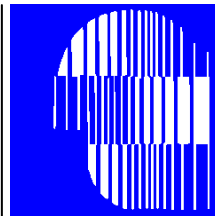


Urheberschutz und Nutzerschutz in der Informationsgesellschaft



Alcatel SEL
Stiftung für
Kommunikations-
forschung im
Stifterverband für
die Deutsche
Wissenschaft



Thomas Dreier
Michael Lehmann
Johann Bizer
Horst Henn
Malte Boecker
Wernhard Möschel/Stefan Bechtold
Klaus Kornwachs

Tagungsdokumentation, Stuttgart, 10./11. Mai 2001

36
Stiftungsreihe

Urheberschutz und Nutzerschutz
In der Informationsgesellschaft

Inhaltsverzeichnis

Seite

Einführung in das Urheberrecht – nationale und europäische Tendenzen und Entwicklungen

5

Thomas Dreier

Electronic Commerce und Verbraucherschutz in Europa

14

Michael Lehmann

Privacy als Schranke des Urheberschutzes

24

Johann Bizer

Implementierungsmöglichkeiten für Urheberschutz in offenen Portalen

38

Horst Henn

Watermarking – protecting the wrong things, and for the wrong reasons

47

Ross Anderson

Copyleft, Geschäftsmodelle und Urheberschutz

50

Malte Boecker

Digital Rights Management aus juristischer Sicht

63

Wernhard Möschel, Stefan Bechtold

Nachbemerkungen

74

Klaus Kornwachs

Impressum

Stiftungs-Reihe

2. Auflage

Redaktion

Dr. Dieter Klumpp

Petra Bonnet M.A.

Renate Förstner

Photos

Alcatel SEL Stiftung

Druck der Broschüre

Alcatel SEL AG

Alle Rechte vorbehalten

Alcatel SEL Stiftung

© 2001

Postadresse

Alcatel SEL Stiftung

Postfach 40 07 49

70407 Stuttgart

Telefon (0711) 821-45002

Telefax (0711) 821-42253

E-mail: sel.stiftung@alcatel.de

<http://www.alcatel.de/stiftung>

ISSN 0932-156x

Teilnehmer

Dr. Ross Anderson	University of Cambridge, Computer Laboratory
Eugen Baacke	Landeszentrale für politische Bildung Baden-Württemberg, Bad Urach
Lars Barteit	Landtag von Baden-Württemberg, Stuttgart
Stefan Bechtold	Universität Tübingen, Juristische Fakultät
Dr. Johann Bizer	Universität Frankfurt, Institut für öffentliches Recht
Malte Boecker	Bertelsmann Stiftung, Gütersloh
Petra Bonnet	Büro für Kommunikationsberatung, freie Mitarbeiterin Alcatel SEL Stiftung, Stuttgart
Dr. Christoph Busch	Fraunhofer-Institut für Graphische Datenverarbeitung, Sicherheits- technologie für Graphik- und Kommunikationssysteme, Darmstadt
Prof. Dr. Thomas Dreier	Universität Karlsruhe, Fakultät für Informatik, Institut für Informa- tionsrecht
Kaspar Dütting	Alcatel SEL AG, Stuttgart
Prof. Dr. Rainer Erd	FH Darmstadt, Fachbereich SuK
Monika Ermert	Freie Journalistin, Tübingen
Heiner Fuhrmann	Deutsche Post eBusiness GmbH, Geschäftsfeld Signtrust. Bonn
Rotraud Gitter	Universität GHS Kassel, provet
Benjamin F. Grzimek	NÖRR STIEFENHOFER LUTZ, Rechtsanwälte Steuerberater Wirtschaftsprüfer, München
Dirk Guennewig	EURUBITS, Ruhr-Universität Bochum
Andreas Hamann	Landesanstalt für Kommunikation Baden-Württemberg, Stuttgart
Dr. Horst Henn	IBM Deutschland Entwicklung GmbH, Technology & Architecture, Global Smart Card Solutions, Böblingen
Jörg Hladjk	Universität Frankfurt, Institut für öffentliches Recht
Birgit Hollerbach	Deutscher Sparkassen Verlag GmbH, Stuttgart
Dr. Simone Kimpeler	Fraunhofer-Institut für Systemtechnik und Innovationsforschung (ISI), Karlsruhe
Dr. Dieter Klumpp	Alcatel SEL Stiftung
Kristian Köhntopp	NetUSE, Kiel
Marit Köhntopp	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel
Prof. Dr. Klaus Kornwachs	BTU Cottbus, Lehrstuhl für Technikphilosophie
Prof. Dr. Michael Lehmann	Max-Planck-Institut für Ausländisches und Internationales Patent-, Urheber- und Wettbewerbsrecht, München

