicht absetzen konnte und die in der Durchsicht als helle Flächen erschienen. Durch partielles Tieferlegen des Siebes, also bei einer Pressung von oben, konnten nach dem gleichen Prinzip im Wasserzeichen aber auch Stoffanreicherungen erzielt werden, die in der Ansicht ein trüberes Aussehen bekamen. Besonders häufig tritt die Dunkelwasserzeichentechnik bei Porträtwasserzeichen auf, die bereits 1793 in Frankreich vorkommt. Dabei wurde diese Technik aber in den seltensten Fällen alleine angewandt, sondern das Hoch- und Tief-Prägen mit Matrizen auf einem Siebgeflecht kombiniert, so dass von Hell-Dunkel-Wasserzeichen oder Schattenwasserzeichen gesprochen wird, die in ihrer Wirkung sehr bildhaft erscheinen (vgl. Weiss/Weiss 1962: 138ff.).

Durch diese konkaven und konvexen Prägungen des Siebes erhielt das Papier viele neue Gesichter; allerdings blieb das Problem der Rohstoffknappheit durch einen exponentiellen Anstieg des Papierbedarfs – maßgeblich hierfür war sicherlich auch die 1445 eingeführte Drucktechnik Gutenbergs – bestehen. Auf das Rohstoffproblem der Papiermacher in den Jahren 1839/40 aufmerksam geworden, hatte Gottlob Friedrich Keller aus Hainichen bereits im darauf folgenden Jahr die Idee, künftig Holzfasern anstatt der Lumpenfasern zur Papierherstellung zu verwenden. Am 1. November 1845 erschien schließlich die Ausgabe 41 des »Intelligenz- und Wochenblatts für Frankenberg mit Sachsenburg und Umgebung« als weltweit erstes Druckerzeugnis auf holzschliffhaltigem Papier (vgl. Dietz/Schmidt 2009: 23).

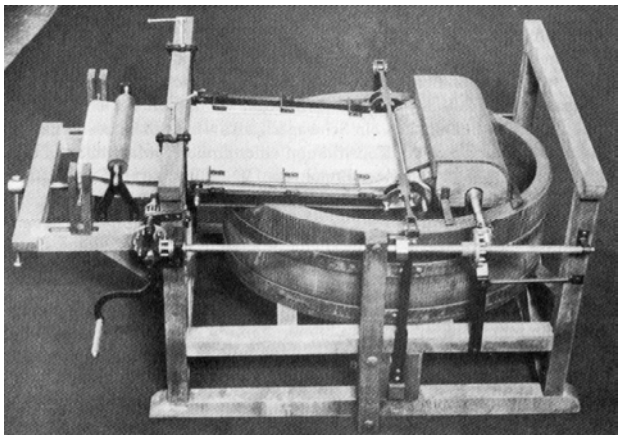

Abb. 6: Die von Nicolas-Louis Robert erfundene Langsiebpapiermaschine (Sandermann 1988: 107).

Auch zur traditionell-handwerklichen Schöpfrahmenkonstruktion wurde eine technologische Alternative mit dem Ziel einer leistungsstärkeren Fertigungsweise gesucht, da der Bedarf an Papier circa um das fünfzigfache zugenommen hatte.

Um diesen stark erhöhten Papierbedarf decken zu können, entwickelte der Franzose Nicolas-Louis Robert in den Jahren von 1796-1798 die Langsiebpapiermaschine, ein Maschinenmodell, das die Fertigung von bis zu fünf Meter langen und sechzig Zentimetern breiten Papierbahnen erlaubte (vgl. Dietz/Schmidt 2009: 24). Wesentlicher Bestandteil der Anlage war das endlose und feinmaschige Sieb aus dünnem Kupferdrahtgewebe, das über der mit Papierstoff gefüllten Bütte über eine vordere Walze und einer hinteren Umkehrwalze lief (vgl. Abb. 6). Zunächst besaß diese Konstruktion zwar noch erhebliche Mängel, so war beispielsweise noch keine Trockenpartie vorhanden; diese Herausforderungen wurden aber sukzessive gelöst und somit wurde die kontinuierliche Papierherstellung ab Mitte der ersten Hälfte des 19. Jahrhunderts ermöglicht. Bei der bis heute gängigen Papierherstellung fließt der Papierbrei auf ein mechanisch angetriebenes Metallsiebband, wird entwässert und anschließend über dampfgeheizten Trommeln getrocknet und satiniert, sprich durch Walzen geglättet.

Eine technologische Alternative zur Robert'schen Erfindung der Langsiebkonstruktion stellte zu seiner Zeit die 1805 von dem englischen Mechaniker Josef Bramah in London entwickelte Rundsiebpapiermaschine dar. Oftmals wird bei der Papierherstellung auf Rundsiebmaschinen fälschlicherweise von »Büttenpapieren« oder sogar »echten Bütten« gesprochen. Beim Herstellungsprozess taucht das zylinderförmige Sieb in die Bütte ein, durch die rotierende Bewegung bleibt der Faserbrei an dem Sieb haften und das Wasser fließt durch das Sieb in das Zylinderinnere ab. Durch die Anbringung stark erhobener Stege auf diesem Sieb entstehen deutlich verdünnte Stellen, an denen die Papierbahn durch Reißen in separate Bögen getrennt werden kann, wodurch beabsichtigter Weise unregelmäßige Ränder, die *Büttenränder* entstehen. Für die Wasserzeichenherstellung auf Rundsieben gilt

bis heute die gleiche Technologie, die bereits bei den handgeschöpften Papieren angewendet wurde, nämlich das Auflöten von Drähten auf das Sieb. Bei dieser Technik sind sowohl Papier als auch die eingebrachten Wasserzeichen schwer von handgeschöpften Bögen zu unterscheiden, weshalb das Rundsiebpapier in Bezug auf die Wasserzeichen eine gewisse Sonderstellung zwischen dem handgeschöpften und dem Langsiebpapier einnimmt, auch wenn es als Maschinenpapier gilt. Aufgrund der geringen Arbeitsgeschwindigkeit von Rundsiebpapiermaschinen kann auf dem Rundsieb hergestelltes Papier und damit auch sein Wasserzeichen in der Wirtschaftlichkeit mit dem auf Langsiebpapiermaschinen hergestellten Wasserzeichen, dem *Maschinenwasserzeichen,* aber nicht konkurrieren (vgl. Weiss/Weiss 1962: 296f.).

1.2.1 INDUSTRIELLE WASSERZEICHENHERSTELLUNG

Mit dem Fortschreiten der maschinellen Papierproduktion ergab sich das Bedürfnis, die von handgeschöpften Papieren her bekannten Wasserzeichen auch auf die industriell hergestellten Papiere zu übertragen, »denn das Wasserzeichen diente zu allen Zeiten nicht nur als Herkunfts-, sondern auch als Gütezeichen und hatte somit stets einen nicht zu unterschätzenden Werbewert« (Keim 1956: 215). Problematisch stellte sich hier allerdings die Tatsache dar, dass Figuren aus Draht oder ausgestanztem Blech nicht auf die Langsiebe angebracht werden konnten, da die Biegung des über zwei Walzen rollenden Metallgewebes so stark war, dass die aufgelöteten Drähte nicht elastisch genug waren, dieser Prozedur Stand zu halten. Der Londoner Formenmacher John Marshall erfand 1826 eine Verbesserung der Langsiebmaschine, nämlich die Siebwalze, englisch *Dandy Roll*, heute vielmehr unter dem französischen Begriff *Egoutteur* bekannt (vgl. Abb. 7).

Ursprünglich hatte diese Siebwalze oder Vordruckwalze auf dem Langsieb liegend den Zweck, die Stoffverteilung der noch nicht gefestigten Papierbahn auf dem Sieb gleichmäßiger zu gestalten und die Papierbahn somit glatter zu machen. Ihr Mantel ist aus einem geeigneten Siebgewebe gebildet, was Marshall ermöglichte, auf diesem Drahtfiguren anzubringen; diese auf dem Sieb erhabenen Stellen drückten sich spiegelbildlich von oben – im Gegensatz zum Handsieb seitenrichtig von unten – in die noch wässrige Papierbahn ein und hinterließen auf dem später getrockneten Papier Wasserzeichen. Somit ließen sich zunächst allerdings lediglich umrisshafte Wasserzeichen darstellen. Das erste maschinell erzeugte schattierte Porträt-Wasserzeichen lässt sich dagegen vermutlich erst auf den Papiermacher W.H. Smith zurückführen, der ein Porträt-Wasserzeichen Napoleons hergestellt hatte, das 1849 auf der Industrie-Ausstellung in Paris präsentiert wurde.

Abb. 7: Abbildung eines Egoutteurs aus dem Jahr 1923 für ein Hell-Dunkel-Wasserzeichen mit dem Schriftzug »REPUBLICANA PERUANA«[13] *(Dietz/Schmidt 2009: 26).*

Abb. 8: Schattenwasserzeichen von 1875, das Papst Pius IX. zeigt. Fabriano, Archivio Storico Cartiere Miliani (Mannucci 1993: 298).

13 Da sich in den Vertiefungen der Schrift mehr Papiermasse ansammelt, erscheint der Papierbogen an diesen Stellen dunkler. An den erhöhten Stellen des Drahtes im Vordergrund ist dies genau entgegengesetzt. Der Draht verdrängt mehr Papiermasse, und das Papier erscheint an diesen Stellen in der Durchsicht heller. Daher wird auch von einem Hell-Dunkel-Wasserzeichen gesprochen. Hersteller dieses Egoutteurs ist die Dürener Metalltuch- und Egoutteurfabrik J.W. Andreas Kufferath & Co.

Hierbei handelte es sich bereits um ein maschinell hergestelltes, schattiertes Wasserzeichen, wie es noch heute als weit verbreitetes Sicherheitsmerkmal Anwendung auf Banknoten oder Urkundenpapieren findet (vgl. Dietz/Schmidt 2009: 25f.; Weiss/Weiss 1962: 296-301; siehe auch Abb. 8).

> »In Deutschland wurden offenbar erst um 1840 die ersten Wasserzeichen im Maschinenpapier mit Hilfe des Wasserzeichenegoutteurs hergestellt. Vielleicht sind die ersten Wasserzeichenwalzen von der Papierfabrik Schäufelen in Heilbronn verwendet worden. Inzwischen ist die Egoutteurherstellung in ungeahnter Weise vervollkommnet worden, so daß heute damit nicht nur Hell- und Dunkelwasserzeichen, sondern auch schattierte, mehrstufige Wasserzeichen auf der Langsiebmaschine hergestellt werden können.« (Weiss/Weiss 1962: 297)

Ein weiterer Vorteil der maschinellen Papierherstellung lag in der Nutzungsdauer der Wasserzeichen-Egoutteure im Gegensatz zu den auf Handschöpfrahmen angebrachten Drahtfiguren. Die Egoutteure nutzen sich kaum ab und können daher erheblich länger als die bei den Schöpfsieben im Normalfall üblichen zwei Jahre verwendet werden. Für die Wasserzeichenkunde sind diese industriell hergestellten Papiermarken aber nur noch bedingt interessant, da sie sich aufgrund dieser Tatsache lediglich eingeschränkt zur Datierung heranziehen lassen (vgl. Dietz/Schmidt 2009: 26).

Daneben gab und gibt es in der Papierindustrie aber noch weitere Verfahren zur Erzeugung von Wasserzeichen. Neben den bereits erwähnten echten Wasserzeichen, die sowohl auf handgeschöpften als auch in maschinell produzierten Papieren hergestellt werden, treten ab 1920 sog. Molette- oder auch halbechte Wasserzeichen auf. Im Gegensatz zu den bereits erwähnten Methoden zur Herstellung von Wasserzeichen, wird die nahezu trockene Papierbahn nach dem Verlassen der Siebpartie hier nur geprägt, es findet keine partielle Reduzierung beziehungsweise Anreicherung des Faserbreis statt. Diese Prägungen in die zwar schon verfestigte, aber noch nicht trockene Papierbahn erfolgen durch gummierte Metallringe, den sog. *Molette-Ringen*, die auf den Prägerollen angebracht sind und sich im Gegensatz zum Egoutteur schnell und beliebig auswechseln lassen.

Die Wasserzeichen der dritten Kategorie werden in der Wasserzeichenkunde als künstliche oder unechte Wasserzeichen bezeichnet. Bei dieser bereits seit 1891 angewandten Methode zur Erstellung von Papiermarken wird das bereits fertige, getrocknete Papier in einem zusätzlichen Arbeitsschritt auf eine Platte gelegt, die mit der Wasserzeichenzeichnung in erhabenen Linien versehen ist. Zwischen zwei polierte Zinkplatten gelegt und wie beim Glätten durch die Walzenpresse geführt, drückt sich bei diesem heute nicht mehr praktizierten Verfahren die erhabene Zeichnung als Prägung in das Papier ein. Diese Methode wurde oftmals zur Fertigung von Brief- und Luxuspapieren, meist in geringer Auflage und immer auftragsbezogen für den Endverbraucher, angewandt.

Auch die sonst als »imitiert« bezeichneten Wasserzeichen oder Druckzeichen können unter die Gruppe der künstlichen und unechten Wasserzeichen subsumiert werden. Hierbei handelt es sich um Papiermarken, die mit dem Buchdruck einhergehen. Mittels einer farblosen, äußerst fetthaltigen Druckfarbe, die eine Veränderung der Papierfaser bewirkt, werden die Papiermarken auf die bereits fertigen Bögen gedruckt. Durch die enthaltenen Fettstoffe erscheinen entsprechend behandelte Stellen auf dem Papier durchscheinend, ohne dass das Papier gegen eine Lichtquelle gehalten werden muss; allerdings handelt es sich hierbei lediglich um eine sehr schwache Durchsicht. Dennoch wurde dieses Verfahren gelegentlich – wahrscheinlich gerade wegen seiner Einfachheit – zur Fälschung von Banknoten und anderen Wertpapieren angewandt (vgl. Weiss/Weiss 1962: 296-301). Daneben griffen Fälscher von Wertpapieren auch auf eine andere Technik zurück:

> »Man druckte Vorder- und Rückseite getrennt. Vor dem Zusammenkleben gab man einer Innenseite einen matten Flächendruck, wobei nur das Muster des Wasserzeichens weiß ausgespart wurde. Dies erscheint dann in der Durchsicht wie ein Wasserzeichen. Hier handelt es sich also lediglich um einen optischen Trick, nur scheinbar um ein Wasserzeichen. Künstliche und imitierte Wasserzeichen können auf Grund der angewandten technischen Methoden nur als Hellwasserzeichen erscheinen. Dunkel- und Schattenwasserzeichen sind auf künstliche Weise nicht hervorzubringen.« (Weiss/Weiss 1962: 301)

Eine Unterscheidung zwischen echten und imitierten Wasserzeichen lässt sich mit Natronlauge leicht durchführen. Während die echten Wasserzeichen durch Stoffverdrängung – bei den Hellwasserzeichen durch eine Stoffverringerung, bei den Dunkelwasserzeichen durch eine Stoffhäufung – im Stadium der Blattbildung entstehen, werden die geprägten oder gepressten Wasserzeichen im fertigen Papier lediglich aufgrund der zusammengepressten Stellen im Material sichtbar. Zur Überprüfung der Echtheit von Wasserzeichen, wird das Papier in eine Natronlauge gelegt, was ein starkes Aufquellen der Fasern bewirkt. Infolge dessen verschwinden die künstlichen Wasserzeichen, die echten dagegen bleiben sichtbar.

1.2.2 WASSERZEICHENMOTIVE

Wasserzeichen haben aber nicht nur eine herstellungstechnische Geschichte, sondern sind ebenfalls in ästhetischer Hinsicht interessant, da die Formenvielfalt einem ständigen Wandel unterliegt. In einschlägigen, bereits genannten Sammlungen, wie beispielsweise der von Piccard[14], lässt sich feststellen, dass die höchst

14 Die Wasserzeichensammlung Piccards mit 92.000 Wasserzeichen gilt als die weltweit größte und bedeutendste ihrer Art und wurde zu Recherchezwecken vollständig unter www.piccard-online.de, [05.12.2005], 01.03.2010, veröffentlicht.

einfachen, geradezu schlicht wirkenden Zeichen der ersten Zeit zunächst komplexere Formen annehmen und später sogar mit Beizeichen zur Unterscheidung von anderen Papiermühlen, die oftmals über die Grenzen hinweg dieselben Motive verwendeten, versehen werden. Diese Entwicklung gipfelt in einer kunstvollen Ausschmückung der Wasserzeichen mit ornamentalen Verzierungen, die in vereinzelten Fällen sogar vom eigentlichen Zeichen losgelöst wurden und ohne einen Hinweis auf Meister, Mühle, Sorte oder Format alleine in Erscheinung traten. Trotz dieser allgemeinen Entwicklung lassen sich interessanterweise auch in späteren Zeiten immer noch sehr einfache schlichte Zeichen nachweisen, wie diese aus der Frühzeit der Wasserzeichen bekannt sind. Allgemein können die Wasserzeichen im Papier als Symbole und Ausschnitte der zeitgenössischen Welt und deren Wahrnehmung erfasst und beschrieben werden: so reichen diese von Tier-, Pflanzen- und Naturdarstellungen über die bildliche Darstellung menschlicher Erzeugnisse bis hin zu Wappen und geometrischen Formen, oft auch religiösen Ursprungs.

1.3 ZUM FUNKTIONALEN WANDEL VON WASSERZEICHEN

Bei oben erwähnter Motivvielfalt stellt sich zugleich die Frage nach Verwendung, Zweck und Aufgaben von Wasserzeichen, die ebenfalls einem facettenreichen Wandel unterlagen. Während die frühesten Wasserzeichen in ihrer Mehrzahl als Namen und Buchstaben vorkommen, wie auch das älteste bekannte Wasserzeichen von 1271 aus Cremona (Buchstabe F) verdeutlicht, ist den Wasserzeichen ebenfalls von Anfang an eine symbolische Funktion zu eigen, wie das aus dem Jahre 1282 dargestellte Kreuz aus Fabriano zeigt. Religiöse, insbesondere christliche Symbole und Embleme kommen in der alten Wasserzeichenkunst verhältnismäßig oft vor (vgl. Kämmerer/Rückert 2009: 51ff.). Neben der Symbolsprache sind es die Entwicklungswege und Wandlungen in der formalen Gestaltung wie auch die Motivik dieser Zeichen, die Denk- und Vorstellungsweisen, soziale Verhältnisse und kulturelle Prozesse widerspiegeln (vgl. Ulbricht 2000: 41). Schon bald ist im Handwerk der Wasserzeichenherstellung eine Entwicklung weg von elementaren Symbolen hin zu einer vielgestaltigeren, komplexeren Formensprache zu beobachten. Narrativere Symbole der zeitgenössischen Alltagskultur, wie Pflanzen, Tiere, jegliche Figuren, Werkzeuge oder auch Fabelwesen finden nun ihr künstlerisches Abbild im Wasserzeichen. Diese Entwicklung wäre aber, wie Gertraude Spoer festhält, ohne die Leistungen derer, die Schöpfformen und Wasserzeichen herstellten, gar nicht denkbar gewesen. In der Anfangszeit der Papiermacherei wurden sie von den Papiermachern selbst oder von Handwerkern, die mit der Metalltechnik vertraut waren, wie bspw. Silberschmiede, hergestellt. Dieses Handwerk entwickelte sich aber im 17./18. Jahrhundert zu einem eigenständigen Gewerbe der Formenmacher. Die Handwerker zogen von Ort zu Ort, boten den verschiedenen Papiermühlen ihre Leistungen an und reparierten auch beschädigte Formen. Hierin kann ebenfalls eine Erklärung für die Verbreitung der unterschied-

lichen Motive über ganz Europa liegen. So treten beispielsweise ein gotisches P oder ein Ochsenkopf über Ländergrenzen hinaus gehäuft auf (vgl. Spoer 1996: 154f.).

Die Funktion der frühen Wasserzeichen als Meister- und Herkunftsmarke des Papiers – modern formuliert: Markenzeichen – ist dabei unbestritten, wie auch aus den bereits erwähnten Darlegungen des Bartolo da Sassoferrato hervorgeht. Ein weiterer Anhaltspunkt für diese ursprüngliche Funktion der Wasserzeichen liegt in ihrer Etymologie. So bürgerte sich die Bezeichnung »Wasserzeichen« erst seit der ersten Hälfte des 19. Jahrhunderts ein, zuvor sprach man zutreffender von »Papierzeichen« oder »Zeichen« schlechthin. Letztere Wortbedeutung findet sich ebenfalls in den auf Latein verfassten Schriften Sassoferratos, der für die erstmalige Erwähnung von Wasserzeichen in der Literatur überhaupt das Wort »signum« gebraucht (vgl. Weiss/Weiss 1962: 5).

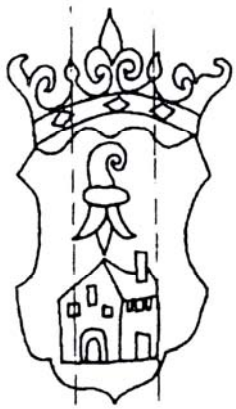

Abb. 9: Wasserzeichen mit Baselstab und Heusler-Wappen, Basel 1592 (Tschudin 1996b: 234).

Zur Kennzeichnung der Herkunft beziehungsweise des Herstellers des Papiers wurden aber nicht nur ausgeschriebene Namen, Monogramme, Abkürzungen und Ziffern verwendet, was anfangs und dann erst wieder seit dem 18. Jahrhundert verstärkt der Fall war, sondern auch auf figürliche Darstellungen jeglicher Art zurückgegriffen. Diese vielfältigen dem Alltag entsprungenen Motive zeigen in ihrer Symbolsprache oftmals Verbindungen zur Heraldik auf. So wurden Haus- und Handelsmarken im Sinne »sprechender Zeichen« ins Papier eingebracht, wie beispielsweise die Abbildung des Hauses der Basler Familie Hüsler, die auf das Jahr 1592 datiert werden kann (vgl. Abb. 9). Daneben waren auf dem Papier als Wasserzeichen eingebrachte Wappen aber meist Ausdruck des Abhängigkeitsverhältnisses zwischen Papiermacher und weltlichem oder geistlichem Auftraggeber. In Verbindung mit dem Aufkommen des Territorialstaates treten im 16./17. Jahrhundert gehäuft heraldische Elemente (Reichsadler, Bourbonenlilie, Pro Patria, Basel-

stab etc.) auf, die bis ins 19. Jahrhundert hinein die wichtigsten Papiermarken prägen.

Im Zuge der Ausdehnung der Papiermacherei in Europa entwickelten sich einige dieser Papiermarken weiter zu Qualitäts- und Sortenzeichen. Qualitativ hochwertige Papiere, wie sie ab Mitte des 16. Jahrhunderts in Frankreich hergestellt wurden, trugen als Wesensmerkmal oftmals voll ausgeschriebene Namen, während qualitativ geringwertigere Papiere lediglich die Initialen der jeweiligen Papiermacher oder -mühle aufwiesen. Eine weitere Bedeutung des Wasserzeichens war das Sortenzeichen, so war beispielsweise in Postpapier ein Posthorn eingelassen (vgl. Tschudin 1996b: 223-236). Zudem wurden besonders im 18. und 19. Jahrhundert Wasserzeichen als Kennzeichen für bestimmte Formate verwendet, die von der Größe des jeweiligen Schöpfsiebes abhängig waren; so steht beispielsweise ein in das Papier eingelassener Bienenkorb für das Format 36 x 45 Zentimeter, ein Bischofsstab für das Format 38 x 48 Zentimeter; Löwe als auch Einhorn werden für das Format 40 x 50 Zentimeter verwendet, das Einhorn kann aber auch für das Format 42 x 53 Zentimeter stehen (vgl. Weiss/Weiss 1962: 160).

1.3.1 WASSERZEICHEN ZUM SCHUTZ VOR FÄLSCHUNG

Zum Schutz gegen Nachahmung und Fälschung – kurz: zum Kopierschutz – treten Wasserzeichen bei Wertpapieren aller Art schon sehr früh auf. »Das Wasserzeichen gehört zu den ältesten und am meisten verwendeten Echtheitssicherungsmitteln« (Meyer 1935: 31). Im Gegensatz zu ihrer ursprünglichen und bis heute allgemein gültigen Aufgabe des Markenzeichens dient die Wasserzeichentechnik hier einem ganz anderen Zweck. In der genannten Funktion haben sich Wasserzeichen bis heute als unentbehrlich erwiesen, obwohl inzwischen weitere Verfahren gegen die Nachahmung von Wertscheinpapieren gefunden wurden, wie weiter unten erläutert werden soll. Das Wasserzeichen auf Wertpapieren ist nur schwer nachzuahmen, besonders dann, wenn dabei die verschiedenen, zuvor erläuterten Wasserzeichentechniken – Hell-, Dunkel- und schattierte Wasserzeichen – zugleich angewendet werden.

Bereits die ersten europäischen Banknoten traten nicht in der Funktion als Herkunfts-, sondern als Firmenzeichen der Banken oder Sonderzeichen auf, die analog zu modernen Banknoten »in eigener Art und Gestaltung ausschließlich zum Zweck des Echtheitsbeweises und zum Schutze gegen Nachahmung gefertigt wurden« (vgl. Weiss/Weiss 1962: 220). Bereits während der Tang-Dynastie in den Jahren zwischen 618-907 unserer Zeitrechnung wurden neben dem verwendeten Münzgeld weltweit erstmals Wertpapiere ausgegeben (vgl. Altmann 1997: 88). Wie bereits zuvor bei der Papierherstellung treten aber auch auf diesen ersten Wertpapieren sowohl aus technischen, als auch religiösen Gründen, keine Wasserzeichen auf. Die ersten Banknoten in Europa wurden ab Juli 1661 von der

schwedischen *Stockholm's Bank* herausgegeben (vgl. kritisch dazu Braudel 1985: 516). Da es bei diesen sog. Kreditzetteln aber schon bald darauf zu Fälschungen kam, wurde bei der Genehmigung zur Herausgabe von neuen Wertpapieren im Jahr 1665 festgelegt, dass für die Noten ein Papier mit dem Wasserzeichen der Bank angefertigt werden soll.

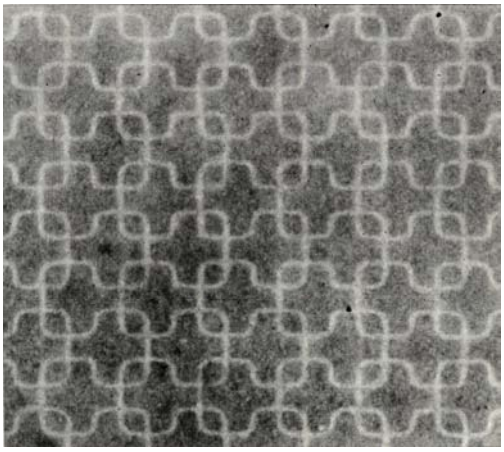

Abb. 10: Beispiel durchgehender Wasserzeichenmusterung (Weiss/Weiss 1962: 306).

Dieser Instruktion entsprechend weisen die 1666 herausgegebenen Banknoten der schwedischen Bank in Stockholm das Wasserzeichen *BANCO* auf, wie aus dieser Zeit erhaltene Noten zeigen. Dieses Wasserzeichen wurde an einer bestimmten Stelle des Bogens angebracht, die später nicht bedruckt wurde und somit das Wasserzeichen in der Durchsicht zur Überprüfung der Echtheit des Scheines deutlich erkennbar war. Zugleich handelt es sich bei diesen Wertpapieren aus Schweden um ein sehr frühes, wahrscheinlich sogar erstes Beispiel eines durchlaufenden Wasserzeichen-Musters im Papier, wie diese noch heute in Wertpapieren, wie Schecks, Briefmarken oder Dokumentenpapieren Verwendung finden. Selbst das für Lebensmittelkarten und Bezugsscheine aller Art im Ersten und Zweiten Weltkrieg verwendete Papier zeigte aus Sicherheitsgründen solche durchgehenden Wasserzeichenmusterungen auf (vgl. Abb. 10).

> »Wenn das besondere Wasserzeichenpapier und damit die auf ihm gedruckten Banknoten zwar nicht ohne weiteres nachgemacht werden konnten, so mußte doch auch dafür Sorge getragen werden, daß in der Papiermühle solches Papier nicht mißbraucht und nicht in fremde Hände gelangen konnte. Daher mußten Meister und Gesellen Reverse mit entsprechenden Verpflichtungen unterschreiben. Das Schöpfformenpaar mit dem Wasserzeichen der Bank mußte nach Gebrauch an diese abgeliefert werden.« (Weiss/Weiss 1962: 221)

Zudem wurden ausgediente Schöpfformen, die zur Herstellung von Wertpapieren genutzt wurden, durch das Entfernen einzelner Buchstaben aus einem Namen oder Wort unbrauchbar gemacht. Neben den Namen von Städten oder städtischer Geldinstitute kommen in Wertpapieren aber auch sonstige Zeichen, wie z.B. Angaben zum Wert der jeweiligen Banknoten, vor. So tragen die am 4. Februar 1854 ausgegebenen 10-Thaler-Scheine des Großherzogtums Weimar beispielsweise neben dem Vollwasserzeichen *WEIMARISCHE BANKNOTE*, das oben und unten am Rand dieser Scheine angebracht ist, entlang der beiden Schmalseiten in der Durchsicht erkennbar zusätzlich die Schriftbilder *10 THLR 10* (vgl. Weiss/Weiss 1962: 221). Daneben lassen sich auf Wertpapieren auch bildliche Motive aufzeigen, wie bspw. eine kleine Krone, die zum Echtheitsnachweis auf der am 6. Mai 1840 herausgegebenen »one penny black«, der ersten Briefmarke der Welt aus Großbritannien als Wasserzeichen ins Papier eingebracht ist (vgl. Hunter 1978: 550).

1.4 ZWISCHENBILANZ

Heute hat das Wasserzeichen – abgesehen von Sicherheitswasserzeichen in Banknoten und Wertpapieren, auf die im zweiten Teil dieser Arbeit eingegangen werden soll – seine ökonomische Funktion weitgehend verloren. Mit der großen technischen Entwicklung der Langsiebpapiermaschine Ende des 18. Jahrhunderts gipfelte die Herstellung von Maschinenpapier zu Beginn dieses Jahrhunderts in Papiermaschinen mit einer Arbeitsbreite von 10 Meter, Geschwindigkeiten von bis zu 72 km/h und einer Tagesleistung von mehr als 1688 Tonnen.[15] Einhergehend mit der Industrialisierung zwangen Wettbewerb und Kostendruck zu rationaler Fertigung. Während Papiermaschinen aber immer größere Siebbreiten und schnellere Maschinengeschwindigkeiten erreichen, werden Markierungen im Papier als störend angesehen, weil diese immer eine Reduktion der Leistung bedeuten. Ebenfalls ist es bei diesen hohen Geschwindigkeiten problematisch, klare Konturen der Papiermarken zu gewährleisten.

Was über Jahrhunderte untrennbar zum Papier gehörte, galt damit innerhalb weniger Jahre als verzichtbar. Das Wasserzeichen spielt zwar in der Funktion eines Logos in der heutigen Werbeindustrie – verdrängt von einem Mix anderer Marketingsstrategien – kaum mehr eine Rolle; umso freier können nun aber moderne Handpapiermacher und Papierkünstler diese graphische Darstellungsform aufgreifen und als Gestaltungsmittel ihrer Produkte einsetzen.

Moderne Wasserzeichenpapiere gelten dabei heute als Prestigeerzeugnisse mit entsprechend höherem Preis. Einen Höhepunkt der kreativen Auseinandersetzung mit Wasserzeichen bilden dabei vom Künstler als Wasserzeichen verfasste Schriftstücke:

15 Die derzeit leistungsfähigste Papiermaschine wird von der Gold East Paper (Jiangsu) Co. Ltd in China/Dagang betrieben (vgl. Birkner International PaperWorld 2005: 6).

> »Die klassische Funktion von Papier als Träger von Information via Handschrift oder Druck wird [hier] zugunsten von Wasserzeichen eliminiert. Papier selbst ist bereits Träger von »transparenten« Informationen. Sie zu lesen bleibt ein spannendes Abenteuer und dessen Nutzung im 21. Jh., dem medialen Zeitalter, eine große Herausforderung.« (Ulbricht 2000: 42)

2 DAS WASSERZEICHEN AUF BANKNOTEN

Das Wasserzeichen auf Geldscheinen ist eines der bekanntesten Sicherheitsmerkmale. Trotz oder vielleicht gerade wegen seiner jahrhundertelangen Tradition in Herstellung und Einsetzbarkeit ist es fester Bestandteil auch auf den neusten Euro-Banknoten. Seine größten Vorteile sind vor allem die schwierige, weil teure und detailreiche Herstellung und der Umstand, dass das Wasserzeichen von Laien schnell zur Überprüfung der Echtheit einer Note gefunden und erkannt wird. Das Wasserzeichen auf Geldscheinen ist wohl *das* Sicherheitsmerkmal, das durch viele Kulturen und Zeiten hindurch Bestand hat. Wenn es also eine Kultur des Kopierschutzes gibt, dann ist das Wasserzeichen der Inbegriff dieser.

Schon mit der Erfindung der Münze begann die Entwicklung des Schutzes »vor unerlaubten Nachahmungen der offiziellen Zahlungsmittel« (Deutsche Bundesbank 1995: 5). In unserer heutigen hoch technisierten Welt gestaltet sich dieser Schutz immer schwieriger. Nur mit einer Vielzahl an Sicherheitsmerkmalen, die harmonisch ineinander greifen, ist es möglich, die Banknote weitestgehend vor Fälschungen zu schützen, auch wenn diese Fälschungsschutztechniken immer nur kurzlebig sind und ständiger Überholung und Erweiterung bedürfen. Zunehmend modernere Reproduktionstechniken treiben die Bundesbanken an, neue Sicherungen in die bestehenden Scheine einzuarbeiten oder sogar neue Serien von Banknoten zu entwickeln.

Um das bekannteste aller fälschungshemmenden Sicherheitsmerkmale auf Banknoten, das Wasserzeichen, soll es in diesem Teil des Textes gehen. Dabei ist dieses Kapitel in zwei Teile gegliedert:

a. Historischer Abriss: Wann, wo und warum entstanden die ersten Banknoten? Wann und in welcher Form tauchen Wasserzeichen erstmals auf Geldscheinen auf?

b. Das Wasserzeichen auf der Euro-Banknote: Thema in diesem Teil wird unter anderem die Herstellung der Euro-Banknote allgemein aber vor allem die Herstellung des auf den Geldnoten angebrachten Wasserzeichens sein.[16]

16 Spezifische Informationen der Herstellung von Euro-Banknoten veröffentlicht die Deutsche Bundesbank aus Gründen des Dienstgeheimnisses nicht. Zum Dienstgeheimnis siehe den Beitrag von Ludwig Andert und Doris Ortinau im Heft »Kulturen des Kopierschutzes I«.

2.1 HISTORISCHER ABRISS

2.1.1 DIE ANFÄNGE DES PAPIERGELDES

Die deutsche Bundesbank datiert die »wahrscheinlich ältesten in Originalstücken erhaltenen« (Weber 1970: 11) Papiergeldscheine auf das 14. Jahrhundert. Sie stammen aus China und sind mit Ausgabedatum versehen. Schon damals sorgte man sich um illegale Kopien und bedrohte daher auf den Scheinen die Geldfälscher mit Strafe und setzte sogar eine Belohnung für die Anzeige von solchen Fälschern aus (vgl. Deutsche Bundesbank 1995: 5; vgl. auch Deutsche Bundesbank 1963). Andere Historiker führen die Anfänge der Nutzung von Papiergeld auf die Mitte des 13. Jahrhunderts zurück. So schreibt z.B. Fernand Braudel:

> »Vermutlich stellte die Ausgabe von Papiergeld eine Reaktion der Chinesen auf die Konjunktur des 13. und 14. Jahrhunderts dar und diente ihnen als Mittel, die mit dem Umlauf der altertümlich schweren kupfernen oder eisernen Lochmünzen verknüpften Schwierigkeiten aus dem Weg zu räumen und den Außenhandel über die Seidenstraßen zu beleben.« (1985: 493/494)

Das erste Papiergeld in Europa taucht erst im 15. Jahrhundert auf. Aus der Not heraus beschriftete Graf Tendilla in Spanien Papierzettel und drückte sein Siegel darauf. Ihm wurde in der langen Belagerungszeit der Mauren das Münzgeld knapp. Doch seine Soldaten wollten bezahlt werden, um die Stadt weiter erfolgreich zu schützen und guter Laune zu bleiben. Nach der Belagerungszeit befahl er den Bürgern der Stadt daher, die selbst geschriebenen Zettel gegen Gold und Silber einzutauschen: »Nach dem Umtausch sollen alle Geldpapierscheine vernichtet worden sein« (ebd.: 4). Das älteste erhaltene europäische Geld aus Papier stammt aus den Niederlanden. Dort wurden während der niederländischen Freiheitskriege in einer Belagerung durch spanische Truppen zwischen 1573 und 1574, ebenfalls weil das Münzgeld knapp wurde, aus Deckeln der Kirchenbücher Pappmünzen hergestellt (vgl. ebd: 4). Auch wenn es sich um Papiergeld als solches handelte, kann man die dargestellten Anfänge der Papiernoten mit den Banknoten wie wir sie heute kennen, nicht vergleichen.

Wesentliche grundlegende Merkmale einer Banknote, wie z.B. die durchdachte professionelle Herstellung, die Ausgabe gegen Wert oder Verdienst und die Aushändigung durch bestimmte Instanzen fehlen bei dieser Art des Papiergeldes. Hinzu kommen die räumliche und zeitliche Begrenzung des damals in der Not entstandenen Geldes. Diese Aspekte flossen erst ab Mitte des 17. Jahrhunderts in die Notenproduktion und -ausgabe ein.

2.1.2 DIE ANFÄNGE DER BANKNOTE

Die Banknote ist Mitte des 17. Jahrhunderts in Gebrauch gekommen. Vor ihrer Existenz erfüllten, bis auf einige wenige Ausnahmen, Gold und Silbermünzen die Funktion von Zahlungsmitteln. Während die Aufdrucke der Banknote heute angeben, welchen Geldwert die Note hat, machten sie früher zunächst Angaben darüber »wie viel Geld die Notenbank für diese Note zu zahlen versprach« (Born 1972: 3). Großbritannien war Mitte des 17. Jahrhunderts *das* Industrie- und Handelsland. Es wurde zum Ursprungsland der Banknote (vgl. ebd.: 4). Damals gaben die reichen Einwohner Englands ihre Münzen und ihr Gold Goldschmieden oder Geldwechslern zu Verwahrung und erhielten als *Quittung* eine notenartige Bescheinigung.

Anlass zu dieser Anlage waren unter anderem die unsicheren Verhältnisse während des englischen Bürgerkriegs Mitte des 17. Jahrhunderts sowie die Eigenschaft der bequemen, weil leichten Zahlungsmittel (vgl. ebd.). Neben diesen quantitativen Gründen waren es auch die wachsenden wirtschaftlichen Dimensionen und die Tatsache, dass »für den Bedarf an Zahlungsmitteln in Produktion und Handel die eigenen Mittel nicht mehr ausreichten und somit Kredit nachgefragt wurde« (Weber 1970: 32).

Die Verwendung war derzeit nur innerhalb eines Ortes bzw. einer bestimmten Region möglich, da derjenige, der die Noten als Zahlungsmittel annahm, die Möglichkeit haben musste, diese auch gegen Gold oder Münzen einzulösen (vgl. ebd.: 4). »Die Erfahrung zeigte, dass niemals alle Dispositionsscheine, alle Noten, gleichzeitig zur Einlösung präsentiert wurden. Die Geldwechsler und Goldschmiede konnten also mehr Dispositionsscheine, mehr Noten ausgeben, als sie Münzgeld oder Gold im Depot hatten« (Born 1972: 5). So beschafften sich die Inhaber der Depots schon damals Kredite und das Geschäft des Bankers bzw. des Privatbankiers entstand. Bald darauf wurde 1668 »die erste Notenbank auf Aktien« (ebd.: 5) gegründet. Im Laufe der Jahre entstanden immer mehr private Notenbanken mit eigenen Noten. In der Krise, nach dem Ende des napoleonischen Krieges (1816/17), gingen an die 90 private Notenbaken bankrott (vgl. ebd.: 6). Sie hatten das Problem, »bei vorsichtiger Notenemission den Geschäftsbedürfnissen nicht genügen zu können oder aber bei starker Notenemission ihre Fähigkeit zur Bareinlösung zu gefährden« (ebd.: 7). Man verlangte daher weitere Aktien-Notenbanken, da zu dieser Zeit nur die Bank of England als Aktien-Notenbank zugelassen war. Das Parlament kam dem Wunsch nach, erließ aber ein Gesetz, das es anderen Banken als der *Bank of England* verbot, im Umkreis von 65 Meilen um London Noten auszugeben. 1833 bestimmte das neue Bankgesetz, »daß die Noten der *Bank of* England in England und in Wales gesetzliches Zahlungsmittel sein sollten« (ebd.: 7). Das Ursprungsland der Banknote wurde also auch zum Vorreiter der Banknote als gesetzlichem Zahlungsmittel. Scheine, die zuvor in Umlauf waren, hatten keine staatliche Allgemeingültigkeit. Das System funktionierte aber noch nicht, da die *Bank of England* mehr Geld ausgab als ihr zur Verfügung stand. Darum musste sie Kredite bei ausländischen Banken aufnehmen, um

die Einlösungsbegehren zu erfüllen. Zwischen den Jahren 1797 und 1819 konnten die Noten daher nicht eingewechselt werden und hatten einen Zwangskurs (vgl. ebd.: 8). Der jahrzehntelange Streit zwischen Vertretern der sog. *Currency-Schule*, die die Banknoten zu Geld erklärte, und Anhängern der sog. *Banking-Schule*, die in den Banknoten ein Kreditmittel sah, entstand genau aus dieser Tatsache, dass in diesen 22 Jahren, zwischen 1797 und 1819, die Noten echtes Papiergeld waren. Die Noten hatten sich in dieser Zeit, wenn auch nur kurz, erstmalig von einem Ersatzmittel für ein hochwertiges Produkt (das Gold oder die Münzen), zu einem Wertgegenstand entwickelt.

Nach diversen Notenbankenkrisen (1816, 1825 und 1839) wurde der *Currency-Theorie,* die sich für eine Deckung der umlaufenden Banknoten zu zwei Dritteln durch Gold und zu einem Drittel durch staatliche Schuldtitel aussprach, Folge geleistet. Im Zuge dessen ging das Merkmal der Einlösbarkeit den Banknoten endgültig verloren. Es kam daher 1844 eine Neuregelung namens *Peel's Act* zustande, die den Weg für die Zentralnotenbank in England ebnete (vgl. ebd.: 9). Im Klartext bedeutete diese Regelung, dass keine neuen Notenbanken mehr gegründet und die bereits bestehenden privaten Banken ihren Notenumlauf nicht mehr erweitern durften. »Und wenn eine dieser privaten Notenbanken auf die Notenemission verzichtete oder das Emissionsrecht verlor – [...], so fiel ihr Notenemissionskontingent an die Bank of England als *Erbin*. Es dauerte Jahrzehnte, bis die englischen und walisischen Privatnotenbanken ihre Emission einstellten oder verloren: [...].« (ebd.: 9).

»Der ursprüngliche Charakter der Banknote wurde durch die Aufhebung der Einlösungspflicht und die Erklärung zum gesetzlichen Zahlungsmittel grundlegend geändert. Die Banknote rückte zum allgemein verwendeten Geld auf« (Weber 1970: 21). Für die meisten Notensysteme dieser Welt waren das englische und das schottische System im Laufe ihrer Entwicklungen wegweisend. In Deutschland allerdings entwickelten sich die Notenbanken von einer staatlichen Notenbank zu vielen einzelnen privaten und öffentlichen Notenbanken und schließlich zur Reichsbank als zentraler Notenbank (vgl. Born 1972: 15).