Hans-Joachim Lemke	Alcatel SEL AG, Stuttgart
Nils Leopold	Datenschutzbeauftragter I-D Media AG, Berlin
Dr. Patrick Mayer	Rechtsanwälte Haver & Mailänder, Stuttgart
Prof. Dr. Wernhard Möschel	Universität Tübingen, Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht
Heinz Müller	Alcatel Deutschland GmbH, Stuttgart
Dr. Markus Müller	Universität Tübingen, Juristische Fakultät
Ansgar Pallasky	Universität Frankfurt, Institut für öffentliches Recht
Prof. Dr. Andreas Pfitzmann	TU Dresden, Fakultät Informatik, Institut für Systemarchitektur
Johannes Ranke	Universität Kassel, provet
Prof. Dr. Alexander Rossnagel	Universität GHS Kassel, Lehrstuhl für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes, Wissenschaftlicher Direktor des Instituts für europäisches Medienrecht, Saarbrücken.
Dr. Tomas Sander	STAR Lab, InterTrust Technologies, Santa Clara/USA
Dr. Anke Schierholz	BILD-KUNST, Verwertungsgesellschaft Bild-Kunst, Bonn
Wolfgang Schlagenhoff	ABB AG, Mannheim
Werner Schmidt	Alcatel SEL AG, Intellectual Property Department, Stuttgart
Jürgen Schwemmer	Regulierungsbehörde für Telekommunikation und Post, Mainz
Karl-Ulrich Templ	Landeszentrale für politische Bildung Baden-Württemberg, Stuttgart
Manfred Weiss	Alcatel SEL AG, Stuttgart
Martina Wiedmaier	Landeszentrale für politische Bildung Baden-Württemberg, Bad Urach
Prof. Dr. Tsuneharu Yonemaru	Ritsumeikan University, College of Law, Kyoto/Japan
Kerstin Zerahn	Landeszentrale für politische Bildung Baden-Württemberg, Bad Urach
Prof. Dr. Axel Zerdick	Freie Universität Berlin, Institut für Publizistik und Kommunikationspolitik

Einführung in das Urheberrecht – nationale und europäische Tendenzen und Entwicklungen

Thomas Dreier

Dem Urheberrecht kommt im Rahmen der Informationsgesellschaft eine tragende Rolle zu, wenn es darum geht, steuernd die Rahmenbedingungen festzulegen, nach denen geistige Güter in immaterieller Form über das Netz erzeugt, bereitgestellt und verbreitet werden sollen. Doch das Urheberrecht ist nicht vor dem Hintergrund des digitalen und vernetzten Kontextes entstanden. Was will das Urheberrecht und wie funktioniert es? Zu diesem Zweck sei zunächst kurz auf Voraussetzungen und Inhalt des Urheberrechts eingegangen, wie wir es heute kennen, ehe die Besonderheiten von Digitalisierung und Vernetzung in ihren Auswirkungen auf eben dieses Urheberrecht beleuchtet werden.

Kurz gesagt hat das Urheberrecht den Schutz von Werken der Literatur und Kunst zum Ziel, wie es in den meisten nationalen Urheberrechtsgesetzen und auch den internationalen Konventionen zum Schutz des geistigen Eigentums programmatisch heißt. Zu diesen Schutzgegenständen der Literatur und Kunst zählen neben literarischen Werken Werke der Musik und der bildenden Kunst ebenso wie auch der Film und die Fotografie. Neben diesen schöpferischen Schutzgegenständen sind inzwischen auch die eher funktionalen Computerprogramme und Datenbanken hinzugekommen. Geschützt werden diese Werke, sofern sie nur eine hinreichende Originalität aufweisen, also eigenschöpferisch sind und einen gewissen Grad an Individualität und Gestaltungshöhe erkennen lassen. Der gesetzliche Schutz besteht umfassend gegen Verwertungshandlungen in körperlicher und unkörperlicher Form, also gegen die Vervielfältigung und Verbreitung materieller Exemplare, welche das betreffende geschützte Werk ver-