Die älteste deutsche Notenbank war die 1765 von Friedrich dem Großen in Berlin gegründete Preußische Bank. Deren Banknoten galten allerdings nicht als gesetzliches Zahlungsmittel, sondern waren nur eine von vielen Noten im Umlauf (vgl. ebd.: 16). Erst 144 Jahre später (1905) wurden schließlich die Reichsbanknoten zum gesetzlichen Zahlungsmittel erklärt: »Gleichzeitig veranlaßte die Reichsbank die Wirtschaftsunternehmen, bei der Lohnzahlung bis auf das nötige Kleingeld Banknoten auszuzahlen« (ebd.: 20). 1944 wurden die Noten der Reichsbank zum definitiven Geld und die Noten der anderen Privatbanken konnten gegen diese eingelöst werden. Auf Grund dieser Allgemeingültigkeit der Reichsbanknote wird auch die Fälschungssicherheit, d.h. der Kopierschutz für das Währungssystem immer bedeutsamer. Dies belegt die Tatsache, dass das erste (wis-

senschaftlich belegte) Wasserzeichen auf Geldscheinen in den Jahren dieser gesetzlichen Umstrukturierung zu finden ist.[17]

Auch in allen anderen großen europäischen Ländern galten die Banknoten zu dieser Zeit als gesetzliches Zahlungsmittel (vgl. ebd.: 20). Im Unterschied zu den Anfängen der Banknoten, musste in Deutschland und Frankreich im 19. Jahrhundert nicht mehr der gesamte Geldumlauf mit Gold gedeckt werden. Die Banken waren lediglich dazu verpflichtet, die in Umlauf gebrachten Noten zu einem Drittel zu decken. Der sog. Goldstandard, also die Deckung einer Währung in Gold, besteht in Deutschland seit Anfang des 19. Jahrhunderts (Bankgesetz vom 14. März 1875, § 17)[18] nur noch theoretisch. Denn die Zentralbanken sind zwar zu einem Umtausch von Geld in Gold verpflichtet, das Bankgesetz vom März 1875 erlaubt aber ebenfalls einen Tausch in »courfähiges«[19] Geld. Früher waren das neben den Goldmünzen und Silbertalern auch Scheidemünzen und Kassenscheine. Seit 1971 haben goldbasierte Währungen nur noch theoretische Bedeutung. Der Dollar war die letzte goldbasierte Währung der Erde.[20]

Heute zirkuliert die Banknote nicht mehr als Geldsurrogat, sondern gilt als endgültiges Geld. »Die Einlösbarkeit bezieht sich nicht auf anderes Geld, sondern auf Güter« (Weber 1970). Derzeitige Währungen sind in der Regel manipulierte Papierwährungen und unterliegen keinem Währungsstandard. »An die Stelle eines Standards traten geldpolitische Maßnahmen der Zentralbanken, die eine Preisniveaustabilität sicherstellen sollen.«[21]

2.1.3 DEFINITION BANKNOTE

Aufgrund der oben kurz skizzierten Entstehung und Entwicklung soll hier die sog. moderne Definition der Banknote zugrunde gelegt werden. Sie wird »als ein von der Notenbank ausgegebenes, bar umlaufendes, papierförmiges Geld definiert« (Weber 1970: 38). Das Zahlungsversprechen ist unwichtig geworden und wird teilweise sogar abgelehnt. »Das Merkmal der Einlösbarkeit in seiner ursprünglichen Form besteht nicht mehr« (ebd.: 38). Vielmehr bilden die unmittelbare Verwendungsform und der bare Austausch das Kennzeichen in dieser Definition der Banknote. Sie allein gilt als Geld (vgl. Braudel 1985: 514-522).

Diese Definition bringt die These mit sich, dass mit der Entmaterialisierung des Geldes auch die Gefahr der Fälschung steigt. Daraus folgt die Notwendigkeit des Kopierschutzes.

---

17 Auf die Geschichte des Wasserzeichens in Deutschland wird im Kapitel 2.1.4.2. »Die ersten Wasserzeichen in Deutschland« näher eingegangen.

18 Vgl. Bankgesetz vom 14. März 1875, § 17, http://de.wikisource.org/wiki/Bankgesetz#.C2.A7._18., 04.05.2010.

19 Cour = frz. Hof.

20 Vgl. http://www.numispedia.de/Goldstandard, 01.03.2010.

21 http://de.wikipedia.org/wiki/Goldstandard, 01.03.2010.

2.1.4 DIE ENTWICKLUNG DER WASSERZEICHEN AUF BANKNOTEN

2. 1.4.1 DIE ERSTEN WASSERZEICHEN

Mitte des 17. Jahrhunderts fand das Papiergeld seinen Weg nach Schweden. Dort sind die ersten Banknoten einer schwedischen Bank 1661 in Umlauf gekommen (s.o.). Zwischen 1662 und 1664 wurden erste Serien von Geldscheinen mit unterschiedlicher Wertigkeit herausgegeben. Doch die bekanntesten historischen schwedischen Banknoten stammen von einem Bankangestellten der Stockholmer Bank, John Palmstruch, aus dem Jahre 1666: die Palmstruchers. »Die Herstellung dieser Bankscheine erfolgte mittels dickem, handgefertigten Papier. Die Noten weisen die ersten Wasserzeichen Europas BANCO auf« (Van Damme 2008). Ebenfalls sehr früh, nämlich 1793, zierten Wasserzeichen die Währungen während der Französischen Revolution, die Assignaten (vgl. Keller 1955: 1). Dem Geldmuseum der Deutschen Bundesbank liegen Wertpapiere mit Wasserzeichen aus dem 18. Jahrhundert vor.

2.1.4.2 DIE ERSTEN WASSERZEICHEN IN DEUTSCHLAND

> §146
> Geldfälschung:
>
> »Mit Freiheitsstrafe nicht unter einem Jahr wird bestraft, wer
>
> 1. Geld in der Absicht nachmacht, daß es als echt in Verkehr gebracht oder daß ein solches Inverkehrbringen ermöglicht werde, oder Geld in dieser Absicht so verfälscht, daß der Anschein eines höheren Wertes hervorgerufen wird
>
> 2. falsches Geld in dieser Absicht sich verschafft oder feilhält oder
>
> 3. falsches Geld, das er unter den Voraussetzungen der Nummern 1 oder 2 nachgemacht, verfälscht oder sich verschafft hat, als echt in Verkehr bringt
>
> (2) Handelt der Täter gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung einer Geldfälschung verbunden hat, so ist die Strafe Freiheitsstrafe nicht unter zwei Jahren.
>
> (3) In minder schweren Fällen des Absatzes 1 ist auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren, in minder schweren Fällen des

> Absatzes 2 auf Freiheitsstrafe von einem Jahr bis zu zehn Jahren zu erkennen.«[22]
>
> §147
> Inverkehrbringen von Falschgeld
>
> (1) Wer, abgesehen von den Fällen des § 146, falsches Geld als echt in Verkehr bringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
>
> (2) Der Versuch ist strafbar.«[23]

Seit der Einführung von Geld versuchen immer wieder, mehr oder minder geschickte Betrüger die jeweilige Währung zu fälschen und in Umlauf zu bringen. Schon 230 n. Chr. versuchte man innerhalb des Römischen Reiches mit Hilfe von Tongussformen die damaligen Denare in großem Stil zu fälschen.[24] Der – heutzutage – obligatorische Biss in eine Medaille auf dem Siegertreppchen diente derzeit unter anderem zur Überprüfung der Münzen. Gefälschte Taler waren häufig aus weicherem Metall und konnten daher durch die Kraft des Kiefers verformt werden. Dem gestellten Betrüger drohten schreckliche Strafen. Er wurde z.B. in siedendes Öl getaucht.[25]

In Deutschland traten Wasserzeichen auf Banknoten, verglichen mit der internationalen Entwicklung, einige Jahrhunderte später auf. Erstmals wissenschaftlich dokumentiert findet man das Wasserzeichen auf der 100-Mark-Reichsbanknote vom 07.02.1908 (vgl. Rosenberg 2001: 37). Schon damals wusste man um den Schaden von Falschgeld und drohte auf den späteren Reichsbanknoten mutmaßlichen Fälschern mit dem Aufdruck: »*Wer Banknoten nachmacht oder verfälscht, oder nachgemachte oder verfälschte sich verschafft und in Verkehr bringt, wird mit Zuchthaus nicht unter zwei Jahren bestraft.*«[26] Ein Zusammenhang zwischen Wasserzeichen und Geldfälschungen liegt also sehr nahe. Von 450 Notengeldscheinen, die zu Beginn des ersten Weltkriegs 1914 erschien, weisen trotzdem gerade zehn ein Wasserzeichen als Sicherheitsmerkmal auf (vgl. Keller 1955: 2). »Mit der Entwicklung des Papiergeldwesens im 19. Jahrhundert verfeinerte sich auch die Banknotentechnik. Allmählich führte jede notenberechtigte Bank ihr eigenes Wasserzeichenpapier, vielfach freilich nur primitiver Art, lediglich auf einer geraden Linie oder längs der 4 Ränder des Scheins den Banknamen in hellen

22 http://dejure.org/gesetze/StGB/146.html, 01.03.2010.

23 http://dejure.org/gesetze/StGB/147.html, 01.03.2010.

24 Vgl. http://www.datensicherheit.de/aktuelles/sechs-roemische-denare-als-sensationeller-informationslieferant-827, 01.03.2010.

25 Vgl. http://www.datensicherheit.de/aktuelles/sechs-roemische-denare-als-sensationeller-informationslieferant-827, 01.03.2010.

26 http://www.briefmarkenhaus-heubach.de/blog/?p=461, 01.03.2010.

Blockbuchstaben zeigend« (ebd.: 1). Verwendete Muster waren damals der Rautenstern, das Mühlrad, das Z-Muster, die Schuppen, die Wellenbündel und die Kreise (vgl. ebd.: 2). Damals wurden auf einen Schein mehrere Muster gedruckt – doch die vielen verschiedenen Wasserzeichen machten es für die Bevölkerung schwer, die Echtheit der Banknote auszumachen (vgl. ebd.: 2). »Erst mit dem Aufkommen der Kleingeldscheine seit 1917 entstand allmählich ein größerer Bedarf, und eine wachsende Zahl von Papierfabriken nahm die Herstellung von Wasserzeichen auf« (ebd.: 2). In den 1920er Jahren entstanden auf Grund der Inflation in Deutschland und den tausenden Ausgaben von Banknotenbogen viele Variationen von Wasserzeichen (vgl. ebd.: 2). Die Drucke reichten von verschiedenen Mustern bis zu aufwendigen Kombinationen von Figuren und Elementen. Die meisten dieser Wasserzeichen waren sehr prägnant und tauchten in einer begrenzten Anzahl auf dem jeweiligen Schein auf. Einige bedeckten jedoch die komplette Note.

Im Laufe der Jahre lässt sich ein gewisser Wechsel der Gestaltung der Wasserzeichen feststellen. Ältere, oben genannte Wasserzeichenmuster treten weniger auf. Es erscheinen neue Motive – weniger aus dem Grund des Geschmacks, sondern vielmehr aus der Notwendigkeit des Kopierschutzes, da Restbestände von Wasserzeichenpapier für andere Zwecke verwendet oder einfach verkauft wurden. Geldfälscher hatten daher leichtes Spiel. Mit den neuen Motiven kam gleichzeitig auch eine kompliziertere Herstellungstechnik mit heller und dunkler Wirkung in Gebrauch (vgl. ebd.: 3-5). Nach dem Zweiten Weltkrieg, genauer seit der Einführung der Banknoten der späteren Bundesrepublik Deutschland ab 1948, stellte man deren Wasserzeichen mit Hilfe einer Technik her, in der man grünes oder lila Färbemittel auf das immer noch feuchte Papier aufgoss. Die Folge war daher ein farbiges Wasserzeichen. Viele dieser deutschen Noten favorisierten geflochtene Kabel- oder säulenartige Wasserzeichenmuster, die bei der Gestaltung des Scheines berücksichtigt und so Teil des Designs wurden. Alle Noten wurden von der Bank deutscher Länder herausgegeben.

2.1.4.3 DIE FRÜHE GESCHICHTE DER WASSERZEICHEN AUF BANKNOTEN WELTWEIT

In anderen Ländern der Welt trat das Wasserzeichen zu der jeweiligen Währungsnote am Randbereich der Note, oder in einem ovalen Feld ohne sonstigen Druck, auf. Im Folgenden seien einige Beispiele internationaler Wasserzeichenmuster aufgeführt. *Hammer und Sichel* setzte sich z.B. 1923 als das offizielle Symbol des Kommunismus durch und taucht als Wasserzeichen in den Währungen von der Sowjetunion und anderer kommunistischer Länder auf. Während des Zweiten Weltkriegs, als die Japaner die Philippinen besetzten, tauchten auf den philippinischen Peso-Scheinen[27] niederer Wertigkeit breitblättrige Pflanzen als Wasserzeichen in nicht bedruckten Bereichen der Banknoten auf. Manche britische Noten

27 Philippinisch = piso.

bildeten ein vertikales Motiv ab, auf dem sich ein Kopf oder ein Portrait drei- bis fünfmal über den Schein hinweg wiederholten. Auch die Taube als Zeichen des Friedens findet man auf verschiedenen Banknoten, wie z.B. auf dem 500-Franc-Schein der Zentralbank der Republik Guinea. Ein sehr schönes Wasserzeichen auf einer Währung ist der große struppige Löwenkopf auf den Noten der Zentralbank von Kenia. Genau wie das Wasserzeichen, das den lockigen und gehörnten Kopf eines Schafsbocks auf der Banknote der Zentralbank von Zypern abbildet (vgl. Crummett 1982).

2.2 DAS WASSERZEICHEN AUF DER EURO-BANKNOTE

Seit 1999 existiert die Europäische Währungsunion (EWU) mit dem Euro als gemeinsamer Währung. Die Euro-Banknoten galten bei ihrer Einführung am 1. Januar 2002 als vermeintlich sicher.[28] Von diesem Wunschdenken hat man sich allerdings schnell verabschiedet.

> »Inzwischen steigt die Zahl der beschlagnahmten Euro-Blüten stetig an, und zwar mit einer jährlichen Wachstumsrate von etwa 30 Prozent. Im Jahr 2004 wurden in Deutschland bereits über 80.000 gefälschte Banknoten eingezogen, europaweit lag diese Zahl bei etwa 525.000 Euro-Blüten.«[29]

Gute Fälschungen sind allerdings schwer herzustellen. Dafür sorgen die zahlreichen Sicherheitsmerkmale der Euro-Banknoten.

2.2.1 HERSTELLUNG DER EURO-BANKNOTE – DIE PAPIERHERSTELLUNG

Bereits bei der Papierherstellung beginnt der Prozess der Einarbeitung verschiedener Sicherheitsmerkmale. Baumwolle bildet das Rohmaterial der Euro-Banknote. Sie wird zu einem Brei verarbeitet, der schon in flüssigem Zustand in der entsprechenden Wertfarbe eingefärbt wird. Diese Farbe ist eine Spezialfarbe, die auf Kopiergeräten nur schlecht wiedergegeben werden kann. Außerdem werden der Papierrohmasse fluoreszierende Fasern zugesetzt, die nur unter UV-Licht sichtbar werden. Dafür sind im Handel Geräte erhältlich. Dieser Methode der Echtheitsüberprüfung bedienen sich vor allem Geschäfte. Nach Fertigstellung des Papierbreis wird die Masse auf ein Siebgewebe geschüttet, auf das zuvor der Sicherheitsfaden geführt wurde. Dieser »besteht aus einer Kunststofffolie, die mit Aluminium beschichtet ist und helle Mikroschriften auf dunklem Untergrund enthält«.[30] »Feine Siebe, auf einen Zylinder gespannt, schöpfen aus einer mit Baum-

28 Vgl. http://www.focus.de/finanzen/banken/euro-banknoten_aid_114045.html, 01.03.2010.

29 http://www.urbs.de/archiv/geld/change.htmgeld153.htm, 01.03.2010.

30 Diese Angaben stammen von den Erklärungstafeln des Geld-Museums der Deutschen Bundesbank in Frankfurt. Besuch am 01.03.2010.

wollbrei gefüllten Wanne eine endlose Papierbahn« (Deutsche Bundesbank 1995: 25). In dieses Siebgewebe sind die Wasserzeichen bereits eingeprägt und das Wertwasserzeichen aufgelötet.

Durch die Prägungen legt sich der Baumwollbrei ungleich auf das Sieb, so dass das fertige Papier an einer Erhöhung des Siebes dünner oder an einer Vertiefung dicker wird. Das echte Anlagerungswasserzeichen entsteht genau durch diese Variierung der Papierdicke während der Papierherstellung. Diese unterschiedliche Papierstärke sorgt für das typische optische Merkmal des echten Wasserzeichens auf Banknoten: den nahezu stufenlosen und feinen Übergängen von hellen zu dunkleren Bereichen. Sie geben dem Wasserzeichen auch den Namen des Mehrtonwasserzeichens. Auf der Euro-Banknote bildet das Architekturmotiv am Rand des Scheins das Mehrtonwasserzeichen und die Wertzahl des Scheines das Drahtwasserzeichen. Das Drahtwasserzeichen besteht aus feinen Linien wie z.B. Buchstaben und Zeichen. »Zur Herstellung der Wasserzeichen wird dünner, rostfreier Draht gebogen und mit Metallfäden spiegelverkehrt auf das Schöpfsieb genäht. Da sich die Fasern auf dem Drahtgebilde in dünnerer Schicht ablagern als in der Umgebung, erscheint das Wasserzeichen in der Durchsicht hell.«[31] Eine dritte Form des Wasserzeichens stellt das Balkenwasserzeichen in der Mitte des Scheins dar. Mehrtonwasserzeichen und Drahtwasserzeichen bilden durch die unterschiedliche Papierdicke eine Reliefdarstellung. Das Papier wird somit dreidimensional und weist Merkmale einer Raumstruktur auf, die sich nur durch Ertasten bemerkbar machen. Die Sicherheitsmerkmale sprechen also verschiedene Sinneskanäle an. Dadurch wird die Sicherheit vergrößert.

Die Urform des Wasserzeichens ist eine Wachsschabung, aus der nach mehrfacher Veränderung »der Prägestempel zur Herstellung des Wasserzeichensiebes entsteht«. Er stempelt »das Motiv des Wasserzeichens in das Drahtgewebe des Rundsiebs«. Von dieser Urform kann man durch die Vielzahl an Korrektur- und Übertragungsvorgängen nur schwer auf das Erscheinungsbild des fertigen Wasserzeichens schließen (vgl. Deutsche Bundesbank 1995: 21). Es ist daher nicht ungewöhnlich, dass das fertige Wasserzeichen den Wünschen und Vorstellungen der Planer und Handwerker nicht immer entspricht und eine neue Urform gestaltet werden muss. Trotz dieser Schwierigkeiten hält man auf Grund der einfachen Handhabung für den Nutzer, dem hohen Wiedererkennungswert und des etablierten Schutzes an dieser Art der Herstellung fest. Wer könnte z.B. auf Anhieb sagen, woran man ein gefälschtes Hologramm – auch ein Sicherheitsmerkmal von Banknoten (s.u.) – erkennt?[32]

Hält man die fertige Banknote gegen das Licht, erscheint das Wasserzeichen auf beiden Seiten des unbedruckten Bereichs. Das echte Wasserzeichen besitzt die Eigenschaft der Helligkeitsumkehr. Gegen das Licht betrachtet erscheinen da-

31 http://papiermuseum.freyerweb.at/RZ_FOLDER_19%2004%2007.pdf, 01.03.2010.

32 Vgl. den Beitrag von Jens Schröter im Heft »Kulturen des Kopierschutzes I«.

her Bildelemente, die vor einem dunklen Hintergrund hell zu sehen waren, plötzlich dunkel und umgekehrt.

Für die Gestaltung der Euro-Banknote, also auch des dazugehörigen Wasserzeichenmotivs, gab der Rat des Europäischen Währungsinstituts (EWI) die Themen *Zeitalter und Stile* und *Abstraktes und Modernes Design* vor. Der europaweite Wettbewerb begann 1996. In den nationalen Zentralbanken gingen daraufhin 44 Vorschläge verschiedener Künstler ein. Pro Thema wählte die Jury fünf Entwürfe aus. Diese wurden in einer öffentlichen Meinungsumfrage in 14 Mitgliedsstaaten der EU auf ihre Akzeptanz getestet. Nach Abschluss dieser Umfrage entschied sich der EWI-Rat für den Entwurf des österreichischen Nationalbankmitarbeiters Robert Kalina (vgl. Berliner Zeitung 1996).

In einer langen Phase des Feuchtigkeitsentzugs, der Trocknung, der Oberflächenleimung und der Glättung wird die Papierbahn der zukünftigen Banknote aufgerollt und in druckfertige Bögen zerteilt.

2.2.2 HERSTELLUNG DER EURO-BANKNOTE: DIE DRUCKVERFAHREN UND WEITERE SICHERHEITSMERKMALE

In einem Siebdruckverfahren wird die Farbe mit einem Rakel (Kratzeisen oder Abstreichholz) über ein feines Sieb aus Polyester gestrichen, welches an den zu bedruckenden Stellen der Bögen, farbdurchlässig ist. Dieses Verfahren ermöglicht eine dicke Farbdeckung, die für den Einsatz von Effektpigmenten nötig ist. Mit diesem Druck wird der Euro-Banknote ihre Wertzahl gegeben, die je nach Betrachtungswinkel ihre Farbe ändert. Man spricht dabei von einer optisch variablen Farbe (vgl. Renesse 2005). Den nächsten Schritt in der Herstellung einer Euro-Note bildet der Simultandruck. Mit dieser Drucktechnik werden Vorder- und Rückseite des Scheines passgenau und gleichzeitig bedruckt. »Die Elemente der Druckplatten werden von Farbwalzen eingefärbt und die kompletten Druckbilder für Vorder- und Rückseite auf zwei Sammelzylinder übertragen. Diese bedrucken anschließend (simultan) beide Seiten des Druckbogens.«[33] In diesem Schritt werden zudem mehrfarbige Bildelemente auf beide Scheinseiten gedruckt. Das Durchsichtsregister ist ebenfalls auf der Vorder- und Rückseite angebracht. Hält man den fertigen Schein später gegen das Licht, erscheint im Durchlicht die Wertzahl.

Die Folienelemente (kleines Folienquadrat und Folienstreifen) sind auf der Vorderseite der Noten zu sehen. Sie erhalten Hologramme, welche durch Bewegung der Banknote entweder das Architekturmotiv oder die Wertzahl zur Erscheinung bringen. Diese sog. Heißprägefolien erhöhen in hohem Maße die Fäl-

33 Zitat von den Erklärungstafeln des Geld Museums der Deutschen Bundesbank in Frankfurt. Besuch am 27.09.2009.

schungssicherheit und werden nach Fertigstellung unter Einsatz von Hitze und Druck auf das Banknotenpapier aufgebracht.[34]

Ebenfalls unter hohem Druck wird im Anschluss das Papier in die mit Farbe gefüllte Druckplatte gepresst. Dieser Stichtiefdruck schafft ausschließlich an der Vorderseite der Note ein fühlbares und sichtbares Relief. Die Dreidimensionalität wird also unter anderem durch den Schriftzug weiter verstärkt. »Im letzten Druckgang wird jede Banknote mit einer eigenen Notennummer versehen.«[35] Weitere Sicherheitsmerkmale der Banknote sind außerdem der Perlglanzstreifen und das Infrarot-Merkmal. »Mit Hilfe eines Infrarotgeräts werden der rechte Teil des Stichtiefdrucks und der Folienstreifen sichtbar.«[36]

Zudem sichert die neue Pit Signal Processing-Technologie (PSP), zur Herstellung farblicher Signale, die Banknoten Diese PSP Technologie kann in die farbliche Gestaltung des Scheins eine Signalstruktur integrieren, die von Kopierern und Scannern u.U. erkannt werden kann.[37] Praktisch heißt das, dass der Kopierer ein einfaches geometrisches Muster bestehend aus fünf, ein Millimeter großen Kreisen in verschiedenen Farben (meistens gelb, aber auch grün und orange), sucht. Dieses Muster kann mit einem passenden Filter leicht aufgespürt und auf die entsprechenden Charakteristika überprüft werden. Findet der Scanner (oder ähnliches) solche Muster, verweigert er den Auftrag. Der Euro verfügt also über technisch hoch moderne, optische und taktile Sicherheitsmerkmale.

Dieses aufwändige Herstellungsverfahren mit den vielfältigen grafischen Elementen, verschiedenen Druckvorgängen und den Sicherheitsmerkmalen nach den Prinzipien »Fühlen, Sehen, Kippen« sorgen dafür, dass die Banknoten des Euros nur schwer zu fälschen sind. Zudem schaffen sie eine hohe Sicherheitsredundanz. Auf vielen verschiedenen Ebenen wird Sicherheit erzeugt. Selbst wenn man einige Merkmale vergisst oder nicht alle Sinne ausgeprägt sind, bleiben weitere Merkmale zur Überprüfung der Echtheit des Scheins. Genau das bedeutet Sicherheit. Einen 100-prozentigen Kopierschutz wird es aber wohl nie geben.

3 DIGITALE WASSERZEICHEN

3.1 EINLEITUNG

Wie bereits gezeigt, kennzeichneten Papierhersteller bereits im 13. Jahrhundert ihre Handelsobjekte mit Wasserzeichen, um Herkunft und Qualität zu dokumentieren. Ähnliches wird durch das Anbringen von digitalen Wasserzeichen versucht:

34 Vgl. den Beitrag von Jens Schröter im Heft »Kulturen des Kopierschutzes I«.

35 Zitat von den Erklärungstafeln des Geld Museums der Deutschen Bundesbank in Frankfurt. Besuch am 01.03.2010.

36 http://www.bundesbank.de/bargeld/bargeld_banknoten_sicherheits-merkmale.php#infrarot, 01.03.2010.

37 Vgl. http://www.kurzefrage.de/computer-internet/111850/Geldscheine-scannen, 01.03.2010.

Der zunehmende Einsatz digitaler Wasserzeichen in Text-, Bild- oder Tondaten erklärt sich aus der Sorge um das Geistige Eigentum, denn der weltweite Zugriff auf digitale Daten über das Internet birgt eine hohe Gefahr der illegalen Vervielfältigung (vgl. Cox 2001: 9). Digitale Wasserzeichen werden direkt in das Datenmaterial eingefügt, allerdings im Gegensatz zu papierbasierten Wasserzeichen in meist nicht wahrnehmbarer Weise (vgl. Schmitz 2006: 93), und dienen dem Nachweis der Authentizität und Integrität der Ursprungsdaten (vgl. Dittmann 2000: 26).

Was sich zunächst einfach anhört, erweist sich jedoch als kompliziert. Um den Einstieg in die Materie zu vereinfachen, sollen die Grundlagen digitaler Wasserzeichen dargestellt werden, um daran anknüpfend auf verschiedene Anwendungsmöglichkeiten des Digital Watermarking eingehen zu können (vgl. Achziger 2003). Danach soll ein Überblick verschiedener Wasserzeichenverfahren gegeben werden (Schutz von Bild-, Audio-, Video- und 3D-Modellen), um nicht zuletzt deren Vor- als auch Nachteile aufzuzeigen.

Auch wenn sich digitale Wasserzeichen seit Anfang der 1990er Jahre im Einsatz befinden (vgl. Koch 2002: 200), so ist die Forschungsarbeit auf diesem Gebiet noch längst nicht abgeschlossen, da alle bisherigen Wasserzeichenverfahren leicht zu umgehen sind. Abschließend soll deshalb der aktuelle Forschungsstand aufgezeigt sowie ein Blick in die Zukunft unternommen werden.

3.2 GRUNDLAGEN DIGITALER WASSERZEICHEN

3.2.1 VORREITER DIGITALER WASSERZEICHEN: KRYPTOLOGIE UND STEGANOGRAPHIE

»Ibich habibebi dibich,
Lobittebi, sobi liebib.
Habist aubich dubi mibich
Liebibä Neibin, verbirgibib.

Nabih obidebir febirn
Gobitt seibi dibir gubit.
Meibin Hebirz habit gebirn
Abin dibir gebirubiht.«
Jochachim Ringelnatz

Die klassische Literatur lehrt uns, dass wo immer eine verliebte Julia ihrem geliebten Romeo eine geheime Nachricht zukommen lassen möchte, ein finsterer Bösewicht im Hintergrund lauert und nur darauf wartet das Brieflein abzufangen, um die Nachricht zu verfälschen und das junge Glück zu zerstören (vgl. Beutelspacher 2007: 1).

Manchmal sind die Verliebten die Leidtragenden, oftmals sind es Internetnutzer, Aktionäre, Diplomaten – kurz alle, deren Alltag aus dem Verschicken ver-

traulicher Nachrichten besteht (vgl. ebd.: 2). Doch was sind die Gegenmaßnahmen, um Angreifer an ihren illegalen Taten zu hindern? Hätte man Julia die Gelegenheit gegeben über eine Lösung für dieses Problem nachzudenken, sie wäre möglicherweise auf die Idee gekommen, sämtliche Buchstaben ihrer Nachricht durch andere Buchstaben, Symbole oder Zahlen auszutauschen. Natürlich ist es kein Können, eine Nachricht so zu verunstalten, dass kein Mensch mehr etwas mit ihr anfangen kann. Laut Beutelspacher besteht die eigentliche Hauptschwierigkeit für die Kryptologie darin, die Mitteilung so zu transformieren, dass niemand außer dem berechtigten Empfänger diese decodieren kann (vgl. ebd.: 2). Dieser Code, welcher nur dem betreffenden Empfänger vorliegt, wird in der Kryptologie als Schlüssel bezeichnet. Die klassischen Verschlüsselungsverfahren sind so angelegt, dass Sender und Empfänger einen gemeinsamen geheimen Code vereinbaren, mit dem der Sender Nachrichten verschlüsseln kann, während der Empfänger in der Lage ist, sie wieder zu entschlüsseln (vgl. Neymanns 2001: 52-58).[38]

Kurz zur Terminologie: Der Terminus der Kryptologie umfasst die Wissenschaft von der Geheimhaltung von Nachrichten. Zu den einzelnen Methoden der Kryptologie zählt u.a. das eng verwandte Verfahren der Steganographie. Bei der Steganographie geht es weniger darum eine Nachricht zu transformieren, sondern vielmehr darum, die Tatsache zu verbergen, dass gerade in diesem Moment eine Nachricht verschickt wird (vgl. Meyn 2003: 21; Werber 2004). Solche Verfahren wurden schon vor rund zweitausend Jahren von römischen Feldherren angewandt, um während der Kriegszeit wichtige Mitteilungen versteckt zu übertragen. So berichtet der griechische Geschichtsschreiber Herodot (490-425 v.Chr.), dass römische Adelige geheime Botschaften auf die kahl geschorenen Köpfe ihrer Sklaven tätowieren ließen. Eine zeitaufwändige Prozedur, denn erst, nachdem die Haare der Sklaven nachgewachsen waren, wurden sie zum Empfänger geschickt. Erreichte der Bote sein Ziel, rasierte man ihm seine Haare erneut ab und die Nachricht kam zum Vorschein (vgl. Klein 2007: 85).

Heutzutage verstecken moderne steganographische Verfahren geheime Nachrichten nicht mehr auf Köpfen, sondern beispielsweise in digitalen Bildern (vgl. ebd.: 86; vgl. Petitcolas et al. 1999). So können in einer Computergrafik einzelne Informationen verborgen eingeschleust werden, ohne dass diese für den Betrachter wahrnehmbar sind – zumindest nicht auf den ersten Blick und nur mit enormer Aufmerksamkeit (vgl. Meyn 2003: 21). Eine weitere Methode der Steganographie lässt sich auch in der digitalen Telekommunikation finden. Beim Telefonieren im ISDN können geheime Daten unhörbar über digitalisiertes Rauschen übertragen werden, ohne dass ein ungebetener Mithörer auf die Idee kommen würde, hier ginge es um etwas anderes als z.B. das tatsächliche Besprechen einer

38 Vgl. als sehr gut lesbare Einführung in die Geschichte der Verschlüsselung überhaupt Singh (2000), insb.: Kapitel 6-8 zur Verschlüsselung digitaler Daten unter Berücksichtigung neuerer Verfahren wie asymmetrischer Verschlüsselung und Quantenkryptographie.

Reise (s.u., vgl. ebd.: 21f.). Der Ursprung digitaler Wasserzeichen ist demnach in der Steganographie zu lokalisieren, da digitale Wasserzeichen nach Möglichkeit *verborgen* in die zu schützenden Daten eingebettet werden. Folgendes Beispiel aus der Steganographie soll diesen Sachverhalt verdeutlichen.

3.2.1.1 VERSTECKTER NOTRUF

Dass es sich bei nachstehendem Urlaubsgruß um eine geheime Botschaft respektive Hilferuf handelt, ist für einen Außenstehenden auf den ersten Blick nicht ersichtlich: »*Liebe Kollegen! Wir genießen nun endlich unsere Ferien auf dieser Insel vor Spanien. Wetter gut, Unterkunft auch, ebenso das Essen. Toll! Gruß, X.Y.*« (Dittmann 2001).

Um die geheime Nachricht entschlüsseln zu können, müssen je acht Wörter aus dem Text in Blöcke unterteilt werden. In diesem Fall entstehen bei der Unterteilung drei Blöcke. Für jeden erhaltenen Block werden nun die Buchstaben der einzelnen Wörter gezählt. Notiert man im Anschluss für sämtliche Wörter, die eine gerade Anzahl von Buchstaben haben eine »1« und bei ungerader Buchstabenanzahl eine »0«, so erhält man folgende Biteinheiten:

Block 1. Wörter: 1-8: 0101 0011
Block 2. Wörter: 9-16: 0100 1111
Block 3. Wörter: 17-24: 0101 0011

Nun wird jeder Biteinheit die entsprechende Dezimalzahl zugeordnet, um letztendlich für diese Zahl den entsprechenden Buchstaben aus dem ASCII-Alphabet[39] ermitteln zu können. Bei Anwendung dieses Verfahrens erhält man sowohl für den ersten als auch für den dritten Block den Buchstaben »S«, während sich für den zweiten Block ein »O« ergibt. Reiht man die Buchstaben aneinander, entsteht der, für einen unwissenden Betrachter überhaupt nicht wahrnehmbare, Notruf »S O S« aus diesem harmlos erscheinenden Urlaubsgruß. Diese »Nicht-Wahrnehmbarkeit« zeichnet die digitalen Wasserzeichen aus, obwohl sie in ihrer Ausprägung in manchen Fällen auch als wahrnehmbare bzw. sichtbare Wasserzeichen auftreten. So kennt man aus dem Fernsehen Wasserzeichen in Form von Senderlogos (vgl. Hlawatsch 2002).

---

39 »Üblicherweise codieren Computer Buchstaben im ASCII-Alphabet. Da das ASCII-Alphabet die Kodierung in einem Byte durchführt, kann es nicht sämtliche landestypischen Zeichen aufnehmen, daher wurden zu Beginn sog. (landestypische) Codepages eingeführt. Auch diese genügen jedoch nicht, um sämtliche chinesischen Schriftzeichen zu kodieren. Hierzu wurde Unicode geschaffen. Dabei handelt es sich um ein neues Alphabet, welches die Kodierung der Zeichen in einem Wort (2 Bytes) vornimmt. Damit können 65.536 Wörter verschiedene Zeichen in Unicode kodiert werden. So gibt es zum Beispiel für das Zeichen / (der Schrägstrich) den ASCII-Code 0×2f und den Unicode 0×c11c.« (Spenneberg, 2005: 303)

3.2.2 ANWENDUNGSGEBIETE UNSICHTBARER DIGITALER WASSERZEICHEN

Unsichtbare Wasserzeichen werden für das menschliche Hör- und Sehvermögen möglichst unauffällig eingebracht, so dass die Originaldatei nicht mehr vom markierten Datenmaterial zu unterscheiden ist. Sie lassen sich weiter in die Kategorien robust und fragil differenzieren, während sichtbare Wasserzeichen nicht weiter zu untergliedern sind (vgl. Abb. 11).

Die letzte Zeile des Diagramms verweist auf die unterschiedlichen Anwendungsgebiete der klassifizierten Verfahren. Robuste Wasserzeichen kommen beispielsweise bei der Urheberidentifizierung zum Einsatz, wobei die zur Verbreitung hergestellten Kopien eines Datensatzes mit einem Urheber- oder Copyrightvermerk versehen werden (vgl. Dittmann 2000: 30). Das Anwendungsgebiet der Kundenidentifizierung kennzeichnet sich durch die Einbettung eindeutiger Kundeninformationen, wie zum Beispiel Fingerabdrücke. Diese werden in das Datenmaterial inkludiert und tragen so zu einem hohen Sicherheitsstandard bei.

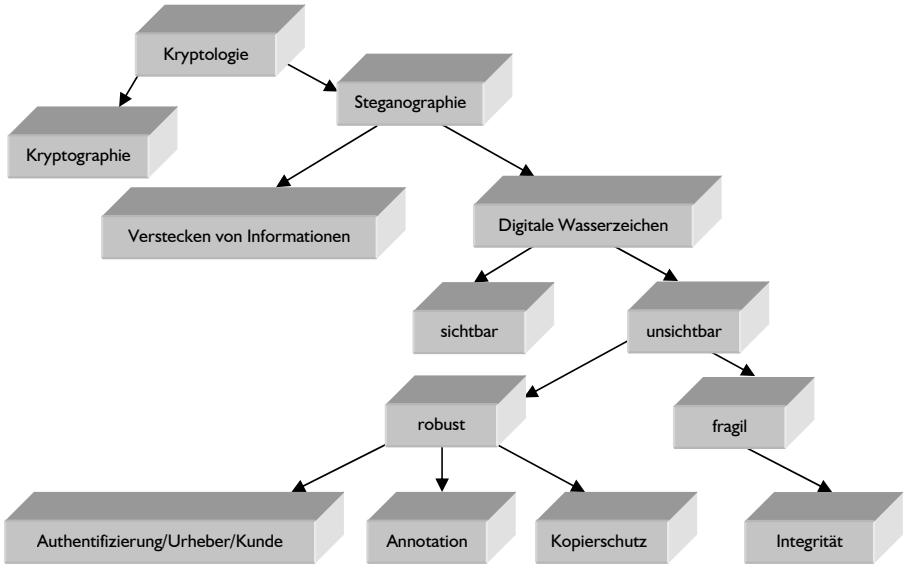

Abb. 11: Klassifikation digitaler Wasserzeichen (nach Dittmann 2001; vgl. Dittmann/Wohlbacher 2000: 119).

Eine ähnliche Vorgehensweise findet sich auch in der Annotation des Datenmaterials. Hier arbeitet man jedoch nicht mit Fingerabdrücken, sondern integriert zusätzliche Metainformationen wie Lizenzhinweise oder Szenenbeschreibungen in das zu schützende Dokument (vgl. ebd.: 30). Weiterhin kann das Einbringen von Markierungen zur Durchsetzung des Kopierschutzes oder der Übertragungskontrolle eingesetzt werden.

Fragile Wasserzeichen haben nur einen Einsatzbereich: Integrität. Um die Unversehrtheit des Datenmaterials nachzuweisen, wird ein unsichtbares, zerbrechliches Wasserzeichen in das Dokument eingesetzt. So lassen sich eventuelle Manipulationen am Datenmaterial feststellen (vgl. Steinebach/Dittmann 2002: 263). Was jedoch das Erkennen des Zeitpunkts der Manipulation sowie des manipulierten Bildteils anbelangt, steckt die Forschung noch in den Kinderschuhen (vgl. Dittmann 2000: 133). Die Anforderungen an fragile Wasserzeichen erweisen sich jedoch als problematisch: Auf der einen Seite müssen sie durch unerwünschte Veränderungen beeinträchtigt werden, auf der anderen Seite müssen sie stabil genug sein, um unproblematische Manipulationen wie z.B. Skalierungen und Kompressionen zu überstehen, damit sie überhaupt eingesetzt werden können.

3.2.3 ANFORDERUNGEN

Die genannten Einsatzgebiete setzen bestimmte Eigenschaften digitaler Wasserzeichen voraus, damit sie ökonomisch verwendet werden können (vgl. zum Folgenden Dittmann/Wohlbacher 2000: 118; Achziger 2003).

Abb. 12: Das rechte Bild erscheint hier in seiner Qualität durch Wasserzeichen stark verrauscht (vgl. Hlawatsch 2002).

Die Einbettung *robuster Wasserzeichen* erfolgt, um sowohl versehentlichen als auch beabsichtigten Transformierungen am Datenmaterial vorzubeugen, beispielsweise geometrische Modifikationen, Verschiebungen oder Skalierungen. Doch die Anforderung ein Dokument gegen jegliche Transformationen widerstandsfähig erscheinen zu lassen, wirft besonders für den Schutz von Bilddaten ein Problem auf. Denn je robuster ein Bild vor Manipulationen geschützt wird, desto größer ist das Risiko eines Qualitätsverlustes des Bildes (vgl. Hlawatsch 2002). Es gilt also abzuwägen, ob eine möglichst hohe Robustheit erzielt werden soll, was zwangsläufig eine Verminderung der Qualität voraussetzt, oder ob auf Resistenz des Wasserzeichens verzichtet werden kann, um ein visuell besseres Ergebnis zu erreichen.

1) Um einen Qualitätsverlust von vornherein zu umgehen, ist die Einbettung fragiler Wasserzeichen in das Datenmaterial sinnvoll. Doch diese Wasserzeichenart ist eben nicht widerstandsfähig und lässt sich im Fall, dass der Angrei-

fer über das entsprechende Wissen verfügt, leicht entfernen. (vgl. Hlawatsch 2002).

2) Von einer *Nicht-Detektierbarkeit* ist die Rede, wenn sich keine statisch signifikanten Unterschiede zwischen dem zu schützenden Datenmaterial und dem Originaldokument erkennen lassen. Ein vermeintlicher Angreifer kann daher nicht ermitteln, ob ein Wasserzeichen im Dokument präsent ist oder nicht.
3) Die Bezeichnung *nicht-wahrnehmbares Wasserzeichen* wird benutzt, wenn eine Unterscheidung zwischen gekennzeichnetem Datenmaterial und Originaldokument weder mithilfe des Seh- noch des Hörsinns erfolgen kann.
4) *Security* ist die Resistenz eines Wasserzeichens gegenüber gezielten Attacken. Bei hoher Security ist das Fälschen oder Zerstören eines Wasserzeichens kaum möglich, es sei denn, der Angreifer beherrscht nicht nur das Wasserzeichenverfahren, sondern kennt ebenso den dazugehörigen, geheimen Schlüssel.
5) Die *Komplexität*: Dieser Parameter benennt die Mühen, die notwendig sind, um das Wasserzeichen einzubringen bzw. wieder auszulesen. Er legt auch fest, ob zum Identifizieren des Wasserzeichens das Originalbild verwendet werden muss oder nicht.
6) Die *Kapazität* benennt die maximale Menge an Wasserzeicheninformationen, welche in die Originaldatenstruktur inkludiert werden können.
7) *Geheime vs. öffentliche Verifikation*.[40] Hierbei geht es um die Frage, ob es nur einer spezifischen Personengruppe möglich ist, das Wasserzeichen auf seine Richtigkeit zu beglaubigen. Bei einer geheimen Verifikation soll nur der Urheber selbst oder eine dedizierte Expertengruppe dazu in der Lage sein. Im Gegensatz zur geheimen Verifikation bezieht sich die *öffentliche Verifikation* auf die öffentliche Prüfbarkeit des Wasserzeichens.

3.2.4 EINBETTUNG DIGITALER WASSERZEICHEN

Wie findet jedoch nun das Wasserzeichen seinen Weg in das Datenmaterial? Zunächst sei festgehalten, dass ein Wasserzeichenalgorithmus sowohl aus einem Einbettungs-, als auch aus einem Abfrage- bzw. Ausleseprozess besteht.

Die Entwicklung verschiedener Algorithmen basiert auf dem Gedanken, Wasserzeichen so zu verschlüsseln, dass diese durch Fremdeinwirkung nur in zerstörter Weise aufgespürt werden können. Die Geheimhaltung der Einbettungsalgorithmen ist deshalb von oberster Priorität, denn nur mittels des geheimen Schlüssels kann die Sicherheit der Daten gewährleistet werden. Der Einbettungsprozess vollzieht sich, indem die Wasserzeicheninformation, bestehend aus Ur-

40 »Geheim, nur vom Markierer oder einer bestimmten Gruppe von Personen (Private Watermarking, manchmal auch als symmetrisches Wasserzeichen bezeichnet), öffentlich (Public Watermarking, manchmal auch als asymmetrisches Wasserzeichen bezeichnet)« (Dittmann 2000: 31; vgl. hierzu auch Neymanns 2001).

heberinformationen oder Metadaten, in das zu schützende Datenmaterial integriert wird, wobei die Wasserzeicheninformationen mit einem Muster, zum Beispiel einem Pseudorauschmuster, markiert werden (vgl. Schmitz 2006: 97-105 zu den kommunikationstheoretischen Grundlagen). Diese Platzierungen des Wasserzeichenmusters auf den digitalen Datenträger werden meist pseudozufällig[41] mittels des geheimen Schlüssels festgelegt (vgl. Dittmann 2000: 19f.).

Betrachtet man die allgemeine Vorgehensweise bei Wasserzeichenverfahren, lässt sich feststellen, dass diese auf den grundlegenden Techniken der Steganographie beruhen. Nach Dittmann (2000: 22) können mit der Methode der substitutionalen Steganographie digitale Datenmaterialien so verändert werden, dass lediglich der verrauschte oder der für den Menschen nicht wahrnehmbare Bestandteil der Daten durch Wasserzeichenmuster ersetzt werden muss. Anders dagegen die konstruktive Steganographie: Hier liegt keine Substitution der vorhandenen Rauschkomponenten vor, vielmehr beruht das Verfahren auf der Nachbildung von Signalen, basierend auf dem Modell des Originalgeräusches (vgl. Kannemann 2003: 6). Des Weiteren unterscheidet sich die konstruktive von der substitutionalen Steganographie insofern, als das Originaldaten nur leicht verändert und nicht komplett ersetzt werden können.