körpern, wie auch gegen die unkörperliche Art der Werkverwertung in Form der Wahrnehmbarmachung, der Rundfunksendung und neuerdings auch des online-Angebots. Dem Eigentum an körperlichen Sachen nicht unähnlich - das dem Eigentümer, wie es in § 903 BGB so schön heißt, die Befugnis verleiht „mit der Sache nach Belieben zu verfahren und andere von jeder Einwirkung [auf die Sache] auszuschließen“ - erhält der Schöpfer eines Werkes das ausschließliche Recht, sein Werk selbst zu nutzen und Dritte von eben dieser Nutzung auszuschließen. Auf der Grundlage dieses Ausschließlichkeitsrechts vermag der Urheber Dritten dann aber auch die Nutzung seines Werkes zu gestatten, und er lässt sich dafür regelmäßig die Zahlung einer Vergütung versprechen. In den Händen des Urhebers dient diese Vergütung dessen Alimentation, und in den Händen der Produzenten der Amortisation der zur Verbreitung des Werkes getätigten Investitionen. Funktioniert der vertragsmäßige Interessenausgleich, so leben wir in der besten aller Welten: Der rechtliche Ausschließlichkeitsschutz stellt für Urheber und Medienunternehmen einen Anreiz zur Schaffung geistiger Werke dar; er stellt sicher, dass das Werk von Dritten nicht ohne Erlaubnis des ursprünglichen Urhebers bzw. des jeweiligen Rechtsinhabers genutzt und verwertet wird; Urheber und Produzenten vermögen auf diese Weise die Nachfrage am Markt optimal abzuschöpfen und schließlich ist der Urheber auf angemessene Weise an den Erlösen der Verwertung seines Werkes beteiligt.

Selbstverständlich sind diese Ausschließlichkeitsrechte in ihrem Umfang nicht grenzenlos. Zwar ordnet das Gesetz dem Urheber erst einmal jede mögliche Art der Verwertung



seiner Werke zu, doch werden diese Ausschließlichkeitsrechte, wird gerade in ihren Randbereichen im Wege der Feinabstimmung mit gegenläufigen Interessen zum Ausgleich gebracht. Zu diesen gegenläufigen Interessen zählen vor allem Informationsinteressen der Allgemeinheit, aber auch die Korrektur eines Marktversagens, wo es - wie etwa beim Kopieren zu privaten Zwecken - nicht zum Abschluss einzelner Nutzungsverträge kommt. Steht wie etwa bei der Nachrichtenberichterstattung ein überragendes Gemeinwohlinteresse in Rede, so bedürfen die dazu erforderlichen, an sich urheberrechtlich relevanten Verwertungshandlungen weder der Zustimmung der betroffenen Urheber, noch geben sie Anlass zu einer Vergütung. Soll dagegen sichergestellt werden, dass der Urheber von seinem Verbotsrecht keinen Gebrauch macht, ohne dass die Notwendigkeit bestünde, ihm auch eine Beteiligung am Verwertungserlös vorzuenthalten, so kommt eine gesetzliche Lizenz in Betracht. Ein solcher Fall ist etwa das Privileg zu Gunsten der Schulbuchverleger, die ihre urheberrechtliche Sonderstellung deshalb innehaben, weil der Gesetzgeber der Auffassung ist, ein schulbuchwürdiger Autor solle der

Aufnahme seines Textes in ein Schullesebuch nicht widersprechen können. Der Anspruch auf die Vergütung des Urhebers bleibt in diesem Fall jedoch erhalten. Auch im bereits genannten Fall der privaten Kopie und der privaten Überspielung sieht das deutsche Urheberrechtsgesetz eine vergleichbare Regelung vor. Denn die Struktur und die Gegebenheiten des Marktes lassen individuelle Transaktionen im analogen Bereich nicht zustande kommen. Überdies kann und will man angesichts des damit verbundenen massiven Eingriffs in die Privatsphäre nicht ermitteln, wer was wann und von wem kopiert hat. So werden bestimmte Handlungen zum Zweck des privaten Gebrauchs vom Verbotsrecht des Urhebers freigestellt, diesem im Gegenzug jedoch eine Vergütung in Form der allen bekannten Geräte-, Betreiber- und Leerkassettenabgabe gesichert, die von den Werkvermittlern an die Verwertungsgesellschaften zu zahlen ist und von diesen an die einzelnen Urheber ausgeschüttet wird. Eingeschränkt werden die Ausschließlichkeitsrechte des Urhebers auch zugunsten solcher Marktteilnehmer, die ihrerseits im Kommunikationsprozess für sinnvoll erachtete Mehrwertdienstleistungen erbringen. Das Hauptbeispiel hierfür ist im geltenden Urheberrecht das Privileg der Presseschauen, das Gesetzgeber und Rechtsprechung stillschweigend auch auf die sog. Pressespiegel erstreckt haben. Ohne Einwilligung der betreffenden Rechteinhaber – wenngleich gegen Zahlung einer an die Verwertungsgesellschaft WORT zu entrichtenden Vergütung – zulässig ist danach, einzelne Artikel aus Zeitungen auszuschneiden, aufzukleben und nach den Interessen bestimmter Abnehmergruppen geordnet in Form von Kopien an die jeweiligen Abnehmer zu verbreiten.