Rückblickend kann die Entwicklung digitaler Wasserzeichen große Fortschritte in den letzten Jahren verzeichnen. Die anfänglich entwickelten Verfahren für Bildmaterial lassen sich heutzutage problemlos auf Audio, Video und 3D-Modelle übertragen (s.u.). Handelt es sich jedoch beim Markieren von digitalen Wasserzeichen um Textdokumente oder Quellcode wird es problematisch: Geringfügige Änderungen in der Datei machen sich stets sofort bemerkbar, sodass der konventionelle Wasserzeichenalgorithmus, der beispielsweise für den Bildbereich klassischerweise eingesetzt wird, keine Anwendung findet. Um für Textdateien einen gewissen Schutz gewährleisten zu können, bietet sich die Möglichkeit digitale Wasserzeichen im Text in Form von Phrasen oder als Leerzeichen zu verbergen (vgl. Steinebach/Dittmann 2002: 261).

3.2.5 ATTACKEN AUF DIGITALE WASSERZEICHEN

Obwohl die technische Entwicklung digitaler Wasserzeichen in den letzten Jahren stetig vorangetrieben wurde, sind gewisse Defizite in diesem Bereich weiterhin erkennbar. Grundsätzlich gilt, dass ein umfassender Schutz von digitalen Daten aufgrund vielzähliger Transformationen, ausgehend von Angreifern, die versuchen das Wasserzeichen zu zerstören oder das Auslesen unmöglich machen wollen, ein

41 In der Berechenbarkeitstheorie wird der Begriff »Pseudozufall« verwendet, wenn etwas zufällig erscheint, in Wirklichkeit jedoch berechenbar ist. So erscheint der Wurf einer Münze und das damit einhergehende Ergebnis zufällig. Aber: Solange sich die Münze in der Luft befindet, könnte das Ergebnis theoretisch aufgrund der Geschwindigkeit vorhergesagt werden. Ohne Messgeräte erscheint das Ergebnis allerdings zufällig (vgl. http://de.wikipedia.org/wiki/Pseudozufall, 01.03.2010).

unrealisierbares Unterfangen ist. Mediadaten zu schützen bedeutet gleichzeitig auch immer einen Qualitätsverlust hinnehmen zu müssen. Laut Schmitz ist es deshalb bei der Auswahl des Verfahrens wichtig, Vor- und Nachteile jeweiliger Prozesse abzuwägen. Folgende Punkte gilt es dabei zu berücksichtigen:

I. Der Wert der zu schützenden Originaldatei.
II. Die Sicherheitsanforderungen sowie das Anwendungsgebiet des Wasserzeichens.
III. Der Aufwand, der betrieben werden muss, um das Wasserzeichen zu knacken (vgl. Schmitz 2006: 106).

Um digitale Wasserzeichen zu brechen, unterscheidet man zwischen verschiedenen Attacken, einige von ihnen sollen an dieser Stelle vorgestellt werden (vgl. ebd.: 106f.).

3.2.5.1 UNZULÄSSIGES EINBETTEN

Diese Attacke liegt vor, wenn es dem Angreifer gelingt, ein eigenes Wasserzeichen in die originale Mediendatei einzubetten. Die Zuordnung der rechtmäßigen Urheberschaft verläuft in diesem Fall nicht ganz unproblematisch, da der Angreifer bei dieser Form der Attacke in der Lage ist zu behaupten, er selbst habe Anspruch auf das Copyright des Originals. Um unbefugtes Einbetten von Wasserzeichen potenziellen Angreifern zu erschweren, ist das Implementieren eines *Watermark Keys* notwendig (vgl. ebd.: 97). Nur wenn der Angreifer Zugriff auf diesen Schlüssel hat, befindet er sich in der Position eigene Wasserzeichen zu integrieren.

3.2.5.2 ILLEGETIMES DETEKTIEREN VON WASSERZEICHEN

Hier ist zu differenzieren, ob das Wasserzeichen selbst wichtige Informationen transportiert oder ob es darum geht, überhaupt geheim zu halten, dass ein Wasserzeichen eingebettet ist. Allein der Test, ob ein Wasserzeichen in einer Mediadatei enthalten ist, kann dem potenziellen Angreifer wichtige Informationen liefern. Dabei ist das Aufspüren von Wasserzeichen mit kryptographischen Methoden nicht zu verhindern (vgl. ebd.: 107).[42]

3.2.5.3 UNRECHTMÄßIGES ENTFERNEN DER WASSERZEICHEN

Es sollte so sein, dass der Versuch ein Wasserzeichen unrechtmäßig zu entfernen die Zerstörung bzw. das Unbrauchbarmachen der Daten zur Folge hat. Demgegenüber versucht der Angreifer Datenmaterial zu produzieren, welches kein

42 Vgl. hierzu den Beitrag von Daniel Köhne in diesem Heft.

Wasserzeichen mehr enthält und dem Original hinreichend ähnlich sieht (vgl. ebd.: 107f.).

3.2.5.4 STIRMARK

Stirmark ist ein häufig eingesetztes Werkzeug, um die Robustheit eines Wasserzeichens in digitalen Bildern zu überprüfen. Es handelt sich um eine Open-Source Software (vgl. Petitcolas 2009). Das Tool ist darauf ausgerichtet zu untersuchen, inwiefern das Wasserzeichen Manipulationen am Bild standhält. Bei dieser Methode gilt es das zu überprüfende Bild mit beispielsweise geometrischen Transformationen (Verzerren, Rotieren, Skalieren) zu attackieren, welche jedoch für das menschliche Auge nicht wahrnehmbar sind, aber dafür sorgen können, dass das eingebettete Wasserzeichen nicht mehr detektierbar ist (vgl. Lang et al. 2003: 399).

Wie Abbildung 13 zeigt, sind geringfügige Manipulationen im Bild für das menschliche Auge nicht wahrnehmbar. Aus dem darunter liegenden Gitternetz wird jedoch ersichtlich, dass im Bild deutliche Transformierungen vorgenommen wurden.

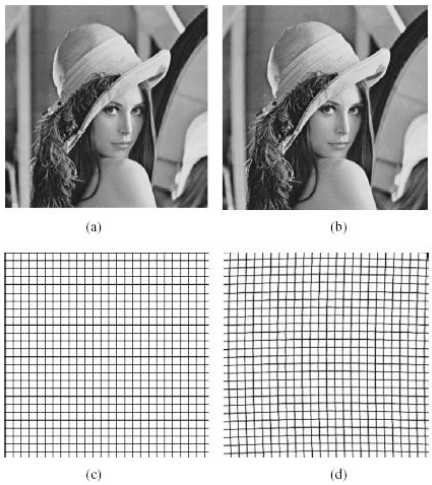

Abb. 13: Das linke Bild weist keine Veränderungen auf, während das rechte Bild durch Stirmark manipuliert wurde (vgl. Petitcolas et al. 1999: 1070).

3.3 WASSERZEICHENARTEN UND IHRE VERFAHREN

3.3.1 ROBUSTE WASSERZEICHEN

Von einem robusten Wasserzeichenverfahren ist die Rede, wenn eingebrachte Informationen trotz einer Modifikation am Datenmaterial ausgelesen werden kön-

nen (vgl. Mittenzwei 2006: 88). Insbesondere bei Bild-, Audio-, Video- und 3D-Modellen kommen nicht-wahrnehmbare robuste Wasserzeichen zum Einsatz und tragen in hohem Maße zur Urheberidentifizierung bei. Im Folgenden soll nun ein Abriss verschiedener Medientypen erfolgen, die sich für das unsichtbare, robuste Wasserzeichenverfahren eignen.

3.3.1.1 VERFAHREN FÜR EINZELBILDER

Wasserzeichenalgorithmen für Bilder lassen sich in zwei Verfahren einteilen, bestehend aus Bild- und Frequenzraumverfahren. Letztere Methode beschreibt jedes Bild durch die jeweilige Frequenzkomponente als Signal. Dies bedeutet, dass das Wasserzeichen im Rauschen des Originaldokuments eingespeist wird (vgl. Hlawatsch 2002). Dabei stehen die schnellen bzw. hohen Frequenzen für Bildteile, die in ihrer Struktur hohe Änderungen im Kontrast oder in der Helligkeit aufweisen (vgl. Dittmann 2000: 44f.), wohingegen gleichmäßige Bildflächen sich eher den tieferen oder langsameren Frequenzanteilen zuordnen lassen. Modifikationen des Bildes im nieder-, mittel- oder hochfrequenten Bereich sind dementsprechend auch als ein nieder- mittel- oder hochfrequentes Wasserzeichen einzustufen.

Abb. 14: Links: Das Bild im Original. Rechts: Die meisten Wasserzeicheninformationen wurden sukzessive in die blaue Feder eingearbeitet.

Niederfrequente Wasserzeichen, die eine sehr hohe Robustheit im Frequenzraumverfahren aufweisen, sind besonders wirksam gegenüber kleineren geometrischen Modifikationen. Demgegenüber können Wasserzeichen, welche im mittel- und hochfrequenten Bereich angesiedelt sind, deutlich mehr Informationen einfacher aufnehmen. Zudem werden sie vom menschlichen Auge nur geringfügig wahrgenommen.

Anders beim Bildraumverfahren, hier setzen Informationen direkt im Bild an, weshalb das Wasserzeichen im Vergleich zum Frequenzraumverfahren leichter

wahrnehmbar ist. Attacken auf Bildraumverfahren liegen meist in Form von Kompressionen oder Nachbearbeitungen des Bildes vor, wobei das eingebettete Wasserzeichen je nach Intensität des Angriffs zerstört werden kann (vgl. Menn 2000). An dieser Stelle soll kurz ein Bildraumverfahren erläutert werden, welches auf dem Blaukanal des Bildes arbeitet. Alle Farbwerte lassen sich durch Kombinationen der drei Grundfarben Rot, Grün und Blau[43] darstellen. Grund für das Verfahren im Blaukanal ist die Tatsache, dass das menschliche Auge gegenüber der Farbe Blau am unempfindlichsten reagiert. Das Wasserzeichenmuster wird deshalb vorwiegend durch die Veränderungen der Blauanteile eines Bildes vorgenommen.

Im Vergleich schneidet das Bildraumverfahren im Gegensatz zum Frequenzraumverfahren hinsichtlich der Nicht-Wahrnehmbarkeit deutlich schlechter ab, sollte aber im Hinblick auf die starke Robustheit gegenüber linearen und nichtlinearen Transformationen nicht außer Acht gelassen werden (vgl. Dittmann 2000: 49f).

3.3.1.2 VERFAHREN FÜR BEWEGTBILDER

Da ein Video technisch gesehen als eine schnelle Aneinanderreihung von Einzelbildern mit einer dazu parallel verlaufenden Tonspur betrachtet werden kann, ist es naheliegend, dass der Algorithmus für Bewegtbilder auf derselben Kombination beruht wie für Einzelbilder. Bei Videoverfahren gilt es die hinzukommende zeitliche Komponente zu berücksichtigen, da Bild und Ton in einer bestimmten zeitlichen Abfolge wiedergegeben werden. Durch die Zeitkomponente ist es möglich ein Wasserzeichenmuster auf eine ausgewählte, zu schützende Sequenz von Bildern anzubringen, wobei es ebenso opportun ist, ausschließlich Einzelbilder des Videos zu sichern (vgl. Dittmann 2000: 75).

Wird eine Wasserzeichenmarkierung über mehrere Bildersequenzen verstreut, so empfiehlt sich eine spezielle Angriffsstrategie, bei der die Reihenfolge der Einzelbilder verändert oder komplett gelöscht wird. Um der Attacke entgegen zu wirken, bietet sich als Gegenmaßnahme an, Komponenten zur Synchronisation und Fehlererkennung in das zu schützende Dokument einzubetten (vgl. ebd.: 75).

Grundsätzlich besitzen Videodaten eine höhere Kapazität als Einzelbilder, da die Wasserzeicheninformation über das gesamte Video verteilt werden kann. Faktisch lassen sich Wasserzeichenmuster über mehrere Sequenzen verstreuen, weshalb zusätzliche Informationen zur Synchronisation inkludiert werden müssen. Trotz des Mehraufwands steht immer noch mehr Kapazität für das Einbringen von Wasserzeichen zur Verfügung, als wenn jeder Bildbereich einzeln gekenn-

43 Additive Farbmischung: »[…] entsprechend den drei Zapfentypen der menschlichen Netzhaut beruht sie auf den drei Grundfarben Rot, Grün und Blau. […] Kommen alle drei Farben in voller Intensität und gleichen Anteilen zusammen, ergänzen sie sich zu Weiß. Das ist das Prinzip, nach dem das Farbfernsehen und die Farbdarstellung am Computer-Bildschirm funktionieren« (Crüger 2002-2004).

zeichnet werden müsste. Der mit der Einbettung und der Abfrage entstehende Aufwand bei Einzelbildern, wird bei Bewegtbildern zu einem Problem, nicht zuletzt dadurch, dass ein Video aus mehreren tausend Sequenzen bestehen kann.

Bereits existierende Verfahren für Videodateien bringen die Wasserzeicheninformationen nicht in einzelne Bilder ein, sondern integrieren diese direkt in die Strukturinformationen der Bewegtbilder, wie beispielsweise in den Bewegungsvektoren bei MPEG-Videos. Visuell betrachtet ist die Qualität jener Verfahren einwandfrei, trotzdem gibt es auch hier ein bisweilen unlösbares Problem. Denn mit der Dekodierung oder einer erneuten Kodierung lässt sich das Wasserzeichen leicht zerstören (vgl. Kannemann 2003: 12).

3.3.1.3 VERFAHREN FÜR AUDIODATEN

Nicht nur Videodokumente enthalten Wasserzeichen, welche über die gesamte Zeit verteilt werden, auch Audiodateien erstrecken sich in der Zeit. Demnach ist es möglich, die Wasserzeicheninformation über das gesamte Musikstück zu verteilen oder auch sie ausschließlich auf einen einzelnen Ton anzusetzen. Da jedoch vielmehr das Gesamtstück von zu schützendem Interesse ist als der einzelne Ton, entscheidet man sich meist für die erste Methode.

Grundsätzlich kann bei Audiodaten eine weitaus geringere Menge an Wasserzeicheninformation aufgenommen werden, als das bei Bewegtbildern der Fall ist. Die Kapazität der einzubettenden Wasserzeichen hängt vor allem von der Toncharakteristik der Audiodaten ab (vgl. Seidenfaden 2006: 43). Probleme entstehen dann, Wasserzeicheninformationen in ein leises Musikstück zu integrieren, weil dadurch Informationen akustisch wahrnehmbar werden. Grund dafür: Wasserzeichendaten für Tonträger werden im Rauschen der Ursprungsdatei untergebracht (vgl. Heise Online 2002) und sind somit in leisen Musikstücken schwer zu verstecken. Bei Audiodaten gilt es demnach stets abzuwägen zwischen einer hohen Kapazität und der Wahrnehmbarkeit vorgenommener Manipulationen. Ein Rauschen im nicht-wahrnehmbaren Frequenzbereich stellt ebenfalls keine Alternative dar, da Wasserzeichen im unhörbaren Bereich anfällig gegenüber Kompressionen[44] sind. Um dem bestehenden Problem, der Zerstörung von Wasserzeichen durch Kompression entgegen zu wirken, wurden im Laufe der Zeit verschiedene Forschungsansätze veröffentlicht, von denen das Verfahren von Steinmetz (2000: 685) an dieser Stelle vorgestellt werden soll. Folgende Methodik beruht auf der Überprüfung erhaltener Wasserzeichendaten nach Durchführung einer Kompression:

I. Generiere ein Wasserzeichen (W).

II. Bette das Wasserzeichen (W) in das Originalsignal (S) ein.

44 Gerade die weitverbreitete MP3-Kompression filtert Geräusche heraus, die unhörbar sind. Dadurch wird eine Reduktion der Datenmenge erreicht, welche die wahrgenommene Audioqualität nicht oder nur geringfügig herabsetzt.

III. Führe eine Kodierung und Dekodierung von (S+W) mit einer möglichst hohen Kompressionsrate durch (S+W CoDec S` + W`).

IV. Unterziehe das Originalsignal (S) einer Kodierung und Dekodierung mit der gleichen Kompressionsrate (S CoDec S`).

V. Ermittle die Differenz der beiden erzeugten Signale: (S`+W`- S`= **W**`). Dabei ist **W**` genau der Teil des Wasserzeichens, welcher die Kompression überstanden hat.

VI. Mische **W**` dem Originalsignal bei (S+W).

Dieses Verfahren besitzt nicht nur den Vorteil, Wasserzeichen mit einer hohen Robustheit gegenüber Angriffen durch Kompression auszustatten, sondern ermöglicht zudem den Ausleseprozess der Wasserzeicheninformation trotz Kompression. Eine absolute Sicherheit vor unerwünschten Modifikationen am Datenmaterial kann allerdings auch dieses Verfahren nicht gewährleisten, da das Wasserzeichen durch Entfernen oder Umordnen einzelner Tonsequenzen zerstört werden kann.

3.3.1.4 VERFAHREN FÜR 3D-MODELLE

3D-Modelle weisen eine geometrische Beschaffenheit auf (Linie, Körper), die sich anhand von unterschiedlichen Attributen wie Farbe, Oberfläche usw. beschreiben lassen. Um ein Wasserzeichen in ein 3D-Modell besonders robust einzubetten, eignen sich die Geometrien, also die Grundelemente eines 3D-Modells, außerordentlich gut. Dabei werden digitale Wasserzeichen in dreieckige Maschennetze (die »Primitive«) eines Gittermodells eingefügt (Ohbuchi-Modell; vgl. Dittmann 2000: 103).

Einige bekannte Wasserzeichenalgorithmen, wie der von Ohbuchi, beruhen auf dem Prinzip der blinden Verfahren, d.h. sie benötigen beim Abfrageprozess kein Original. Doch auch die Wasserzeichenverfahren für 3D-Modelle weisen gewisse Schwachpunkte auf. So sind Angriffe auf 3D-Modelle mit geringer Anzahl der Primitiven, zum Leidwesen der Urheber, häufig erfolgreich (ebd.: 103).

3.4 FAZIT

Auf dem noch recht jungen Forschungsgebiet digitaler Wasserzeichen existieren bereits zahlreiche verschiedene Wasserzeichenverfahren, von denen jedes Verfahren spezifische Vor- und Nachteile für spezifischen Anwendungen aufweist. Universelle Verfahren sind nicht verfügbar.

Doch nicht nur in der Medienlandschaft, auch im Rechtswesen ist die Entwicklung sicherer Verfahren digitaler Wasserzeichen von Bedeutung. So ist eine absolut zuverlässige Authentifizierung via digitaler Wasserzeichen leider noch nicht möglich. Digitale Wasserzeichen gewährleisten zwar ein hohes Potenzial an

Datenschutz, doch bis dieses vollkommen ausgeschöpft werden kann, ist noch eine Menge Forschungsarbeit zu leisten.

4 RESÜMEE

Durch die enorme Ausbreitung digitaler Medien und der damit verbundenen Leichtigkeit schnell und einfach Kopien des Datenmaterials zu erstellen, avancieren digitale Wasserzeichen zu einer unverzichtbaren Technologie für Wirtschaft und Justiz. Mit dem Rückgang des Papiers tritt auch das Wasserzeichen auf Papier in den Hintergrund, obwohl es als Sicherheitsmerkmal auf Banknoten und Wertpapieren unverzichtbar bleibt. Es zeigt sich: Das Verfahren des Wasserzeichens als Technologie des Kopierschutzes bleibt *bestehen* – nur sind mit den digitalen Medien *neue Formen* des Wasserzeichens, unsichtbare Formen und auch Wasserzeichen in Klang- und Bewegtbildmedien, entstanden. Wie so oft in der Mediengeschichte hat man es mit der Koexistenz von Kontinuität und Diskontinuität zu tun.

LITERATURVERZEICHNIS

Achziger, Roman (2003): »Digitale Wasserzeichen«, http://www.wi.uni-muenster. de/pi/lehre/ws0304/seminar/03_DigitaleWasserzeichen.pdf, [17.12.2003], 01.03.2010.

Altmann, Jörn (1997): *Volkswirtschaftslehre*, Stuttgart: Lucius & Lucius/UTB.

Ash, Nancy/Fletcher, Shelley (1998): *Watermarks in Rembrandt's Prints with a Contribution by J.P. Filedt Kok*, Washington D.C.: National Gallery of Art.

Berliner Zeitung (1996): »EWI Rat über Design der Euro-Banknoten einig«, http://www.berlinonline.de/berlinerzeitung/archiv/.bin/dump.fcgi/1996/1204/none/0165/index.html, 01.03.2010.

Beutelspacher, Albrecht (2007): *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen,* Wiesbaden: Vieweg Verlag.

Beyerling, Magdalene (1940): *Das Papier und seine Zeichen*, Bergisch Gladbach: Zanders.

Birkner International PaperWorld (Hg.) (2005): »PaperWorld Journal«, http://www.paper-world.com/pdf/papierwirtschaft.pdf, [04.02.2005], 01.03.2010.

Born, Karl Erich (1972): *Die Entwicklung der Banknote vom „Zettel" zum gesetzlichen Zahlungsmittel*, Wiesbaden: Steiner Verlag.

Braudel, Fernand (1985): *Sozialgeschichte des 15.-18. Jahrhunderts. Band 1: Der Alltag*, München: Kindler.

Cox, Ingemar J. (2001): *Digital Watermarking,* San Francisco: Morgan Kaufmann Publishers.

Crüger, Ingrid (2002-2004): »Farbmischgesetze«, http://www.ipsi.fraunhofer.de/~crueger/farbe/farb-misch.html, [2002-2004], 01.03.2010.

Crummett, Clovis von T. (1982): »The Ancient Art of Watermarks«, in: *The Numismatist,* Vol. 95, No. 12, S. 2929-2935.

Deutsche Bundesbank (Hg.) (1963): *Deutsches Papiergeld 1772-1870*, München: Giesecke und Devrient.

Deutsche Bundesbank (Hg.) (1995): *Von der Baumwolle zum Geldschein*, Frankfurt a.M.: Knapp.

Dietz, Georg/Schmidt, Frieder (2009): »Papierproduktion im Übergang zur industriellen Revolution«, in: Rückert, Peter et al. (Redaktion): *Ochsenkopf und Meerjungfrau. Papiergeschichte und Wasserzeichen vom Mittelalter bis zur Neuzeit*, Stuttgart/Wien: herausgegeben in englischer und deutscher Sprache vom Projekt Bernstein, S. 20-26.

Dittmann, Jana (2000): *Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete,* Berlin u.a: Springer-Verlag.

Dittmann, Jana (2001): »Anwendungsgebiete digitaler Wasserzeichen«, http://www.ipsi.fhg.de/merit/teaching/fh01/ecss/wok-shop-koethen-2001-2.pdf, [2001], 01.03.2010.

Dittmann, Jana/Wohlmacher, Petra (2000): »Aspekte der Sicherheit multimedialer Daten und Anwendungen mittels Kryptographie und digitaler Wasserzeichentechniken«, in: Schumacher, M./Steinmetz, R. (Hg.): *Sicherheit in Netzen und Medienströmen*, Berlin u.a.: Springer, S. 107-123.

Duda, Erich (2000): *Das musikalische Werk Franz Xaver Süßmayrs. Thematisches Werkverzeichnis (SmWV) mit ausführlichen Quellenangaben und Skizzen der Wasserzeichen*, Kassel/Basel: Bärenreiter.

Exner, A.H. (1889): *China. Skizzen von Land und Leuten mit besonderer Berücksichtigung kommerzieller Verhältnisse*, Leipzig: Weigel.

Gerardy, Theodor (1964): *Datieren mit Hilfe von Wasserzeichen. Beispielhaft dargestellt an der Gesamtproduktion der Schaumburgischen Papiermühle Arensburg von 1604-1650*, Bückeburg: Grimme.

Gerardy, Theodor (1974): »Die Vinlandkarte – eine Fälschung«, in: *IPH-Information 8*, Marburg: Assoc., S. 27.

Gerardy, Theodor (1975): »Das älteste Wasserzeichen der Welt«, in: *IPH-Information 9*, Marburg: Assoc., S. 51-52

Griffiths, Antony/Hartley, Craig (1997): »Watermarks in the Paper of Bellange Etchings«, in: *Jacques Bellange c. 1575-1616*, London: printmaker of Lorraine (Katalog zur Ausstellung), S. 125-135.

Haidinger, Alois (2004): »Datieren mittelalterlicher Handschriften mittels ihrer Wasserzeichen«, in: *Anzeiger der Phil.-Hist. Klasse 139*, S. 5-30.

Hanebutt-Benz, Eva (1999): »Technik des Buches«, in: Leonhard, Joachim-Felix et al. (Hg.): *Medienwissenschaft: Ein Handbuch zur Entwicklung der Medien und Kommunikationsformen*, Berlin/New York: Walter de Gruyter, S. 390-420.

Heise Online (2002): »Digitale Wasserzeichen: Unsichtbarer Schutz für Filme und Musikstücke«, http://www.heise.de/news-ticker/meldung/30116, [2002], 01.03.2010.

Hlawatsch, Sven (2002): »Digitale Wasserzeichen«, http://homepages.fh-giessen.de/~hg10013/Lehre/MMS/SS02/Hlawatsch/text.htm, [2002], 01.03.2010.

Hudson, Frederick (1987): »Musicology and Paper Study: a Survey and Evaluation«, in: Spector, Stephen (Hg.): *Essays in Paper Analysis*, Washington/London/Toronto: Associated University Presses, S. 34-60.

Hunter, Dard (1978): *Papermaking. The History and Technique of an Ancient Craft*, New York: Alfred A. Knopf.

Kämmerer, Carmen (2009a): »Papiergeschichte und Papierherstellung im historischen Kontext«, in: Rückert, Peter et al. (Redaktion): *Ochsenkopf und Meerjungfrau. Papiergeschichte und Wasserzeichen vom Mittelalter bis zur Neuzeit*, Stuttgart/Wien: herausgegeben in englischer und deutscher Sprache vom Projekt Bernstein, S. 12-14.

Kämmerer, Carmen (2009b): »Vitae sanctorum«, in: Rückert, Peter et al. (Redaktion): *Ochsenkopf und Meerjungfrau. Papiergeschichte und Wasserzeichen vom Mittelalter bis zur Neuzeit*, Stuttgart/Wien: herausgegeben in englischer und deutscher Sprache vom Projekt Bernstein, S. 51-59.

Kämmerer, Carmen/Rückert, Peter (2009): »Die Welt im Wasserzeichen«, in: Rückert, Peter et al. (Redaktion): *Ochsenkopf und Meerjungfrau. Papiergeschichte und Wasserzeichen vom Mittelalter bis zur Neuzeit*, Stuttgart/Wien: herausgegeben in englischer und deutscher Sprache vom Projekt Bernstein, S. 28-30.

Kannemann, Fabian (2003): *Digitale Wasserzeichen,* München: Grin.

Keim, Karl (1956): *Das Papier. Seine Herstellung und Verwendung als Werkstoff des Druckers und Papierverarbeiters*, Stuttgart: Otto Blersch.

Keller, Arnold (1955): *Deutsche Wertpapierwasserzeichen*, Selbstverleger.

Klein, Andreas (2007): *Visuelle Kryptographie,* Berlin u.a: Springer-Verlag.

Koch, Eckhard (2002): »Content Security: Digitale Wasserzeichen«, in: Eberspächer, Jörg (Hg.): *Die Zukunft der Printmedien,* Berlin u.a: Springer-Verlag, S. 195-206.

La Rue, Jan (1961): »Watermarks and Musicology«, in: *Acta Musicologica 33*, S. 120-146.

Lang, Andreas et al. (2003): »Psychoakustische Modelle für Stirmark Benchmark – Modelle zur Transparenzevaluierung«, http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-44.pdf, [2003], 01.03.2010.

Mannucci, Ulisse (1993): »La filigrana nelle applicazioni dei cartai fabrianesi«, in: Castagnari, Giancarlo (Hg.): *Carta e cartiere nelle Marche e nell'Umbria dalle manifatture medioevali all'industrializzazione*, Fabriano: Museo di Storia della Mezzadria, S. 291-309.

Mariani, Franco/Pellegrini, Georgio (2009): »Das Papier: von Fabriano nach Europa«, in: Rückert, Peter et al. (Redaktion): *Ochsenkopf und Meerjungfrau. Papiergeschichte und Wasserzeichen vom Mittelalter bis zur Neuzeit*, Stuttgart/Wien: herausgegeben in englischer und deutscher Sprache vom Projekt Bernstein, S. 14-16.

Menn, Ralph (2000): »Versteckter Schutz gegen Datenraub«, http://www.tecchanel.de/sicherheit/identity_access/401366/versteckter_schutz_gegen_datenraub/, [2000], 01.03.2010.

Meyer, Josef Bernhard (1935): *Die Sicherungstechnik der Wertpapiere unter besonderer Berücksichtigung der Sicherheitspapiere, der graphischen und schreibtechnischen Sicherungsmethoden*, Zürich: Paco-Verlag.

Meyn, Christian (2003): Verschlüsselung und innere Sicherheit, Wiesbaden: DUV.

Mittenzwei, Julius (2006): Informationen zur Rechtewahrnehmung im Urheberrecht, München u.a.: Grin.

Neymanns, Harald (2001): Verschlüsselung im Internet, Frankfurt a.M.: Campus Verlag.

Peticolas, Fabien et al. (1999): »Information Hiding – A Survey«, in: Proceedings of the IEEE, Vol. 87, No. 7, S. 1062-1078.

Petitcolas, Fabien (2009): »Stirmark Benchmark 4.0«, http://www.petitcolas.net/fabien/watermarking/stirmark/, [2009], 01.03.2010

Piccard, Gerhard (1954): »Die Wasserzeichenforschung als historische Hilfswissenschaft«, in: *Der Archivar 4*, Sp. 263-265.

Piccard, Gerhard (1956): »Die Wasserzeichenforschung als Historische Hilfswissenschaft«, in: *Archivalische Zeitschrift 52*, S. 62-115.

Renesse van, Rudolf L. (2005): *Optical Document Security*, Boston/London: Artech House.

Renker, Armin (1950): *Das Buch vom Papier*, Wiesbaden: Insel-Verlag.

Rosenberg, Holger (2001): *Die deutschen Banknoten ab 1871*, Büttenberg: Gietl Verlag.

Rückert, Peter (2009): »Zur Einführung«, in: Rückert, Peter et al. (Redaktion): *Ochsenkopf und Meerjungfrau. Papiergeschichte und Wasserzeichen vom Mittelalter bis zur Neuzeit*, Stuttgart/Wien: herausgegeben in englischer und deutscher Sprache vom Projekt Bernstein, S. 9-10.

Sandermann, Wilhelm (1988): *Die Kulturgeschichte des Papiers*, Berlin: Springer.

Schmitz, Roland (2006): »Mediensicherheit«, in: Schmitz, Roland/Kiefer, Roland/Maucher, Johannes et al. (Hg.): *Kompendium Medieninformatik. Medienetze,* Berlin u.a.: Springer Verlag, S. 83-126.

Schöberl, Matthias (2009): »Slowakei begrüßt den Euro«. http://www.phoenix.de/content/217405.htm, [02.01.2009], 01.03.2010.

Schwenck, Konrad (1934): *Wörterbuch der deutschen Sprache in Beziehung auf Abstammung und Begriffsbildung*, Frankfurt a.M.: Sauerländer.

Schwieger, Heinz G. (1973): *Papier-Praktikum. Herstellung – Beurteilung – Verarbeitung*, Wiesbaden: PR-Vlg. H.G. Schwieger.

Seidenfaden, Lutz (2006): »Absatz digitaler Produkte und Digital Rights Management: Ein Überblick«, in: Hagenhoff, Svenja/Hogrefe, Dieter/Mittler, Elmar et al. (Hg.): *Internetökonomie der Medienbranche,* Göttingen: Universitätsverlag, S. 19-49.

Singh, Simon (2000): *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*, München.

Spenneberg, Ralf (2005): *Intrusion Detection und Prevention mit Snort 2 & Co.*, München: Addison-Wesley Verlag.

Spoer, Gertraude (1987): *Rosen, Tulpen, Nelken: Aus der Formenwelt der Wasserzeichenkunst*, Leipzig: Deutsche Bücherei.

Spoer, Gertraude (1996): »Drahtgeschichten«, in: Schmidt, Frieder (Hg.): *Papiergeschicht(en)*, Wiesbaden: Harrassowitz, S. 153-170.

Steinebach, Martin/Dittmann, Jana (2002): »Digitale Wasserzeichen: Grundlagen, Anwendungen – Grenzen«, in: *Information, Wissenschaft und Praxis*, Jg. 53, Nr. 5, S. 261-268.

Steinmetz, Ralf (2000): *Multimedia Technologie – Grundlagen, Komponenten und Systeme,* Berlin u.a.: Springer.

Tschudin, Peter F. (1996a): »Methodik der Papierdatierung«, in: *IPH-Congress Book 11*, S. 29-35.

Tschudin, Peter F. (1996b): »Der Ursprung der Haus- und Handelsmarken in Wasserzeichen«, in: Schmidt, Frieder (Hg.): *Papiergeschicht(en)*, Wiesbaden: Harrassowitz, S. 223-236.

Tschudin, Peter F. (2002): *Grundzüge der Papiergeschichte*, Stuttgart: Hiersemann.

Ulbricht, Gangolf (2000): »Wasserzeichen oder die transparente Geschichte des Papiers«, in: *Lebendiges Rheinland-Pfalz 37/1-2*, S. 37-44.

Van Damme, Ingrid (2008): »Die Wiege der europäischen Banknote steht in Schweden«, http://www.nbbmuseum.be/de/2008/04/cradle-european-banknote.htm, [11.04.2008], 01.03.2010.

Weber, Bernt (1970): *Die Banknote. Eine volkswirtschaftlich- historische Betrachtung*, Frankfurt a.M.: Knapp.

Weiss, Karl Theodor/Weiss, Wisso (1962): *Handbuch der Wasserzeichenkunde*, Leipzig: VEB Fachbuchverlag.

Weiss, Wisso (1986): *Historische Wasserzeichen*, Leipzig: VEB.

Werber, Niels (2004): »Vom Unterlaufen der Sinne. Digitalisierung als Codierung«, in: Schröter, Jens/Böhnke, Alexander (Hg.): *Analog/Digital – Opposition*

oder Kontinuum? Zur Theorie und Geschichte einer Unterscheidung, Bielefeld: Transcript, S. 81-96.

Will, Matthias O. (2002): *Aufbau und Nutzung einer digitalen Bibliothek in einer universitären Ausbildungsumgebung*, Münster: Waxmann.

Wolbe, Eugen (1923): *Handbuch für Autographensammler*, Berlin: Rich. Carl Schmidt.

Woodward, David (1987): »The Analysis of Paper and Ink in Early Maps«, in: Spector, Stephen (Hg.): *Essays in Paper Analysis*, Washington u.a.: Associated University Press, S. 200-221.

FAIR PLAY IM DIGITALEN ZEITALTER

Anspruch und Wirklichkeit des Digital Rights Management

VON DANIEL KÖHNE

1. KENNEN SIE DRM?

Sie hören gerne Musik? Sie schauen Filme? Sie spielen gerne mit Ihrer Spielkonsole? Sie benutzen einen Computer? Dann hatten und haben Sie mit an Sicherheit grenzender Wahrscheinlichkeit schon mit *Digital Rights Management* (DRM) zu tun! Falls Sie diesen Begriff dennoch zum ersten Mal hören, dann geht es Ihnen vermutlich nicht viel anders als den meisten anderen Nutzern digitaler Inhalte. Der Umgang mit DRM ist mit der Nutzung digitaler Werke zwar (fast) unvermeidlich geworden, bewusst wird das vielen Verbrauchern allerdings erst in dem Augenblick, wo sie die restriktive Seite dieser Rechteverwaltungssysteme kennenlernen.

Abb. 1: Eine Persiflage von DRM-Gegnern auf die 1980 von der British Phonographic Industry veröffentlichten Kampagne »Home Taping Is Killing Music«.

Drei typische Beispiele: Eine legal erworbene Software lässt sich partout nicht auf dem heimischen Zweit-Computer installieren. Die erst kürzlich erworbenen Filme aus dem Onlineshop können nach der Neuinstallation des Betriebssystems nicht mehr abgespielt werden. Der CD-Player im Auto verweigert die Wiedergabe des neuen Albums Ihrer Lieblingsband.

Vor allem solche *Pannen* haben zu einer großen Zahl von Missverständnissen, Mythen und vor allem jeder Menge Ärger über das sog. Digital Rights Management geführt. Von »elektronischer Leine für Kunden« ist da beispielweise die Rede, von Einschränkungen der Privatsphäre und der Blockade von Kulturgütern durch die Medienindustrie. Ganze Foren im World Wide Web beschäftigen sich ausschließlich mit dem Thema der digitalen Rechteverwaltung, diskutieren über deren (Un)Sinn und Zweck, liefern Tipps, wie man die oft lästige Kontrollinstanz umgehen kann und gelangen oft zu der Überzeugung, dass das *R* in DRM wohl eher für *Restriction* als den Begriff *Rights* stehe.[1] Gerald Fränkl[2] fasst die Ausgangslage knapp aber treffend zusammen: »DRM, ist ein stark polarisierendes Schlagwort der aktuellen Medienlandschaft« (Fränkl 2005: 13; vgl. ebd.: 35ff.).

2. DIGITAL RIGHTS MANAGEMENT – VERSUCH EINER DEFINITION

Was ist und bezweckt DRM überhaupt? Es ist schwer, vielleicht sogar unmöglich, digitale Rechteverwaltungssysteme allgemeingültig zu definieren. Das zeigt sich schon daran, dass selbst dem Gesetzgeber bislang eine solche Definition nicht gelingen will oder vielleicht auch nicht gelingen soll. In der juristischen Literatur wird DRM teilweise synonym zu dem Begriff »technische Schutzmaßnahme« verwendet. Auf den ersten Blick scheint es – vor allem aus Verbrauchersicht – auch leicht zu fallen, DRM-Systeme einer Kopierschutztechnik gleich zu setzen. Immerhin erlangen die meisten Verbraucher erst durch diese Funktion der digitalen Rechteverwaltungssysteme Kenntnis über deren Existenz. Bei einer genaueren Betrachtung muss diese Bewertung jedoch differenzierter ausfallen.

Für eine Konkretisierung ist es wichtig, zwischen Schutzmaßnahmen im Sinne des Urheberrechts auf der einen Seite und DRM-Systemen auf der anderen Seite klar zu unterscheiden. Das ist schon deshalb zwingend erforderlich, da eine »industrielle Massenproduktion von urheberrechtlichen Werken [...] im Urheberrecht nicht vorgesehen« (Höhne 2007: 7) ist, diese aber nun einmal de facto der Realität entspricht.

Festhalten lässt sich in jedem Fall: nicht jede technische Schutzmaßnahme ist zwangsläufig ein DRM-System. Gegen die These, dass es sich bei DRM-Systemen um komplexere Kopierschutzverfahren handelt, spricht auch die Tatsache, dass die Produzenten digitaler Werke ein erhebliches Interesse an der massenhaften Vervielfältigung und Verbreitung ihrer digitalen Inhalte haben und ihnen dabei ein Kopierschutz eher hinderlich sein dürfte. Was also ist unter digitaler Rechteverwaltung zu verstehen?

---

1 Siehe dazu beispielsweise ein kritisches Internetportal unterstützt von der Free Software Foundation Europe: http://drm.info/, 18.12.2009.

2 Neben zwei Buchpublikationen zum Thema digitale Rechteverwaltung, ist Gerald Fränkl u.a. als Autor auf der Internetseite http://www.digital-rights-management.info, 20.06. 2009, aktiv.

Zunächst einmal ist festzuhalten, dass es *das* DRM-System nicht gibt. Der Begriff des Digital Rights Management beschreibt weder eine bestimmte Software noch eine konkrete Handlung, sondern vielmehr ein komplexes System, das auf der Kombination vieler verschiedener Technologien basiert und dessen Zweck die Kontrolle des Zugangs und Steuerung der Nutzung digitaler Inhalte ist (vgl. Fränkl 2005: 35ff.; Zeng 2006). »Es ist das Ziel der Rechteinhaber an Geistigem Eigentum durch ein sogenanntes Digitales Rechtemanagement (DRM) den Verlust der physischen Bindung eines digitalen Produkts zu kompensieren« (Grimm 2009: 27; vgl. Tsolis 2009).

Dieses Zitat zeigt bereits drei wesentliche Kontroversen der digitalen Rechteverwaltung auf: Erstens, die Debatte um das geistige Eigentum. Zweitens, der Umgang mit digitalen Produkten an sich und drittens, die physische Bindung, welche mit dem Siegeszug des Digitalen verloren ging. Aber dazu an späterer Stelle mehr.

Selbst über die typischen Merkmale einer digitalen Rechteverwaltung gibt es unterschiedliche Ansichten. Die Firma Microsoft erklärt ihr DRM beispielsweise wie folgt:

> »Windows Media DRM ist eine bewährte Plattform, die das Schützen und sichere Übermitteln von Inhalten für die Wiedergabe auf einem Computer, einem tragbaren Gerät oder einem Netzwerkgerät ermöglicht. Ihre Flexibilität ermöglicht die Unterstützung einer Reihe von Geschäftsmodellen: von einzelnen Downloads bis hin zur Übertragung in Form physischer Medien. Die neueste Version von Windows Media DRM enthält neue Szenarien und bietet Heimanwendern noch besseren Zugriff auf geschützte Audio- und Videoinhalte.« (Microsoft 2009)

Martin Schippan charakterisiert DRM dagegen schlicht als »ein vollautomatisiertes, elektronisches Vertriebs- und Abrechnungssystem, [welches] [...] digitale Inhalte zu definieren versucht« (Schippan 2004: 190).

Auch wenn eine exakte Definition offenbar schwerfällt, so lassen sich DRM-Systeme allgemein dennoch wie folgt beschreiben: Die digitale Rechteverwaltung identifiziert digitale Werke, regelt den Zugang und die Nutzung dieser und überwacht gleichzeitig die Einhaltung ebendieser Kontrollinstanzen. Letztlich erfüllen DRM-Systeme aber vor allem die Rolle eines anspruchsvollen Vertriebssystems, insbesondere für digitale Angebote im Internet.

Folglich muss man DRM-Systeme weniger als Kopierschutz, sondern eher als Vertriebsinfrastruktur für die Produzenten digitaler Werke einerseits und die Nutzer dieser Inhalte andererseits sehen, da ein wichtiges Ziel von digitaler Rechteverwaltung letztlich auch der Authentizitäts- und Integritätsschutz der zur Verfügung gestellten medialen Inhalte ist. Darüber hinaus lässt sich ein System digitaler Rechteverwaltung durch weitere technische Prozesse wie beispielsweise

Bezahlsysteme und Metainformationen, die Rückschlüsse auf den digitalen Inhalt bzw. dessen Urheber ermöglichen, beliebig erweitern.

Diese technischen Möglichkeiten sind mit Sicherheit nicht allein charakteristisch für DRM-Systeme, allerdings machen sie deutlich, dass die Bezeichnung »Vertriebsinfrastruktur« im Zusammenhang mit digitaler Rechteverwaltung einer allgemeingültigen Definition schon sehr nahe kommt. Denn vereinfacht dargestellt steht bei einfachen digitalen Rechteverwaltungssystemen das Ziel im Vordergrund, potenziellen Kunden einen Zugang zu digitalen Inhalten zu verschaffen. Dieser erfolgt dann in der Regel gegen Bezahlung (vgl. Höhne 2007: 43ff.; Roßnagel 2009: 18f.). Nach dem Kauf eines digitalen Produktes und der damit bestandenen Zugangskontrolle kann der Kunde nun über das erworbene Produkt theoretisch frei verfügen. In der Praxis haben die Produzenten digitaler Inhalte allerdings ein erhebliches Interesse daran, dass ein Kunde die erworbenen Inhalte eben nicht völlig frei verwenden kann, vor allem aber, dass es dem Kunden nicht möglich ist, diesen Content beliebig zu vervielfältigen und weiterzugeben. An dieser Stelle greifen technische Maßnahmen zur Nutzungskontrolle ein, welche zum Ziel haben, den Umgang des Kunden mit den erworbenen Produkten zu steuern bzw. einzuschränken (vgl. Höhne 2007: 43ff.).

Festzuhalten bleibt also zunächst, dass DRM kein klassisches und eindeutiges Verfahren zum Schutz und zur Verwaltung von Rechten oder einen Kopierschutz darstellt, sondern viel mehr eine komplexe Infrastruktur bestehend aus verschiedenen Basistechnologien beschreibt. Zum Verständnis von DRM ist daher zum einen die Kenntnis der entsprechenden Technologien und zum anderen das Wissen um die technischen Entwicklungen der vergangenen Jahrzehnte erforderlich, welche die digitale Rechteverwaltung *nötig*, auf jeden Fall aber erst *möglich* machten.

3. TECHNISCHE ENTWICKLUNGEN ALS GRUNDLAGE FÜR DIGITAL RIGHTS MANAGEMENT

In den vergangenen Jahren fand ein gewaltiger Umbruch bei der Produktion medialer Werke bzw. Inhalte statt, vereinzelt wird sogar von einem Paradigmenwechsel gesprochen: Der Wechsel von analogen zu digitalen Medien wurde vollzogen (vgl. Fränkl 2005: 15). Maßgeblich dazu beigetragen haben technische Entwicklungen im Bereich der Vervielfältigungs- aber auch der Kommunikationsmöglichkeiten innerhalb der letzten Jahrzehnte. Als besonders markante Punkte sind in diesem Zusammenhang sicherlich die Ablösung der Schallplatte durch die Audio-CD zu nennen, sowie die spätere DVD, die ihrerseits den bis dato analogen Standard VHS im Bereich Video und Film verdrängte (vgl. ebd.: 2005: 14ff.; Höhne 2007: 2-6, 19ff.; Schollin 2008: 269ff.).

Die Vervielfältigungstechnologien wurden zunehmend preiswerter und damit – zum ersten Mal – auch für eine breite Masse von Privatpersonen erschwinglich. In diesem Kontext spielt vor allem der – wenn auch noch analoge – Kassettenrekorder eine herausragende Rolle. Mit einem einfachen Rekorder war es plötzlich

auch im privaten Bereich problemlos möglich, die eigene Lieblingsmusik auf MC zu kopieren, neu zu mischen oder weiterzugeben. Durch die massenhafte Verbreitung der VHS-Technik und des VHS-Videorekorders, der um 1980 eingeführt wurde, zeichnete sich darüber hinaus für die Filmindustrie eine ähnliche Entwicklung ab.

Diese Beispiele sind insofern nicht unerheblich, da sie verdeutlichten, dass die Thematik des Kopierschutzes nicht per se eine der neuen *digitalen* Welt ist. Im Gegenteil – insbesondere durch den Siegeszug der MC erkannten die Produzenten medialer Inhalte, dass ihnen die immer leistungsfähigere Technik nicht nur (Kosten-)Vorteile, sondern auch ein neues Problem bescherte: den Kontrollverlust über die Vervielfältigungen im privaten Bereich (vgl. Eggert 2005: 12f.; Fränkl 2005: 14ff., Höhne 2007: 19ff.; Schollin 2008: 269ff.).

So beliebt die neuen Techniken jedoch auch waren, sie hatten einen nicht unerheblichen Makel: Jede analoge Vervielfältigung ging technisch bedingt mit einem deutlichen Qualitätsverlust einher, der zumindest »die Anfertigung der Kopie einer Kopie unattraktiv machen« (Höhne 2007: 3) konnte. Dies allerdings änderte sich schlagartig mit dem Durchbruch der digitalen Medien, der im Audio-Bereich 1981 auf der Internationalen Funkausstellung in Berlin mit der Vorstellung der Audio-CD begann. Das Problem der unerlaubten Vervielfältigung von Software, das bereits seit der 1980er Jahre bestand, wird durch massenhafte Einführung von Heimcomputern ab den frühen 1990er Jahren weiter verschärft. Die wenig später folgenden CD- und DVD-Brenner in modernen Computern ermöglichten plötzlich jedem Privathaushalt in kurzer Zeit, bei geringem Kostenaufwand und vor allem ohne nennenswerte Qualitätsverluste die Vervielfältigung von digitalem Content jeglicher Art. Moderne Computer haben sich so zu einem »Kommunikations- und Unterhaltungszentrum« (Höhne 2007: 5) für Privatanwender entwickelt. Auch in anderen Bereichen, beispielsweise bei der Übertragung von Radio- und insbesondere Fernsehprogrammen, haben sich mittlerweile digitale Standards durchgesetzt – zunächst via Satellit und Kabel, schließlich mit dem *Digital Broadcasting Standard* auch über den terrestrischen Weg.

Beschleunigt wurde dieser Prozess zudem durch leistungsfähigere und preiswertere Kommunikationsmöglichkeiten, insbesondere dem schnellen Breitband-Internet. Während zu Beginn der privaten Nutzung des Internets die langsamen Übertragungsraten von gerade einmal 56 kBit den Austausch größerer Datenmengen noch unattraktiv machten, erhöhten sich diese Raten durch die nahezu flächendeckende Einführung von Breitband-Internet mittels der DSL-Technik bereits um den Faktor 10 und mehr. Durch die Verwendung von Funk-Netzwerktechniken und schnellen Mobilfunknetzen, wie EDGE und insbesondere UMTS, sowie immer leistungsfähigeren und kleineren mobilen Endgeräten, ist ein schneller Zugang zum World Wide Web mittlerweile an nahezu jedem beliebigen Ort möglich. Der Austausch und die Übertragung von Daten jeglicher Art und Größe über das Internet wurde so praktikabel und wird durch immer kostengünstigere Internetzugänge für Privatpersonen kontinuierlich attraktiver.

In diesem Zusammenhang muss sicherlich auch die Entwicklung der sog. Peer-to-Peer-Protokolle (P2P) erwähnt werden, mit denen eine dezentrale Speicherung von Daten auf Servern realisiert werden konnte. Aufgrund dieser neuen Protokolle zum Austausch von Daten im Internet konnten schließlich auch die populären Tauschbörsen entstehen, die es möglich machten, digitale Kopien innerhalb kürzester Zeit weltweit über das Internet zu verbreiten (vgl. Mittenzwei 2006: 10ff.). Technische Fortschritte bei den Kompressionsmöglichkeiten digitaler Inhalte taten ihr Übriges. An dieser Stelle sind vor allem die Entwicklung des JPEG-Formats für Bilder sowie die des MP3-Formats für Audio-Inhalte im Jahr 1992 hervorzuheben; neue Standards die sich rasant verbreiteten, und mit deren Hilfe sich große Datenmenge weitestgehend ohne sicht- oder hörbare Qualitätsverluste erheblich komprimieren ließen und so ohne großen Zeitaufwand über das Internet übertragen und ausgetauscht werden konnten (vgl. Fränkl/Karpf 2004: 21; Fränkl 2005: 14-16, Höhne 2007: 4ff.).

4. KONSEQUENZEN DER TECHNISCHEN ENTWICKLUNG

Vor allem in ihrer Gesamtheit betrachtet haben diese technischen Fortschritte erhebliche Konsequenzen für die Produktion, aber auch die Nutzung von medialen Inhalten. Im Zuge der kompletten Digitalisierung des Medienmarktes sanken für die Urheber der digitalen Inhalte die Herstellungskosten erheblich, so dass diese mittlerweile vernachlässigt werden können. Gleichzeitig entfällt, insbesondere durch die Popularität des Internets, eine Beschränkung auf bestimmte regionale Märkte. In diesem Zusammenhang von einer »Industrialisierung der Werkschöpfung« (Höhne 2007: 7f.) zu sprechen, liegt daher nahe.

Zum anderen stehen die Produzenten digitaler Inhalte vor einem Problem: Genauso simpel und günstig, wie sie ihre eigenen Inhalte produzieren können, ist es nun auch Privatnutzern möglich, einen beliebigen digitalen Content zu vervielfältigen. Das illegale Kopieren von digitalen Daten führt dabei zweifelsohne zu ökonomischen Einbußen der Produzenten (vgl. Kühne 2009: 3ff.). Die unrechtmäßige Vervielfältigung digitaler Inhalte ist praktisch nicht kontrollierbar, die Rückverfolgung nahezu aussichtslos. Qualitätsverluste, wenn es sie denn überhaupt gibt, sind so marginal, dass sie in der Regel komplett vernachlässigt werden können.

Diese Folgen der rasanten technischen Entwicklung haben im Wesentlichen zu zwei Reaktionen der Medienproduzenten und -urheber geführt. Erstens dem vermehrten Einsatz von Schutz- und Kontrollmaßnahmen zur Wahrung der Urheberrechte an medialen Inhalten. Und zweitens, vor allem bedingt durch den mäßigen Erfolg der erwähnten Schutz- und Kontrolltechniken, zu einer Verschärfung der gesetzlichen Rahmenbedingungen, die unter dem entsprechenden Druck der Medienproduzenten politisch umgesetzt worden sind und weiter verschärft zu werden scheinen (vgl. Krempl 1998; Krempl 2001).

Als Konsequenz aus den rasanten technischen Fortschritten der vergangenen Jahrzehnte wurde allerdings auch die digitale Rechteverwaltung mittels DRM erst denkbar und vor allem realisierbar. Eine Tatsache, die nicht unbeachtet bleiben sollte, da sie den Medienproduzenten zunächst einen wesentlichen Vorteil verschaffte: Die lückenlose und vor allem oftmals heimliche Kontrolle darüber, wie, wann und wo digitale Inhalte erworben werden und vor allem die Möglichkeit dazu, die spätere Nutzung dieser Werke zu steuern – Optionen, die im analogen Zeitalter noch undenkbar waren (vgl. Grimm 2009: 27ff.; Grassmuck 2004: 24f.). Als Reaktion auf die neuen Vervielfältigungsmöglichkeiten entwickelten die Produzenten digitaler Inhalte Kopierschutzmaßnahmen für ihre Werke. Techniken, die einen Kopierschutz gewährleisten sollten, wurden für Filme, Musik, Software, also im Grunde alle erdenklichen Varianten digitaler Inhalte, entwickelt.

Ein erster populärer Ansatz solcher Mechanismen, um die unerlaubte Nutzung und Vervielfältigung von Software zu unterbinden, waren sog. »Dongles«. Die Funktionsweise dieser kleinen Geräte, die zusammen mit der entsprechenden Software ausgeliefert wurden, war vergleichsweise simpel: Eine in die Software integrierte Abfrage überprüfte, ob der dazugehörige Dongle ebenfalls an den Computer angeschlossen war. War dies nicht der Fall, wurde das Programm beendet bzw. ließ sich erst gar nicht vollständig starten oder nutzen. Wirklich durchsetzen konnten sich Dongles jedoch nicht. Das hatte verschiedene Gründe: Zum einen gab es häufig Kompatibilitätsprobleme, unter denen zwangsläufig auch die Anwenderfreundlichkeit litt. Zum anderen basierte die Dongle-Variante auf einem relativ einfachen Sicherheitsverfahren, welches dazu führte, dass entweder die in die Software integrierten Abfragen manipuliert oder sogar Dongles selbst illegal kopiert bzw. nachgebaut werden konnten.

Eine weitere eingesetzte Kopierschutzvariante sollte das Kopieren von Software mit einem herkömmlichen Computer bzw. der darauf installierten Software durch eine verschlüsselte Beschriftung der Datenträger verhindern – aber auch dieser Schutz konnte innerhalb kurzer Zeit durch speziell entwickelte Kopiersoftware umgangen werden.

Interessante Ansätze gab es bei der Kombination von Software und der – zumindest noch damals – beiliegenden gedruckten (sic!) Dokumentation. Bei dieser Schutzvariante unterbrach die Software in unregelmäßigen Abständen ihren Nutzer, um von ihm bestimmte Informationen aus dem Handbuch abzufragen. Natürlich war es kein allzu großes Problem, die entsprechenden Fragestellungen bzw. Antworten unerlaubt weiterzugeben. Das erkannten auch die Software-Produzenten und lieferten schließlich in weiter entwickelten Varianten dieser Schutztechnik beispielweise selbst kopiergeschützte Dokumentationen aus. Zumindest als kreativ muss ein Versuch der Produzenten gewertet werden, die Abfragen am Bildschirm bzw. deren Antworten in der Dokumentation nur über die Verwendung von speziellen Farbfolien, die der Software beilagen, zu ermöglichen. Diese ersten Versuche, eine unerlaubte Nutzung oder Vervielfältigung von Software zu unterbinden, muten aus heutiger Sicht zweifelsohne laienhaft an und er-

innern eher an ein Gimmick für junge Detektive aus einem Comic-Heft (vgl. Höhne 2007: 18ff.).

5. DIE GRUNDLAGEN VON DRM-SYSTEMEN

Wie bereits einleitend erwähnt, stellen Systeme der digitalen Rechteverwaltung Infrastrukturen dar, die verschiedene Basistechnologien kombiniert einsetzen, um so den Zugang und die Nutzung digitaler Werke zu kontrollieren und zu steuern.

Dazu ist es erforderlich, dass in einem ersten Schritt digitaler Content vor unberechtigtem Zugang geschützt wird. Dies lässt sich wirkungsvoll durch eine Verschlüsselung realisieren, weshalb auch kryptographische Verfahren zu den wichtigsten Basistechnologien von DRM-Systemen zählen. Auch wenn die Begriffe »Kopierschutz« und das sog. Digital Rights Management – wie bereits erwähnt – nicht gleichzusetzen sind, so hat sich das digitale Rechtemanagement doch aus den klassischen Kopierschutzverfahren, wie sie bereits zuvor kurz beschrieben worden sind, entwickelt. Im Gegensatz zu den meisten altbekannten Kopierschutzverfahren basieren moderne DRM-Systeme allerdings auf deutlich komplexeren Mechanismen, kombinierten Verfahren der Stegano- und Kryptographie[3] (vgl. Abie 2009; Agnew 2008: 295ff.; Höhne 2007: 23ff.; Schollin 2008: 144ff.).

In Form von digitalen Wasserzeichen[4] und Fingerabdrücken, elektronischen Signaturen und Verschlüsselungstechnologien sind diese Kernbestandteile eines jeden DRM-Systems, die jedoch nur auf den ersten Blick absolut sicher gegenüber Manipulationen erscheinen. Seit Beginn der Kryptographie gibt es einen regelrechten Wettbewerb zwischen den Entwicklern neuer Verschlüsselungstechniken auf der einen Seite und den Entwicklern von Methoden, die genau jene Verschlüsselung zu umgehen oder auch aufheben versuchen, auf der anderen Seite (vgl. Eggert 2005: 12ff.). Wobei erste Verfahren dieser Art keine Erscheinungen der digitalen Welt sind, sondern in Form von Geheimschriften bereits im 5. Jahrhundert v. Chr. in Griechenland Verwendung fanden.

Es gibt diverse Formen von Verschlüsselungsmethoden[5], die sich zum Teil erheblich voneinander unterscheiden. Entscheidend für moderne Verfahren der Kryptographie ist allerdings, dass die Sicherheit der angewandten Verschlüsselung nur von der Geheimhaltung des entsprechenden Schlüssels, aber niemals von der Geheimhaltung des eingesetzten Algorithmus abhängen sollte. Dabei wird zwischen symmetrischer, asymmetrischer und hybrider Verschlüsselung sowie dem sog. Hash-Verfahren unterschieden.

---

3 Eine sehr umfangreiche Linksammlung zu den Themen Kryptographie, Steganographie, Datenschutz und -sicherheit findet sich bei Burkhard Schröder: http://www.burks.de/krypto.html, 10.12.2009.

4 Siehe den Beitrag von Carina Gerstengarbe, Katharina Lang und Anna Schneider in diesem Heft.

5 Einen spannenden Einblick in dieses komplexe Thema bietet Singh (2000).

Symmetrische Verschlüsselungsverfahren (Private-Key-Verfahren) verwenden dabei für die Codierung und Decodierung denselben Schlüssel, in dessen Kenntnis oder Besitz logischerweise sowohl der Sender als auch der Empfänger der so codierten Inhalte sein muss. Dieser Schlüssel muss wiederum zwingend über einen sicheren Übertragungskanal übermittelt werden, da ansonsten der Schutz des gesamten Verfahrens nicht mehr gewährleistet ist.

Bei der asymmetrischen Verschlüsselung (Public-Key-Verfahren) wird dagegen ein Schlüssel verwendet, der sowohl aus einem öffentlichen (Public Key) und einem geheimen, privaten Schlüssel (Private Key) besteht. Diese stehen in einem mathematischen Zusammenhang, wodurch sich aus dem privaten Schlüssel der öffentliche Teil ableiten lässt, nicht jedoch umgekehrt. So kann der Sender digitale Inhalte mit dem öffentlichen Schlüssel codieren; die Decodierung ist allerdings nur mit dem privaten Schlüssel des vorgesehenen Empfängers möglich. Asymmetrische Verschlüsselungsverfahren haben jedoch einen Nachteil; sie erfordern einen relativ hohen Rechenaufwand.

Dies hat zur Entwicklung der sog. hybriden Verschlüsselung geführt, welche bis heute Standard ist und die symmetrischen und asymmetrischen Verfahren entsprechend ihrer Vor- und Nachteile nutzt. So werden die eigentlichen Daten oder Informationen zwar symmetrisch verschlüsselt, der Schlüssel zur Decodierung jedoch mittels eines asymmetrischen Verfahrens codiert und über einen öffentlichen Kanal übertragen. Dadurch wird lediglich eine geringe Rechenleistung benötigt, aber gleichzeitig die Sicherheit bei der Schlüsselverteilung gewährleistet. Eine andere Methode verwenden Hash-Verfahren. Mittels eines sog. Hash-Wertes oder digitalen Fingerabdrucks weisen sie beliebigen digitalen Daten einen nahezu eindeutigen Wert fester Länge zu, also sozusagen eine »Kurzfassung« des originalen Contents (vgl. Agnew 2008: 295ff.; Höhne 2007: 30; Mittenzwei 2006: 67ff.; Schollin 2008: 144ff.). Originale Information und Hash-Wert werden dabei abgeglichen; ändert sich die originale Information, führt dies auch zu einem veränderten Hash-Wert. Aufgrund ihrer festgelegten Länge können mehrere identische Hash-Werte kollidieren, da sie jeweils unterschiedlichen Original-Dateien zugeordnet sind. Deshalb ist es erforderlich, dass bei diesem Verfahren Hash-Funktionen eingesetzt werden, mit denen es praktisch – also mit den Rechenleistungen heutiger oder in naher Zukunft verfügbarer Computer – unmöglich ist, zwei verschiedene digitale Dateien mit identischen Hash-Wert zu ermitteln.

In letzter Konsequenz hat jedoch jede – zumindest zweckmäßige – Codierung einen entscheidenden Nachteil: Soll ein verschlüsselter digitaler Inhalt wieder les- und nutzbar sein, muss er sich zwangsläufig mindestens einmal wieder entschlüsseln lassen. Andernfalls wäre schließlich auch jeglicher Inhalt für den Nutzer unbrauchbar. Kurzum: »Im Prinzip [ist] jede Operation, die ein Computer vornimmt, von einem Computer auch wieder rückgängig zu machen, und muss es auch sein, da autorisierte Nutzer das Werk schließlich dafür bezahlt haben, es zu rezipieren« (Grassmuck 2004: 102).

Eine perfekte Codierung digitaler Inhalte kann es allerdings schon deshalb nicht geben, da jede Sicherheitsinstanz spätestens bei der legitimen Nutzung hinfällig oder zumindest angreifbar ist. Und sei es über den Umweg einer – wenn auch mit Qualitätsverlusten einhergehenden – analogen Kopie. Entscheidend für die Funktionalität eines DRM-Systems ist es daher, dass die beiden wichtigen Kontrollfunktionen, also die Zugangs- und Nutzungssteuerung, so verschlüsselt und integriert sind, dass sie nicht beliebig, also z.B. durch den Nutzer selbst, außer Kraft gesetzt werden können. Insbesondere die dem Kauf zeitlich nachgestellte Nutzungskontrolle ist dabei eine technische Herausforderung. Ohne die entstandenen neuen Kommunikationswege, insbesondere dem Internet, wäre eine solche Kontrolle des Anwenders nicht denkbar. Mit ihr und mittels einer speziellen Software kann jedoch eine Kommunikation zwischen Anwender-(Software) und Produzenten über einen zwischengeschalteten Server ermöglicht werden.

6. DAS FUNKTIONSSCHEMA VON DRM-SYSTEMEN

Grundsätzlich lässt sich die Funktionsweise eines DRM-Systems in vier Bereiche gliedern:

Erstens einem sog. »Secure Container«, der das eigentliche digitale Werk enthält und mittels – bereits zuvor erläuterter – verschlüsselter Algorithmen vor unberechtigtem Zugriff schützen soll.

Zweitens definiert eine »Rights Expression Language« die Zugangsberechtigung zu den Inhalten des Secure Containers. Bereits Mitte der 1990er Jahre entwickelte die Firma Xerox die *Digital Rights Property Language*[6], eine spezielle Sprache, die ebendiese Kommunikation zum ersten Mal möglich machte. Mittlerweile haben sich sozusagen zwei Kommunikationsstandards durchgesetzt: die *Open Digital Rights Language*[7] und die *eXtensible rights Markup Language*[8]. Beide Sprachen sind inkompatibel zueinander; die eine wird bevorzugt von der *Open Mobile Alliance*[9] eingesetzt, die andere verwendet zum Beispiel der *Windows Media Rights Manager*. Was machen diese Sprachen im Detail?

6 Für weiterführende Informationen zur *Digital Rights Property Language* (DPRL) siehe u.a.: http://xml.coverpages.org/dprl.html, 11.01.2010.

7 Für weiterführende Informationen zur *Open Digital Rights Language* (ODRL) siehe u.a.: http://odrl.net/, 08.01.2010.

8 Für weiterführende Informationen zur *eXtensible rights Markup Language* (XrML) siehe u.a.: http://www.xrml.org/about.asp, 08.01.2010.

9 Für weiterführende Informationen zur *Open Mobile Alliance* (OMA) siehe: http://www.openmobilealliance.org/, 08.01.2010.

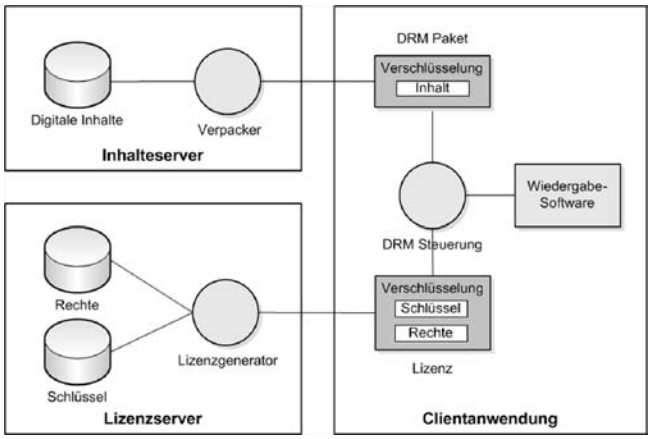

Abb. 2: Die Funktionsweise von DRM-Systemen vereinfacht dargestellt. Quelle: Prussio (CC-Linzenz), http://de.wikipedia.org/w/index.php?title=Datei:DRMS.png&filetimestamp=20050908195600, 08.01.2010

Sie erkennen, welche Lizenzbedingungen erworben worden sind und schränken den Nutzer bei Bedarf dementsprechend ein. So ist es zum Beispiel möglich, bestimmte Funktionen einer Software einzuschränken oder aber auch die Nutzungsdauer von digitalen Inhalten zu begrenzen. Dabei lässt sich im Wesentlichen zwischen inhaltlichen, zeitlichen, räumlichen und persönlichen Beschränkungen, sowie der vorgegebenen Nutzungsart unterscheiden. Beispiele dafür sind die Einschränkung der Exportmöglichkeiten in DRM-freie Formate, die Unterbindung des Anlegens von Sicherheitskopien, die Beschränkung der Gesamtnutzungsdauer, die Bindung an bestimmte Abspielgeräte bzw. Hardware oder auch der Ausschluss der gewerblichen Nutzung von digitalen Inhalten (vgl. Fränkl 2005: 25ff.; Höhne 2007: 45f.; Schollin 2008: 144ff.).

Drittens und ebenso wichtig ist die Identifikation des digitalen Inhaltes, beispielsweise durch eine Seriennummer, sowie die eindeutige Zuordnung der Nutzer.

Und schließlich wird, viertens, im Anschluss an den Verkauf der digitalen Werke und einer erfolgreichen Identifikation durch das System, eine Kontrollinstanz aktiv, die ggf. Nutzungsberichte übermitteln oder auch zur Bezahlung eingesetzt werden kann (vgl. Eggert 2005: 17f.; Höhne 2007: 47ff.). Da eine Manipulation nun aber nicht sicher ausgeschlossen werden kann, setzen die Produzenten digitaler Werke zusätzlich auf spezielle verborgene Kennzeichen, die dem Kunden – zumindest im Optimalfall – verborgen bleiben, dem Urheber der Werke jedoch einen direkten Rückschluss auf den legitimen Nutzer oder Inhaber des entsprechenden Werkes zulassen.[10]

10 Siehe den Beitrag von Carina Gerstengarbe, Katharina Lang und Anna Schneider in diesem Heft.

An dieser Stelle wird klar, dass DRM-Systeme die Persönlichkeitsrechte der Kunden berühren. Transparenz und Zustimmung des Kunden sind daher ein wichtiges Thema für DRM-Funktionen.

7. DIE PRAKTISCHE ANWENDUNG VON DIGITAL RIGHTS MANAGEMENT

DRM-Systeme werden vielfältig eingesetzt. Zu den populärsten Einsatzgebieten zählen aber sicherlich der Vertrieb von digitaler Musik und elektronischen Text-Dokumenten. Zu den bekanntesten Systemen auf dem digitalen Markt zählten (sic!) *Fairplay*, das die Firma Apple in seinem Online-Musikshop *iTunes* einsetzte oder auch der *Windows Media Rights Manager* von Microsoft, der u.a. durch das deutsche Musikportal *Musicload* von T-Online eingesetzt wird (vgl. Grimm 2009: 35f.).

Digitales Rechtemanagement fand und findet also Anwendung in populären Bereichen. Dennoch ist die Kritik an DRM-Systemen laut und vielfältig. Und tatsächlich scheint sich die umfangreiche Kontrolle und Steuerung der Nutzer durch die Medienindustrie nicht durchsetzen zu können. Schlussfolgern lässt sich dies zumindest anhand der Tatsache, dass mittlerweile alle vier großen Musikverleger von DRM-Systemen wieder abgekommen sind. Dafür gibt es mit Sicherheit vielfältige Gründe – entscheidend dürfte aber die mangelnde Akzeptanz der Kunden gewesen sein, welche sich vor allem dadurch erklären lässt, dass es bislang eben *das* DRM-System nicht gibt.

Möglicherweise hätte sich eine digitale Rechteverwaltung gerade im digitalen Musikvertrieb durchsetzen können. Immerhin boomt der Markt der Online-Musikshops, wie nicht nur das Beispiel von Apples *iTunes* zeigt (Grimm 2009: 33). Kurzum: entgegen aller Befürchtungen und – vielleicht auch beabsichtigter – Panikmache in Form diverser Szenarien über den Untergang der Musikindustrie gibt es offenbar nach wie vor zahlreiche Kunden, die bereit sind, für ihre Lieblingsmusik zu bezahlen, anstatt sie – fast genauso bequem – kostenlos, wenn auch illegal, aus dem Internet herunterzuladen. Durch die Vielzahl der eingesetzten Systeme ergibt sich für die Kunden allerdings eine nicht unerhebliche Unsicherheit, insbesondere was die Verfügbarkeit der von ihnen erworbenen digitalen Werke betrifft. Denn so bequem wie die Lizenzen für digitale Musik, Texte und Software über das Internet mittlerweile bezogen werden können, so schnell können genau diese Lizenzen auch wieder erlöschen bzw. ihre Gültigkeit verlieren.

Besonders deutlich wird das an dem Fall *Playsforsure* der Firma Microsoft. Kunden, die Musik über Microsofts Onlineshop *msn music* gekauft hatten, sahen sich ab dem 31. August 2008 mit einem Problem konfrontiert. Wenige Monate zuvor hatte Microsoft lapidar mitgeteilt, dass es sein in *msn music* eingesetztes DRM-System *Playsforsure* nicht weiter unterstützen werde. Das Problem: ohne das entsprechende DRM-System lässt sich die legal erworbene Musik nicht weiter nutzen. Für die Kunden von Microsoft bedeutete das im Klartext, dass sie spätes-

tens mit einem Wechsel des Betriebssystems nicht mehr auf ihre gekauften Musiktitel zurückgreifen konnten. Dieser Vorgang zeigt sehr deutlich, wie flüchtig die Lizenzierung von digitalen Inhalten ausfallen kann. Nebenbei bemerkt: Microsofts Problemlösung für die verständlicherweise aufgebrachten Kunden wirkt vor dem Hintergrund, dass es sich um ein DRM-System handelt, besonders paradox: man empfahl den Kunden kurzerhand die in Deutschland illegale Umgehung des in die Musikwerke eingebundenen Kopierschutzes per Anleitung auf der eigenen Internetseite (vgl. Kreutzer 2007: 103ff., 135ff.; Lischka 2008; Microsoft 2009; Pantalog 2008; Schollin 2008: 147).

Der Fall *Playsforsure* verdeutlicht, neben dem Chaos durch die – zumindest bislang – fehlende Standardisierung, die Defizite im Umgang mit DRM-Systemen sowohl bei den Produzenten digitaler Waren als auch deren Kunden. Letztere gehen beispielsweise völlig selbstverständlich davon aus, dass sie über die von ihnen legal erworbenen digitalen Werke im gleichen Umfang frei verfügen können, wie sie es bislang im Umgang mit *stofflichen* Produkten gewohnt waren (vgl. Kreutzer 2001; Lohoff 2007; Meretz 2007: 52ff.).

Ein einfaches Beispiel soll das Dilemma verdeutlichen: Kein Buchhändler wird sich weder ernsthaft darüber beklagen, noch rechtliche Bedenken äußern, für den nicht ganz ungewöhnlichen Fall, dass ein Kunde das bei ihm erworbene Buch weiter verschenkt, verleiht oder gar verkauft. Viele Kunden wissen jedoch nicht, dass sich der Fall bei digitalen Inhalten meist völlig anders verhält. Nehmen wir also an, derselbe Kunde erwirbt ein digitales E-Book. So schließt beispielweise Amazon, der Anbieter des populären E-Books *Kindle*, eine Weitergabe, einen Weiterverkauf und sogar einen Verleih der digitalen Bücher kategorisch über seine Geschäftsbedingungen aus:

> »Unless specifically indicated otherwise, you may not sell, rent, lease, distribute, broadcast, sublicense or otherwise assign any rights to the Digital Content or any portion of it to any third party, and you may not remove any proprietary notices or labels on the Digital Content. In addition, you may not, and you will not encourage, assist or authorize any other person to, bypass, modify, defeat or circumvent security features that protect the Digital Content.« (Amazon 2009)

Und natürlich sichert sich Amazon darüber hinaus auch für den Fall ab, dass das eigene DRM-System nicht mehr weiter zur Verfügung stehen sollte:

> »Your rights under this Agreement will automatically terminate without notice from Amazon if you fail to comply with any term of this Agreement. In case of such termination, you must cease all use of the Software and Amazon may immediately revoke your access to the Service or to Digital Content without notice to you and without refund of any fees. Amazon's failure to insist upon or enforce your strict

> compliance with this Agreement will not constitute a waiver of any of its rights.« (Amazon 2009)

Häufige Kritik gibt es darüber hinaus für DRM-Systeme im Zusammenspiel mit dem gesetzlich geforderten Datenschutz. Grundsätzlich darf dieser zwar nicht berührt werden, tatsächlich gibt es aber in diesem Bereich teilweise erhebliche Defizite.

Beispielweise codierte Apple in seinem DRM-System *Fairplay* für *iTunes* die Apple-Benutzerkennung eines Kunden – in der Regel also dessen E-Mail-Adresse – direkt und unverschlüsselt (!) in die an ihn verkauften digitalen Werke ein. Obwohl dies gesetzlich zwingend erforderlich gewesen wäre, erfuhr der Verbraucher von dieser Praxis nichts im Rahmen des Kaufvorgangs oder innerhalb der Datenschutzerklärung, welcher der Kunde vorab ausdrücklich zustimmen musste. Die erforderliche Transparenz gegenüber den Kunden bezüglich des Einsatzes und der Verwendung derer persönlicher Daten fehlte also. Nebenbei bemerkt – vor diesem Hintergrund betrachtet scheint die Bezeichnung *Fairplay* für Apples DRM-System mehr als paradox (vgl. Bizer 2009: 95ff.; Kreutzer 2007: 103ff.; 135ff.; Mittenzwei 2006: 23ff.).

Aber auch die Kunden bewegen sich beim Thema Kopierschutz und DRM oft in einer rechtlichen Grauzone. Entgegen der häufigen Annahme gibt es beispielsweise kein gesetzlich eindeutig definiertes Recht auf Privatkopien. Zwar wird das Urheberrecht in Bezug auf private Vervielfältigungen eingeschränkt, allerdings ist es unter keinen Umständen erlaubt zu diesem Zwecke einen Kopierschutz zu umgehen. Selbst die Vorbereitung der Umgehung eines DRM-Systems ist nicht zulässig und strafbar. Grundsätzlich verhalten sich die gesetzlichen Regelungen gerade beim Thema Privatkopie sehr schwammig. So gibt es beispielsweise eindeutige Vorgaben für die Privatvervielfältigungen von Büchern, ob damit aber auch Texte die digital zur Verfügung stehen, gemeint bzw. abgegolten sind, bleibt weitgehend offen (vgl. Fränkl 2004: 49ff.; Kronner 2008: 101ff.; von Diemar 2002: 40ff.).

Das Phänomen der sog. Raubkopien ist dabei in jeder sozialen Schicht und auch unabhängig vom Alter anzutreffen. Dies begründet sich vor allem darin, dass für die Vervielfältigung kein spezielles Verständnis oder Wissen benötigt wird. Grundlegende Kenntnisse im Umgang mit dem Heim-Computer und der entsprechenden Software reichen völlig aus (vgl. Kühne 2009: 32). Die Beweggründe, unberechtigte Kopien zu erstellen, sind dabei durchaus unterschiedlich. Vielen Raubkopierern geht es nicht in erster Linie um die digitalen Inhalte selbst, sondern eher um Anerkennung in einer Art Wettbewerb um digitalen Medien und um deren Neuheit und Menge. Aber natürlich spielen auch finanzielle Interessen eine Rolle, was sich letztlich auch im Umsatzrückgang z.B. der Musikindustrie widerspiegelt. Schließlich, aber sehr wesentlich, führen die neuesten technischen Entwicklungen, die von den Produzenten digitaler Medien angetrieben werden, dazu, dass die Vervielfältigungsmöglichkeiten zunehmend simpler werden und gleichzeitig sinkt die Hemmschwelle der Konsumenten, illegal zu kopieren. In diesem Zu-

sammenhang sind vor allem das MP3-Format und die diversen Onlineshops zu erwähnen, das Video on Demand-Verfahren (VoD) im Filmbereich sowie Hörbücher und E-Books auf dem Literaturmarkt (vgl. ebd.: 36-40).

Die Medienproduzenten setzen deshalb zunehmend auf die Entwicklung von neuen Kopierschutzmechanismen. Das Problem ist nur, dass parallel dazu die entsprechende illegale Kopiersoftware entwickelt wird, bzw. »Hacker« vor allem über das Internet sehr zeitnah Möglichkeiten zur Umgehung solcher Schutzmechanismen preisgeben. Da die Effektivität der Kopierschütze deshalb nur sehr begrenzt ist, setzen vor allem die großen Produzenten parallel dazu auf die Sensibilisierung der Konsumenten durch *Aufklärungskampagnen*, die dem Verbraucher verdeutlichen sollen, dass Raubkopieren eine Straftat darstellt (vgl. ebd. 63ff.; Krempl 2004b).

Eine weitere Maßnahme stellen Urheberrechtserweiterungen des Gesetzgebers dar. Zwar bleiben Privatkopien weiter zulässig, allerdings nur dann, wenn das Originalmedium vorliegt und für eine Kopie nicht ein Kopierschutz umgangen werden muss (vgl. ebd.: 66ff.; Meretz 2007: 77). »Auf der einen Seite sind Privatkopien erlaubt, gleichzeitig ist aber nicht erlaubt, einen Kopierschutz zu umgehen, womit das eine das andere relativiert« (Kühne 2009: 107).[11] Schließlich gibt es heutzutage nahezu kein Medium mehr, das nicht mit einem Kopierschutz versehen ist. Tatsächlich liegt das Problem auf Seiten der Medienproduzenten. Diese haben offensichtlich schlichtweg den Zeitpunkt verpasst, ihren Angebote dem heutigen digitalen Umfeld anzupassen (vgl. ebd.: 108f.; Lodigkeit 2006: 98ff.).

Zusammenfassend lässt sich festhalten, dass DRM-Systeme insbesondere durch die Musikindustrie eingesetzt wurden, aber bereits kurze Zeit später – vor allem auf Grund mangelnder Akzeptanz durch die Verbraucher – wieder vom Markt verschwanden. So bietet beispielsweise Apples *iTunes* seit Anfang 2009 fast sein gesamtes Sortiment DRM-frei an.[12] Auch der Mitbewerber *Musicload* hat nachgezogen.

Beliebt war und ist die digitale Rechteverwaltung verständlicherweise nie beim Verbraucher, da sie ihn einschränkt (Kühne 2009: 98ff.). Allerdings auch deshalb, weil es keinen einheitlichen Standard gibt, der die permanente Verfügbarkeit sichert. Während ein Buch mit relativ hoher Wahrscheinlichkeit auch noch in 100 Jahren gelesen werden kann, verhält sich dies mit einem E-Book anders und setzt zumindest voraus, dass das entsprechende DRM-System noch läuft und die erworbene Lizenz auch noch Gültigkeit besitzt.

11 Vgl. dazu den Beitrag von Martin Senftleben im Heft »Kulturen des Kopierschutzes I«.

12 Siehe dazu auch: http://www.pcwelt.de/it-profi/business-ticker/76271/drm_freie_songs_branche_bejubelt_emi_und_apple/, 05.10.2009.

8. ARGUMENTE GEGEN EINEN KOPIERSCHUTZ DIGITALER INHALTE UND GRÜNDE FÜR DEN MISSERFOLG VON DRM-SYSTEMEN

Technische Entwicklungen der vergangenen Jahrzehnte haben zu tiefgreifenden Veränderungen und Fortschritten bei Vervielfältigungs- und Übermittlungstechniken von Werken aller Art geführt. Auch wenn einzelne technische Entwicklungen für sich alleine genommen keine größeren Auswirkungen hatten, so haben diese in Kombination doch erhebliche Veränderungen bewirkt (vgl. Höhne 2007: 2). DRM stellt kein klassisches und eindeutiges Verfahren zum Schutz und der Verwaltung von Rechten oder der Wahrung eines Kopierschutzes dar, sondern beschreibt vielmehr eine komplexe Infrastruktur, die auf verschiedenen Basistechnologien aus unterschiedlichen Bereichen basiert. Zum technischen Verständnis von DRM ist daher die Kenntnis solcher klassischen Technologien erforderlich.

In der digitalen Zeit ist es in der Regel leicht, Kopien von Daten jeglicher Art anzufertigen.[13] Die Maßnahmen, die unternommen werden, um das Kopieren zu unterbinden oder zumindest zu erschweren, sind enorm aufwendig und kostenintensiv. Allerdings sind sie in der Regel auch bereits nach kurzer Zeit wieder veraltet bzw. können mit vergleichsweise geringem Aufwand umgangen werden (vgl. Kühne 2009: 107ff.). Das Thema wird kontrovers diskutiert.

Insbesondere das »Recht auf Privatkopie« wird in diesem Zusammenhang regelmäßig aufgegriffen. So kritisiert beispielsweise der *Chaos Computer Club* (CCC), dass Konsumenten, insbesondere durch die Kampagnen der Musik- und Filmindustrie, regelrecht zu potenziellen Straftätern abgestempelt werden. Auch das Urheberrecht steht in der Kritik, da es das Grundrecht auf Informationsfreiheit einschränke[14] (vgl. Kühne 2009: 78ff.). Der CCC ruft sogar zum Boykott der Musikindustrie auf, weil der Verein der Industrie unterstellt, die Verkaufserlöse zu einem wesentlichen Teil zur Finanzierung von Klagen und für die Entwicklung neuer Kopierschütze einzusetzen. Die Gründe für die sinkenden Verkaufszahlen sieht der CCC in den zu hohen Preisen für CD und DVD bei gleichzeitig gesunkener Qualität. Außerdem hindere der Kopierschutz oftmals den Konsumenten daran, die legal erworbenen Inhalte auf dem eigenen CD-Player wiederzugeben. Auch die Initiative »Recht auf Privatkopie«[15] setzt sich gegen die Beschränkungen durch das Urheberrecht ein.

Andererseits ist ein ökonomischer Schaden durch unerlaubte Vervielfältigungen nicht zu leugnen.[16] Auch Bibliotheken und Informationszentren, aber auch Vi-

13 Eine Ausnahme stellen hier beispielweise viele strategisch wichtige staatliche Dokumente dar, zu deren Verschlüsselung und Geheimhaltung von Seiten der offiziellen Stellen erheblicher Aufwand betrieben wird. Siehe dazu den Beitrag von Ludwig Andert und Doris Ortinau im Heft »Kulturen des Kopierschutzes I«.

14 Weitere Informationen zum *Chaos Computer Club*: http://www.ccc.de, 27.10.2009.

15 Vgl.: http://www.privatkopie.net, 13.11.2009.

16 Vgl.: http://www.musikindustrie.de/jwb_musikkopien07.html, 13.11.2009.

deotheken leiden unter Raubkopien. Beschränkte sich die illegale Vervielfältigung erst noch auf das Kopieren von Büchern oder Zeitschriften mit einem herkömmlichen Fotokopierer, nehmen nun die Diebstähle digitaler Inhalte zu. Natürlich untersagen die entsprechenden Institutionen diese Nutzung in ihren Allgemeinen Geschäftsbedingungen. Allerdings nimmt der Verkauf solcher Medien parallel über neue Distributionswege zu.[17] Dass der ökonomische Schaden allein auf die Verbreitung entsprechender Kopiersoftware zurückzuführen ist, darf also bezweifelt werden.

Zumindest muss bedacht werden, dass der CCC mit seiner Kritik an der Qualität durchaus nicht Unrecht hat. Zudem sind Online-Musikshops ja durchaus erfolgreich und wären möglicherweise bei einem entsprechend größerem Angebot (wie es beispielsweise von Tauschbörsen angeboten wird) noch wesentlich populärer. Jedenfalls scheint es zu einfach, den Verbrauchern zu unterstellen, dass sie nicht mehr bereit wären, für digitale Inhalte zu bezahlen.

Generell lässt sich feststellen, dass DRM-Systeme zusammen mit einer Ausweitung des Urheberrechts zu einer deutlichen Verschlechterung des Verbraucherschutzes geführt haben, da Nutzungsbedingungen digitaler Werke nun über Vertragswerke und nicht mehr über das Urheberrecht allein geregelt werden (vgl. Strube 2008; Akester 2010). Dies hat zur Folge, dass die Rechteinhaber, also die Produzenten digitaler Werke, sich in einer – entgegen der von ihnen selbst oftmals öffentlich inszenierten Darstellung – sehr starken Position gegenüber dem Nutzer befinden. Auch Bürger- und Datenschutzrechte werden von Rechteverwaltungssystemen tangiert, denn »wenn etwa DRM-Systeme überwachen sollen, dass nur bestimmte, berechtigte Personen einen Inhalt nutzen, heißt das auch, dass sie wissen müssen, wer sie nutzt« (Spielkamp 2005). Darüber hinaus sind die, wie bereits erwähnt, fehlenden Standards bei den derzeit eingesetzten DRM-Systemen alles andere als verbraucherfreundlich. Praktisch muss für jeden digitalen Content ein eigenes DRM-System installiert werden und bei einem Anbieterwechsel wird in der Regel sogar die Anschaffung neuer Abspielgeräte zwingend erforderlich (Höhne 2007: 250ff.).

Schon deshalb scheint es nur konsequent, dass auch über völlig neue Bezahlsysteme für digitale Inhalte diskutiert wird (vgl. Umeh 2007). So gibt es beispielsweise Überlegungen, pauschale Abgaben für Breitbandanschlüsse oder Abspielgeräte einzuführen, ähnlich dem in Deutschland bestehenden Rundfunkgebührensystem (Krempl 2004a; Spielkamp 2004). Allerdings werden auch weiter Alternativen zu den derzeit eingesetzten DRM-Systemen gesucht. So wurden etwa in Deutschland von der Fraunhofer Gesellschaft zwei Systeme entwickelt, die auf unterschiedlichen Konzepten basieren:

Das sog. *Light Weight Digital Rights Management* (LWDRM)[18] implementiert ein DRM-System, welches dem Nutzer mehr Freiheiten insbesondere bei der

17 Vgl.: http://www.ivd-online.de/f_markt.html, 10.11.2009.

18 Vgl.: http://www.emt.iis.fhg.de/de/projekte_themen/ lwdrm.htm, 20.11.2009.

Weitergabe digitaler Inhalte einräumt. Allerdings hat es wieder einen entscheidenden Nachteil, da LWDRM die digitalen Inhalte in einem eigenen Dateiformat verschlüsselt, so dass diese nur auf speziellen Wiedergabegeräten wieder entcodiert werden können.

Das zweite alternative System *Potato*[19] arbeitet dagegen völlig ohne Verschlüsselung und Markierung digitaler Inhalte und versucht deren unberechtigte Weitergabe allein über wirtschaftliche Anreize zu minimieren. So erhalten Nutzer Verkaufsprovisionen, wenn sie ein legal erworbenes digitales Werk anstatt über Tauschbörsen im Rahmen eines speziell zur Verfügung gestellten Reseller-Systems anderen Nutzern zur Verfügung stellen. Letztere müssen dafür allerdings bezahlen. Gerade das Potato-Modell scheint dabei zumindest für populären digitalen Content vielversprechend zu sein, ist derzeit aber nicht besonders praktikabel, da auch für dieses – wie schon für die bereits eingesetzten DRM-Systeme – noch keine einheitlichen Standards existieren. Eine dauerhafte Lösung, die verbraucherfreundlich ist und zugleich Profite einbringt, die also gleichermaßen attraktiv für die Konsumenten als auch die Produzenten digitaler Inhalte ist, scheint jedenfalls in naher Zukunft nicht in Sicht (vgl. Grimm et al 2002; Höhne 2007: 76ff.; Kühne 2009: 83ff., 110ff.; Nützel 2003).