In der Praxis gehen viele der zunächst beim ursprünglichen Urheber entstehenden Ausschließlichkeitsrechte auf vertraglichem Wege dann auf den Werkvermittler und Verwerter

über. Zum Schutze des in seiner Verhandlungsposition strukturell zumeist unterlegenen Urhebers enthält das Gesetz dann eine Reihe urheberschützender Vorschriften, wie vor allem die Zweckübertragungstheorie, der zufolge der Urheber im Rahmen eines Vertrages im Zweifel nur so viel an Rechten auf den Verwerter überträgt, wie dieser zur Durchführung des vertraglich vereinbarten Zwecks benötigt. Sonderregelungen enthält darüber hinaus das Verlagsgesetz, doch sind die meisten seiner Vorschriften ohnehin dispositiver Natur und können also abbedungen werden. Das gilt letztlich auch für alle urheberrechtlichen Befugnisse bis auf einen Kern der Urheberpersönlichkeitsrechte. Um die Position der Urheber insoweit zu stärken, hat die Bundesregierung jüngst einen Entwurf eines Gesetzes zur Stärkung der vertraglichen Stellung von Urhebern und ausübenden Künstlern veröffentlicht.¹

Mit diesen kurzen Ausführungen ist der urheberrechtliche Rahmen für das bisherige analoge Urheberrecht bereits umschrieben, von der Schöpfung eines Werkes über die Produktion und den Vertrieb des Produktes, das dieses Werk - und ggf. mehrere Werke - enthält bis hin zum Vertrieb der materiellen Vervielfältigungsstücke. Jetzt setzt die Digitalisierung ein.

Spricht man von elektronischen Publikationen, so ist damit nicht gemeint, dass lediglich einzelne Schritte der Produktionskette aus Gründen der Rationalisierung digitalisiert werden, das Endprodukt jedoch nach wie vor ein analoges Produkt bleibt. Für digitale Werke ist vielmehr charakteristisch, dass das Endprodukt selbst eine digitale Form annimmt, sei es nun ein offline-Produkt auf CD-Rom oder aber ein online zugänglicher Datensatz. Die Frage ist nun, ob bzw. inwieweit dieser technologische Wandel eine Änderung der rechtlichen Rahmenbedingungen erfordert oder

nicht. Immerhin gehen mit der Digitalisierung nicht nur quantitative, sondern auch zwei qualitative Änderungen einher.

Zum einen kann jeder digitale Datensatz ohne nennenswerten Aufwand an Kosten und Zeit von jedermann vervielfältigt werden und dies darüber hinaus ohne jeglichen Qualitätsverlust. Das ist ein einschneidender Wandel gegenüber dem bisherigen Fotokopiergerät, das zwar auch die Kopie eines fremden Buches ermöglicht, aber eben zu welchen Mühen, Kosten und unter welchen Qualitätsverlusten. Zum zweiten ist angesichts der globalisierten Vernetzung theoretisch nur noch ein einziges Vervielfältigungsstück erforderlich, das auf irgendeinem Server abgelegt dann die weltweite Nachfrage zu befriedigen vermag. Zusammengefasst führt dies aus der Sicht der Urheber und Rechteinhaber zu einem erheblichen Kontrollverlust, in dem die an die Freiheit im Sinne des kostenlosen Zugriffs auf fremde Inhalte gewöhnte Internet-Gemeinde umgekehrt freilich gerade die große Segnung der neuen Technologien sieht. Produzenten hingegen könnten zur Überzeugung gelangen, dass ihre Aufgabe obsolet geworden ist. Die Herstellung materieller Vervielfältigungsstücke eines Werkes und deren Verbreitung haben bislang die Kerntätigkeiten des Verlagsgeschäftes ausgemacht. Beide Aufgaben fallen im Zeitalter von Digitalisierung und Vernetzung aber ersatzlos weg. Entscheidend sind allein Inhalt, Qualität und Aufbereitung des Inhaltes in einer möglichst benutzerfreundlichen digitalen Form. Hierin wird dann künftig auch der eigentliche Schwerpunkt der Tätigkeit des Produzenten liegen. Nach wie vor kommt es ja darauf an, dass ein bestimmtes Produkt am Markt von einem namhaften Hersteller angeboten und über eine weithin sichtbare Plattform oder ein Portal „an den Mann“ bzw. „an die Frau“ gebracht wird. Die Zukunft der Content-Provider, wie Urheber und Produzenten neuhochdeutsch heißen, sieht also vermutlich