LITERATURVERZEICHNIS

Abie, Habtamu (2009): *Distributed Digital Rights Management: Frameworks, Processes, Procedures and Algorithms*, Saarbrücken: VDM Verlag.

Agnew, Grace (2008): *Digital Rights Management: A Librarian's Guide to Technology and Practise*, Oxford: Chandos Publishing (Oxford) Limited.

Akester, Patricia (2010): »The Impact of Digital Rights Management on Freedom of Expression: the First Empirical Assessment«, in: *IIC: International Review of Intellectual Property and Competition Law,* Bd. 41, Nr. 1, S. 31-58.

Amazon (2009): »Amazon Kindle: License Agreement and Terms of Use«, http://www.amazon.com/gp/help/customer/display.html?nodeId=20014453, 11.09.2009.

Bizer, Johann (2009): »Datenschutzgerechte Rechteverwaltung«, in: Roßnagel, Alexander (Hg.): *Digitale Rechteverwaltung*, Baden-Baden: Nomos, S. 91-104.

Eggert, Denis (2005): *Digital Music Service, Digital Rights Management & Alternativen. Bestandsaufnahme, Analyse und Perspektiven des deutschen Marktes*, Bochum: projektverlag.

Fränkl, Gerald (2005): *Digital Rights Management in der Praxis. Hintergründe, Instrumente, Perspektiven, (und) Mythen,* Berlin: VDM Verlag Dr. Müller.

19 Vgl.: http://www.idmt.fraunhofer.de/de/projekte_themen/ potato.htm, 20.11.2009 sowie http://www.potatosystem.com/de/, 10.01.2010.

Fränkl, Gerald / Karpf, Phlipp (2004): *Digital Rights Management Systeme. Einführung, Technologien, Recht, Ökonomie und Marktanalyse,* München: Pg Medien.

Grassmuck, Volker (2004): *Freie Software. Zwischen Privat- und Gemeineigentum*, Bonn: bpb.

Grimm, Rüdiger (2009): »Digitale Rechteverwaltung als Techniksystem«, in: Roßnagel, Alexander (Hg.): *Digitale Rechteverwaltung*, Baden-Baden: Nomos, S. 27-38.

Grimm, Rüdiger / Nützel, Jürgen (2002): »A Friendly Peer-to-Peer File Sharing System with Profit but without Copy Protection«, in: Unger, Herwig et al. (Hg.): *Innovative Internet Computing Systems*, Berlin: Springer-Verlag, S. 133-142.

Höhne, Sven (2007): *Digital Rights Management System aus Verbrauchersicht. Eine urheberrechtliche Untersuchung der Folgen des Einsatzes von Digital Rights Management Systemen*, Norderstedt: Books on Demand GmbH.

Krempl, Stefan (1998): »Copyright«, http://www.heise.de/tp/r4/artikel/2/2471/1.html, [17.11.1998], 18.12.2009.

Krempl, Stefan (2001): »Kopieren verboten«, http://www.heise.de/tp/r4/artikel/4/4756/1.html, [24.01.2001], 18.11.2009.

Krempl, Stefan (2004a): »Alternatives Kompensationssystem für Künstler verzweifelt gesucht«, http://www.heise.de/newsticker/meldung/Alternatives-Kompensationssystem-fuer-Kuenstler-verzweifelt-gesucht-92745.html, [01.02.2004], 18.12.2009.

Krempl, Stefan (2004b): »Raubkopierer sind immer noch Verbrecher«, http://www.heise.de/tp/r4/artikel/18/18923/1.html, [30.11.2004], 18.12.2009.

Kreutzer, Till (2001): »Selbsthilferecht zum Umgehen von Kopierschutz. Die Zukunft der privaten Nutzung nach der Umsetzung der europäischen Urheberrechts-Richtlinie«, http://www.heise.de/tp/r4/artikel/9/9817/1.html, [18.10.2001], 05.12.2009.

Kreutzer, Till (2007): *Verbraucherschutz bei digitalen Medien*, Berlin: Berliner Wissenschafts-Verlag.

Kronner, Ralf (2008): *Digitaler Werktransfer: Zum Interessengleichgewicht zwischen Verwertern, Nutzern und dem Gemeinwohl*, Berlin: Olaf Gaudig & Peter Veit GbR.

Kühne, Sascha (2009): *Phänomen Raubkopie. Illegale Vervielfältigung von Medien im Digitalen Zeitalter,* Saarbrücken: VDM Verlag Dr. Müller.

Lischka, Konrad (2008): »DRM-Debakel. Bürgerrechtler wüten gegen Microsoft-Musik mit Verfallsdatum«, http://www.spiegel.de/netzwelt/web/0,1518,550686,00.html, [30.04.2008], 20.08.2009.

Lodigkeit, Klaus (2006): *Intellectual Property Rights in Computer Programs in the USA and Germany*, Frankfurt a.M.: Peter Lang GmbH.

Lohoff, Ernst (2007): »Der Wert des Wissens«, http://www.krisis.org/2007/der-wert-des-wissens/print/, 05.12.2009.

Meretz, Stefan (2007): »Der Kampf um die Warenform. Wie Knappheit bei Universalgütern hergestellt wird«, in: *krisis. Beiträge zur Kritik der Warengesellschaft*, Nr. 31.

Microsoft (2009): »Informationen über Windows Media DRM«, http://www.microsoft.com/windows/windowsmedia/de/drm/default.aspx, 26.10.2009.

Mittenzwei, Julius (2006): *Informationen zur Rechtewahrung im Urheberrecht. Der Schutz von Digital Rights Management-Systemen und digitalen Wasserzeichen durch § 95c UrhG*, München: GRIN Verlag.

Nützel, Jürgen (2003): »Wie kann man mit dem Potato-System eine Ware verkaufen, die alle schon haben?«, http://www.4fo.de/download/Tonmeister02_Nuetzel.pdf, [20.05.2003], 10.01.2010.

Pantalog, Frank (2008): »Amazon komplett DRM-frei. Kopierschutz ist tot«, http://www.spiegel.de/netzwelt/web/0,1518,527992,00.html, [11.01.2008], 15.08.2009.

Roßnagel, Alexander (2009): »Digitale Rechteverwaltung - Ein gelungenes Beispiel für die Allianz von Recht und Technik?«, in: Roßnagel, Alexander (Hg.): *Digitale Rechteverwaltung*, Baden-Baden: Nomos, S. 15-26.

Schippan, Martin (2004): »Rechtsfragen bei der Implementierung von Digital Rights Management-Systemen«, in: *Zeitschrift für Urheber- und Medienrecht*, Ausgabe 3/2004, S. 188-198.

Schollin, Kristoffer (2008): *Digital Rights Management. The New Copyright*, Stockholm: Jure Förlag.

Singh, Simon (2000): *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*, München.

Spielkamp, Matthias (2004): »Mit Technik allein lässt sich DRM nicht durchsetzen«, http://www.heise.de/tp/r4/artikel/16/16673/1.html, [03.02.2004], 05.01.2010.

Spielkamp, Matthias (2005): »Rechte oder Restriktionen?«, http://irights.info/index.php?id=140, [01.04.2005], 11.01.2010.

Strube, Jochen (2008): »Der Einfluss von Digital Rights Management auf die Zahlungsbereitschaften für Online-Musik: Untersuchung auf Basis einer Conjoint-Analyse«, in: *Medienwirtschaft*, Bd. 5, Nr. 4, S. 6-15.

von Diemar, Undine (2002): »Die digitale Kopie zum privaten Gebrauch«, in: *Schriftenreihe der Stipendiatinnen und Stipendiaten der Friedrich-Ebert-Stiftung*, Band 17.

Tsolis, Dimitrios (2009): *Digital Rights Management for E-commerce Systems*, Hershey u.a.: Information Science Reference.

Umeh, Jude C. (2007): *The World Beyond Digital Rights Management*, Swindon: British Computer Society.

Zeng, Wenjun (2006) (Hg.): *Multimedia Security Technologies for Digital Rights Management*, Amsterdam: Academic Press.

CAGING THE COPYCAT

Wie neue Technologien eingeschränkt werden. Eine Fallstudie: Das *Google Book Search Settlement*

VON BRIAN WINSTON

»In staubigen Winkeln und abgelegenen Bücherregalen schuften von Google beauftragte Teams, um digitale Kopien von Büchern anzufertigen. Bis heute hat Google 10 Millionen Titel aus amerikanischen und europäischen Bibliotheken eingescannt.«
(Sidelsky 2009: 20)

Der Plan von Google, eine allumfassende und freie Online-Bibliothek zu schaffen, wurde 2002 ausgebrütet und beinhaltet nicht weniger als die digitale Aneignung aller vergriffenen Bücher der Welt. Für einen großen Teil dieser Bücher gilt, dass sie sowohl vergriffen sind als auch, dass es für sie kein Verwertungsrecht mehr gibt; sie sind ›public domain‹, was bedeutet, dass deren Vervielfältigung, abgesehen von der Arbeit des Einscannens, kein unmittelbares Problem darstellt. Andererseits gibt es eine bedeutend höhere Anzahl von attraktiven und nützlichen Titeln, die zwar vergriffen, deren Verwertungsrecht aber noch nicht ausgelaufen ist, obgleich keinerlei kommerzielle Verwertung mehr an ihnen hängt und die Rechtsinhaber oft nicht identifiziert und gefunden werden können. Diese ›verwaisten‹ Werke bereiteten einige Probleme. Das Verwertungsrecht von Werken, die noch kommerziell genutzt werden, steht nicht zur Disposition und Google stellt sein Projekt nicht als einen Angriff auf das Prinzip des Copyrights dar, sondern vielmehr als eine öffentliche Dienstleistung, die diese ›verwaisten‹ Titel ›zum besten der Gesellschaft‹ wiederveröffentlicht. Googles altruistische Ambitionen bestanden – nach Angabe eines leitenden Managers – darin, »die Grenzen des menschlichen Wissens zu erweitern«. Dan Clancy, der für dieses Vorhaben verantwortlich ist, sagte: »Ich musste mich gegenüber den Firmengründern niemals für die Höhe meiner Ausgaben rechtfertigen.«

Gleichwohl – Ironie des Schicksals – wurde Google bald herausgefordert. 2005 strengten die Authors Guild of America und die Association of American Publishers einen ›class action suit‹[1] gegen Google an, um die Verwertungsrechte

1 Ein ›class action suit‹ ist ein amerikanisches Rechtsmittel, das es erlaubt, auch Personen in einen juristischen Prozess einzubeziehen, die nicht anwesend, nicht identifizierbar oder sich dieser Einbeziehung gar nicht bewusst sind. Diese ›virtuelle Repräsentation‹ erlaubt es einem Kläger (in diesem Fall die Gruppenorganisationen, die die Autoren und Verlage repräsentieren) eine dritte Partei (in diesem Fall Google) zu verklagen (in diesem Fall wegen einer Verletzung des Urheberrechts) – und zwar im Namen sowohl al-

an diesen ›verwaisten‹ Werke zu schützen. Die Unternehmenskultur von Google scheint in dem Sprichwort ›Es ist besser, um Vergebung zu bitten als um Erlaubnis‹ zu wurzeln. In diesem Fall war es so, dass die Bitte um Vergebung sich als ein ein viele, viele Monate dauerndes, komplexes (wenn nicht, wie manche fanden, unverständliches[2]) juristisches Tauziehen hinter den Kulissen darstellte, an deren Ende das 385-seitige *Book Search Settlement* stand. Dieses wurde von Google, den Autoren und den Verlagen, unter der Kontrolle der US-amerikanischen Gerichte,[3] am 28. Oktober 2008 unterzeichnet. Dank dieser beiden unerwarteten ›Stiefeltern‹ hatte Google nun Zugriff auf die ›Waisen‹. Die Übereinkunft kostet Google 45 Millionen Dollar bei einer Gebühr von 60 Dollar pro Buch. Mit anderen Worten: die Vereinbarung verschafft Google 750.000 Titel. Für den Fall, dass Google nun mehr Titel wollte, müsste in Höhe des gleichen Satzes – also 60 Dollar pro Buch – nachgekauft werden; da diese Titel aber ›verwaist‹ sind, was bedeutet, dass kein offensichtlich Begünstigter in Sicht ist, ist es nicht sehr wahrscheinlich, dass die 45 Millionen Dollar jemals ausgeschöpft werden (vgl. *Book Settlement Agreement* 2008: 19-20). Dies war der Preis der ›Vergebung‹.

Andere Stimmen aber blieben feindselig und misstrauisch, indem sie in den guten Absichten Googles nichts anderes sahen als einen schwerwiegenden ‚Raubzug', der eine große Menge von – zugegebenermaßen – etwas unzugänglichem, aber gleichwohl umsonst erhältlichem Material – zumindest potenziell – in eine proprietäre Ressource von Google verwandelte. Entgegen der Firmenrhetorik gab es eindeutig die Möglichkeit, dass langsam aber sicher der Zugriff auf diese Texte eingeschränkt würde, damit sich die Investition auch auszahlte. So wurde Google durch das *Settlement* erlaubt, »Anzeigen auf Vorschauwebseiten und anderen Online-Buch-Seiten« zu schalten (*Book Settlement Agreement* 2008: 41); und man darf nicht vergessen, dass Googles Verantwortlichkeit gegenüber den Anteilseignern Profitmaximierung verlangt. Obwohl das *Settlement* lediglich ›nichtexklusive Digitalisierungsrechte‹ regelt, war man allgemein der Ansicht, dass es *de facto* Google ein Monopol gewähren würde, da von keiner anderen Organisation erwartet werden konnte, eine konkurrierende Online-Bibliothek mit diesen Titeln aufzuziehen.

Doch auch ohne dass diese Androhungen wahr geworden wären, wurde das *Agreement* als rechtlich unbefriedigend angefochten. Am 18. September 2009, als der Bezirksgericht des südlichen Bezirks von New York über das *Settlement* beriet, griff das Justizministerium ein. Wie viele andere Kritiker glaubt es auch, dass

ler ihrer Mitglieder als auch derjenigen, die zu der ›class‹ der Autoren und Verleger gehören, auch wenn diese nicht notwendigerweise bekannt sein müssen.

2 Es gibt beispielsweise nicht weniger als 160 besondere Definitionen der Vertragskonditionen (viele davon speziell hierfür geprägt), die 17 Seiten des Dokuments einnehmen. (*Settlement Agreement*, S. 2-19).

3 Diese ist obligatorisch, da die ›class action‹ gegen Google vor Gericht verhandelt wurde. Das Gericht muss sich daher davon überzeugen, dass beide Parteien die Angelegenheit befriedigend gelöst haben.

»das *Settlement* ernsthafte rechtliche Fragen aufwirft und hat das Gericht gedrängt, es nicht ohne Änderungen zu bestätigen«: Das Justizministerium sagt, dass das *Settlement* Google eigentlich eine exklusive Lizenz auf Millionen von vergriffenen, ›verwaisten‹ Büchern gewähren würde, deren Rechteinhaber unbekannt sind oder nicht gefunden werden können. Dies macht es anderen unmöglich, eine ähnliche digitale Bibliothek aufzubauen (vgl. Helft 2009).

Für viele technologische Deterministen – oder ›Technizisten‹ – stellt diese ganze rechtliche Tatktiererei nichts anderes als den Versuch dar, eine unaufhaltbare Welle des technologischen Fortschritts aufzuhalten. Ihrer Ansicht nach muss er sich als vergeblich herausstellen. So erklärt der Kulturtheoretiker und -kritiker Raymond Williams (1989: 120), Technizisten glaubten, dass neue Technologien (wie die Digitalisierung) durch einen im Wesentlichen internen Prozess von Forschung und Entwicklung entdeckt werden, der dann die Bedingungen von sozialem Wandel und Fortschritt setzt.

Solche allgemein anerkannten Meinungen implizieren, dass alte Konzepte, wie etwa das Urheberrecht, im Zeitalter der digitalen Reproduktion nicht überleben können, da sie inadäquate Antworten auf veränderte Umstände darstellen. Sie sind nicht länger ›zweckmäßig‹. Angesichts der Mühelosigkeit, mit der Duplikate angefertigt und verbreitet werden können, ist die ganze Idee, Originale davor zu schützen, kopiert zu werden, völlig töricht. In diesem Licht ist das *Book Search Settlement* ein perfektes Beispiel dafür, dass die Gesellschaft darauf angewiesen ist, zu klären, wie sie mit Technologie umgeht.

Gleichwohl konstatiert Raymond Williams, dass der Technizismus hier irrt und ein anderer Blickwinkel auf den Fall möglich ist. Technologie existiert in der sozialen Sphäre, nicht außerhalb; und sie wird durch diese Sphäre bestimmt und determiniert. Im Gegensatz zu der Idee, dass Technologie die Gesellschaft überrumpelt, ist das, was im Google-Fall passiert ist, ein Beispiel für die genaue Umkehrung der Annahmen der Technizisten: Die Gesellschaft (indem sie – was nicht ungewöhnlich ist – die Justiz einsetzt) schränkt das Potenzial dieser Technologie ein und setzt ihm Grenzen. Mit anderen Worten: Das Soziale drückt sich aus, indem es sich durch das Recht vertreten lässt – hier durch das Urheberrecht. Dieses bestimmt die Art und Weise der Verbreitung dieser Technologie – in diesem Fall der Versuch von Google, das Potenzial der Digitalisierung auszubeuten. Wonach bei diesem Tauziehen gesucht wird, ist ein *modus vivendi*, durch den das erschütternde Potenzial dieser Technologie beschränkt werden kann. Ich meine, dass dies tatsächlich der Fall ist. Meine Hypothese ist, dass – entgegen den allgemein anerkannten Ansichten der Technizisten – das Soziale der primäre Antrieb ist, der die Ausbreitung von Kommunikationstechnologien bestimmt und determiniert; und dies ist seit dem Telegraphen so. Der Fall Google bestätigt ein altbekanntes Muster der Technologiegeschichte.

Man kann sagen, dass sich der Westen in den letzten 500 Jahren in einer Balance zwischen der üblichen Tendenz des Menschen gegenüber Wandel und Umbruch einerseits und einer spezifischen Innovationsfreundlichkeit andererseits be-

fand – eine ungewöhnliche Toleranz und Akzeptanz gegenüber dem technologischen Fortschritt. In der Tat könnte diese Innovationsfreundlichkeit[4] – die sich in der Menschheitsgeschichte nicht häufig so bleibend manifestiert hat – eine Schlüsselrolle für die technologische Dominanz spielen, die vom Westen in der Moderne erreicht wurde. Sie ist tatsächlich das Alleinstellungsmerkmal der Moderne; aber da die menschliche Natur nun einmal ist, was sie ist, ist ihr Absolutheitsanspruch nicht unangefochten. Trotz der Sympathie für neue Dinge gibt es weiterhin einen gewissen Argwohn, wenn nicht Feindschaft, gegen Veränderungen. Der Historiker der *Annales*, Fernand Braudel, beschreibt diese Spannung in den Begriffen der Beschleunigung und des Abbremsens:

> »Die Technik kann die Entwicklung beschleunigen oder bremsen und übt oft genug beide Wirkungen nacheinander aus. Sie treibt das Leben voran, bis in kleinen Schritten auf einer höheren Stufe ein neues Gleichgewicht erreicht ist, und bleibt dann entweder lange auf dieser Stufe stehen, d. h. stagniert oder schreitet unmerklich von einer ›Revolution‹ oder Neuerung zur nächsten fort.« (Braudel 1985: 468)

›Beschleuniger‹ ist eine Metapher für Innovationsfreundlichkeit, die die end- und ruhelose Suche der modernen westlichen Zivilisation nach Innovation in Gang hält.

Der Technizist, im Griff der Innovationsfreundlichkeit, sieht in der Ausbreitung von Innovationen einen vergleichsweise unproblematischen Aneignungsprozess, der zu einem revolutionären sozialen Wandel führt; aber eine solche Sichtweise ist unempfindlich gegenüber der Stärke des menschlichen Widerstands und Argwohns gegenüber Veränderungen. Sie ignoriert die Komplexität der menschlichen Gesellschaft und ist nicht in der Lage, die Hartnäckigkeit sozialer Ordnungen und Gewohnheiten anzuerkennen. Kurz gesagt: Der Technizismus berücksichtigt nicht Braudels ›Bremse‹, also die menschliche Natur und die sozialen Strukturen, die sie ausdrücken.

Diese ›Bremse‹ wird gemeinhin ignoriert, denn die Rhetorik der ›Informationsrevolution‹ besteht schrill darauf, dass lediglich der ›Beschleuniger‹ von Bedeutung ist. Das Technologische wird hierbei als das angesehen, das die Art und Weise, in der wir leben, entscheidend bestimmt. Es wird für alle Bereiche und Zwecke als allmächtig wahrgenommen; aber solch ein Technizismus, so überzeugend er auch klingen mag, ist, laut Raymond Williams, nicht dazu geeignet, eine Erklärung des technologischen Wandels zu geben. Er ist falsch, da er sowohl den Grad ignoriert, in dem die Agenda der Innovationen durch die gesellschaftliche Sphäre bestimmt wird, als auch das Maß, in dem Innovationen darauf angewiesen sind, den realen gesellschaftlichen Bedürfnissen zu begegnen, wenn sie sich vollständig ausbreiten sollen.

4 [Im Original deutsch (A. d. Ü.)]

Tatsächlich wird Innovation durch gesellschaftliche Faktoren bestimmt und gebändigt; die Ausbreitung jeglicher Innovation hängt wesentlich davon ab, wie effektiv sie diese Beschränkungen überwindet und trotzdem vorbestimmten sozialen Bedürfnissen entgegenkommt.

Braudels ›Beschleuniger‹ sollte daher nicht nur in Begriffen der Technologie gedacht werden, sondern als technologischer Ausdruck der Antwort auf ein gesellschaftliches Bedürfnis; eine soziale Notwendigkeit, die tatsächlich den letztlichen Erfolg – also die Ausbreitung – der technologischen Forschungs- und Entwicklungsagenda bestimmt. Solche gesellschaftlichen Notwendigkeiten können vielgestaltig sein. Eine Technologie (z.B. die Eisenbahn) kann die Entwicklung einer anderen Technologie notwendig machen (z.B. eine nichtzeitversetzte elektrische Signalübertragung: der Telegraph); oder sie kann mehr in der Natur gesellschaftlicher Kräfte liegen, wie etwa die Notwendigkeit, den bürgerlichen, städtischen Massen des neunzehnten Jahrhunderts ein Unterhaltungsangebot bereitzustellen, das zu der eigentlichen Mechanisierung der Theater-Unterhaltung führte; erst in Form des Kinos, dann des Rundfunks (vgl. Winston 1996: 32-35; Winston 1998: 24, 77-78).

Ohne die umgestaltende Kraft einer neu entstandenen gesellschaftlichen Notwendigkeit in irgendeiner Form bleibt die technologische Forschung und Entwicklung unfruchtbar – ganz gleich, wie effektiv sie für sich genommen auch sein mag; ihre Ergebnisse sind dazu verdammt, als wissenschaftliche Kuriositäten oder Spielzeuge zurückgewiesen zu werden. Entsteht nun eine neue soziale Notwendigkeit, stehen die Chancen für eine erfolgreiche Ausbreitung der Innovation gut; trotzdem wird auch hier ›gebremst‹. Es gibt ein (fast kann man sagen) ›soziales Gesetz‹, das das erschütternde Potenzial von Innovation unterdrückt.

Obwohl der Innovation eine ziemlich erschütternde Kraft innewohnt – denn sie kommt einer neu entstandenen gesellschaftlichen Notwendigkeit entgegen, die einen gesellschaftlichen Wandel herbeiführen kann –, wird diese auch eingeschränkt, denn die beunruhigendsten Aspekte ihres Potenzials werden gebändigt und tatsächlich unterdrückt, um sicherzustellen, dass die Veränderung nicht zu erschütternd ausfällt. Daraus geht hervor, dass Innovationen in den Kommunikationstechnologien – und dies mehr oder weniger beständig – weit häufiger evolutionärer denn revolutionärer Natur sind. Dies ›Gesetz‹ der Unterdrückung des radikalen Potenzials entspricht der ›Bremse‹ Braudels, wie die ›neu entstandene gesellschaftliche Notwendigkeit‹ seinem ›Beschleuniger‹ entspricht.

Die Spannung zwischen diesen beiden Tendenzen offenbart sich auch im Fall von Google und den ›verwaisten Büchern‹. Weit davon entfernt, den unaufhaltbaren Fortschritt des Digitalen zu verkörpern, zeigt dieser Fall, wie technologische Auswirkungen verlangsamt und gezwungen werden, mit vorher existierenden sozialen Formationen konform zu gehen. Natürlich gibt es einen Antrieb – eine neu entstandene gesellschaftliche Notwendigkeit – auf Seiten von Google, nämlich die etablierten kulturellen Funktionen des Schreibens, Lesens und der

Bibliotheken; kurzum: Ein Gespür dafür, dass es ein soziales ›Gut‹ ist, Wissen erhältlich zu machen.

Darüber hinaus hat Google die Unangemessenheit des Urheberrechts auf seiner Seite. Allein schon die Tatsache, dass die genannten Bände ›verwaist‹ heißen, weist auf ein uraltes Problem des Urheberrechts hin:

Es war einmal eine Zeit, in der es drei Wahrheiten gab:

1.) Verwertungsrechte galten nur über einen verhältnismäßig kurzen Zeitraum.
2.) Sie mussten erneuert werden (die meisten Leute taten dies nicht).
3.) Man bekam keine Verwertungsrechte eingeräumt, wenn man nicht danach gefragt hatte.

Nun gilt keine dieser Wahrheiten mehr. Verwertungsrechte können für über 100 Jahre gültig sein. Was kommt dabei heraus? Die großen Bibliotheken sind voll von Büchern, für die a.) immer noch das Urheberrecht gilt, b.) die im Handel nicht erhältlich sind, und die, in vielen Fällen c.) ›verwaiste Werke‹ sind, bei denen kein Rechteinhaber ausfindig gemacht werden kann. Obwohl das Urheberrecht seine Funktion eingebüßt hat, bleiben die Werke in unserem kulturellen Schwarzen Loch gefangen (vgl. Boyle 2009).

Die Funktion des Urheberrechts ist es, abzusichern, dass es eine sichere Einkommensquelle für diejenigen darstellt, die mit der Produktion von Wissen befasst sind, indem sie intellektuellen Besitz zu einer Handelsware machen. Wenn es aber niemanden gibt, der davon profitiert, ist das Urheberrecht überflüssig.

Das Urheberrecht ist eine besondere Art von Patent. Im Allgemeinen ist der Schutz von Innovationen und die Ermutigung zum Unternehmertum der Zweck von Patenten. Dabei ist es vermutlich kein Zufall, dass eines der frühesten bekannten Patentmonopole an einen Drucker vergeben wurde, nämlich an Johannes von Speyer, einer von Gutenbergs Mitarbeitern, der 1469 in der Republik Venedig die neue Technologie verwertete.

> »Venedig, 18. September 1469
>
> Die Buchdruckkunst wurde in unseren angesehenen Staat eingeführt, und durch die Anstrengungen, die Gelehrsamkeit und Genialität des Meisters Johannes von Speyer, der unsere Stadt vor allen anderen ausgesucht hatte, wurde sie von Tag zu Tag beliebter und allen vertrauter. [...] Da solch eine Erfindung, einzigartig und besonders in unserem Zeitalter, durch all unser Wohlwollen und unsere Reichtümer unterstützt und gepflegt sein will, [und da] der gleiche Meister Johannes, der unter den großen Ausgaben seines Haushalts und den Gehältern seiner Handwerker leidet, mit den Mitteln ausgestattet werden muss, dass er in froherem und besserem Geist fortfahren kann und seine Kunst als etwas erachtet, dass eher erweitert als abgeschafft gehört [...] haben die unterzeichnenden Herren des gegenwärtigen Rates, in Antwort auf die bescheidene und ehrerbietige Nachfrage des

> genannten Meisters Johannes, beschlossen und durch diesen Beschluss verfügt, dass in den nächsten fünf Jahren überhaupt niemand das Verlangen, die Möglichkeit, das Vermögen oder das Wagnis haben soll, die genannte Buchdruckkunst in diesem angesehenen Staat von Venedig und seinen Besitzungen auszuüben, abgesehen von Meister Johannes selbst.« (Venezianisches Staatsarchiv 1469)

Man bemerke, dass bereits hier, am Beginn der Kultur des Drucks, die Risse im Konzept des Urheberrechts – bzw. des Monopols – schon notwendigerweise vorhanden sind. Einerseits müssen die Produkte der Erzeuger und Verbreiter von Wissen geschützt werden, so dass sie davon profitieren und leben können. Andererseits ist es aber so, dass je größer der Schutz, der ihnen gewährt wird, desto größer die Bedrohung einer breiten und zugänglichen Verteilung von Wissen. Die Lösung liegt darin, den Zeitraum des Monopols, das sie genießen, einzuschränken. Das erste moderne Urheberrecht – das 1710 in England verabschiedet wurde und beanspruchte »Ein Gesetz zum Ansporn der Gelehrsamkeit [zu sein], indem das Recht an einem Exemplar eines gedruckten Buchs nur bei den Autoren oder den Erwerbern eines Exemplars liegt« – beschränkte den Zeitraum des Monopols auf 14 Jahre (*Copyright Act* 1710). Danach lief das Verwertungsrecht aus.

Zu Beginn kam es aber den Autoren gar nicht zugute, da das Gesetz nicht zu deren Schutz entworfen worden war, sondern vielmehr den Handel zwischen Verlagen und Buchhändlern regelte. Der Gedanke, dass das Urheberrecht auch den Erzeugern von Texten zugute kommen sollte, kam erst später nach dem englischen Gesetz auf; er wurde in Frankreich als *droit d'auteur* zu der gleichen Zeit entwickelt, als dort das Urheberrecht eingeführt wurde. *Le droit* überquerte bald den Kanal und ging schließlich ein in die (mehr oder weniger) allgemeine Übereinkunft der *Berne Convention for the Protection of Literary and Artistic Works*; diese wurde 1886 unterzeichnet und in der Folge immer wieder verbessert. Dies löste natürlich nicht das wesentliche Problem; ganz im Gegenteil: es verschlimmerte es nur, indem es den Urheberschutz universalisierte.

Die Gefahr wurde auch gesehen; so schrieb der Historiker und Politiker Lord Macauly 1841:

> »Es ist gut, dass Autoren entlohnt werden; und der Weg der keine Ausnahme hinsichtlich dieser Entlohnung gestattet, ist das Monopol. Doch ein Monopol ist ein Übel. Um des Guten willen, müssen wir uns diesem Übel unterwerfen; aber das Übel darf keinen Tag länger dauern, als es benötigt wird, das Gute zu wahren.« (zit. n. Boyle 2008: 22)

Diese Mahnung wurde nicht beachtet und das ›Übel‹ des Monopols blühte auf. Es hat sich als so profitabel für alle Parteien erwiesen, dass die ursprünglichen 14 Jahre im Wandel der Gerichtsbarkeit immer wieder erweitert wurden. Das Ergebnis sieht so aus:

Da das Verwertungsrecht nun von so langer Dauer ist, in vielen Fallen sogar weit über ein Jahrhundert, stehen die meisten Werke der Kultur des 20. Jahrhunderts immer noch unter dem Urheberrecht – geschützt, aber nicht erhältlich. Mit anderen Worten: Viel davon ist verlorene Kultur. Niemand legt Bücher wieder auf, bringt Filme wieder auf die Leinwand oder spielt urheberrechtlich geschützte Lieder. Niemandem ist es erlaubt. Tatsächlich wissen wir manchmal noch nicht einmal, wer die Inhaber der Rechte sind. Firmen haben sich aus dem Geschäft zurückgezogen. Aufzeichnungen sind unvollständig oder gar nicht vorhanden (Boyle 2008: 9).

Der Jurist James Boyle macht deutlich, dass etwa 85% aller Bücher im Schnitt nach 28 Jahren vergriffen sind. Es gibt hier also eine neu entstandene gesellschaftliche Notwendigkeit. Das gesamte Urheberrecht bedarf dringend einer Reform. Google hat sich auf die Mängel des Gesetzes als eine Rechtfertigung für ihr Vorgehen eingeschossen; dies ist aber nur eine Art Täuschungsmanöver, das den Prozess des technologischen Wandels verschleiert. Die Reform des Urheberrechts ist aber auch ungeachtet der Technologie notwendig. Dessen Ursprünge bedurften ja auch nicht der Einführung des Buchdrucks.

Zu Gutenbergs Zeit war die Produktion von Manuskripten hochspezialisiert, wobei simultan viele verschiedene Kopien eines Manuskripts angefertigt werden konnten. Es gab ein Geschäft mit autoritativen Texten, den *exemplaria*, die an Schreiber zu Kopierzwecken vermietet wurden; dadurch, dass man die Lagen voneinander löste, konnten viele Gehilfen gleichzeitig an demselben Text arbeiten. Ein florentinischer Manuskript-Verleger und *stationarius*[5] des Quatrocento beschäftigte 50 Kopisten in Daueranstellung (Winston 2005: 6). Diese *stationarii* waren lizenziert und geschützt, wobei sie als Gegenleistung das tatsächliche Ausmaß ihrer Produktion kontrollieren lassen mussten – so erhielt auch Johannes durch sein Patent Schutz vor dem Wettbewerb, wie er ihn auch als Mitglied der Gilde erhalten hätte. Die neue Technologie verlangte nicht wirklich nach einem neuen Konzept des Patents. Die *stationarii* hätten über einen langen Zeitraum Nutzen daraus ziehen können. Andererseits hätte der venezianische Rat einfach darauf bestehen können, dass Johannes der Zugang zur Gilde der *stationarii* gewährt würde. Das Konzept des Patents hatte mehr mit den Bedürfnissen eines wachsenden merkantilistischen, ökonomischen Systems zu tun als mit einer bestimmten technologischen Entwicklung. Ganz bestimmt brauchte man es nicht speziell für die Buchdrucker.

Der Fall des *Book Search Settlement* wirft ein Schlaglicht auf eine neu entstandene soziale Notwendigkeit – die Reform des Urheberrechts – aber diese Notwendigkeit existiert unabhängig von der Technologie, die damit zu tun hat. Es bietet Google ein vernünftiges, soziales Argument zu seinen Gunsten; aber es verleiht dem Argument der Technizisten, dass alleine das Aufkommen von digitalen

5 [Dies meint, dass dieser Verleger auch ein festes Ladenlokal hatte, in dem man die Manuskripte erwerben konnte. Sie konnten also nicht nur von fahrenden Händlern oder auf Messen bezogen werden (A. d. Ü).]

Technologien eine Revision des Konzepts des Urheberrechts vorantreibt, keine Beweiskraft. Dieses Bedürfnis war ohnehin schon da.

Das *Book Search Settlement* wirft viel eher ein Licht auf das ›Gesetz‹ der Unterdrückung eines sich im Gange befindlichen radikalen Potenzials. Ohne Berücksichtigung des Status des Urheberrechts ist das Ergebnis des Rechtsstreits, dass das erschütternde Potenzial des Digitalen gebändigt wird. Dass dies durch die Gerichte geschieht, ist überhaupt nicht ungewöhnlich. Der Streit um das *Book Search Settlement* folgt hierbei den rechtlichen Einschränkungen von *Napster* und *Pirate Bay*. Es ist auch ein Echo all der vorhergehenden historischen Beispiele, wo solche Verbreitungen durch schwebende Gerichtsverfahren aufgehalten wurden. In jedem einzelnen dieser Beispiele, ob vor Gericht verhandelt oder nicht, haben alle beteiligten Parteien – besonders die, die von den älteren bedrohten Technologien profitiert haben, aber auch die rivalisierenden Anhänger der Innovation – einen *modus vivendi* erreicht. Die Verbreitung von Telegraphie, Kino, Radio, terrestrischem, Satelliten- und Kabelfernsehen sowie Computern wurde in jedem Falle durch juristische Streitigkeiten, *cross-patenting agreements*, Kämpfe um Lizenzen, Diskussionen über Standards verzögert (Winston 1998). Dies ist die Funktionsweise unterdrückender Kräfte.

Vielleicht ist das Telephon die genaueste Parallele zur gegenwärtigen Situation, denn auch hier stand ein bestimmtes Recht an sich in Frage: Wie es Lücken im Urheberrecht gab, so gab es auch Lücken in dem Patentrecht, das im 19. Jahrhundert in den Vereinigten Staaten entwickelt wurde. Ein Prä-Patentierungssystem erlaubte es Erfindern, eine Idee schon registrieren zu lassen, bevor sie ausgeführt wurde; es verlangte auch, dass jene über andere Erfinder, die in dem gleichen Bereich arbeiteten, informiert wurden. Dies führte zu einer ziemlichen Verwirrung, für die das Telephon das berühmteste Beispiel ist. Alexander Graham Bell schien durch das Patent über einen Konkurrenten informiert worden zu sein, Elisha Gray, aber Gray war nicht über Bell informiert. Es sieht so aus, dass Bell die Grundidee des Telephons, den variablen Widerstand, von Grays Arbeit übernommen hat. Daher wurde die Legitimität von Bells Patent vom Anfang an angezweifelt und es bedurfte wiederholter Gerichtsverfahren zwischen 1878 und 1908, um es zu bestätigen. Das Monopol wurde erst 1923 gesichert[6] (Winston 1998: 38-59, 156-260).

Während der drei Jahrzehnte, in denen über das letztliche Eigentum am Telephonpatent gestritten wurde, blühte die Telephonie durch verschiedene sehr kostspielige Erstattungen und andere Vereinbarungen mit konkurrierenden Firmen wie Gray und Western Union auf. Es sieht so aus, dass das gleiche mit bei der Digitalisierung von Bibliotheken geschehen wird. Es wird voranschreiten, aber gemessenen Schritts, um die bestehen ökonomischen Interessen zu wahren. Es steht nicht zur Disposition, die Möglichkeiten des digitalen Kopierens zurückzu-

6 Was aber gleich vom Justizministerium angefochten wurde, dessen anhaltende Feindseligkeit gegenüber Bells Firma AT&T schließlich die Übereinkunft von 1923 im Jahr 1982 kippte, als es einen Gerichtsbeschluss erwirkte, um das Monopol zu brechen.

weisen. Dies wird natürlich nicht geschehen. Was der Fall Google viel eher zeigt, ist, dass die Fähigkeit, die Erstellung von Kopien einfacher zu machen, schließlich so gestaltet werden muss, dass sie auch schon vorher bestehenden Vereinbarungen genügt – und dies auf eine Weise, die diese Vereinbarungen zwar verändert und umgestaltet, sie aber nicht vollständig zerstört. Wir sind Zeugen des Austarierens zwischen einer neu entstandenen gesellschaftlichen Notwendigkeit und der Unterdrückung eines erschütternden Potenzials, die Anwendung sowohl des Beschleunigers als auch der Bremse. Dies ist die Art und Weise, wie der Prozess der technologischen Verbreitung in den Kommunikationsmedien funktioniert.

Übersetzt von Holger Steinmann

LITERATURVERZEICHNIS

An Act for the Encouragement of Learning, by Vesting the Copies of Printed Books in the Authors or Purchasers of such Copies, During the Times therein mentioned (1710) 8 Anne, c.19.

Authors Guild Inc./Association of American Publishers Inc./Google Inc. et al. (2008): *Book Settlement Agreement*; Case No 05 CV 8136-JES, http://books.google.com/googlebooks/agreement/, 29.09.2009.

Boyle, James (2008): *The Public Domain: Enclosing the Commons of the Mind*, New Haven: Yale.

Boyle, James (2009) »A Copyright Black Hole Swallows Our Culture«, in: *Financial Times*, 06.11.2009, http//www.thepublicdomain.org/2009/09/06/google-books-and-the-escape-from-the-black-hole/, 29.9.2009.

Braudel, Fernand (1985): *Sozialgeschichte des 15.-18. Jahrhunderts. Band 1: Der Alltag*, München: Kindler.

Helft Miguel (2009): »Google Working to Revise Digital Books Settlement«, in: *New York Times*, 20.09.2009, http://www.nytimes.com/2009/09/21/technology/internet/21google.html, 30.09.2009.

Skidelsky, Wlliam (2009): »Google's Plan for World's Online Library: Philanthropy or Act of Piracy?«, in: *The Observer*, 30.08.2009.

Venitian State Archives (1469): ASV, NC, reg. 11, c. 55, http://www.copyrighthistory.org, 29.09.2009.

Williams, Raymond (1989): *The Politics of Modernism*, New York: Verso.

Winston, Brian (1996): *Technologies of Seeing*, London: BFI.

Winston, Brian (1998): *Media, Technology & Society. A History from the Telegraph to the Internet*, London: Routledge.

Winston, Brian (2005): *Messages: Free Expression, the Media and the West from Gutenberg to Google*, London: Routledge.

DIGITALE KODIERUNG UND REPRÄSENTATION

DVD, CSS, DeCSS

VON TILL A. HEILMANN

Die Logik von Digitalcomputern lässt sich anhand zweier, auf den ersten Blick gegensätzlicher, technischer Leistungen charakterisieren: der Wiederholbarkeit von Daten und ihrer Übersetzbarkeit. Beide ziehen für digitale Artefakte in Zweifel, was ›analogen‹ Werken gemeinhin als Wesensmerkmal zugesprochen wird: die Möglichkeit von Originalen bzw. ›echten‹ Kopien sowie die Identität eines Werkes mit sich selbst, insofern sie sich in dessen Erscheinung äußern kann. Die Folgen, welche digitale Kodierung für die Frage der Repräsentation im Computerzeitalter hat, will dieser Beitrag am Beispiel des digitalen Speichermediums DVD, des ›Kopierschutzes‹ CSS und dessen ›Hack‹ DeCSS illustrieren.

DIGITALCOMPUTER UND WIEDERHOLBARKEIT

Digitalcomputer sind Kopiergeräte.

Von der Informatik werden sie gemeinhin als ›symbolverarbeitende Maschinen‹ aufgefasst (Pflüger 2005: 70). Die zu verarbeitenden Symbole mögen z.B. Zahlen, Buchstaben oder Töne kodieren – je nachdem, ob ein Computer als Rechner, Schreibmaschine oder Musikbox verwendet wird. In jedem Fall schließt die Funktionsweise von Computern aber notwendig die Möglichkeit mit ein, die Symbole in identischer Form zu wiederholen, d.h. wieder und wieder zu speichern und zu übertragen. Das scheint bereits in dem theoretischen Modell auf, welches Alan Turing dem Computer noch vor dem Bau der ersten programmierbaren Rechenmaschinen gegeben hat. Turing (1936) beschreibt bekanntlich eine ›universelle Maschine‹, mit der sich sämtliche Zahlen berechnen lassen, die überhaupt berechnet werden können. Die hypothetische Maschine setzt Rechenvorgänge um, indem sie ein Papierband nach festgelegten Regeln schrittweise bewegt und solange Symbole davon liest und darauf schreibt, bis die zu berechnende Zahl endlich als Symbolkette auf dem Band geschrieben steht. Ein Rechenvorgang zerfällt so in eine Vielzahl kleinster Arbeitsschritte, die sich zu komplexeren und wiederkehrenden Abläufen ordnen, u.a. dem Löschen, Vergleichen und Vervielfältigen von Symbolketten: »These processes include copying down sequences of symbols, comparing sequences, erasing all symbols of a given form etc.« (Turing 1936: 235). Turings universelle Maschine ist daher mit verschiedenen Kopierroutinen ausgestattet, die unverzichtbare Bestandteile jeder Berechnung bilden.

Das Prinzip der Kopie als identischer Wiederholung findet sich nicht nur in der mathematisch-logischen Modellierung, sondern ist auch bestimmendes Merkmal der technisch-apparativen Implementierung von Digitalcomputern. Der amerikanische Literaturwissenschaftler Matthew Kirschenbaum (2008) hat kürz-

lich die Unterscheidung von forensischer und formaler Materialität zur Beschreibung digitaler Informationsverarbeitung vorgeschlagen. Kirschenbaum weist darauf hin, dass auf der physikalischen Ebene von Digitalcomputern jede Informationseinheit als einzigartige ›Einschreibung‹ in ein materielles Substrat existiert. So sind z.B. alle auf einer Festplatte aufgezeichneten, wenige Nanometer messenden magnetischen Flusswechsel, welche die Bits einer Datei speichern, aufgrund minimaler Verzerrungen ihrer Form unverwechselbare Spuren. Keine magnetische Markierung gleicht vollkommen einer anderen. Dasselbe gilt bei der Verarbeitung und Übertragung von Signalen für Spannungspegel in Schaltkreisen oder Kabeln. Forensisch gesehen ist jede materielle Einschreibung ein Unikat. Die Leistung von Digitalcomputern besteht darin, durch ein umfassendes technisches Regime aus Signalverstärkung und Fehlerkorrektur eine strikte Diskretisierung stabiler Zustände vorzunehmen, um auf der Grundlage ›verrauschter‹ und ›schmutziger‹ materieller Spuren ein scheinbar immaterielles Reich reiner Formen zu errichten, in dem die irreduzible Vielgestaltigkeit forensischer Spuren als Einförmigkeit rein formaler Identitäten und Differenzen behandelt wird. Ungeachtet seiner forensischen Einschreibung trägt jedes Bit den logischen Wert 0 oder 1 – niemals einen anderen, niemals etwas dazwischen. Alle gleichwertigen Bits tragen somit nicht nur den gleichen Wert; formal gesehen *sind* sie absolut gleich. Folglich ist jeder Akt der Speicherung, Übertragung und Verarbeitung digital kodierter Daten hinsichtlich deren formaler Materialität mit restlos identischem Ausgang wiederholbar.