¹ Abrufbar unter <http://www.bmj.bund.de/ggv/urhebver.pdf>.

doch nicht so schwarz aus, wie Pessimisten argwöhnen könnten.

Eine weitere entscheidende Veränderung in Folge von Digitalisierung und Vernetzung wird unter dem Stichwort „Konvergenz“ beschrieben. Dabei geht es nicht nur um eine Konvergenz der Medien, d.h. es bedürfen die bislang disparaten Medien Text, Bild und Ton nunmehr eines einheitlichen Träger- oder Verbreitungsmediums, sondern es geht auch und vor allem um eine Konvergenz der „Player“, wie es ebenfalls neuhochdeutsch heißt. Das sei am Beispiel der Buchbranche verdeutlicht. Verfasste bislang der Autor ein Manuskript, das er seinem Verleger überbrachte, der das Buch „machte“ und an den Buchhandel vertrieb, über den die Bücher dann entweder direkt oder über den Umweg eines Antiquariats sowie in vielen Fällen einer Bibliothek an den Leser als Endnutzer gelangten, so sind bei elektronischen Publikationen alle Beteiligten - Autor, Verleger, Buchhändler, Antiquar wie auch Bibliothekar - Anbieter eines digitalen Datensatzes. Bieten aber alle das Gleiche an, so stehen auch alle grundsätzlich im Wettbewerb zueinander. Auch dies ist freilich eine Vereinfachung, tun sich auch insoweit Möglichkeiten der Differenzierung des eigenen Angebots von demjenigen der potentiellen Konkurrenten auf, lässt sich doch der Inhalt auf eine Weise aufbereiten und mit anderen Inhalten verknüpfen, zu der eben nur diejenigen in der Lage sind, die eine Vielzahl von Werken anbieten.

Die entscheidende Frage ist nun: Welche Folgen ergeben sich aus diesen beiden, soeben konstatierten grundsätzlichen Änderungen des Umfeldes für die rechtlichen Rahmenbedingungen?

In wirtschaftlicher Hinsicht kommt es zunächst einmal zu einem verschärften Kampf um Märkte. Jeder will sich ein möglichst großes Stück vom Kuchen der Verwertungsmöglichkeiten sichern, die sich durch die neuen

Technologien auftun. Zugleich ist jeder Marktteilnehmer überaus vorsichtig darauf bedacht, von seinem bisherigen Marktanteil nichts zu verlieren. Dass eine derartige Steigerung für *alle* Marktteilnehmer - wenn überhaupt - so gleichzeitig nur in Bezug auf absolute Umsatzzahlen, nicht jedoch im Hinblick auf prozentuale Marktanteile funktionieren kann, ist auch klar.

In rechtlicher Hinsicht besteht für das Urheberrecht zunächst einmal ein punktueller Anpassungsbedarf in Bezug auf die noch weitgehend am Analogen ausgerichteten Sprache des Gesetzestextes. So ist im Urheberrechtsgesetz gegenwärtig nur von Bild- oder Tonträgern die Rede; gemeint sind damit „Vorrichtungen zur wiederholbaren Wiedergabe von Bild- oder Tonfolgen“. Wiederbeschreibbare CDs und Festplatten von Computern konnte der Gesetzgeber von 1965 noch nicht im Auge haben. Dennoch besteht kein Zweifel daran, dass auch letztere schon nach geltendem Recht dem Begriff der Bild- oder Tonträger unterfallen, mögen sie über Bilder und Töne hinaus auch ganz generell Daten speichern können. Fraglich ist aber insbesondere, ob PCs - und wenn ja, welcher Teil von ihnen - „Geräte“ sind, die „erkennbar zur Vornahme von Vervielfältigungen“ zum privaten oder sonstigen eigenen Gebrauch i.S.d. §§ 53 ff. UrhG benutzt werden, mit der Folge, dass die Hersteller von PCs an die dafür zuständigen Verwertungsgesellschaften dann von Gesetzes wegen die sog. Geräteabgabe entrichten müssten. Hierüber herrscht gegenwärtig in Deutschland erbitterter Streit.² Weitere Unsicherheit bestand einige Zeit in Bezug darauf, ob das Bereithalten geschützter Werke zum Abruf durch Dritte in Datenbanken, auf Bulletin-boards u.ä. nur eine private Handlung oder aber einen Akt der öffentlichen Wiedergabe in Form des Zu-

² Vgl. nur den „2. Bericht der Bundesregierung über die Entwicklung der urheberrechtlichen Vergütung gemäß § 54 ff. Urheberrechtsgesetz“ vom 5. Juli 2000, abrufbar unter <http://www.bmj.bund.de/ggv/bervgint.pdf>.

gänglichmachens darstellt. Für Urheber war das nach deutschem Recht eigentlich nie streitig. Lediglich für einige Inhaber sogenannter Nachbarrechte - also für ausübende Künstler und diejenigen, die wie Sendeunternehmen, Tonträgerhersteller oder Filmproduzenten kaufmännisch organisatorische Leistungen zur Ermöglichung der kulturellen Produktion und Verbreitung erbringen - war bzw. ist dies gegenwärtig noch immer umstritten.

Freilich bedarf es angesichts der Globalität der Vernetzung letztlich einer weltweit weitgehenden einheitlichen Regelung. Allerdings sei insoweit angemerkt, dass mit den beiden WIPO-Verträgen vom Dezember 1996³ bereits der Grundstein für einen solchen internationalen Rahmen gelegt ist, mögen die Verträge einstweilen auch noch nicht in Kraft getreten sein. Innerhalb der EU ist mit der Richtlinie betreffend das Urheberrecht in der Informationsgesellschaft das vergleichbare Gesetzeswerk inzwischen ebenfalls verabschiedet.⁴ Die Richtlinie über den elektronischen Geschäftsverkehr,⁵ die sich u.a. mit Fragen der Haftung von Mittelspersonen - typischerweise also den Service- und Zugangsdienstleistern - befasst und die im deutschen Informations- und Kommunikationsdienstegesetz (IuKDG)⁶ ein Vorbild hat, ist ohnehin bereits verabschiedet. Sicherlich ist bei jeder Harmonisierung auf

übernationaler Ebene zu berücksichtigen, dass eine Harmonisierung nie vollständig sein kann noch vollständig sein will. Denn es besteht weder ein Bedürfnis nach totaler Rechtsgleichheit, noch lassen sich historisch gewachsene nationale Unterschiede einfach beseitigen. Denn nationale Unterschiede wurzeln ja nicht allein im Rechtlichen, sondern haben ihre spiegelbildliche Entsprechung zumeist auch in den wirtschaftlichen Besonderheiten der jeweiligen Staaten. Hier ist es weder damit getan, von der Nationalstaatlichkeit mit all ihren Möglichkeiten der Verwirklichung einer nationalen Ordnungspolitik direkt in die einstweilen noch weitgehend akteurlose Globalität zu springen. Zugleich erscheint es unangemessen, angesichts der längst grenzüberschreitenden Technologien ängstlich und rückwärts gewandt an den nationalen Regelungsräumen festhalten zu wollen. Wie schwierig es hier ist, einen für alle Beteiligten gangbaren Kompromiss zu finden, der überdies sachgerechte Lösungen bereit hält, hat vor allem der Streit um die Schrankenbestimmungen in der genannten EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft gezeigt.