> »Whereas forensic materiality rests upon the potential for individualization inherent in matter, a digital environment is an abstract projection supported and sustained by its capacity to propagate the illusion (or call it a working model) of *immaterial* behavior: identification without ambiguity, transmission without loss, repetition without originality.« (Kirschenbaum 2008: 11)

›Wiederholung ohne Eigenwilligkeit‹ ist das Kennzeichen digitaler Vervielfältigung.

Die Wiederholbarkeit, wie Walter Benjamin (1989) sie als technische Reproduzierbarkeit für die ›analogen‹ Medien Photographie und Kinofilm analysiert hat, erreicht mit Digitalcomputern also einen neuen techno-*logischen* Stand. Schwierig, wenn nicht gar unmöglich wird nicht nur der Begriff des Originals, sondern auch die Unterscheidung ›echter‹ Kopien (durch eine Zentralbank herausgegebene Banknoten etwa) von ›falschen‹. Weil Computer Daten symbolisch-diskret kodieren, statt sie mit kontinuierlichen Funktionen abzubilden, stellen alle ›Kopien‹ eines digitalen Artefaktes exakte Duplikate dar und sind, was ihren informationellen Gehalt anbelangt, prinzipiell nicht voneinander zu unterscheiden. Wiederholungen und – mehr noch – wiederholte Wiederholungen digitaler Daten, d.h. ›Kopien‹ von ›Kopien‹, kennen keine Qualitätseinbußen, wie sie für die Reproduktionen analoger Daten (überspielte VHS-Bänder oder photokopierte Texte beispielsweise) typisch sind. Digitale Information muss in ihrer Wiederholung nicht ›verrau-

schen‹. Daher sind Digitalcomputer nicht irgendwelche Kopiergeräte; sie sind gewissermaßen die *perfekten* Kopiergeräte. In Kombination mit der massenhaften Verfügbarkeit von Computertechnik, den stetig sinkenden Preisen für Speichermedien sowie den steigenden Übertragungskapazitäten elektronischer Datennetzwerke hat dieser technische Umstand für Computer als Medien weitreichende ökonomische Folgen – was vor allem Anbieter digitalisierter ›Medieninhalte‹ (Filme, Musik, Anwendungssoftware, Videospiele usw.) alarmiert, die gegen teures Geld verkaufen wollen, was potenzielle Käufer selbst so leicht und günstig vervielfältigen und verteilen können.

DAS CONTENT SCRAMBLE SYSTEM

Ein mustergültiger Fall für die Bestrebungen der Unterhaltungsindustrie, die unkontrollierte Verbreitung digitaler Daten technisch und rechtlich zu unterbinden, ist die DVD-Video, die Ende der 1990er Jahre die Nachfolge der VHS-Kassette antrat.[1] Die DVD-Spezifikation[2] beinhaltet verschiedene Verfahren zur Nutzungskontrolle von DVDs, darunter die *Regional Playback Control* (RPC) und das *Content Scramble System* (CSS). Aus dem Wissen darum geboren, dass digital kodierte Information prinzipiell verlustfrei kopierbar ist, stellen beide keine Kopierschutzmechanismen im herkömmlichen Sinne dar. Weder RPC noch CSS verhindern, dass der Inhalt einer DVD kopiert wird.[3] Beide Verfahren sind eher zum Komplex des Digital Rights Management (DRM), der sog. digitalen Rechteverwaltung, zu zählen, welche die kommerzielle Verwertbarkeit digitaler Daten durch strikte Beschränkung ihrer Nutzung garantieren soll (Grassmuck 2006). Während das RPC zur geographisch differenzierten Vermarktung von DVD-Titeln eine Einteilung der Welt in sechs große Regionen vornimmt und sich technisch gesehen einigermaßen

1 Die folgenden Ausführungen stützen sich wesentlich auf im Internet zugängliche Quellen, unter anderem auf die *DeCSS Central* (http://www.lemuria.org/DeCSS/, 27.02.2010), die *CSS Specifications Version 1.1* (http://cyber.law.harvard.edu/seminar/internet-client/readings/week2/02-08CSS.pdf, 27.02.2010); Gregory Kesdens *15-412 Operating Systems Lecture 33* (http://www-2.cs.cmu.edu/~dst/DeCSS/Kesden/, 27.02.2010), die FAQ-Liste des *Openlaw/DVD Forum* (http://cyber.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html, 27.02.2010) sowie die FAQ-Liste *DVD Demystified* (http://www.dvddemystified.com/dvdfaq.html, 27.02.2010).

2 Die *DVD Books*, welche die DVD-Spezifikation ausführen und von der DVD Format/Logo Licensing Corporation (DVD FLLC) herausgegeben werden, enthalten vertrauliche und rechtlich geschützte technische Informationen. Mit dem Kauf der Bücher wird daher ein Geheimhaltungsvertrag (*non-disclosure agreement*) abgeschlossen, der Käufern die Weitergabe der vertraulichen Informationen untersagt; siehe http://www.dvdfllc.co.jp/format/f_nosbsc.html, 27.02.2010.

3 Eigentliche Kopierschutzverfahren für DVDs sind etwa das *Analog Protection System* (APS) von Rovi – vormals Macrovision – gegen Videoband-Aufnahmen, das *Copy Generation Management System* (CGMS) sowie verschiedene ›Anti-Ripping‹-Mechanismen wie *ARccOS* von Sony, *RipGuard* von Rovi oder *ProtectDISC* von Protect Software. Nur APS und CGMS sind Teil der DVD-Spezifikation; alle anderen Techniken wurden unabhängig von dieser erst später entwickelt und umgesetzt.

simpel gestaltet, ist das CSS ein aufwändiges kryptographisches System, dessen Funktionsweise nun in seinen Grundzügen vorgestellt werden soll.

CSS ist eine symmetrische Verschlüsselungstechnik, die von Matsushita und Toshiba speziell für die DVD-Video entwickelt wurde (Marks/Turnbull 1999: 13). Obwohl von deren Spezifikation nicht zwingend vorgeschrieben, kommt sie bei so gut wie allen kommerziellen DVDs zur Anwendung. CSS erlaubt es, die mit Kompressionsalgorithmen digital kodierten Bild- und Toninhalte zusätzlich kryptographisch zu kodieren, um deren Wiedergabe durch unautorisierte Geräte zu verhindern. Nach den Plänen der von den großen Filmstudios eingerichteten DVD Copy Control Association (DVD CCA) darf allein Hard- und Software, die von ihr für eine »Verwaltungsgebühr« von jährlich 15.500 US-Dollars lizenziert wurde, den Datenstrom einer CSS-kodierten DVD dekodieren und wiedergeben können. Zu diesem Zweck installiert CSS ein in seiner Verschachtelung paranoisch anmutendes Verschlüsselungssystem mit ›Beglaubigungsschlüsseln‹ (*authentication keys*), ›Sitzungsschlüsseln‹ (*session keys*), ›Spielerschlüsseln‹ (*player keys*), ›Plattenschlüsseln‹ (*disk keys*), ›Titelschlüsseln‹ (*title keys*) und ›Bereichsschlüsseln‹ (*sector keys*). Entsprechend umständlich oder gar verwirrend mag die folgende Darstellung erscheinen.

Vereinfacht gesagt funktioniert die Wiedergabe einer CSS-kodierten DVD so, dass das Abspielgerät mit seinem Schlüssel die Schlüssel der DVD entschlüsselt, um mit diesen Schlüsseln wiederum die eigentlichen Bild- und Toninhalte zu entschlüsseln. Jedes CSS-lizenzierte Abspielgerät aus Hardware oder Software, d.h. jeder DVD-Player, aber auch jedes kommerzielle PC-Programm wie z.B. CyberLink PowerDVD, besitzt einen kleinen Satz an Spielerschlüsseln, welche dem Hersteller von der DVD CCA unter strengen Auflagen zugeteilt werden. Insgesamt gibt es 409 solcher Schlüssel, die selbstredend der Geheimhaltung unterliegen. Auf der anderen Seite besitzt jede CSS-kodierte DVD einen Plattenschlüssel, der auf ihr genau 410 Mal gespeichert ist: nämlich je einmal mit jedem der 409 möglichen Spielerschlüssel sowie ein weiteres Mal mit sich selbst verschlüsselt. Zusätzlich enthält die DVD einen sog. Hashwert des unverschlüsselten Plattenschlüssels, eine Art digitale ›Erkennungsmarke‹. Alle diese Informationen sind in einem geschützten Bereich der DVD abgelegt, auf den nur autorisierte Geräte zugreifen dürfen. Ist das abspielende Gerät keine Hardware mit speziellen Schaltkreisen zur CSS-Entschlüsselung (also kein ›regulärer‹ DVD-Player, der an einen Fernseher angeschlossen wird), sondern als Software implementiert, muss es sich daher zunächst gegenüber dem auslesenden Computerlaufwerk authentifizieren, was mithilfe des Beglaubigungsschlüssels geschieht. Im Rahmen dieses Vorgangs wird zudem ein temporärer Sitzungsschlüssel ausgehandelt, der den folgenden Datenaustausch zwischen Laufwerk und Abspielgerät verschlüsselt, damit die verschiedenen Schlüssel bei ihrer Übertragung nicht in unverschlüsselter Form abgefangen werden können. Soll die DVD wiedergegeben werden, muss das Abspielgerät deren Plattenschlüssel in Erfahrung bringen. Dazu liest es nach erfolgter Authentifizierung dessen 410 unterschiedlich verschlüsselte Instanzen aus und pro-

biert sie solange mit seinen Spielerschlüsseln durch, bis die Entschlüsselung gelingt. Dass der Plattenschlüssel korrekt entschlüsselt wurde, kann anhand seiner mit sich selbst verschlüsselten Instanz und seinem Hashwert verifiziert werden. Die Ton- und Bildinhalte wiederum sind mit einzelnen Titelschlüsseln verschlüsselt, welche ihrerseits durch den Plattenschlüssel verschlüsselt auf der DVD gespeichert sind. Als nächstes werden daher der entschlüsselte Plattenschlüssel und die noch unverschlüsselten Titelschlüssel an das Abspielgerät übermittelt (was wohlgemerkt alles durch den Sitzungsschlüssel *ver*schlüsselt geschieht). Daraufhin liest das Laufwerk nacheinander die in Bereiche unterteilten Daten des wiederzugebenden Titels aus und schickt sie an das Abspielgerät. Dieses entschlüsselt nun mit dem Plattenschlüssel den Titelschlüssel, damit den aktuellen Bereichsschlüssel und mit diesem schließlich die Bild- und Tondaten des jeweiligen Bereichs. Die eigentliche Ver- bzw. Entschlüsselung erfolgt, indem die zu en- bzw. dekodierenden Daten (also die verschiedenen Schlüssel wie auch die Bereichsdaten für Bild und Ton) Stück für Stück mit einer pseudo-zufällig erzeugten Bitfolge XOR-verknüpft werden.[4] Die logische XOR-Operation ist selbstinvers, d.h. ihre zweimalige Anwendung führt wieder zum Ursprungswert zurück, weshalb dieselbe Funktion für Ver- wie Entschlüsselung verwendet werden kann. Die Bitfolge, die dafür als Chiffrierstrom mit den Daten verknüpft wird, kommt durch Verschaltung eines Schlüsselpaars (z.B. des Titel- und des Bereichsschlüssel für die Kodierung der Bild- und Tondaten) mit zwei linear rückgekoppelten Schieberegistern (LFSR) zustande. Das Schlüsselpaar bildet die Anfangswerte der LFSRs, deren schrittweise Ausgabewerte miteinander verrechnet die pseudo-zufällige Bitfolge ergeben.

Ziel dieses mehrstufigen kryptographischen Verfahrens ist es offenkundig nicht, das Kopieren auf DVD gespeicherter Daten zu verunmöglichen. Vielmehr macht CSS den ›Besitz‹ kopierter Daten für all jene nutzlos, die nicht über ein autorisiertes Abspielgerät und den zu den Daten gehörigen Schlüssel verfügen. Einer privat angefertigten Kopie einer CSS-kodierten DVD aber fehlt eben dieser Plattenschlüssel, der im geschützten Lead in-Bereich der Scheibe gespeichert ist. Erschwerend kommt hinzu, dass brennbare Rohlinge – wenigstens des Typs DVD-R(W) – in diesem Bereich nicht beschrieben werden können. Auch wenn der Plattenschlüssel also bekannt wäre, könnte man ihn nicht mit auf die kopierte DVD geben. Kurz: Ohne den Spielerschlüssel eines von der DVD CCA lizenzierten Geräts und ohne den Plattenschlüssel einer industriell gepressten DVD sollten deren Bild und Ton nicht in unverschlüsselter Form zu haben sein.

DER ›HACK‹: DeCSS

Im Spätherbst 1999, gut zwei Jahre nach der Markteinführung der DVD-Video, waren die Sicherheitsmechanismen von CSS ausgehebelt. Jeder Computerbenut-

4 Somit ergeben eine 0 (des Datenstroms) und eine 0 (der pseudo-zufälligen Bitfolge) eine 0, 0 und 1 eine 1, 1 und 0 eine 1, 1 und 1 eine 0.

zer konnte nun mit geringem technischem Aufwand aber ohne autorisiertes Gerät und Plattenschlüssel alle CSS-kodierten Scheiben auf seinem Heimrechner abspielen und auch unverschlüsselt abspeichern. Möglich machten das verschiedene Computerprogramme, die aus Kreisen der Hacker-Subkultur und der Bewegung für freie und Open-Source-Software stammten.

In der journalistischen Berichterstattung wird das Knacken von CSS meist mit dem Norweger Jon Johansen in Verbindung gebracht. Johansen, zum Zeitpunkt des Geschehens knapp 16 Jahre alt, gehörte zu einer Gruppe von Hackern, die sich *Masters of Reverse Engineering* (MoRE) nannten. Im Oktober 1999 kündigte er auf der LiViD-Mailingliste zur Entwicklung eines freien Linux-Mediaplayers ein Windows-Programm namens DeCSS an, das alle CSS-kodierten DVDs würde entschlüsseln können. Kurz danach wurde dieses Programm von unbekannter Person im Quelltext (sozusagen der von jedermann einsehbaren und lesbaren ›Bauanleitung‹) wirklich auf der Mailingliste veröffentlicht und in Windeseile über das Internet in alle Welt getragen. Die Abspielsperre für unautorisierte Geräte war damit faktisch aufgehoben. Der genaue Ablauf der Ereignisse, die zu DeCSS und seiner weltweiten Verbreitung führten, bleibt bis heute unklar.[5] Als einigermaßen gesichert gelten darf, dass es MoRE sowie einem weiteren Hackerkollektiv mit Namen *Drink or Die* (DoD) im September 1999 gelang, die Funktionsweise von CSS aufzudecken und zu umgehen. Die entscheidende Information dazu soll angeblich ein unbekannter Hacker geliefert haben, der einen Spielerschlüssel aus der kommerziellen DVD-Software der Firma Xing extrahiert hatte. Noch vor dem Erscheinen von DeCSS brachte die Gruppe DoD das Programm DVD Speed Ripper heraus, das zunächst jedoch nicht alle geschützten Scheiben entschlüsseln konnte und auch nicht im Quelltext, sondern nur als ausführbare Datei verteilt wurde. Eine verbesserte Dekodierroutine, die mit sämtlichen DVDs funktionierte, floss wenig später von DoD über einen anonym bleibenden deutschen Hacker in die Entwicklung von DeCSS ein. Außerdem gelangten die Informationen zum Entschlüsseln CSS-kodierter Scheiben an die Gemeinde der Linux-Entwickler. Von diesen hatte der Engländer Derek Fawcus bereits einige Zeit zuvor den Authentifizierungsvorgang, der Zugriff auf den geschützten Bereich einer DVD gab, als Programm implementiert und im Quelltext veröffentlicht. All diese Anstrengungen kulminierten schließlich in DeCSS, das erstmals die bequeme Entschlüsselung einer DVD per Mausklick gestattete. Tatsächlich soll Johansens eigener Beitrag zum Windows-Programm, das ihm bald großen juristischen Ärger einbringen würde, lediglich in der Zusammenführung von Fawcus' Authentifizierungspro-

5 Siehe dazu u.a. die Stellungnahme von DoD und MoRE (http://www.lemuria.org/DeCSS/dvdtruth.txt, 27.02.2010), Frank A. Stevensons Erklärung vor Gericht (http://w2.eff.org/IP/Video/DVDCCA_case/20000107-pi-motion-stevensondec.html, 27.02.2010), das erstinstanzliche Osloer Gerichtsurteil im Fall Johansen (http://w2.eff.org/IP/Video/Johansen_DeCSS_case/20030109_johansen_decision.html, 27.02.2010) und die Chronologie der Ereignisse – mit inzwischen nicht mehr funktionierenden Links auf die entsprechenden Einträge der LiViD-Mailingliste – des *Openlaw/DVD Forum* (http://cyber.law.harvard.edu/DVD/research/chronology.html, 27.02.2010).

ramm und DoDs verbesserter Dekodierroutine unter einer graphischen Benutzeroberfläche bestanden haben.

Kaum war DeCSS im Quelltext bekannt und das Funktionieren von CSS damit offengelegt, meldete sich der Spielentwickler Frank A. Stevenson im Internet mit einer Kryptoanalyse des Verschlüsselungsverfahrens zu Wort.[6] Stevenson entdeckte fundamentale Designfehler, die CSS prinzipiell unsicher machten. Eine der entscheidenden Schwächen bestand in der geringen Länge der Schlüssel, die mit 40 Bit deutlich zu kurz waren.[7] Daher hielt CSS schon Ende der 1990er Jahre einer *brute force attack*, einem Angriff mit der geballten Rechenkraft eines zu jener Zeit handelsüblichen PCs nicht stand, welcher in weniger als einem Tag einfach alle 2^{40} möglichen Schlüssel durchrechnen konnte. Stevenson fand darüber hinaus schwerwiegende Mängel in der Erzeugung der pseudo-zufälligen Bitfolge, die als Chiffrierstrom dient. Die von den beiden LFSRs generierte Bitfolge war kryptographisch so schwach (so wenig ›zufällig‹ also), dass man von den Ausgabewerten auf die Anfangswerte der LFSRs und damit die zur Kodierung verwendeten Schlüssel schließen konnte. Auch der auf einer DVD gespeicherte Hashwert des Plattenschlüssels (dessen digitale ›Erkennungsmarke‹) erwies sich als anfällig für kryptoanalytische Angriffe, sodass aus ihm der Plattenschlüssel selbst rekonstruiert werden konnte, womit sich die Kenntnis eines funktionierenden Spielerschlüssels erübrigte. Im Oktober 1999 stellte Stevenson im Internet seine verschiedenen Methoden vor, anhand einer beliebigen CSS-kodierten DVD alle gültigen Spielerschlüssel – dieses von der DVD CCA so sorgsam gehütete Geheimnis – zu eruieren. Ein *reverse engineering* eines lizenzierten Schlüssels aus einer kommerziellen Software, wie es DeCSS erst möglich gemacht haben soll, war nicht mehr nötig. Hinfällig geworden war damit auch der Notfallplan der DVD CCA, kompromittierte Schlüssel ›zurückzurufen‹ und bei künftigen Geräten und Scheiben nicht mehr zu berücksichtigen.

Das Erscheinen von DeCSS und Stevensons daran anschließende kryptoanalytische Dokumentation lösten zugleich ein Problem, welches die Benutzer und Entwickler von Linux-Betriebssystemen lange umgetrieben hatte: Ende der 1990er Jahre gab es keine autorisierte DVD-Software für Linux und somit keine Möglichkeit, DVDs auf einem solchen System abzuspielen. Den etablierten Softwareproduzenten erschien der Markt für ein kommerzielles Programm zu klein und die für CSS jährlich anfallenden »Verwaltungsgebühren« waren restriktiv hoch. Dazu kam, dass die Linux-Entwicklergemeinde, die der Bewegung für freie und Open-Source-Software entstammte, nicht quelloffene Programme und Geheimhaltungsverträge, wie sie die Lizenzierung von CSS erforderte, grundsätzlich

6 Siehe Frank A. Stevenson: »Cryptanalysis of Contents Scrambling System«, 08.11.1999 (http://www.cs.cmu.edu/~dst/DeCSS/FrankStevenson/analysis.html, 27.02.2010).

7 Diese Wahl erfolgte u.a. mit Rücksicht auf die zu jener Zeit geltenden Exportbestimmungen der US-Regierung, die eine Ausfuhr von stärkeren Verschlüsselungsverfahren verboten oder zumindest erschwerten; siehe http://en.wikipedia.org/wiki/40-bit_encryption, 27.02.2010.

ablehnt. Mit dem neugewonnenen Wissen konnten die Entwickler nun aber Dekodierroutinen und Programme schreiben, die nicht auf ›gestohlene‹ Spielerschlüssel oder andere offensichtlich illegale Methoden zurückgreifen mussten und den Inhalt CSS-kodierter DVDs gleichwohl ohne lizenzierten Schlüssel wiedergeben konnten. Die bekannteste und heute am weitesten verbreitete Software dieser Art ist die Programmbibliothek libdvdcss, die wesentlich auf den Vorarbeiten von Fawcus und Stevenson aufbaut.[8] Um eine geschützte Scheibe abzuspielen, erzeugt libdvdcss zunächst selbständig eine Anzahl möglicher Spielerschlüssel. Sollten diese nicht funktionieren, startet es eine *brute force attack*, um den Platten- und zuletzt die Titelschlüssel zu brechen. Die Programmbibliothek ist weitgehend unabhängig von einzelnen Betriebssystemen und wird von vielen populären Open-Source-Programmen wie VLC Player, xine oder MPlayer zur Wiedergabe von DVDs verwendet.[9]

In seiner ursprünglichen Windows-Version ist das von der Industrie als ›Piraterie-Programm‹ verschrieene DeCSS wohl nie breitenwirksam zur praktischen Anwendung gekommen, schon gar nicht zum massenhaften ›Raubkopieren‹ von DVDs. Zwar konnte man den Inhalt einer DVD damit entschlüsseln, aber dieser Inhalt – mehrere Gigabyte große Dateien – ließ sich nicht leicht vervielfältigen und verbreiten. Geeignete Rohlinge hatten nur etwa die halbe Speicherkapazität einer kommerziellen Scheibe und waren zudem so teuer, dass sich der gesamte Aufwand für das Dekodieren, Komprimieren und Brennen einer Kopie im Vergleich zum Kauf eines Titels kaum lohnte. Festplattenspeicher war ebenfalls kostbar und ein damals handelsübliches Laufwerk mit zwei bis drei dekodierten Filmen bereits gefüllt. Und einer großflächigen Verbreitung über das Internet standen die gemessen an der Datenmenge eher geringen Übertragungsgeschwindigkeiten im Weg. Gewiss gab (und gibt) es ›Raubkopien‹. Diese wurden aber hauptsächlich von organisierten Gruppen aus dem südostasiatischen Raum gewerbsmäßig und mit professionellem Gerät hergestellt. Solche Kopien stellen vollständige 1:1-Duplikate kommerzieller DVDs dar, mitsamt der CSS-Verschlüsselung, Scheibenaufdruck und Verpackung. Auch war DeCSS keineswegs die erste technische Lösung, die Kontrollmechanismen von CSS zu umgehen und die Bild- und Tondaten in unverschlüsselter Form zu speichern. Zuvor schon hatte es eine erste Generation von ›Ripping‹-Programmen gegeben, die das Dekodieren einem autorisierten Gerät überließen und den von diesem entschlüsselten Datenstrom bei der Wiedergabe ›abfingen‹. Jenseits der Ermöglichung unverschlüsselter DVD-Kopien ist die Bedeutung von DeCSS vor allem darin zu sehen, dass sein Quelltext der Öffentlichkeit zum ersten Mal Einblick in die bis dahin weitgehend geheim gehaltene Funk-

8 Siehe die entsprechenden Hinweise im Quelltext der Datei css.c der Programmbibliothek, die von http://www.videolan.org/developers/libdvdcss.html (27.02.2010) heruntergeladen werden kann.

9 Die meisten großen Linux-Distributionen wie Debian, openSUSE oder Ubuntu werden aus rechtlichen Gründen ohne libdvdcss ausgeliefert, machen ihren Benutzern eine nachträgliche Installation der Programmbibliothek aber sehr leicht.

tionsweise von CSS bot und Entwicklern freier und Open-Source-Software erlaubte, Programme zur Wiedergabe geschützter Scheiben (seien diese ›legale‹ kommerzielle DVDs oder ›Raubkopien‹) für alternative Plattformen wie Linux-Betriebssysteme zu schreiben, ohne dabei die mit einer Lizenzierung durch die DVD CCA verbundenen finanziellen und rechtlichen Zugeständnisse machen zu müssen. Die historische Relevanz von DeCSS ist daher mehr theoretischer als praktischer Natur – mit sehr praktischen Auswirkungen allerdings.

Dass das Verschlüsselungsverfahren überhaupt gebrochen bzw. so problemlos umgangen werden konnte, dürfte drei Gründe haben: Erstens stellte bereits seine Umsetzung auch als Software ein beträchtliches Risiko dar. Software lässt sich ungleich einfacher analysieren als ein in die miniaturisierten Schaltkreise versiegelter Spezialchips gegossenes Hardware-Äquivalent. Sie kann mit Editoren eingesehen und – im Falle von DeCSS gar im ›menschenfreundlichen‹ Quelltext – ›gelesen‹, wenn nötig aus dem ausführbaren Objektcode in leichter verständliche Assemblerbefehle rückübersetzt und bei ihrem Vollzug im Arbeitsspeicher des ausführenden Computers ›beobachtet‹ werden. Dieser Umstand begünstigt ein *reverse engineering* der Technik, wie es mit der Player-Software von Xing geschehen und DeCSS in seiner ersten Version ermöglicht haben soll. Zweitens stellten sich entscheidende Teile von CSS (die verschiedenen Schlüssel, die Hashwerte der Plattenschlüssel und die den Chiffrierstrom erzeugenden LFSRs), nachdem sie in ihrer Software-Form analysiert worden waren, als mangelhaft implementiert heraus. Was zum dritten und wohl entscheidenden Punkt führt: CSS war als proprietäre Technik entworfen worden. Seine Mechanismen wurden von Matsushita und Toshiba geheim gehalten und nur Lizenznehmern unter Auflage höchster Vertraulichkeit bekannt gemacht. Dies verhinderte, dass es einer eingehenden Prüfung durch unabhängige Experten unterzogen werden konnte, wie es bei allen kryptographischen Systemen geschehen sollte. Der heute vielfach verwendete und als derzeit sicher eingestufte *Advanced Encryption Standard* (AES) beispielsweise durchlief einen mehrjährigen öffentlichen Begutachtungs- und Auswahlprozess. In einer scheinbar paradoxalen Verkehrung kann die Verlässlichkeit eines Verfahrens zum Schutz von Geheimnissen nach Kerckhoffs' Prinzip bzw. Shannons Maxime nur dann sichergestellt werden, wenn seine Funktionsweise vollständig offengelegt ist.

ELEKTRONISCHER ZIVILER UNGEHORSAM

Die Veröffentlichung von DeCSS im Internet zeigte kurz darauf die erwartbaren Folgen: Die DVD CCA und der Wirtschaftsverband der US-amerikanischen Filmstudios, die Motion Picture Association of America (MPAA), versuchten, die Bekanntmachung und Verbreitung des Programms rechtlich zu unterbinden. Die sich teilweise über Jahre hinziehenden juristischen Auseinandersetzungen zwischen den Interessensvertretern der Unterhaltungsindustrie und verschiedenen Privatpersonen sowie Fürsprechern der freien und Open-Source-Software können hier

nicht ausführlich dargestellt werden.[10] Es sollen nur einige Punkte aus dem rechtlichen und öffentlichen Geschehen rund um DeCSS herausgegriffen werden, die für Fragen der digitalen Kodierung und Repräsentation von Belang sind.

Nach dem ersten Erscheinen von DeCSS auf der LiViD-Mailingliste Ende Oktober 1999 wurde das Programm schnell ›weitergereicht‹ und auf Dutzenden von thematischen Webseiten angeboten. Der breiteren Öffentlichkeit blieb das nicht lange verborgen. Bereits am 1. November berichtete etwa Wired News unter dem Titel »DVD Piracy: It Can Be Done« über den DVD-›Hack‹.[11] Nun reagierte auch die MPAA und begann haufenweise Abmahnschreiben zu versenden, in denen die Betreiber entsprechender Webseiten aufgefordert wurden, DeCSS unverzüglich zu entfernen. Während einige der Forderung nachkamen, sahen sich zahlreiche andere durch das Vorgehen der MPAA in ihrer Überzeugung bestärkt, Information im allgemeinen und das Wissen um CSS bzw. DeCSS im Besonderen müsse frei verfügbar sein, und machten sich deshalb daran, das Programm auf möglichst viele Webseiten zu stellen und diese wiederum auf möglichst vielen anderen Seiten weltweit zu verlinken.

Der rapiden Verbreitung von DeCSS begegnete die DVD CCA, indem sie Ende Dezember vor dem Obergericht des Staates Kalifornien eine einstweilige Verfügung gegen fünfundzwanzig namentlich bekannte sowie fünfhundert weitere, ungenannt bleibende Webseitenbetreiber in den USA und anderen Ländern zu erwirken suchte.[12] Die Kläger behaupteten, das Programm verletze Betriebsgeheimnisse, da es durch *reverse engineering* der DVD-Software von Xing hergestellt worden sei (wofür sie allerdings keinerlei Beweise vorlegen konnten). Die Verteidigung – zwei von der Electronic Frontier Foundation (EFF) gestellte Anwälte – berief sich dagegen auf den 1. Zusatzartikel zur Verfassung der Vereinigten Staaten und das darin verbriefte Recht auf Meinungsfreiheit, welches die Veröffentlichung von DeCSS schütze. Nachdem das Gericht der einstweiligen Verfügung zwar nicht stattgegeben, in erster Instanz jedoch einen vorläufigen Rechtsschutz erlassen hatte, der die Veröffentlichung des Programms verbot, entschied das Appellationsgericht im November 2001 schließlich zugunsten der Angeklagten. Ausschlaggebend für den Entscheid war, dass das Gericht, gestützt auf einen Präzedenzfall, einen qualitativen Unterschied zwischen zwei verschiedenen Kodierungen von Computerprogrammen machte, dem Quelltext und dem Objektcode. Die Urteilsbegründung hält dazu fest:

10 Siehe dazu etwa das *Video and DVD Archive* der Electronic Frontier Foundation (http://w2.eff.org/IP/Video/DVDCCA_case/, 27.02.2010) oder das Archiv des *Openlaw/DVD Forum* (http://cyber.law.harvard.edu/openlaw/DVD/, 27.02.2010).

11 Siehe Andy Patrizio: »DVD-Piracy: It Can Be Done«, *Wired News*, 01.11.1999 (http://www.wired.com/science/discoveries/news/1999/11/32249, 27.02.2010).

12 DVD Copy Control Association, Inc. v. McLaughlin, No. CV 786804, 2000 WL 48512 (Cal. Super. Ct. Jan. 21, 2000); siehe http://cryptome.org/dvd-v-500.htm, 27.02.2010.

> »Like the CSS decryption software, DeCSS is a writing composed of computer source code which describes an alternative method of decrypting CSS-encrypted DVDs. Regardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS. If the source code were ›compiled‹ to create object code, we would agree that the resulting composition of zeroes and ones would not convey ideas. That the source code is capable of such compilation, however, does not destroy the expressive nature of the source code itself. Thus, we conclude that the trial court's preliminary injunction barring Bunner [Angeklagter, der Berufung eingelegt hatte; T.A.H.] from disclosing DeCSS can fairly be characterized as a prohibition of ›pure‹ speech.«[13]

Den Quelltext von DeCSS verstand das Appellationsgericht also als *Schriftstück*, das *Ausdruck* der *Ideen und Informationen* eines *Autors* sei – im Gegensatz zur ausführbaren Fassung des Programms (dem kompilierten Objektcode), welche lediglich eine Anordnung aus Nullen und Einsen darstelle und keine Ideen vermittle. Die *›reine‹ Rede* des DeCSS-Quelltexts hingegen, und damit auch dessen Wiedergabe auf der Webseite des Angeklagten Andrew Bunner, sei durch das Recht auf freie Meinungsäußerung geschützt.

Eine vergleichbares Verfahren der MPAA, das im Januar 2000 an einem New Yorker Bundesgericht gegen David Corley, den Betreiber der Hacker-Webseite 2600.com, wegen Veröffentlichung von DeCSS angestrengt wurde, ging weniger glücklich für den Angeklagten aus. Geklagt wurde hier nicht, wie in Kalifornien, wegen Verletzung von Betriebsgeheimnissen, sondern wegen Verstoßes gegen den *Digital Millennium Copyright Act* (DMCA). Mit der Beharrlichkeit und dem Einfallsreichtum der Hackergemeinde rechnend und wissend, dass Verfahren wie CSS überwunden werden können, hatte die Unterhaltungsindustrie in den 1990er Jahren darauf gedrängt, neue rechtliche Schranken zum Schutz ihrer wirtschaftlichen Interessen zu errichten (Marks/Turnbull 1999: 25). Bekanntester und folgenreichster Ausdruck dieser Bestrebungen ist eben der 1998 vom damaligen US-Präsidenten Clinton unterzeichnete DMCA, der vor allem den *Performances and Phonograms Treaty* (WPPT) der Weltorganisation für geistiges Eigentum (WIPO) von 1996 für das US-amerikanische Rechtssystem umsetzt.[14] Wichtige Teile beider Gesetze betreffen die Frage der sog. *anti-circumvention*: WPPT (Art. 18) und DMCA (Abs. 1201) legen fest, dass technische Maßnahmen zur Nutzungskontrolle rechtlich geschützter Werke, also etwa DRM-Verfahren wie CSS, nicht umgangen werden dürfen – wo technische Sperren vor technischen Angriffen versagen,

13 DVD Copy Control Association, Inc. v. Bunner, No. CV 786804 (Cal. App. Dep't Super. Ct. Nov. 1, 2001); siehe http://cryptome.org/dvd-v-bunner.htm (27.02.2010).

14 Siehe die Gesetzestexte in der US-Kongressbibliothek (http://thomas.loc.gov/cgi-bin/bdquery/z?d105:H.R.2281:, 27.02.2010) und bei der WIPO (http://www.wipo.int/treaties/en/ip/wppt/, 27.02.2010).

da sollen juristische Sperren helfen. Die Verteidigung berief sich, wie bereits im kalifornischen Gerichtsfall, auf die freie Meinungsäußerung, aber auch auf Ausnahmeklauseln im US-amerikanischen Urheberrechtsgesetz und im DMCA, die unter bestimmten Bedingungen eine nicht autorisierte Nutzung, ein *reverse engineering* und Kryptoanalysen geschützter Inhalte erlauben. Darüber hinaus zog die Verteidigung die Verfassungsmäßigkeit des DMCA überhaupt in Zweifel, weil sie durch diesen die vom 1. Zusatzartikel und dem Urheberrechtsgesetz garantierten Rechte verletzt sah. Trotz des Einsatzes und der Fürsprache zahlreicher angesehener Computerwissenschaftler wie Marvin Minsky, Ron Rivest und Harold Abelson gab das Gericht der MPAA Recht und untersagte Corley die Veröffentlichung von DeCSS sowie das Setzen direkter Weblinks darauf.

Aber nicht nur Personen, die DeCSS veröffentlichten und verteilten, hatten sich vor Gericht zu verantworten, sondern auch dessen Entwickler: Auf Betreiben der DVD CCA und der MPAA klagte die norwegische Staatsanwaltschaft im Jahr 2002 Jon Johansen, den einzig namentlich bekannten Schöpfer des Programms, nach dem norwegischen Strafgesetzbuch wegen ›unautorisierten Zugriffs‹ auf Computerdaten und -programme an. Weil gemäß norwegischem Recht jedoch bereits der Kauf einer kommerziellen DVD den Zugriff auf deren Daten autorisiert, das Anfertigen von Kopien für Privatzwecke nicht strafbar ist und Johansen selbst keine anderen illegalen Tätigkeiten nachgewiesen werden konnten, wurde er im Januar 2003 freigesprochen.[15]

Auf das juristische Vorgehen der Unterhaltungsindustrie antwortete die Hackergemeinde im Internet – unterstützt von Bürgerrechtsorganisationen wie der EFF – mit ›elektronischem zivilem Ungehorsam‹. Abgemahnte und verurteilte Webseitenbetreiber wie Corley entfernten DeCSS zwar aus ihren eigenen Angeboten; dafür verlinkten sie und hunderte weiterer Aktivisten systematisch andere Webseiten und solche außerhalb der USA, die das Programm immer noch bereithielten. Zudem ersannen sie Möglichkeiten, es in Formen zu kodieren und zu verbreiten, die ihrer Meinung nach von juristischen Verboten nicht berührt wurden. Der Informatiker David Touretzky, der beim Verfahren gegen Corley als Experte zugunsten des Angeklagten aussagte, richtete im Internet eine »Gallery of CSS Descramblers« ein, die verschiedene Varianten des DeCSS-Quelltexts vorstellte.[16] Mit den ›Ausstellungsstücken‹ der Galerie wollte Touretzky (2001) seine vor Gericht vertretene Position verdeutlichen, dass man keine klare Grenze zwischen Rede und Programm-Quelltexten ziehen könne und folglich auch diese durch den 1. Zusatzartikel geschützt seien. Nach der ersten Anhörung des Falles hatte das New Yorker Gericht – anders als das kalifornische – nämlich entschieden, Erläuterungen des Quelltexts von DeCSS seien durch das Recht auf freie

15 Siehe die engl. Übersetzung der Urteilsbegründung im *Video and DVD Archive* der Electronic Frontier Foundation (http://w2.eff.org/IP/Video/Johansen_DeCSS_case/20030109_johansen_decision.html, 27.02.2010).

16 Siehe David S. Touretzky: »Gallery of CSS Descramblers« (http://www.cs.cmu.edu/~dst/DeCSS/Gallery/, 27.02.2010).

Meinungsäußerung geschützt, nicht aber der Quelltext selbst, weil dieser in den ausführbaren Objektcode eines funktionsfähigen Programms kompiliert werden könne. Touretzkys Galerie enthält neben dem Quelltext des Programms in der Sprache C u.a. einen GIF-Screenshot davon, der als graphische Kodierung nicht kompilierbar ist, am Bildschirm aber alle im Quelltext enthaltene Information ›anzeigt‹. Eine andere Variante gibt den Quelltext in einem eigens für die Galerie erfundenen, formal rigorosen Dialekt von C wieder, für welchen jedoch kein Compiler existiert. Außerdem ›übersetzte‹ Touretzky die Funktionsweise von DeCSS bzw. dessen Quelltext Zeile für Zeile in schriftsprachliches Englisch. Zu guter Letzt präsentierte er den Besuchern seiner Webseite das Bild eines käuflich zu erwerbenden T-Shirts, auf welchem der Quelltext gedruckt stand. In der Folge steuerten Dritte weitere Varianten bei: DeCSS als Leseaufführung, als Strichcode, als Musicalnummer, als Haiku-Gedichte, als MIDI-Musikdatei, als Laufschrift-Animation in Star Wars-Manier, als ASCII-Art, als Beschreibung einer Hardware-Implementierung, als Yahoo-Grußkarte oder als in einer Bilddatei steganographisch verborgene Botschaft. Dazu kamen Umsetzungen in andere Programmiersprachen wie Scheme, Perl, Java, Javascript, PHP oder Pascal.

Die außergewöhnlichste Kodierung von DeCSS demonstrierte jedoch der Mathematiker Phil Carmody. Als Reaktion auf das Urteil des New Yorker Gerichts suchte er nach einer Darstellungsweise des Programms, die an sich, d.h. unabhängig von einer möglichen Verwendung zur Entschlüsselung CSS-kodierter DVDs, publikations- und archivierungswürdig war und deren Veröffentlichung daher nicht ohne weiteres verboten werden konnte. Ausgangspunkt von Carmodys Überlegungen war die Tatsache, dass sich ein Computerprogramm als Zahl begreifen lässt:[17] So kann man etwa die Bitfolge, welche die Reihe der Schriftzeichen kodiert, aus denen der DeCSS-Quelltext besteht, nicht nur als separate, 8-bittige ASCII-Kodenummern lesen, sondern ebenso gut als aufeinanderfolgende Stellen einer einzigen großen Zahl. Geeignete Kandidaten für archivierungs- und publikationswürdige Zahlen schienen Carmody Primzahlen zu sein, da Primalität ungeachtet etwaiger rechtlicher Bestimmungen eine grundlegende zahlentheoretische Eigenschaft mathematischer Objekte ist, und das Archiv, das er im Sinn hatte, waren die »Prime Pages«[18] des Mathematikprofessors Chris Caldwell, der im Internet verschiedene Listen von Primzahlen besonderer Art veröffentlicht. Carmodys Leistung bestand nun darin, eine Primzahl zu finden, die aufgrund ihrer Eigenschaften in eine von Caldwells Listen aufgenommen werden musste und dazu noch die Informationen des DeCSS-Quelltexts ›enthielt‹. Mit einigem mathematischem Geschick und der Rechenkraft seines PCs gelang es ihm, eine passende Primzahl mit 1905 Stellen auszumachen.[19] Weil diese Zahl erstens zum Zeitpunkt

17 Das gilt selbstredend nicht nur für Programme, sondern für alle digital kodierten Daten.

18 Siehe Chris Caldwell: »The Prime Pages. Prime number research, records, and resources« (http://primes.utm.edu/, 27.02.2010).

19 Für die mathematischen Einzelheiten siehe Phil Carmody: »The world's first illegal prime number?« (http://asdf.org/~fatphil/maths/illegal1.html, [19.03.2001], 27.02.2010) sowie

ihrer Entdeckung die zehntgrößte mithilfe des *elliptic curve*-Verfahrens aufgespürte Primzahl war, wurde sie in der entsprechenden Top 20-Liste von Caldwell publiziert. Zweitens kodierte sie auf ausgeklügelte Weise das DeCSS-Programm. Nimmt man die Binärdarstellung der Primzahl und entpackt sie mit dem weit verbreiteten Kompressionsprogramm gzip, ist das Resultat der Quelltext von DeCSS. Die von Carmody gefundene Zahl ist also selbst ein digitales ›Archiv‹ des für illegal befundenen Programms. Sie ist eine Primzahl *und* eine vollständige Darstellung des Entschlüsselungsverfahrens für CSS-geschützte DVDs. Einige Zeit später legte Carmody nach und präsentierte eine 1811-stellige Primzahl, deren Binärdarstellung zugleich der Objektcode eines CSS-Dekodierers für Linux-Betriebssysteme auf x86-Mikroprozessorarchitektur ist.[20] Diese Zahl muss nicht erst von einem Algorithmus wie gzip in eine andere überführt werden, sondern kann von entsprechenden Computern ›direkt‹ als Programm ausgeführt werden.

DIGITALCOMPUTER UND ÜBERSETZBARKEIT

Digitalcomputer sind Übersetzungsmaschinen.

Sie automatisieren En- und Dekodierprozesse von Symbolketten, indem Bitfolgen programmgesteuert zu neuen Bitfolgen ›umgeschrieben‹ werden. Beispiele für einen solchen weitgefassten Begriff von Kodierung als regelgeleiteter Übersetzung wurden verschiedene angeführt: die Übersetzung des Plattenschlüssels einer DVD in seinen Hashwert; der Titel- und Bereichsschlüssel in einen pseudozufälligen Chiffrierstrom; der CSS-verschlüsselten Bereichsdaten in unverschlüsselte Bild- und Tondaten; des ›menschenfreundlichen‹ Quelltexts von DeCSS in den ausführbaren Objektcode, aber auch eine Bilddatei, eine Musikdatei oder eine Primzahl; der Dezimaldarstellung einer Primzahl in deren Binärdarstellung; schließlich die Übersetzung der Binärdarstellung einer Archivdatei in den Quelltext eines Programms.

Die *Übersetzbarkeit* digital kodierter Information bildet gewissermaßen die Kehrseite ihrer Wiederholbarkeit. Die formale Materialität, wie Kirschenbaum sie durch Digitalcomputer verwirklicht sieht, bezeichnet nicht allein den Umstand absoluter Identität, d.h. vollkommener Einförmigkeit und eindeutiger Wertigkeit der informationstragenden Einheiten. Sie meint ebenso sehr (und noch mehr), dass diese Einheiten – die Bits – als typisierte Elemente mühelos und augenblicklich von einem Zustand in den anderen umgeschaltet werden können. Miniaturisierung, Menge und Geschwindigkeit der physikalischen Schaltungen erzeugen einen vermeintlich immateriellen Darstellungsraum, in welchem die von der Trägheit der Materie befreite Information beliebig formbar ist. Digitale Kodierung und Schalttechnik ermöglichen so ›endlose Permutationen‹ des Kodierten (Kirschen-

die entsprechende Seite von Caldwells »Prime Pages« (http://primes.utm.edu/glossary/xpage/Illegal.html, 27.02.2010).