Besonderen Schwierigkeiten begegnet darüber hinaus die begrenzte Möglichkeit einer effektiven Rechtsdurchsetzung. Im Vordergrund steht hier die Frage, wieweit die digitale Kopie auch im digitalen vernetzten Kontext zulässig sein soll. Anzeichen für die Bedeutung dieser Frage ist der gegenwärtig allseits zäh geführte Kampf um die Einführung bzw. Verhinderung einer Abgabe auf digitale Speichermedien und insbesondere die Festplatten von PCs. Probleme bestehen aber auch dort, wo die Frage nach dem genauen Umfang des Ausschließlichkeitsrechts darüber entscheidet, wer von den Beteiligten ein bestimmtes Geschäft machen bzw. lizenzieren können soll. Elektronische Pressespiegel sind hier das beste Beispiel. Bei ihnen geht der Streit im Wesentlichen darum, ob die Hersteller traditioneller

³ WIPO Copyright Treaty (WCT) und WIPO Performances and Phonograms Treaty (WPPT), abrufbar unter <http://www.wipo.int/treaties/ip/copyright/index.html> bzw. <http://www.wipo.int/treaties/ip/performances/index.html>.

⁴ Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. Nr. L 167 v. 22.6.2001, S. 10.

⁵ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), ABl. Nr. L 178 v. 17.7.2000, S. 1.

⁶ Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) v. 22. Juli 1997 (BGBl. I S.1870); abrufbar unter <http://www.iid.de/iukdg/gesetz/iukdg.html>.

Pressespiegel diese künftig in elektronischer Form anbieten dürfen oder ob dieses Geschäft künftig den Verlegern der Primärerzeugnisse vorbehalten bleiben soll. Dass mit den Verfassern der einzelnen wiedergegebenen Artikel eine dritte Gruppe mit eigenständigen, gegenwärtig von der Verwertungsgesellschaft WORT wahrgenommenen Interessen ins Spiel kommt, macht die Sache nicht gerade leichter. Entscheiden lassen sich derartige Fragen letztlich wohl im Wege der Verhandlung und des Kompromisses zwischen den Beteiligten. Sollte dies scheitern, so bleibt wohl nur eine rechtspolitische Lösung durch den Gesetzgeber. Die Rechtsprechung der Instanzgerichte hat die Tür für unabhängige Anbieter von Informationsmehrwertdienstleistungen bislang jedenfalls weitgehend geschlossen gehalten.

Dieselben Fragen stellen sich auch im Hinblick auf einen angemessenen Zuschnitt der Ausschließlichkeitsrechte. Denn es besteht eine, wie ich meine, reelle Gefahr, dass ein in Reaktion auf den Kontrollverlust allzu weitreichender Schutz den Spielraum für an sich durchaus nützliche Mehrwertdienstleistungen allzu sehr schmälert. Ein Beispiel ist die Rechtsprechung zum elektronischen Kopienversand und zu den elektronischen Pressespiegeln. Um - auch im Lichte gemeinschaftsrechtlicher Vorgaben - sicher zu stellen, dass die Rechteinhaber in der Verwertung ihrer Werke durch digitale Konkurrenten nicht über Gebühr beeinträchtigt werden, sind die Grenzen so gezogen worden, dass elektronische Pressespiegel nicht ohne Zustimmung der ursprünglichen Rechteinhaber angeboten werden dürfen. Und das, obwohl doch nichts sinnvoller und umweltverträglicher wäre, als die über unsere Straßen transportierte Papierflut durch einen umweltverträglichen und nachhaltigen Datenstrom zu ersetzen. Vielleicht lässt sich die bisherige Rechtsprechung aber auch dahin gehend interpretieren, dass die Frage, wie die Regelungen aussehen sollen, nach de-

nen sich die Beteiligten im digitalen und vernetzten Kontext zu richten haben, nicht von den Gerichten, sondern vom Gesetzgeber entschieden werden sollen. In der Tat könnte wohl am besten der Gesetzgeber das urheberrechtliche System als eine der Rahmenbedingungen für das elektronische Publizieren mit anderen Rahmenbedingungen und rechtspolitischen Vorgaben in Einklang bringen.