20 Siehe Phil Carmody: »An Executable Prime Number?« (http://asdf.org/~fatphil/maths/illegal.html, [10.09.2001], 27.02.2010).

baum 2008: 145-146). Lautete die Botschaft des mechanischen Zeitalters und der technischen Reproduzierbarkeit ›Mehr vom selben‹, so ist das Versprechen der computerisierten Informationsgesellschaft und der digitalen Übersetzbarkeit ein alchemistisches ›Jedes Ding in jede Form‹.

An ihrer Übersetzbarkeit wird aber auch deutlich, wie problematisch die Frage danach ist, was digital kodierte Information ›eigentlich‹ repräsentiert. Bits *als* Bits, d.h. als Elemente formaler Materialität, gehören nicht der Ordnung des sinnlich Wahrnehmbaren an und müssen nach ihren übersetzenden Umschaltungen erst für menschliche Augen und Ohren (oder andere Sinne) transformiert werden – ein Vorgang, der seinerseits eine Übersetzung darstellt. Soll etwa der digital gespeicherte Quelltext eines Programms wie DeCSS für Menschen lesbar werden, müssen die Bitfolgen des Zeichensatzes, nach welchem die einzelnen Schriftzeichen kodiert sind, in die Bitfolgen der Glyphen einer Outline-Schrift wie TrueType übersetzt werden und diese wiederum in die Bitfolgen eines Bitmaps, welches dann in ein Leuchtmuster auf dem Bildschirm umgewandelt wird. Diese mehrstufigen Übersetzungen können sehr unterschiedlich ausfallen. Wer einmal ein aufwändig formatiertes Textdokument an einem Computer ›geöffnet‹ hat, auf welchem nicht alle zur gewünschten Darstellung notwendigen Schriften installiert sind, oder eine Webseite besucht, deren Zeichensatz vom Browser nicht ›richtig‹ erkannt wird, weiß, wie wandelbar die ›äußere Gestalt‹ digital kodierter Information ist.

Die Übersetzbarkeit von Computerdaten in verschiedene Repräsentationen betrifft jedoch nicht allein eher nebensächliche Aspekte wie die graphische Realisierung von Schriftzeichen. Sie stellt ganz grundsätzlich die ›Identität‹ digitaler Artefakte in Frage. Digital kodierte Information kann nie ›an sich‹, ›als solche‹ oder als ›sie selbst‹ erscheinen, sondern immer nur *in Übersetzung*. Dabei äußert sich nicht eine den Daten immanente ›Wahrheit‹. Die Übersetzung folgt einer Programmierung, deren potenziell unendliche Effekte durch Normen geregelt werden: Protokolle, Datenformate oder Zeichensätze wie HTTP, JPEG oder ASCII, und Anwendungssoftware wie Webbrowser, Bildbearbeitungsprogramme oder Texteditoren. Durch offene oder proprietäre Standards reglementiert (Galloway 2006) gelangen stets nur ausgewählte Übersetzungen von Computerdaten an die Benutzer. Vergleichbar der von Roland Barthes (1987: 13-14) beschriebenen Markierung einer Konnotation unter vielen als der scheinbar ›natürlichen‹ Denotation, wird üblicherweise eine Übersetzung digital kodierter Information als deren ›eigentliche‹ Repräsentation naturalisiert (Kirschenbaum 2008: 145-146). Die häufig getroffene Unterscheidung von ›kulturellen‹ Kodes wie denen der Poesie oder der Alltagssprachen und ›technischen‹ Kodes wie denen der elektronischen Datenverarbeitung, die u.a. in der juristischen Differenzierung zwischen der Rede des Autors im DeCSS-Quelltext und dessen verziffertem Objektcode ein Echo findet, ist also zumindest dann fragwürdig, wenn damit einem tendenziell endlosen Spiel von Bedeutungen auf der einen eine rigide Syntaktik ohne Freiheitsgrade auf der anderen Seite gegenübergestellt werden soll. Auch die Effekte ›techni-

scher‹ Kodierungen sind variabel und vom Kode selbst nicht völlig beherrschbar; auch die ver- und aufschiebende Bewegung der ›digitalen Differenz‹ (Tholen 1997) lässt sich nicht stillstellen.

Liegen das Vermögen und die Leistungsfähigkeit von Digitalcomputern in der unabschließbaren Übersetzbarkeit von Kodes begründet, dann ist die Tatsache, dass Computerdaten nach Belieben in neue Zustände umgeschaltet und d.h. eben verarbeitet werden können, wenigstens aus medientheoretischer Sicht nur deren uninteressantester Ausdruck. Das nichttriviale Moment der computerisierten Übersetzbarkeit von Daten besteht darin, dass digital kodierte Information eine irreduzible Vielzahl von Repräsentationen kennt, von denen keine als ihre ›richtige‹ oder ›authentische‹ identifiziert werden kann. Ein und dieselbe Webseite beispielsweise ist in sehr verschiedener Weise darstellbar: Man kann sie mit einem graphischen oder einem bloß textbasierten Browser öffnen, Schriftarten und -größen verändern, mit entsprechenden Erweiterungen zwischen mehreren Farbschemen auswählen, bestimmte Elemente (Werbebanner o.ä.) ausblenden oder sich den vom Browser verarbeiteten HTML-Quelltext anzeigen lassen. Alle daraus resultierenden Ansichten sind ›gültige‹ Darstellungen der Webseite.

Dasselbe gilt für einzelne Dateien, etwa eine JPEG-Datei: Bei der Arbeit am Computer erscheint sie dem Benutzer wahrscheinlich zuerst als Listeneintrag in einem Verzeichnisfenster mit Angabe ihres Namens, der Größe, des Typs und verschiedenen Zeitstempeln. Möglicherweise taucht sie auch als graphisches Icon oder als miniaturisierte Vorschau in einem Bildverwaltungsprogramm auf. Vielleicht ist der Benutzer nur an in die Datei eingebetteten Metadaten interessiert, welche die genauen Umstände der Bildaufnahme durch eine Digitalkamera beschreiben. Bildbearbeitungsprogramme können die Datei zudem als Histogramm darstellen, welches die Tonwertverteilung visualisiert. Selbstverständlich kann man in der Bilddarstellung Details vergrößern, so dass ein kleiner Ausschnitt den ganzen Monitor füllt. Und in besonderen Fällen können in der Datei steganographisch verborgene Informationen (z.B. der Quelltext von DeCSS) sichtbar gemacht werden. Für die Mehrzahl der Benutzer mag sich die Vollbilddarstellung einer JPEG-Datei wie deren ›eigentliche‹ Repräsentation ausnehmen; sie ist aber nur eine unter mehreren möglichen Übersetzungen.

Und noch denkbar einfach kodierte Daten, wie die in einer sog. reinen Textdatei gespeicherten, lassen sich nicht auf eine Darstellung reduzieren. Der ›Inhalt‹ auch einer solchen Datei kann in verschiedenen Schriftarten und -größen wiedergegeben werden, mit umgebrochenen oder trunkierten Zeilen, eingeblendeter Zeilennummerierung, Syntaxhervorhebung usw. Die Ausgabe ist jedoch keineswegs auf die graphischen Mittel des Alphabets beschränkt: Der Zeichensatz einer Textdatei, ASCII beispielsweise, beschreibt ja nicht die Gestalt von Schriftzeichen (die Glyphen), sondern deren Charaktere als Grapheme. Mit einem sog. Hexeditor kann man sich deshalb die numerischen Werte der Charaktere bzw. der einzelnen Bytes in hexadezimaler Notation anzeigen lassen. Noch einen Schritt weitergehend könnte man diese Bytes mit einem selbst geschriebenen kleinen Pro-

gramm oder Skript in die Binärdarstellung ihrer Bitwerte übersetzen, eine lange Folge von Nullen und Einsen. Nun mag man versucht sein, eben diese Zahlenwerte als ›richtige‹ Darstellung der Datei zu verstehen. Sind nicht die Zahlen die ›Essenz‹ der Datei, der Ursprung ihrer vielfältigen Übersetzungen? Aber schließlich stehen die Zahlen als Ziffern auf einem Bildschirm oder Blatt geschrieben. Auch sie sind das Produkt eines komplexen Übersetzungsvorganges, der im Lichtschein eines Monitors oder auf Papier fixiertem Farbstoff endet. Als formale Materialitäten existieren die Ziffern nicht. Im ›Innern‹ von Digitalcomputern, in Speicherchips und auf Festplatten, finden sich keine Ziffern, auch keine Zahlen, keine Nullen und Einsen. Was sich finden lässt (das notwendige mikroskopische Gerät vorausgesetzt), sind Spuren forensischer Materialität, die als formale Materialitäten erst programmgesteuert umgeschaltet und zuletzt in Repräsentationen übersetzt werden müssen, von welchen *eine* die auf einem Bildschirm oder Blatt sichtbare Folge der Ziffern 0 und 1 ist.

Die prekäre Identität digitaler Artefakte ist durchaus keine bloß akademische Angelegenheit. Als Amazon – um ein letztes Beispiel anzuführen – die zweite Version des *Kindle* auf den Markt brachte, konnte das Lesegerät digitale Bücher neu auch ›vorlesen‹, d.h. mittels einer synthetischen Stimme in gesprochene Rede übersetzen. In Umkehrung der phonozentrischen Tradition abendländischer Metaphysik behauptete die US-Autorenvereinigung, dies stelle eine unbefugte Tonaufführung der Bücher dar, ein laut Urheberrechtsgesetz vom ursprünglichen ›abgeleitetes Werk‹ (»derivative work«):[21] *Eine* Übersetzung (graphische Schriftzeichen auf dem E-Ink-Display) sollte die ›eigentliche‹, ›primäre‹ Repräsentation des Werkes sein, alle anderen dagegen (wie z.B. die stimmliche Sprachausgabe) davon ›abgeleitet‹ und ›sekundär‹. Technisch und juristisch kann die Übersetzbarkeit digital kodierter Information in bestimmte Darstellungen – im Falle der DVD durch CSS oder beim *Kindle* durch gezielte Deaktivierung der Sprachausgabefunktion – erschwert oder eingeschränkt werden. Die Frage aber, deren Problematik Carmodys Primzahlen-Bitfolgen-Dateiarchive-Computerprogramme deutlich zu machen suchen, bleibt in jedem Fall bestehen: Was ›bedeutet‹ digital kodierte Information? Was stellen digitale Artefakte dar? Die Antworten, welche die jeweiligen Repräsentationen darauf geben, sind nie nur Ergebnis ›neutraler‹ technischer Verfahren. Sie sind immer auch Resultate von Entscheidungen, die im weitesten Sinne computerpolitische genannt werden dürfen.

21 Siehe Michael Kwun: »Does the Authors Guild Want to Sue You for Reading Aloud to Your Kids?« (http://www.eff.org/deeplinks/2009/02/does-authors-guild-want-sue-you-reading-aloud-your, [11.02.2009], 27.02.2010).

LITERATURVERZEICHNIS

Barthes, Roland (1987): *S/Z,* Frankfurt a.M.: Suhrkamp.

Benjamin, Walter (1989): »Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit (Zweite Fassung)«, in: ders.: *Gesammelte Schriften*, Bd. VII, Frankfurt a.M.: Suhrkamp, S. 350-384.

Galloway, Alexander R. (2006): »Protocol vs. Institutionalization«, in: Chun, Wendy Hui Kyong/Keenan, Thomas (Hg.): *New Media, Old Media. A History and Theory Reader*, New York: Routledge, S. 187-198.

Grassmuck, Volker (2006): »Wissenskontrolle durch DRM: von Überfluss zu Mangel«, in: Hofmann, Jeanette (Hg.): *Wissen und Eigentum. Geschichte, Recht und Ökonomie stoffloser Güter*, Bonn: Bundeszentrale für politische Bildung, S. 164-186.

Kirschenbaum, Matthew G. (2008): *Mechanisms. New Media and the Forensic Imagination*, Cambridge, MA u.a.: MIT Press.

Marks, Dean S./Bruce H. Turnbull (1999): »Workshop on implementation issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)«, http://www.lemuria.org/DeCSS/imp99_3.pdf, 27.02.2010.

Pflüger, Jörg (2005): »Wo die Quantität in Qualität umschlägt«, in: Warnke, Martin/Coy, Wolfgang/Tholen, Georg Christoph (Hg.): *HyperKult II. Zur Ortsbestimmung analoger und digitaler Medien*, Bielefeld: Transcript, S. 27-94.

Tholen, Georg Christoph (1997): »Digitale Differenz«, in: Warnke, Martin/Coy, Wolfgang/Tholen, Georg Christoph (Hg.): *HyperKult. Geschichte, Theorie und Kontext digitaler Medien*, Basel u.a.: Stroemfeld, S. 99-116.

Touretzky, David S. (2001): »Free Speech Rights for Programmers«, *Communications of the ACM*, Vol. 44, No. 8, S. 23-25.

Turing, Alan M. (1936): »On computable numbers«, *Proceedings of the London Mathematical Society*, Vol. 42, No. 2, S. 230-265.

UNIX, Unix, *nix

Kopierschutz in der Softwareentwicklung

VON ALEXANDER FIRYN

»SCO is claiming parenthood of that child and now
wants to make money off the earnings of that child. Even
though SCO has refused to undergo the technical
equivalent of DNA testing, and even though my
(and other people's) DNA is probably all over Linux.«
(Linus Torvalds, 2003)

TECHNISCHER KOPIERSCHUTZ UND TECHNISCHE STANDARDS

Wenn von technischem Kopierschutz die Rede ist, dann geht es mehrheitlich um den Schutz von Nutzdaten, etwa Text-, Musik- oder Videodaten. Im einfachsten Fall sind die Besitzverhältnisse an den zu schützenden Daten vollkommen klar, der legitime Verwerter hat eine genaue Vorstellung davon, wem er welche Rechte an den Daten zugestehen möchte und die für die Distribution der Daten ausgewählten Kanäle unterstützen die für die Umsetzung dieser Vorstellung notwendigen Maßnahmen. Moderne Verfahren für das *Digital Rights Management* (DRM), wie sie etwa von Microsoft, Apple oder Adobe bereitgestellt werden, erfüllen selbst exotische Wünsche von Verwertern und verwenden in der Zwischenzeit so sichere Verschlüsselungsverfahren, dass bei der Umgehung der eingesetzten Schutzmaßnahmen wohl tatsächlich eine gewisse kriminelle Energie vorausgesetzt werden muss, die zumindest im juristischen Sinne als hinreichender Beleg für einen Straftatbestand gewertet werden darf, der laut UrhG, §95a Abs. 1 in Deutschland dann vorliegt, wenn »wirksame technische Maßnahmen zum Schutz eines nach diesem Gesetz geschützten Werkes [...] ohne Zustimmung des Rechteinhabers [...] umgangen werden«.

Natürlich gibt es auch weniger einfache Fälle. Als Philips und Sony vor fast dreißig Jahren mit der Spezifikation der Audio-CD begannen, dachte von den Entwicklern niemand daran, dass es eines Tages einen Bedarf an technischen Kopierschutzmaßnahmen für das neue Medium geben würde. Die 1980 veröffentlichte ANSI-Spezifikation[1] der Audio-CD, das sog. *Red Book*[2], sah entsprechend einen

1 Das *American National Standards Institute* (ANSI) wurde 1916 von drei amerikanischen Ministerien, dem Kriegsministerium, dem Schifffahrtsministerium und dem Wirtschaftsministerium, gegründet und zählt neben der internationalen Organisation für Normung (ISO) und deren nationalen Vertretungen, etwa der DIN in Deutschland, zu den wichtigsten Standardisierungsgremien für Technologien und Prozesse. Wie in den meisten Standardisierungsgremien kann auch bei der ANSI jedes – in der Regel dafür zahlende –

solchen Schutz nicht vor. Als 20 Jahre später der Bedarf da war, waren weltweit längst Millionen von Audio CD-Playern im Einsatz, die von ihren Entwicklern brav nach ANSI-Spezifikation entwickelt worden waren. Nachträglich einen technisch wirksamen Kopierschutz in die Audio-CD einzubauen, hätte bedeutet, all diese Geräte in nutzlose Wohnungsdekorationen zu verwandeln. Der dabei sicher entstandene Vertrauensverlust der Kunden in eine ganze Industrie hat glücklicherweise eine Erweiterung des *Red Books* um DRM-Verfahren verhindert. Die Musikindustrie versuchte nun, die effizienten Fehlerkorrekturalgorithmen, die zwar in den meisten reinen Softwareplayern, üblicherweise aber nicht in Hardwareplayern, enthalten waren, durch geschickt angeordnete Bitfehler in den Daten der CDs zum Absturz zu bewegen. Das war für kurze Zeit in vielen Fällen sehr verbreiteter Software wirksam, allerdings auch ausgerechnet bei vielen teuren und hochwertigen Hardwareplayern und führte letztlich nur zu einer Generation neuer Software mit angepassten Korrekturverfahren – und einem massiven Protest der Besitzer hochwertiger CD-Player.[3]

Weitsichtiger war die Industrie bei der Entwicklung der Video-DVD, die von vornherein ein Kopierschutzverfahren enthielt. Mit dem *Content Scrambling System* (CSS) können die Daten auf Video-DVDs verschlüsselt werden. Der Algorithmus für die Verschlüsselung ist standardisiert, einer der gültigen Schlüssel wird Herstellern von DVD-Playern in Hard- oder Software gegen eine Lizenzgebühr zur Verfügung gestellt. Der Einfachheit halber wurde allerdings kein Verfahren für den Austausch oder die Sperre eines Schlüssels bereitgestellt. Würde ein gültiger Schlüssel einmal bekannt werden, könnte jeder durchschnittlich begabte Programmierer eine Software zum lesen – und kopieren – von DVDs entwickeln. Und natürlich wurden Schlüssel bekannt und das schon vor elf Jahren, 1999.[4]

Obwohl Audio-CD und Video-DVD de Facto schutzlos ausgeliefert werden, gibt es keinen Grund anzunehmen, Nutzdaten ließen sich nicht hinreichend vor unerwünschten Zugriffen schützen. Beide Formate sind vor Urzeiten entwickelt worden und beide sind durch die massenhafte Verbreitung von Consumer-Endgeräten dazu verdammt, sich bis zu ihrem bitteren Ende an ihre mangelhaften Standards zu halten. Aber Hand aufs Herz: dieses Ende ist längst eingeläutet. Die

---

Mitglied Vorschläge für Standards machen, die in einem aufwändigen Prozess von Experten geprüft, diskutiert, ggf. überarbeitet und im besten Fall verabschiedet werden.

2 Das *Red Book* ist das erste der sog. *Rainbow Books*, in denen die verschiedenen Standards für CD-Formate definiert sind (vgl. Lehtinen/Russell/Gangemi 2006).

3 Der Heise-Verlag, der in Deutschland die weit verbreiteten Computerzeitschriften *iX* und *c't* herausgibt, hat zu dieser Zeit in Deutschland den Begriff der »Un-CD« geprägt und eine umfangreiche Online-Datenbank mit nicht Standardkonformen Audio-CDs aufgebaut. Dass die Musikindustrie diesen Weg aufgegeben hat, wird auch dadurch belegt, dass diese Datenbank ebenso wie ihre diversen internationalen Pendants inzwischen nicht mehr bereitgestellt wird.

4 Auf dem ersten *Hack*, *DeCSS*, basiert noch heute die *libdvdcss*, die bis vor nicht langer Zeit die einzige technische Möglichkeit bot, unter Linux verschlüsselte Video-DVDs anzuschauen (vgl. Schwabach 2006). Vgl. den Beitrag von Till Heilmann in diesem Heft.

DVD verblasst neben BlueRay und stirbt mit jedem verkauften Großbild-Fernseher einen kleinen Tod. Und den iPod oder irgendeinen seiner Verwandten mit Audio-CDs zu füttern, kommt nur noch für die Archivierung längst verstaubter Bestände in Frage. Die neuen Formate bieten mehr Schutz, als die Musikindustrie inzwischen noch für notwendig hält und die Zeit, als in die Erforschung von DRM-Technologien Milliarden investiert wurden, ist vorbei. Die noch aktiv betriebenen Forschungsfelder aus dem Dunstkreis der DRM-Technologien, etwa das *Perceptual Hashing*[5], werden längst auf den Einsatz in verbesserten Suchtechnologien hin optimiert statt für den Einsatz bei der Plagiatssuche. Und im Laufe des vergangenen Jahres haben alle großen Plattenlabels den Onlinevertrieb von Digitalisaten ohne *technisch* erzwungene Nutzungseinschränkungen erlaubt, nachdem die Industrie erkannt hat, dass der allzu sichere Schutz sich negativ auf den Absatz auswirkt.

Diese Beispiele zeigen, dass die Spielräume für die Einführung und Modernisierung *technischer Kopierschutzverfahren* zum einen davon abhängen, ob und in welchem Maße solche Verfahren in den zugrundeliegenden *technischen Standards* der zu schützenden Medien vorgesehen sind, zum anderen davon, wie weit diese technischen Standards verbreitet sind, wie weit sie also als *de facto Standards* tatsächlich zum Einsatz kommen.

Für die oben besprochenen Nutzdaten entscheiden sich die Möglichkeiten der Einführung technischer Schutzverfahren im Wesentlichen im Zuge einer Kosten-/Nutzenrechnung durch die Industrie. Viel komplizierter ist die Lage allerdings, wenn es nicht um den Schutz der Endprodukte für den Endkunden geht, sondern um den Schutz partieller Produktbestandteile im Produktentstehungsprozess. Bevor etwa ein Hollywood-Film auf DVD gepresst an den Endkunden ausgeliefert wird, mussten schon hunderte, oft tausende von Menschen in den verschiedensten Unternehmen Zugriff auf das zugrunde liegende Material haben. Das betrifft die Cutter, die Digital Composer, die Synchronisationsfirmen, die Kopierwerkstätten und viele weitere Instanzen. Wenn nur an einer dieser Stellen ein Leck entsteht, durch das ein vollständiger Film – unter Umständen schon vor der Kinopremiere – an die Öffentlichkeit dringt, geht es nicht mehr um einen Schaden von ein paar hundert Euro durch illegale DVD-Kopien, sondern schnell um Millionenverluste. Was die Einführung technischer Schutzverfahren in diesen Teil des Prozesses so schwierig macht, ist nicht etwa der Kampf gegen de facto Standards, sondern der Kampf gegen die Komplexität des Prozesses. Effiziente Schutzverfahren müssten jeden Schritt der kooperativen Produktentstehung reflektieren und würden schon bei kleinen Fehlern den gesamten Arbeitsprozess massiv behindern. Um diesem diffusen Begriff der Komplexität Fleisch zu geben, sollen die Schwierigkeiten der Realisierung eines technischen Kopierschutzes, der im Pro-

5 *Perceptual Hashing* bezeichnet eine Gruppe technischer Verfahren zur Erzeugung digitaler Wasserzeichen, mit denen nicht nur 1:1-Kopien digitaler Dateien, sondern auch Varianten mit einem bestimmten Maß an Unterschieden zum Original als Kopie identifiziert werden können (vgl. Ng/Nesi 2008).

duktentstehungsprozess vornehmlich digitaler Produkte wirksam werden müsste, an einem Beispiel aufgezeigt werden, nämlich der Mutterdisziplin aller digitalen Produktentwicklungen: der Entwicklung von Software. Konkret wird diese Problematisierung am Beispiel der Entwicklung des Betriebssystems UNIX vollzogen, das wegen seiner langen Geschichte fast als ein Vergrößerungsglas der Herausforderungen gesehen werden kann, die letztlich alle digitalen Produktlebenszyklen treffen.

VERGLEICHE

> »Dear Steve: As you requested below is a draft of my report on existence the of Unix derived code in Linux. What we tried to do is to determine if there was any material from Unix in the Red Hat Linux release 5.2. To make this determination we used a copy of Red Hat Linux which was purposed from the local Best Buy. We then compared it to multiple copies of Unix. We received sources from SCO of OpenServer 5.0 dated January 27, 1998, Gemini Source dated January 27, 1998, it being UnixWare 7, UnixWare 3.2, UnixWare 4.0 and UnixWare 4.2. Additionally we received various versions of files which were not on the release described. To perform this work we unpacked and obtained the sources for Red Hat from the CDs which are provided and files in Linux and the various versions of Unix. For example we compared Unix yacc to the Linux bison and the Unix awk to the Linux mawk. We performed this comparison on all files which had similar functionality.« (Swatz 1999: 1)

Mit diesen Worten aus einem Memorandum an Steve Sabbath, seinerzeit Vice President of Law der Santa Cruz Operation (SCO), beginnt eines der traurigeren Kapitel der Softwaregeschichte. SCO war einst berühmt und erfolgreich geworden, weil sie das – gerade im profitablen Unternehmensgeschäft – wichtige Betriebssystem UNIX in einer Version verkauften, die auf der i386-Architektur lief, also auf handelsüblichen Intel-kompatiblen PCs, die sich auch Privatanwender und eben kleine Unternehmen leisten konnten. Im Laufe der neunziger Jahre konnte SCO in diesem Segment erhebliche Marktanteile gewinnen und verdiente genug Geld, um 1995 sogar den Quellcode von Novells UnixWare erwerben und damit in das Unix-Geschäft auch mit Großrechnern einsteigen zu können.

Damit ist der glückliche Teil der Unternehmensgeschichte von SCO aber auch schon erzählt: Novell konnte sich die Hände reiben, UnixWare für viel Geld verschachert zu haben, bevor der Markt für Unix-Großrechnersysteme einbrach und SCO musste mit ansehen, wie nicht nur das gerade neu betretene Segment sich auflöste, sondern auch die Einnahmen im alten i386-Geschäft wegbrachen. Diese Entwicklung hatte vor allem drei Ursachen: Die i386-Plattform wurde mit Einführung des Pentium-Prozessors 1993 erheblich leistungsfähiger, so dass es sich für immer mehr Unternehmen lohnte, viele preiswerte PCs anzuschaffen,

statt eines (sehr) teuren Großrechners und vieler preiswerter Terminalplätze. Zugleich gelang es Microsoft, sein Betriebssystem Windows auch im Bewusstsein von IT-Entscheidern in Unternehmen mit der Aura eines konkurrenzlosen Standards zu etablieren. Mit Windows NT 4.0 existierte spätestens 1998 eine Windows-Variante, die zumindest die am häufigsten benötigten Funktionalitäten eines Servers unterstützte und zugleich viel preiswerter war als Unix. Und letztlich wurde im Laufe der neunziger Jahre eine ganze Reihe quelloffener Nachbauten von Unix entwickelt, die vollkommen kostenlos über das Internet verteilt wurden und ebenfalls auf i386-PCs liefen. Der erfolgreichste dieser Nachbauten war schon Ende der 1990er Jahre Linux und weil Linux den Markt für kostenpflichtige i386-Unixe vernichtete, war es SCO ein Dorn im Auge.

Noch wenige Jahre vorher war es kaum denkbar, dass der gesamte Unix-Markt eines Tages einbrechen könnte. Die Geschichte von UNIX beginnt schon in den 1960er Jahren, lange vor der aller anderen heute noch bekannten Betriebssysteme. Einige Entwickler der Bell Laboratories, vor allem Ken Thompson und Dennis Ritchie, waren damals in ein großes Entwicklungsprojekt zahlreicher Unternehmen involviert, dessen Ziel es war, ein standardisiertes Betriebssystem zu schaffen, das auf vielen verschiedenen Computern lauffähig sein sollte. Thompson und Ritchie hatten viele Vorschläge für dieses System, das MULTICS heißen sollte, aber in einem so großen Konsortium ließen sich nur wenige dieser Vorschläge durchsetzen. Als die Bell Labs sich 1969 aus dem Konsortium zurückzogen, hatten die beiden die Freiheit, Ihre Pläne intern umzusetzen – und wohl auch den Ehrgeiz, ein besseres Ergebnis zu schaffen als der Rest des Konsortiums, das sich währenddessen weiter über MULTICS stritt.[6] Der Vorzug des nun kleinen Teams waren die kurzen Entscheidungswege, die eine ganze Reihe seinerzeit sehr radikaler Designentscheidungen ermöglichten. In diesem Sinne war es sicherlich auch hilfreich, dass die Bell Labs selber kein strategisches Interesse an diesem Projekt hatten und so zwar wenig Unterstützung leisteten, aber eben auch nicht störend eingriffen. Thompson, Ritchie und einige Kollegen entwickelten eine eigene Programmiersprache, C[7], ein sehr leistungsfähiges Dateisystem und vor allem eine zukunftsweisende Entwicklungsphilosophie. Statt, wie es bis dahin üblich war, die Software möglichst gut auf die Fähigkeiten der Hardware zu optimieren, legte das Team großen Wert darauf, möglichst einfachen, gut lesbaren und damit auch gut wartbaren Quellcode zu schreiben, der so weit von der Hardware abstrahiert, dass er sich auf möglichst vielen Hardwareplattformen ohne Codeänderungen in Binärcode übersetzen lässt. Schnell, so war der propagierte Gedanke, wird die Software von selber, wenn die Hardware der nächsten Generation schneller wird.[8] Wer seinen Code optimiert, der muss für jede neue Hardware neuen Co-

6 Zur Geschichte von MULTICS vgl. Ceruzzi 2003.

7 Die klassische Einführung in C, die nicht nur für angehende Programmierer immer noch interessant ist, stammt von den Erfindern selber (vgl. Kernighan/Ritchie 1988).

8 Das berühmte *Moore's Law* von der jährlichen Verdoppelung der Schaltkreise auf einem Computerchip und dem damit einhergehenden Geschwindigkeitszuwachs wurde von

de schreiben – und das kostet viel mehr Zeit und Geld, als einfach auf die neue Hardware zu warten. Ein ähnliches Vorgehen hatte IBM bereits in den 1960er Jahren bei der Entwicklung des Betriebssystems OS/360 gewählt. OS/360 sollte nicht auf einzelne Computer, die fast in Handarbeit für die Bedürfnisse eines einzigen Kunden gefertigt wurden, zugeschnitten sein, sondern alle Bedürfnisse erfüllen können, die Kunden an ein Betriebssystem stellen könnten. Während IBM diese Kompatibilität aber dadurch sicherstellte, dass sie eine skalierbare Hardwarearchitektur, das System/360[9], entwickelten, das über alle seine Möglichkeiten hinweg vom OS/360 unterstützt wurde, war der Ansatz von UNIX noch radikaler. UNIX sollte grundsätzlich mit möglichst geringem Aufwand auf jede Hardware jeden Herstellers portiert werden können, was überhaupt erst die Geburtsstunde von Software als eigenständigem, von der Hardware unabhängigem, Produkt markiert.[10]

Ein weiterer wesentlicher Leitsatz der UNIX-Philosophie lautet: »Do one thing and do it right.«[11] Dieser unscheinbare Satz ist untrennbar mit dem Namen Douglas McIlroy verbunden, der das sog. *Pipes*-Konzept erfunden hat.[12] Die Idee ist, grundsätzlich nur winzige Mikroanwendungen zu programmieren, die genau eine Aufgabe erfüllen, als Eingabeparameter eine Zeichenfolge erhalten und als Ergebnis auch wieder eine Zeichenfolge ausgeben. Über eine Folge McIlroy'scher Pipes sollen sich die Ausgaben eines Programms dann als Eingabe für ein weiteres Programm verwenden lassen, so dass zur Erledigung einer komplexen Aufgabe eine Pipeline aus sehr einfachen Programmen erzeugt wird. Dieses Pipe-Konzept wurde in UNIX zum ersten Mal umgesetzt und ist bis heute ein wichtiger Grund für die Leistungsfähigkeit aller Unix-artigen Betriebssysteme. Statt beispielsweise ein Programm zu schreiben, das die Anzahl aller Zeilen einer *Datei* ausgibt, in denen ein bestimmtes *Wort* vorkommt, werden für diese ›komplexe‹ Aufgabe zwei Programme verwendet: eines, das alle Zeilen ausgibt, in denen das Wort vorkommt (*grep*) und ein weiteres, das diese Zeilen zählt und die Summe ausgibt (*wc*), verkettet über den Pipeoperator »|«.

Als Befehl liest sich das Beispiel dann: *grep »Wort« < »Datei« | wc*. Um noch ein Beispiel zur Veranschaulichung zu bringen, nehmen wir den Fall an, ein Nutzer möchte alle Jpeg-Dateien in einer Verzeichnisstruktur auf eine CD-Rom brennen.

Gordon Moore erstmals 1965 postuliert. 1975 korrigierte er seine Prognose auf eine Verdoppelung alle zwei Jahre; 2007 sagte er das nahende Ende seines ›Gesetzes‹ voraus (vgl. Lanzerotti 2006).

9 Zum System/360 vgl. Brooks 1995.

10 Wer dies für einen Widerspruch zu einem der berühmtesten Aufsätze über Computergeschichte hält, lese noch einmal: Kittler: »Es gibt keine Software« (1993).

11 Die beste und vollständigste Darstellung dieser Philosophie, deren Leitsätze hier nur tangiert werden, findet sich in: Raymond: *The Art of Unix Programming* (2004).

12 Als Leiter des Computing Techniques Research Department der Bell Labs zählt McIlroy neben Thompson und Ritchie zu den wichtigsten, in historischen Darstellungen aber häufig unterschlagenen Initiatoren hinter UNIX. Er ist übrigens tatsächlich promovierter Philosoph.

Unter Linux und vielen anderen UNIX-artigen Betriebssystemen könnte dafür eine Pipeline aus dem Programm *find* zum Suchen nach Dateien, dem Befehl *mkisofs* zum Erzeugen eines CD-kompatiblen (ISO-9660 konformen) Dateisystems sowie dem Befehl *cdrecord*[13] zum Schreiben eines Datenstroms auf einen CD-Rohling verwendet werden. Das könnte sich dann (etwas vereinfacht) so lesen: *find . -iname *.jpg | mkisofs -Jr | cdrecord -*.

Auch wenn solche Befehlsfolgen dem einen oder anderen spontan nicht sonderlich attraktiv anmuten, wird eines doch hoffentlich nachvollziehbar: der Entwicklungsaufwand für die Unterstützung immer komplexerer und individuellerer Anforderungen lässt sich mit dem Pipe-Konzept erheblich reduzieren. Statt immer wieder einzelnen Programmen die Fähigkeit zu geben, Dateien nach einem bestimmten Muster finden zu können – mal besser, mal schlechter implementiert – wird diese Funktionalität auf einem Unix-System nur ein einziges mal bereitgestellt, nur an dieser Stelle so gut wie möglich implementiert, und alle Prozesse im System können auf diese eine Implementierung zugreifen. Im Pipe-Konzept spiegelt sich aber auch noch einmal der Leitsatz, auf eine Optimierung zu verzichten. Drei Programme hintereinander zu starten, um eine Aufgabe zu erfüllen, kostet natürlich mehr Systemressourcen, als all diese Funktionen in einem einzigen, speziell für diese Anforderung optimierten Programm zusammenzufassen. Dieser Nachteil wird aber dadurch belanglos, dass sich im Pipe-Konzept nach der einmaligen Entwicklung aller wichtigen Basisfunktionen quasi endlos viele komplexe Anforderungen erfüllen lassen, ohne auch nur einen einzigen weiteren Moment in die Entwicklung zu investieren. UNIX opfert also ein wenig der preiswerten Ausführungszeit, um im Gegenzug sehr viel teure Entwicklungszeit einzusparen.[14]

FRÜHE GENEALOGIE VON UNIX: VON OPEN SOURCE ZUM SCHÜTZBAREN EIGENTUM

Die erste, nach heutigem Verständnis eines Unix, vollständige Version wurde 1973 fertiggestellt und erhielt bei den Bell Labs die Versionsnummer 4. UNIX V4 war vollständig in der neuen Sprache C geschrieben und setzte McIlroys Pipe-Konzept mit einer Menge einfacher Tools um. Die Version war zudem durch das neu entwickelte Dateisystem und die Prozesssteuerung mehrbenutzerfähig – auch eine Eigenschaft, die vollkommen neu war. Diese Version wurde am Anfang nur von den Bell Labs selber genutzt, zunächst für die Textverarbeitungssysteme der eigenen Patentabteilung. Weil es der Muttergesellschaft der Bell Labs, AT&T, seit 1956 verboten war, außerhalb des Telefonmarktes kommerziellen Aktivitäten

13 Weder *cdrecord* noch *mkisofs* zählen zu den historischen UNIX-Programmen, sondern zu den *cdrtools*, die von Jörg Schilling seit 1996 für Linux und viele andere Unix-Derivate entwickelt werden.

14 Gerade unter diesem Aspekt werden die Grundlagen für die bestmögliche Softwareentwicklung auch heute noch in der Tradition der UNIX-Philosophie weiter erforscht; inzwischen unter dem Stichwort »Agile Software« (vgl. etwa Shore/Warden 2007).

nachzugehen, konnten die Bell Labs allerdings sehr schnell anfangen, offensive Werbung für ihre neue Errungenschaft zu machen. Und offensiv hieß hierbei, dass sie UNIX inklusive der Quellcodes jedem unentgeltlich zur Verfügung stellten, der daran ein Interesse hatte.[15] Im Laufe der siebziger Jahre konnte UNIX sich deshalb mit ungeheurer Geschwindigkeit verbreiten und avancierte zum Standardlehrmaterial für Betriebssystem-Vorlesungen an Universitäten. Es wurde aber nicht nur verbreitet: weil die in C geschriebenen Quellcodes ohne Restriktionen mitgeliefert wurden, konnte auch jeder das System nach Belieben ändern und erweitern. Bereits nach wenigen Jahren brachte die University of Berkeley mit der *Berkeley Software Distribution* (BSD) ein eigenständiges System auf den Markt, das sich an vielen Stellen vom Original unterschied – teilweise waren neue Programme hinzugefügt, teilweise waren auch in Bells UNIX vorhandene Programme neu implementiert oder die vorhandenen Implementierungen geändert worden. Bis in die achtziger Jahre hinein war BSD allerdings das einzige UNIX-Derivat, das sich in großen Teilen von der Originalversion unterschied.

Das änderte sich grundlegend, als AT&T sich 1982 durch das Abstoßen einer Reihe von Tochterunternehmen von den Auflagen befreien konnte, die 1956 erlassen worden waren. UNIX war zu diesem Zeitpunkt schon das am weitesten verbreitete Betriebssystem der Welt und der Computermarkt wurde zunehmend interessanter, wenn man Geld verdienen wollte. AT&T erklärte kurzerhand, dass das 1979 veröffentlichte UNIX V7 die letzte frei zur Verfügung gestellte Version bleiben würde und eine künftige Verwendung des UNIX-Codes lizensierungspflichtig sei. Der Schwerpunkt war nun nicht mehr die Entwicklung im akademischen Eigeninteresse, sondern ein kommerzieller Vertrieb. Unter Rückgriff auf eine bereits 1978 bei den Bell Labs begonnene Erweiterung von UNIX, die aber bis dahin unveröffentlicht geblieben war, wurde das Betriebssystem in sehr schneller Zeit um viele Funktionalitäten erweitert, die im frei verfügbaren UNIX V7 nicht enthalten waren.[16] Dieses neue System sollte vor allem als hauseigenes Betriebssystem verkauft werden und zwar ohne eine gleichzeitige Auslieferung des Quellcodes. Weil AT&T klar war, dass auch weiterhin Interesse am Quellcode bestehen würde, den vor allem viele Hardwarehersteller benötigten, um UNIX auf ihre Hardwarearchitekturen zu portieren, wurde 1983 außerdem das UNIX System V freigegeben, das im Unterschied zu den UNIX-Versionen bis V7 allerdings kostenpflichtig lizensiert werden musste. Die Lizenznehmer durften den entstandenen Quellcode auch nicht weitergeben.

Allerdings hatte AT&T die Rechnung ohne die Berkeley University gemacht. In BSD war bis zur Kommerzialisierung des Ur-UNIX bereits viel Geld und Arbeit

15 Nicht ganz kostenlos: Die Interessenten mussten die Kosten für die Datenträger und das Porto übernehmen. Marc Shuttleworth hat auch darauf noch verzichtet, um seine Linux-Distribution Ubuntu seit 2004 als Standard-Linux-Distribution zu etablieren – mit Erfolg.

16 Die Rede ist von *PWB*. Eine sehr wertvolle und stetig aktualisierte graphische Darstellung der gegenseitigen Einflüsse diverser UNIX, Unix und *nix-Derivate stellt Éric Lévénez auf seiner Webseite http://www.levenez.com/ bereit.

geflossen. Unter anderem verfügte BSD bereits 1981 über eine Implementierung des TCP/IP-Protokolls[17], das sich in kurzer Zeit zum grundlegenden Netzwerkprotokoll für das Internet entwickeln sollte. Neben der *Digital Equipment Corporation* (DEC), die mit ihren PDP und VAX-Maschinen zu den wichtigsten Computerlieferanten dieser Zeit gehörte, war auch die DARPA[18], die Forschungsabteilung des amerikanischen Verteidigungsministeriums, Kunde und Förderer der Distribution aus Berkeley. Als dann noch der schnell wachsende Hardwarehersteller SUN auf Basis von BSD das kommerzielle SunOS entwickelte und zu verkaufen begann, war der Geschäftsplan von AT&T erheblich gefährdet. Zum Glück für den erfahrenen Monopolisten wurden in BSD – und damit auch in SunOS – trotz aller Eigenständigkeit immer noch einige wenige, aber wesentliche, Stücke aus dem originalen UNIX-System verwendet, was AT&T Gelegenheit bot, von jedem Kunden von BSD und SunOS Lizenzgebühren für die Nutzung dieser Bestandteile einzufordern. Diese Forderung führte gleichzeitig zu einer Zersplitterung wie auch einer Konsolidierung: Sun und AT&T konnten sich schnell darauf einigen, dass sie mit einem gemeinsamen Vorgehen die besten Chancen im Markt haben würden. Bereits 1986 wurde mit SunOS 3.0 ein grundlegend überarbeitetes Betriebssystem veröffentlicht, das nun nicht mehr auf BSD, sondern auf AT&Ts System V basierte, allerdings die immer noch frei verfügbaren ›mehrwertigen‹ Tools aus BSD integrierte. Gleichzeitig gab die Berkeley University eine Variante von BSD frei, in der keine Komponenten aus dem Besitz von AT&T mehr enthalten waren. Dieses sog. *Networking Release* war zwar ohne den AT&T-Anteil zunächst kein vollständiges, lauffähiges Betriebssystem, enthielt aber soviel Funktionalität, dass die nun fehlenden Teile nach einiger Zeit von neuen Entwicklern nachgerüstet werden konnten. In dieser Linie war 386BSD das erste vollständige Unix-Betriebssystem, das keinen Code des Ur-UNIX mehr verwendete. Die bekanntesten heute noch existierenden Systeme auf dieser Basis sind FreeBSD und das darauf aufbauende Darwin, das wiederum den Kern von Apples Mac OS X bildet.[19]

---

17 Entwickelt wurde die TCP/IP-Familie seit etwa 1972 bei der DARPA von Robert E. Kahn und Vinton Cerf. 1982 wurde TCP/IP zum verbindlichen Standard für militärische Netzwerke in den USA erhoben, was den Vorsprung von BSD gegenüber AT&T-UNIX überhaupt erst zu einem, zumindest kleinen, Wettbewerbsvorteil werden ließ. Die Besonderheiten der BSD-Implementierung sowie die Auswirkungen dieser Implementierung werden in Stevens: *TCP/IP Illustrated* (1995) behandelt.

18 Die *Defense Advanced Research Projects Agency* (DARPA) wurde Ende der 1950er Jahre gegründet, um den amerikanischen Technologievorsprung vor der UDSSR sicherzustellen. Die Behörde hat mit ihren Forschungsprojekten maßgebliche technische und methodische Grundlagen für alle Bereiche der IT-Industrie gefördert (vgl. Ceruzzi 2003; Flamm 1988).

19 Neben FreeBSD bildet eine Weiterentwicklung des Mach-Kernels einen wesentlichen Baustein für Darwin, den Steve Jobs schon Ende der 1980er Jahre als Grundlage für sein (erfolgloses) NeXTSTEP-Betriebssystem gewählt hatte. Der Mach-Kernel selber ist aus 4.2BSD an der Carnegie Mellon University entstanden und war eines der ersten wichti-

UNIX-KRIEG UND KONSOLIDIERUNG

Neben den beiden Lagern, BSD auf der einen Seite, AT&T und Sun auf der anderen, traten noch eine Reihe von Unternehmen auf den Plan, die auf Basis des lizensierten AT&T Quellcodes eigene UNIX-Derivate entwickelten und binär vertrieben. Dazu zählten vor allem Hewlett & Packard mit HP-UX sowie Microsoft, die ihr XENIX aber schon 1984 verkauften: an SCO.[20] Die schnell entstandene Vielfalt an UNIX-Derivaten war aber all den Unternehmen ein Dorn im Auge, die UNIX zwar an Endkunden verkauften, selber aber keine Betriebssysteme entwickelten. Je mehr sich die verschiedenen Derivate voneinander entfernten, desto schwieriger wurde es plötzlich wieder, vorherzusagen, ob eine bestimmte Software auf einem bestimmten UNIX-Derivat laufen wird. Genau diese Sicherheit verlangen aber die Endkunden. 1984 schloss sich eine Gruppe solcher Unternehmen zum X/Open-Konsortium zusammen und formulierte eine Reihe von Standards, die ein Unix-System ihrer Auffassung nach erfüllen müsste, um eine minimale Kompatibilität unter den Derivaten sicherzustellen. Als klar wurde, dass eine solche Forderung wenig Eindruck machte, insbesondere auf AT&T, gründeten einige der X/Open-Mitglieder noch eine zweite Initiative: die *Open Software Foundation* (OSF).[21] Statt nur zu standardisieren, setzten die Mitglieder der OSF die formulierten Standards auch gleich um, indem sie die freien Teile von BSD um eigene Komponenten ergänzten, insb. um einen eigenen Betriebssystemkernel, den *Mach*-Kernel. Aus dieser Initiative entwickelten sich mit NeXTSTEP (1988) und OSF/1 (1990) zwei Betriebssysteme, die die Anforderungen der X/Open erfüllten und keinen Code von AT&T enthielten. Weil auch Hewlett & Packard und IBM der OSF beigetreten waren, wurden auch deren Betriebssysteme HP-UX und AIX vom System V unabhängig, so dass AT&T auch von diesen wichtigen Betriebssystemherstellern keine Lizenzgebühren mehr einfordern konnte. AT&T machte zwar noch einige erfolgreiche juristische Vorstöße wegen Markenrechtsverletzungen gegen X/Open, gegen den Vertrieb der Software konnte AT&T aber keine Rechte geltend machen. Als sich abzeichnete, dass Systeme, die sich an mehrheitlich vereinbarte Industriestandards halten, leichter verkauft werden konnten, trat AT&T schließlich selber dem Konsortium bei. Kurze Zeit später, 1993, verkaufte AT&T sogar seine gesamten UNIX System Laboratories, inklusive dem nun schon erheblich entwerteten UNIX System V, an den Netzwerkspezialisten Novell und konzentrierte seine Gewinninteressen auf den Vertrieb der Markenrechte.

---

gen Ergebnisse der OSF: ein Unix-Kernel, der ohne Codebestandteile von AT&T auskam.

20 XENIX war der erste Versuch von Microsoft, ein Standard-Betriebssystem für IBM-PCs zu liefern. Allerdings war die UNIX-Portierung zu ressourcenhungrig für die frühen IBM-PCs, so dass erst der zweite Versuch, das erheblich leistungsärmere MS-DOS, zum Ziel führte. Mit der Etablierung von MS-DOS als Standardbetriebssystem für PCs war XENIX für Microsoft strategisch wertlos geworden (vgl. Clukey 1985).

21 1996 sind OSF und X/Open zur Open Group fusioniert.

TECHNISCHE SCHUTZMAßNAHMEN

Nach soviel Geschichtsaufarbeitung muss begonnen werden, über Schutzmaßnahmen nachzudenken. Es wird klar geworden sein, dass UNIX eine ganze Reihe von Elementen mitbringt, die aus jeweils verschiedenen Perspektiven des Schutzes bedürfen. Zumindest drei dieser Elemente sollen hier benannt werden:

Zum ersten die Philosophie hinter Unix. Die Unix-Philosophie und ihre konsequente Anwendung bildet die Grundlage für den einmaligen Erfolg dieses Betriebssystems. Als Philosophie allerdings lässt sie sich schwerlich mit technischen Mitteln schützen, sondern nur durch ihre Anwendung. Es wird aber klar werden, dass sie gerade durch ihre Anwendung Einfluss auf die technische Schützbarkeit anderer Elemente hat.

Zum zweiten stellt die Marke UNIX ein schützenswertes Gut dar, das allerdings auch wiederum nicht unmittelbar durch technische Mittel geschützt werden kann.

Zum dritten bedarf die Architektur von Unix, gewissermaßen die Gemeinsamkeit aller verschiedenen Unix-Derivate, eines Schutzes, durch den die Kompatibilität der einzelnen Derivate untereinander auf jeweils verschiedenen Ebenen sichergestellt wird. Dieser Schutzbedarf wird nicht jedem sofort als ein Bedarf an Kopierschutzmechanismen plausibel sein – tatsächlich geht es aber genau darum. In den Anfangsjahren von UNIX schützte die kleine Entwicklergruppe an den Bell Labs die Architektur von Unix dadurch, dass ihr eigenes UNIX die Ausformung dieser Architektur bildete. Technisch gesprochen: Das Betriebssystem UNIX war die einzige Instanz der Unix-Architektur, die unabhängig von dieser Instanz noch überhaupt nicht existierte. Mit dem Beginn der aktiven Eigenentwicklung BSD in Berkeley bildete sich eine zweite Instanz heraus, die sich in vielen Punkten von der Bell Labs-Instanz unterschied, sehr wohl aber auf ihr aufbaute und von ihr profitierte. Die Bell Labs hatten zum Beispiel entschieden, dass sämtliche Netzwerkkommunikation unter UNIX mittels *Streams* realisiert wird, einem speziellen Verfahren, um den Datenaustausch zwischen Betriebssystemkernel und Endanwendungen zu unterstützen. Das war eine Architekturentscheidung die letztlich in jeder Netzwerkanwendung für UNIX reflektiert werden musste. In Berkeley entschied man sich aber gegen Streams und stellte die Netzwerkfunktionen stattdessen über Sockets bereit – mit der Folge, dass für UNIX entwickelte Netzwerkprogramme, etwa FTP, Telnet, später die ersten Webbrowser, entweder nur auf einer der beiden Architekturinstanzen lauffähig waren oder beide Varianten unterstützen mussten, was die Entwicklung jeder einzelnen Anwendung aufwändiger machen müsste. Weil BSD sehr schwergewichtige Förderer hatte, konnte aus Berkeley schon an dieser einen Stelle ein erheblicher Druck auf die Architekturentscheidungen der Bell Labs ausgeübt werden, mit den Anwendungsentwicklern und Endnutzern als Leidtragenden. Bei einer stetig wachsenden Zahl von Instanzen müssen solche Machtkämpfe letztlich zur Auflösung der ganzen Architektur führen.

Dass inzwischen zwar kaum noch ein relevantes Betriebssystem existiert, das in direkter Linie vom ursprünglichen UNIX abstammt[22], dafür aber eine Familie von Unix-Betriebssystemen, die sich durch die Bindung an gemeinsame Architekturentscheidungen auszeichnen und dadurch untereinander – auf verschiedenen Ebenen – kompatibel sind, ist dem technischen Schutz dieser Architektur durch technische Standards zu verdanken, wie sie zuerst vom X/Open-Konsortium gefordert und aufgestellt und dann von der OSF in Instanzen dieser standardisierten Architektur umgesetzt worden sind. Der *X/Open Portability Guide*, der in mehreren Abschnitten von 1984 bis 1992 veröffentlicht wurde, war in seiner letzten Fassung in drei Themenkomplexe unterteilt: Erstens: »System Interfaces and Headers«, also alle technischen Voraussetzungen, die auf einer Instanz der Unix-Architektur gegeben sein müssen, um auf diesen aufbauend Anwendungen entwickeln zu können. Zweitens: »Commands and Utilities«, also alle Anwendungen, die auf einer solchen Instanz mindestens vorhanden sein müssen, inklusive einer Beschreibung der zulässigen Parameter, der Namen der Programme sowie der zu liefernden Ergebnisausgaben – all das ist elementar wichtig, um dieselben Pipelines auf verschiedenen Unix-Instanzen ausführen zu können. Drittens: »System Interface Definitions«, also alle Funktionsaufrufe (Calls), die von Programmen an die Basis des Betriebssystems gemacht werden können müssen sowie die zu liefernden Rückgaben dieser Systemaufrufe. In diesen Bereich fällt beispielsweise auch, dass eine Unix-Instanz Calls bereitstellen muss, die es Netzwerkanwendungen erlauben, über Streams mit dem Betriebssystemkernel zu kommunizieren, der wiederum die reale Hardware, etwa eine Netzwerkkarte, verwaltet. Diese X/Open-Standards bilden auch heute noch die Grundlage für die sog. »Single UNIX Specification«, die zuletzt 2001 von der heute zuständigen Austin Group[23] in Version 3 freigegeben wurde. Jedes Betriebssystem, das heute den Markennamen UNIX nutzen will, muss diese Spezifikation in der aktuellen Form fehlerfrei umsetzen. Ergänzt wird dieser Standard durch den sog. POSIX-Standard[24], in dem noch viele weitere Gebiete behandelt werden, auf denen technische Kompatibilität wichtig ist, dabei aber keine grundsätzliche UNIX-Kompatibilität fordert. Der POSIX-

22 SUN lässt sein Solaris seit 2004 überwiegend unter einer Open Source Lizenz – und unter dem Namen *Open Solaris* - entwickeln. In diesem Zuge werden die historischen Bestandteile aus UNIX Stück für Stück ersetzt. Bleibt als verbreitetes System aus der UNIX-Linie noch HP-UX, dessen Verbreitung sich aber auf einen kleinen Teil der von HP vertriebenen Server beschränkt und das auf den inzwischen wichtigsten Hardwareplattformen, i386 und x86_64, nicht lauffähig ist.

23 Die Austin Group ist eine Arbeitsgruppe innerhalb der Open Group. Auf der Webseite der Austin Group werden zahlreiche Protokolle zur Verfügung gestellt, die einen interessanten Einblick in die Arbeit eines Standardisierungsgremiums geben.

24 Der Name POSIX wurde vom Leiter des GNU-Projekts, Richard Stallman, eingeführt und steht für *Portable Operating System Interface*. Der offizielle Name des Standards, der vom *Institute of Electrical and Electronics Engineers* (IEEE) verabschiedet wird, lautet »IEEE 1003.1«. IEEE 1003.1 ist zugleich von der ISO als »ISO9945« bestätigt worden (vgl. dazu die UNIX-Seiten der Open Group unter www.unix.org).

Standard lässt sich also auch erfüllen, ohne Pipe-Konzept und viele andere wesentliche Teile der Unix-Philosophie und der UNIX-Architektur umzusetzen. Insbesondere im Themenkomplex der Netzwerkkommunikation werden in POSIX stattdessen viele umfangreichere und präzisere Anforderungen an POSIX-konforme Betriebssysteme gestellt, deren Einhaltung den Datenaustausch zwischen verschiedenen Betriebssystemen sicherstellt. So verfügt etwa auch Microsofts Betriebssystem Windows über optional installierbare POSIX-Erweiterungen, so dass es zu den POSIX-konformen Systemen gehört – ohne auch nur im Ansatz ein Unix zu sein.

Jeder, der in der Lage ist, einen Standard mitzubestimmen oder sogar zu kontrollieren, der sich als technischer Standard in einer ganzen Industrie durchsetzen lässt, hat viel mehr Macht als jene, die nur über Produkte verfügen, die sich an diese Standards halten. Insofern war es eine brillante Entscheidung von AT&T, sich aus der Entwicklung einer einzigen Instanz von Unix – UNIX – zurückzuziehen, um stattdessen zumindest einen Teil der Kontrolle über alle Instanzen der Unix-Architektur zu erringen. Wer diese sehr effektive Art des Kopierschutzes ›knacken‹ will, der muss aus eigener Kraft einen neuen Standard setzen, den er selber kontrollieren kann. Das aber ist eine schwierige Aufgabe.

Obwohl mit dem Aufkommen der Macht von Architekturen über die konkrete Implementierung einzelner Instanzen der konkrete Quellcode einer Implementierung fast in den Hintergrund tritt, steckt doch auch in der Implementierungsarbeit soviel Zeit, Wissen und letztlich Geld, dass dieser Quellcode als viertes Element mit Schutzbedarf zu bemerken ist. Nun lässt sich Quellcode am effektivsten vor unerwünschten Kopien schützen, indem man ihn gar nicht erst verfügbar macht. Auch hier helfen die oben benannten technischen Standards, den Quellcode zu schützen, ohne den Wert des Systems zu gefährden. Wer eine Anwendung für eine bestehende Instanz der Unix-Architektur entwickeln will, kann zwar die notwendigen Informationen über die verfügbaren Schnittstellen, die Ein- und Ausgabemöglichkeiten, die bereitstehenden Systemcalls etc. aus dem Quellcode dieser Instanz extrahieren – so ihm dieser zur Verfügung steht –, das wäre aber ohnehin eine mühselige Aufgabe. Viel effizienter ist es, wenn er sich bei seiner Entwicklung nicht an der zugrundeliegenden Instanz orientiert, sondern an den übergeordneten Architektur-Standards, die wohl dokumentiert zur Verfügung stehen. Für den Hersteller des Betriebssystems entfällt damit die Notwendigkeit, einem Anwendungsentwickler den eigenen Quellcode zur Verfügung zu stellen. Der Anwendungsentwickler profitiert davon, dass seine Anwendung nicht nur auf der einen Instanz laufen wird, sondern auf allen Instanzen der Architektur, auf deren technischen Standards er aufbaut. Das heißt, auch für Quellcodes können technische Standards als Kopierschutzverfahren herangezogen werden.[25]

25 Das ist sogar der übliche Weg, Schnittstellen für die Softwareentwicklung bereitzustellen.

Eine Ausnahme muss hier allerdings gemacht werden und die führt auf das Memorandum an Steve Sabbath zurück: Wer nicht nur Anwendungen für Unix-Instanzen entwickeln will, sondern selber eine vollständige eigene Instanz von Unix kontrollieren möchte, der wird vom Einblick in den Quellcode einer anderen Unix-Instanz unter Umständen profitieren können.

SCO VS. RED HAT

Novell erkannte recht schnell, dass der Abkauf des Ur-UNIX von AT&T dem Unternehmen kaum Nutzen bringen würde, weil der Markt für UNIX einzubrechen begann und die Entwicklung guter Unix-Systeme vom originalen UNIX-Code kaum noch profitieren konnte. Bereits zwei Jahre nach dem Kauf, 1995, verkaufte das Unternehmen seine UNIX-Abteilung und die bei Novell entwickelten, auf UNIX basierenden, Derivate UnixWare und OpenServer weiter an SCO. SCO hielt damit zwar die Rechte am Quellcode dieser Derivate, war aber in die wichtigen Gremien, die die Architektur kontrollierten, nicht involviert. Als man endlich auch bei SCO merkte, dass diese Derivate keinen nachhaltigen Wert mehr hatten, wurde ein Schuldiger gesucht – und in Form des jungen, aber extrem erfolgreichen Unternehmens Red Hat schnell gefunden, vielleicht zu schnell.

Red Hats Erfolg basierte auf einem Betriebssystem, das Unix in vielen Punkten sehr ähnlich war, selber aber nicht auf Unix basierte, nämlich *Linux*. Die Entwicklung von Linux wurde Anfang der neunziger Jahre von einem einzigen Studenten, Linus Torvalds, begonnen, der zunächst nur zum Eigenbedarf ein sehr einfaches System entwickelt hatte, mit dem er von seinem heimischen PC auf die Unix-Großrechner in seiner Universität zugreifen konnte. Als Torvalds in einer UseNet-Group im Internet nach einer Bezugsquelle für den POSIX-Standard fragte, den er übungshalber bei seiner Entwicklung berücksichtigen wollte, wurden einige Leser aufmerksam und boten an, Torvalds bei seiner Arbeit zu unterstützen.[26] In relativ kurzer Zeit entstand so tatsächlich ein kleiner Betriebssystemkernel, der einige POSIX-Anforderungen erfüllte und seit der ersten veröffentlichten Version Linux[27] genannt wurde. Bereits vor dieser Entwicklung, 1984, hatte Richard Stallmann, ein früherer Entwickler am MIT, aus Protest gegen die Kommerzialisierung von UNIX seinen Arbeitsvertrag gekündigt und das GNU-Projekt gegründet. GNU, als Akronym für *GNU is not UNIX*, verfolgte das Ziel, ein vollständiges Betriebssystem zu entwickeln, das die UNIX-Philosophie umsetzte, auch den POSIX-Standard, nicht aber zwingend die X/Open-Standards. Vor allem

26 Dass Torvalds für diese Diskussionen und die dann folgende Koordination der Entwicklung die Newsgroup des *NIX-Systems Minix des berühmten Informatik-Professors Andrew S. Tanenbaum nutzte, führte schon recht früh zu legendären Auseinandersetzungen zwischen Torvalds und Tanenbaum (vgl. Torvalds/Daimond 2002).

27 Torvalds selber hatte als Namen FREAX vorgeschlagen. Zum Glück hat der Administrator des FTP-Servers eine sehr eigenmächtige Entscheidung gegen Torvalds Vorschlag gefällt.

aber sollte jedes noch so kleine Stückchen Code des GNU-Systems bis in alle Ewigkeit Open Source bleiben, der Quellcode also jedem legitimen Nutzer zur Verfügung gestellt werden, inklusive dem Recht, diesen Code nach Belieben zu ändern. Einzige Einschränkung war, dass auch dieser geänderte Code wieder unter denselben Bedingungen weitergegeben werden musste. Quellcode unter der GNU-Lizenz darf also niemals ›geschlossen‹ werden.[28] Das GNU-Projekt entwickelte in kurzer Zeit viele der Anwendungen, die ein vollständiges System ausmachten, nicht aber einen Betriebssystemkernel.[29] So lag es für Torvalds nah, die GNU-Anwendungen mit seinem Kernel zusammenzuführen und so ein vollständiges Betriebssystem, sowohl in der Hardwareunterstützung wie auch auf der Anwendungsebene, zu haben. Und weil auch Torvalds keine kommerziellen Interessen verfolgte, lizensierte er seinen Kernel unter der selben Lizenz, die auch das GNU-Projekt verwendete.[30]

Weil weder Linux noch GNU einen zwingenden Grund hatten, sich an die standardisierte Unix-Architektur zu halten, hatten sie bei der Entwicklung erhebliche Freiheiten, ein moderneres System zu schaffen. Technische Standards sichern zwar die Kompatibilität, sie zementieren aber eben auch Designentscheidungen, die Entwicklungsfortschritte behindern. Viele der bewussten Inkompatibilitäten von GNU/Linux machten das System tatsächlich effektiver nutzbar, als das beim großen Vorbild der Fall war. Beispielsweise existierte in UNIX schon sehr früh das Programm *grep*, mit dem in Textdateien nach Zeichenketten gesucht werden konnte. Dieses POSIX-grep konnte aber immer nur Dateien in einem Verzeichnis durchsuchen, was durchaus im Sinne der UNIX-Philosophie war. Wenn man also unter UNIX eine ganze Verzeichnishierarchie nach Dateien durchsuchen will, die eine bestimmte Zeichenkette enthalten, muss man eine Pipeline aus *grep* und *find* verwenden, etwa: *find . | grep »Zeichenkette«*. Das grep, das GNU bereitstellte, beherrschte selber die Möglichkeit, rekursiv durch Verzeichnisbäume zu gehen, so dass ein einfaches *grep -r »Zeichenkette«* ausreichte. Das war nicht ganz die reine Schule der UNIX-Philosophie und deshalb in der Unix-Architektur auch anders gefordert. Es war aber ungemein praktisch und fand deshalb viele Liebhaber. Neben dem in Versalien geschriebenen *UNIX* und den nicht auf den Quellcode von UNIX zurückgehenden – nun klein geschriebenen – Unix-Derivaten bildet Linux den prominentesten Vertreter der *nix-

28 Gemeint ist die *GNU General Public License* (GPL), unter deren zweiter Version (GPLv2) Linux lizensiert ist.

29 Eine erste Version des GNU-Betriebssystemkernels *Hurd* erschien bereits 1991, produktiv nutzbar ist Hurd aber bis heute nicht. Weitere Informationen zu Hurd gibt es auf der Webseite des GNU-Projekts.

30 Wobei Torvalds die Lizenz vor allem verwendete, weil er sich Vorteile für die technische Entwicklung versprach, während das GNU-Projekt mit der Lizenz politische Ziele verfolgt. Die Version 3 der GPL, in der Stallmann die politischen Ziele noch weiter in den Vordergrund gestellt hat und dafür auch Behinderungen der technischen Entwicklungsspielräume in Kauf genommen hat, wird von Torvalds deshalb bis heute abgelehnt (vgl. Schäfer 2007).

Betriebssysteme, die sich zwar an UNIX und Unix anlehnen, selber aber kein Unix sind.[31]

Red Hat gründete sich 1993 als eines der ersten Unternehmen, die mit diesem sehr praktischen Betriebssystem Geld verdienen wollten. Dazu stellte Red Hat eine Auswahl der GNU-Anwendungen mit einer gut getesteten Version des Linux-Kernels zusammen, trug ein selbstentwickeltes Installationsprogramm und einige Wartungstools[32] bei und lieferte dieses Paket als vollständige Distribution aus, inklusive Support für jene, die auch bei der Verwendung dieser fertigen Zusammenstellung noch Unterstützung brauchten. Weil die ganze verwendete Software kostenlos im Internet zur Verfügung stand und Red Hat so auch für die installationsfreundliche Zusammenstellung nur wenig Geld nehmen konnte[33], wurde das Unternehmen von den alteingesessenen Unix-Firmen ebenso verlacht wie auch alle anderen Linux-Distributoren. Das änderte sich, als Red Hat Jahr für Jahr größere Gewinne mit dem Support des quasi verschenkten Systems verbuchen konnte, während die Gewinne durch den Vertrieb von Unix-Lizenzen immer weiter einbrachen. Als Red Hat im August 1999 an die Börse ging, gelang eine fast unglaubliche Kapitalisierung von 3,48 Milliarden Dollar – und diese Bewertung musste in der folgenden Dotcom-Blase nicht einmal nach unten korrigiert werden. Zum Vergleich: Novell hatte 1993 gerade einmal 350 Millionen Dollar für sämtliche UNIX-Rechte samt der UNIX System Laboratories an AT&T gezahlt und seitdem hatte dieses Paket einen stetigen Wertverlust erlitten.

SCO schwammen die Felle davon und ihr Vice President Sabbath beauftragte umgehend einen externen Consultant, Robert Swartz, Beweise dafür zu finden, dass in der Red Hat Distribution unerlaubt Quellcode von UNIX eingesetzt wurde.

Robert Swartz stand nun vor einer großen Herausforderung. Er hatte zwar Zugriff auf die verschiedenen Versionen des UNIX-Quellcodes, die ja im Besitz von SCO waren, auch auf den Red Hat-Quellcode, der wegen der GNU-Lizenz frei verfügbar war. Insgesamt standen ihm damit aber schätzungsweise an die hundert Millionen Zeilen Quellcode zur Verfügung[34], in denen er nach übereinstimmenden Zeilen zu suchen hatte.

---

31 Der bekannteste Vertreter dieser Gattung neben Linux ist Minix, das von Andrew S. Tanenbaum seit 1984 als Lehrbetriebssystem entwickelt wird und unter dem Torvalds die ersten Versionen von Linux entwickelt hat (vgl. Torvalds/Daimond 2002).

32 Das bekannteste und einflussreichste Tool ist der *Red Hat Package Manager* (RPM). Bis heute verwenden die meisten Linux-Distributionen das RPM-Format, um die System- und Anwendungssoftware zu verwalten.

33 Dass die wichtigste Einnahmequelle im IT-Geschäft einmal im Beratungs- und Support-Bereich liegen würde und nicht im Lizenzgeschäft, mussten viele IT-Riesen in den letzten Jahren sehr schmerzhaft lernen (vgl. Stare/Rubalcaba 2008).

34 Das ist eine sehr grobe Schätzung. Dokumentiert ist lediglich, dass der Linux-Kernel 1999 aus ca. 2 Mio. Zeilen Quellcode bestand. Der Kernel macht aber nur einen Bruchteil der gesamten Distribution aus, die Swartz untersucht hat. Eingeflossen sind auch die

Swartz beschreibt in seinem Memorandum an Sabbath ein systematisches Vorgehen:

> »We used the following method to determine whether there was any similarity between the Linux and the various releases of Unix. First we found the comparable files in the various version of Unix and Red Hat. This might not always be files with the same name. Further in general for the purposes of this work we would often concatenate the files together which represented a single programm. We then used a programm call ef to perform the comparison.
>
> Ef works by looking for the number of consecutive line in two files which are identical. So for example if you have two files A and B.

a	*K*
b	*L*
c	*M*
d	*duplicate1*
duplicate1	*duplicate2*
duplicate2	*X*
e	*Y*
f	*Z*

> Then the program ef would report that the lines, duplicate1 and duplicate2 where in both files. The program ef can detect similarities as small as one line.« (Swartz 1999: 2)

Swartz' Verfahren mag auf den ersten Blick etwas naiv anmuten, es dürfte aber tatsächlich auch heute noch der in der Praxis einzig gangbare Weg sein, Code-Plagiate aufzuspüren. Zugleich ist das Verfahren damit das einzig praktikable technische Verfahren, um den Kopierschutz von Quellcode in komplexen Softwareprojekten zu unterstützen. Um dieses Ziel zu erreichen, muss die Existenz kopierter Codefragmente erst einmal nachgewiesen werden. Diesen Weg manuell zu gehen, ist bei Millionen von Codezeilen in zigtausenden von Quelldateien schlechterdings unmöglich. Und weil Programmiersprachen im Unterschied zu natürlichen Sprachen einen sehr kleinen Sprachschatz und kaum Möglichkeiten

Libraries und ein Teil der Anwendungen – soweit sie Vorläufer im Ur-Unix hatten. Relevant dürften ca. 20 Mio. Zeilen Code der Red Hat-Distribution gewesen sein, die Swartz laut seiner Beschreibung mit fünf verschiedenen UNIX-Derivaten verglichen hat.

zur spontanen Wortschöpfung mitbringen, würde auch die Suche nach exotischen Wortschöpfungen kaum fruchten.

Hätte Swartz nun nach Codebestandteilen aus Microsoft Windows, aus Mac-OS Classic oder irgendeinem anderen proprietären Betriebssystem suchen sollen, wäre das Verfahren wohl effizient gewesen, in dem Sinne, dass dem Vergleich eine gewisse Aussagekraft zugekommen wäre. Aber es ging um UNIX und damit um eine standardisierte Betriebssystemarchitektur, deren maßgebliche Designrichtlinien seit X/Open nicht mehr einfach aus dem Quellcode hervorgingen, sondern öffentlich zugänglich dokumentiert waren. Viele der übereinstimmenden Zeilen, die Swartz fand, ließen sich so schlicht mit Anforderungen aus dem POSIX-Standard begründen und es war vollkommen legitim, ja sogar dringend erwünscht, POSIX zu folgen, selbst wenn POSIX Codezeilen forderte, die zur historischen Errungenschaft von UNIX gehören. Erschwerend kam hinzu, dass die UNIX-Philosophie möglichst einfachen, lesbaren und portierbaren Code forderte. Man kann zehn Programmierer beauftragen, ihren Code möglichst effizient zu optimieren und man wird zehn sehr verschiedene Lösungen für dieselbe Aufgabe finden. Der eine Programmierer wird sich darauf konzentrieren, die Mathematik seiner Algorithmen zu optimieren, ein anderer wird vorhersagbare Zwischenergebnisse statisch deklarieren, anstatt sie zu berechnen, ein dritter wird seinen Code in mehrere Threads verteilen, um ihn auf mehreren Prozessoren parallel auszuführen und so fort. Es gibt unzählige Möglichkeiten, Code zu optimieren. Es gibt aber nur wenige Wege, einfachen, lesbaren und portierbaren Code zu schreiben. Neben den POSIX-Anforderungen tritt hier also auch noch die UNIX-Philosophie als Gegner des Plagiatsfinders auf. Aber selbst da, wo tatsächlich eine ansatzweise belastbare Zeile identischen Codes gefunden wäre, müsste immer noch nachgewiesen werden, dass diese Zeile *ursprünglich* aus dem originalen UNIX-Code stammt, nicht aber aus dem BSD-Code, nicht aus den Modifikationen, die IBM, HP, SUN, Microsoft und viele weitere diesem Code irgendwann hinzugefügt haben, bis er dann in die UNIX-Linie zurückgeflossen ist.

Obwohl Swartz all diese Probleme bewusst waren und er sie explizit in seinem Memorandum benannte, schrieb er doch genau das, was Sabbath hören wollte: »*First many portions of Linux were clearly written with access to a copy of Unix sources. This of course would* [sic!] *be a violation of the License agreements under which Unix is distributed. Second there is some code where Linux is line for line identical to Unix*« (Swartz 1999: 3). Insgesamt konnte Swartz 48 übereinstimmende Code-Fragmente identifizieren. Alleine 26 von diesen Übereinstimmungen betrafen aber Header-Dateien, in denen üblicherweise in den öffentlich zugänglichen Standards geforderte Konstanten und mögliche Funktionscalls deklariert werden und auch die restlichen Übereinstimmungen betreffen sehr generische Basisfunktionalitäten, die sich in C kaum anders lösen ließen. Dass unter den monierten Zeilen auch etliche zu finden sind, die die Implementierung von TCP/IP-Funktionen auf Basis von Sockets betreffen, also jene erste Technologie, mit der

sich BSD entscheidend von UNIX abhob, spricht letztlich nicht für eine präzise historische Kenntnis der genealogischen Stränge auf Seiten von Swartz.

Der verdient sich dennoch sein Geld mit einem Hoffnungsschimmer, wenn er abschließend bemerkt:

> »Additionally in areas where the code is identical for compatibility reasons, the code in certain instances is character by character identical. There is a Grove Press case where the court found that making plates from the pages of an out of copyright book was a violation of law. This practice here may be similar.« (ebd.)

Alleine auf dieser vagen Hoffnung aber einen Prozess zu beginnen, wäre einem Vabanque-Spiel gleichgekommen.

»THEY ARE SMOKING CRACK«

SCO zog die Konsequenzen und suchte nun selber einen Käufer für das unglückselige UNIX. Bemerkenswerterweise zeigte sich das Unternehmen Caldera interessiert, das nicht nur neben Red Hat zu den erfolgreichen Linux-Distributoren und Supportern gehörte, sondern selber eine Ausgründung von Novell war, dem Vorbesitzer von UNIX. Sie hätten es also besser wissen müssen, kauften aber sehenden Auges 2001 die Rechte am UNIX-Code samt der Rechte am Namen SCO. Seit 2002 firmierte Caldera dann unter dem Namen *The SCO Group* und baute neben dem bis dahin erfolgreichen Linux-Geschäft einen verlustträchtigen Bereich für UNIX auf. Alle anderen historisch großen UNIX-Distributoren hatten sich längst auf den umgekehrten Weg gemacht: Novell kaufte 2003 den wichtigsten europäischen Linux-Distributor SuSE auf[35] und fuhr das UNIX-Geschäft dramatisch zurück; IBM investierte um die Jahrtausendwende eine Milliarde(!) Dollar, um die Entwicklung von Linux zu beschleunigen, das sie selber in Kundenprojekten einsetzen wollten, das aber trotz vieler Vorzüge noch nicht alle Anforderungen für große Architekturen erfüllte.[36] Einzig SUN und HP, die nicht nur Software, sondern integrierte Server aus Hardware und vorkonfigurierten Betriebssystemen vertrieben, konnten sich noch halbwegs stabil mit Unix über Wasser halten. The SCO Group unter ihrem Vorsitzenden Darl McBride aber suchte die Entscheidungsschlacht. Ohne einen wirklichen Beweis in Händen zu halten und nur auf Basis der Vagheiten in Swartz' Memorandum beklagte sich McBride über den Diebstahl an UNIX-Code durch die Linux-Gemeinde und klagte kurz darauf,

35 SuSE gehört neben Red Hat zu den ältesten Linux-Distributoren und war wegen seiner guten Deutschen Dokumentation lange Zeit die wichtigste Linux-Distribution in Deutschland.

36 IBM gibt auf der eigenen Webseite ausführlich Auskunft über die Gründe für das Linux-Engagement: http://www-03.ibm.com/linux/, 10.11.2009.

nun vor Gericht, gegen IBM.[37] IBM, so SCO, hätte nicht nur mit einer unverhältnismäßigen Investition den Markt für UNIX ruiniert, sondern auch das Eigentum von SCO aus dem IBM-eigenen und ursprünglich auf UNIX basierenden AIX in Linux einfließen lassen. Sechs lange Jahre wurde nun taktiert, prozessiert und gegenprozessiert. Alle großen IT-Unternehmen und viele der großen IT-Kunden waren involviert. Nach SCO gegen IBM folgte IBM gegen SCO, dann SCO gegen Novell und Novell gegen SCO und als SCO begann, Großkunden von Linux-Systemen zu verklagen und ihnen UNIX-Lizenzen anerpresste, damit sie ihre Linux-Systeme betreiben dürften, klagte auch noch Linux gegen SCO. Als SCO dann, um den letzten Rest an Glaubwürdigkeit zu erhalten, auch noch den eigenen Geschäftsbereich mit Linux aufgab, nahte das finanzielle Ende.[38] Immer neue Codezeilen lieferte SCO den Gerichten, niemals mit einer belastbaren Herkunft. Ein kleines Fragment, das wohl tatsächlich aus AIX stammte, kommentierte Linus Torvalds süffisant mit den Worten:

> »The code SCO showed represents an algorithm that can be used to manage a computer's memory... Not a very interesting piece of code in itself, this is very basic ›allocate a smaller chunk of memory out of a list of bigger chunks‹. The function is described in a lot of places, and exists in original Unix code and is apparently written by Ken Thompson himself. It shows up in the Lion book (a commentary on the traditional Unix), and the code is described in [Maurice J.] Bach's ›The Design of the Unix Operating System‹. In other words, it's not only 30 years old; it's actually been documented several times. It's also part of BSD Unix, which was shown to not be a derived work of the AT&T copyrights 10 years ago.«[39]

Torvalds kurgefasstes Fazit zur Schlacht von SCO gegen den Rest der Welt lautet folgerichtig: »*They are smoking crack*« und das traf wohl das, was man auch bei IBM und Novell dachte, wenn es dort auch von den Justiziaren etwas aufwändiger und kostspieliger formuliert wurde.

Wäre es darum gegangen, diesen Prozess so lange zu führen, bis mit technischen Mitteln die eine oder andere Position bewiesen worden wäre, der Prozess würde wohl nie enden wollen. Ab einer gewissen Komplexität gibt es schlicht kein technisches Verfahren, um illegitime Codeplagiate in verschiedenen Betriebssystemen zu finden, die der selben Architektur angehören und die der selben Phi-

37 Anlässlich dieser Klage ist die – inzwischen mehrfach preisgekrönte – Webseite *Groklaw* (www.groklaw.net) gegründet worden, auf der alle Schritte der SCO gegen Linux-Prozesse sorgfältig dokumentiert und kommentiert sind.

38 Dieses Ende konnte allerdings durch Investitionen der BayStar Capital noch lange heraus gezögert werden. Groklaw konnte schließlich enthüllen, dass diese Investitionen pikanterweise von Microsoft vermittelt wurden (vgl. http://www.groklaw.net/article.php?story=20061008014426 92, 10.11.2009).

39 Vgl. www.linuxtoday.com/developer/2003082101326INKNDV, 10.11.2009.

losophie folgen – *wenn Architektur und Philosophie hinreichend präzisiert sind*. Und so wurde auch dieser Prozess mit rein juristischen Mitteln beendet: Im April 2007 kann Novell nach einer jahrelangen Analyse der Verträge glaubhaft belegen, dass Sie zwar den UNIX-Code, nicht aber das Copyright an diesem Code an SCO veräußert haben. Als die Revisionsversuche durch SCO scheitern, klagt Novell die letzten Dollar aus SCOs Kriegskasse heraus, indem sie nun Lizenzgebühren für den Verkauf von UNIX-Installationen durch SCO fordern. Am 25. August 2009 entscheidet zwar das Berufungsgericht, dass die Frage der Copyright-Veräußerung erneut überprüft werden müsse, bestätigt aber Novells Anrecht auf 2,5 Millionen Euro Lizenzgebühren von SCO. Damit ist SCO endgültig zahlungsunfähig. Am 26. August wird der Insolvenzverwalter bei SCO eingesetzt, am 16. Oktober wird Darl McBride als zunächst letzter, der sich noch an den Wert des UNIX-Codes klammerte, entlassen.

EIN FAZIT

Wenn die Sache gut läuft, ist die Geschichte von UNIX hier zu Ende, Unix ist zumindest in der Reinkarnation MacOS X ein Coup gelungen[40] und die Geschichte von *nix wird durch Linux immer erfolgreicher. Vielleicht wird sich aber auch jemand aus der Konkursmasse der SCO Group bedienen und die nächste Runde einläuten. Das würde immerhin einer fast zwanzigjährigen Tradition folgen. An einem wird beides nicht vorbeiführen: *hinreichend* umfangreiche und *hinreichend* präzise formulierte Architekturstandards und Designrichtlinien nehmen jeder konkreten Instanz, in der diese Richtlinien umgesetzt werden, ihre Individualität. Das heißt nicht, dass eine Implementierung nicht in irgendeinem Sinne besser sein könnte als eine andere, wohl aber, dass der Wert der einzelnen Instanzen sich weitestgehend auf die investierte Arbeitskraft reduziert, während das schützenswerte geistige Eigentum in den Standards verbleibt. Plagiate auf Ebene solcher Quellcodes suchen zu wollen, ist zum einen sinnlos und zum anderen hoffnungslos, weil jede potenziell kopierte Codezeile nur dann werthaltig sein kann, wenn dieser Wert schon in der Architektur vorgegeben ist, die der Code reproduziert. Dem entgegenzuwirken ist nur dort möglich, wo die definierten Architekturen ignoriert und die Standardisierung wieder im Code selber stattfinden würde – wo der Code die Architektur ist. Solcher Code wäre hinreichend individuell, um mit Swartz' *ef* oder vergleichbaren technischen Mitteln unzulässige Kopien zu identifizieren. Ob diese Möglichkeit des Schutzes die notwendige Aufgabe der Möglichkeit zur Kollaboration und Kooperation oder, im Web 2.0-Slang, zur *Community*-

40 Bemerkenswert im Zusammenhang dieses Artikels ist, dass Apple für die proprietären Teile von MacOS X, insbesondere für die Cocoa-API, mit Objectice-C eine extrem selten verwendete Programmiersprache verwendet. Cocoa-Plagiate dürften also im Unterschied zu den OpenSource-Bestandteilen sehr schnell aufgespürt und zweifelsfrei identifiziert werden können.

Bildung rechtfertigt, wird jedes Unternehmen selbst entscheiden müssen, gleich, ob es Software produziert oder irgendein anderes Gut.

LITERATURVERZEICHNIS

Brooks, Frederick P. (1995): *The Mythical Man-Month: Essays on Software Engineering, 20th Anniversary Edition,* Reading, MA: Addison-Wesley.

Ceruzzi, Paul E. (2003): *A History of Modern Computing*, Cambridge, MA: MIT Press.

Clukey, Lee Paul (1985): *UNIX & XENIX demystified*, Blue Ridge Summit, PA.: TAB Books.

Flamm, Kenneth (1988): *Creating the Computer: Government, Industry, and High Technology*, Washington, DC: Brookings Institution.

Kernighan, Brian/Ritchie, Dennis (1988): *The C Programming Language*, 2nd Edition, Englewood Cliffs, NJ: Prentice Hall.

Kittler, Friedrich (1993): »Es gibt keine Software«, in: ders.: *Draculas Vermächtnis. Technische Schriften*, Leipzig: Reclam, S. 225-242.

Lanzerotti, Mary Y. (Hg.) (2006): *The Technical Impact of Moore's Law. IEEE solid-state circuits society newsletter*, Vol. 20, No. 3.

Lehtinen, Rick/Russell, Deborah/Gangemi, G. T. (2006): *Computer Security Basics*, 2nd Edition, Beijing u.a.: O'Reilly.

Ng, Kia/Nesi, Paolo (2008): *Interactive Multimedia Music Technologies*, Hershey, PA: Information Science Reference.

Raymond, Eric S. (2004): *The Art of Unix Programming*, Boston u.a.: Addison-Wesley.

Schäfer, Fabian (2007): *Der virale Effekt. Entwicklungsrisiken im Umfeld von Open Source Software. Schriften des Zentrums für angewandte Rechtswissenschaft Karlsruhe*, Karlsruhe: Universitätsverlag.

Schwabach, Aaron (2006): *Internet and the Law. Technology, Society, and Compromises*, Santa Barbara u.a.: ABC-CLIO.

Shore, Jim/Warden, Shane (2007): *The Art of Agile Development*, Beijing u.a.: O'Reilly.

Stare, Metka/Rubalcaba, Luis B. (2008): »Research on Services: From Exploring the ›Residual‹ to Services Science«, in: Stauss, Bernd/Engelmann, Kai/Kremer, Anja et al. (Hg.): *Services Science. Fundamentals, Challenges and Future Developments*, Berlin u.a.: Springer, S. 41-54.

Swartz, Robert (1999): »Memorandum«, http://www.sco.com/company/legal/update/memorandum_19991004.pdf, 10.11.2009.

Stevens, W. Richard (1995): *TCP/IP Illustrated, Volume 2: The Implementation*, Reading, MA: Addison-Wesley.

Torvalds, Linus/Diamond, David (2002): *Just for Fun. Wie ein Freak die Computerwelt revolutionierte*, München u.a.: Hanser.

WEB-RESSOURCEN

American National Standards Institute (ANSI): http://www.ansi.org/

Austin Group der Open Group: http://www.opengroup.org/austin/

Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG): http://www.gesetze-im-internet.de/bundesrecht/urhg/gesamt.pdf

GNU General Public License, Version 2 (GPL v2): http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt

GNU General Public License, Version 3 (GPL v3): http://www.gnu.org/licenses/gpl.txt

Groklaw: www.groklaw.net

Hurd-Kernel: http://www.gnu.org/software/hurd/

IBM und Linux: http://www-03.ibm.com/linux/

UNIX-Seiten der Open Group: http://www.unix.org

Wikipedia: http://en.wikipedia.org/wiki/ {AT%26T|Bell_Labs|Posix|Santa_Cruz_Operation|Unix|Xenix}

AUTORINNEN UND AUTOREN

Alexander Firyn, M.A., studierte Theaterwissenschaft, Linguistik, Philosophie und Kulturwissenschaft in Leipzig und Berlin. Mitherausgeber der Schriftenreihe »Kaleidoskopien«. Bis 2001 zahlreiche Arbeiten als freier Regisseur, danach zunehmend als Anwendungsentwickler. Seit 2007 wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Software- und Systemtechnik ISST in Berlin, Schwerpunkt Internettechnologien. Weitere Veröffentlichungen: »Nullen dieser großen Summe«, in: de Kerckhove, Derrick/Leeker, Martina/Schmidt, Kerstin (Hg.): *McLuhan neu lesen*, Bielefeld: Transcript 2008; »Gegen die Zeit«, in: Volmar, Axel (Hg.): *Zeitkritische Medien*, Berlin: Kadmos 2009.

Carina Gerstengarbe, B.A., studierte Journalismus und Public Relations an der Fachhochschule Gelsenkirchen. Seit 2008 Studium des Masterstudiengang Medienkultur an der Universität Siegen, voraussichtlicher Abschluss 2010. Als freie Mitarbeiterin schrieb sie für verschiedene Essener Stadtmagazine sowie für das *Handelsblatt*. Weitere praktische Erfahrungen: RTL Nachrichtenredaktion, Heinrich Bauer Verlag, Zeitschrift *Prinz*.

Till A. Heilmann, Dr. phil., studierte Germanistik, Medienwissenschaft und Geschichte in Basel. Seit 2003 forscht und lehrt er am Institut für Medienwissenschaft der Universität Basel. Er promovierte 2008 mit einer Arbeit zur Geschichte der Textverarbeitung. Seine aktuellen Forschungsschwerpunkte sind Theorie und Geschichte des Digitalen, Computertechnik und -kultur sowie die Anfänge der Medienwissenschaft. Weitere Veröffentlichungen: *Textverarbeitung. Eine Mediengeschichte des Computers als Schreibmaschine*, Bielefeld: Transcript 2010 (im Erscheinen).

Daniel Köhne, studiert seit Oktober 2005 den integrierten Diplom-Studiengang Medienplanung, -Entwicklung und -Beratung an der Universität Siegen.

Katharina Lang, B.A., studierte Medienwissenschaft und Vergleichende Kulturwissenschaft an der Universität Regensburg. Seit Oktober 2008 Studium des M.A.-Studiengangs Medienkultur an der Universität Siegen, das sie voraussichtlich im Sommer 2010 abschließen wird.

Anna Schneider, B.A., studierte von 2004 bis 2008 an der Hochschule Siegen den Bachelorstudiengang Social Science mit dem Schwerpunkt Medienwissenschaften und den Nabenfächern Soziologie und Politik. Zur Zeit studiert sie im Masterstudium Medienkultur, das sie voraussichtlich im Frühjahr 2011 abschließen wird.

Brian Winston, Prof. Dr., lehrt im Department of Media and Humanities an der Lincoln University (UK). Er hat neben seiner akademischen Laufbahn, die ihn an die Universitäten Westminster, Cardiff, Pennsylvania State und New York führte,

als Journalist und Dokumentarfilmer gearbeitet. Publikationen*: Media Technology and Society*, London: Routledge 1998; *Messages: Free Expression, Media and the West from Gutenberg to Google*, London: Taylor & Francis 2005.