Weitere Themen, die durch das elektronische Publizieren aufgeworfen werden, betreffen vor allem das Verhältnis von Recht und Technik. Wenn die Technik zu einem Kontrollverlust führt, so liegt es nahe - gleich dem Besen in Goethes Zauberlehrling - diejenigen Kräfte zur Hilfe zu rufen, die für den Kontrollverlust selbst verantwortlich sind. „The answer to the machine is in the machine“ lautete lange Zeit ein in Urheber- wie Produzentenkreisen geflügeltes Wort. Wird die Technik aber als legitimes Mittel eingesetzt, um dem durch die Technik selbst hervorgerufenen Kontrollverlust zu begegnen, so bedürfen derartige technische Sicherungsmechanismen ihrerseits wiederum flankierend des rechtlichen Schutzes gegen ihre Umgehung. Das gilt für Zugangssperren ebenso wie für Kopierschutzmechanismen. Denn anders blieben die rechtlich für schutzwürdig erachteten Inhalte trotz technischer Sicherungen auch weiterhin rechtlich ungeschützt. Oder um es bildhaft auszudrücken: Wer um sein vom Recht geschütztes geistiges Gut einen elektronischen Zaun errichtet, dem muss das Recht die Möglichkeit an die Hand geben, gegen denjenigen vorzugehen, der den elektronischen Zaun mit einem elektronischen Bolzenschneider zu durchtrennen versucht. Dabei stellt sich jedoch ein Problem. Denn wer garantiert, dass der elektronische Zaun Dritten den Zugang tatsächlich nur zu solchen Gütern verwehrt, die das Gesetz für schutzwürdig erachtet? Oder anders formuliert: Steht dem Rechteinhaber der rechtliche Schutz gegen den digitalen Einbrecher auch

dann zur Verfügung, wenn mit Hilfe seines elektronischen Zaunes etwas eingezäunt wird, das ihm nach dem Gesetz gar nicht gebührt, sondern bei dem es sich um „Niemandland“, urheberrechtlich gesprochen um die „domaine public“ handelt? Die Urheberrechtsgemeinde ist in diesem Punkt geteilter Meinung. Vor allem in den USA fürchten kritische Stimmen, dass der individuelle Einsatz technischer Zugangs- und Kopiersperren die gesetzlichen Wertungen unterlaufen bzw. überspielen könnten und die Nutzer unter Außerachtlassung gesetzlich geschützter Zugangsinteressen in allzu weitem Umfang von der Nutzung bestehenden Materials ausgeschlossen werden könnten. Das Problem erweist sich deshalb als so schwierig, weil sich im Zeitpunkt des Überwindens der digitalen Sperrvorrichtung nicht ermitteln lässt, ob der Überwindende nachfolgend eine erlaubte oder aber eine dem Rechtsinhaber vorbehaltene Verwertungshandlung in Bezug auf das geschützte Material vornehmen will. Eines scheint jedoch festzustehen: Wenn überhaupt, so wird auch hier eine Lösung nur von Seiten der Technik erfolgen können.

„Wer um sein vom Recht geschütztes geistiges Gut einen elektronischen Zaun errichtet, dem muss das Recht die Möglichkeit an die Hand geben, gegen diejenigen vorzugehen, der den elektronischen Zaun mit einem elektronischen Bolzenschneider zu durchtrennen versucht.“

Ein ähnliches Problem stellt sich in Bezug auf das Verhältnis von Gesetzesrecht und privatem Vertrag. Auch hier ist denkbar, dass der Rechtsinhaber dem Nutzer mittels vertraglicher Vereinbarung insbesondere im Zuge der

Verwendung allgemeiner Geschäftsbedingungen erheblich weniger gestattet als dieser nach der sorgfältigen gesetzlichen Abwägung widerstreitender Güter und Interessen von Gesetzes wegen tun dürfte. Auch dazu ein - wenn gleich etwas übertrieben anmutendes, gleichwohl jedoch reales - Beispiel: Es hatte ein Software-Haus die Beta-Version seines neuen Programms an einen Fachjournalisten übergeben und ihm die zum Test erforderlichen urheberrechtlichen Nutzungsrechte einräumen, geknüpft allerdings an die Bedingung, nur positiv über das Programm zu berichten. Zu kritisieren steht dem Journalisten natürlich frei und er ist insoweit durch die Meinungsfreiheit gem. Art. 5 GG geschützt; dennoch macht er sich im Fall der Kritik rein formal betrachtet einer Urheberrechtsverletzung schuldig.

In praktischer Hinsicht werden sich die traditionellen Rollen der Beteiligten sicherlich verschieben, wenn nicht gar in Teilen neu verteilen. Produzenten werden bestimmte Geschäfte, die bislang von Dritten unternommen wurden, künftig selbst machen wollen. Das aber führt zu der Frage, ob ein Urheberrechtsschutz, der dem Erbringer einer Primärleistung zugleich auch sämtliche möglichen Sekundärmärkte vorbehält - und zwar gleichviel, ob der Erbringer der Primärleistung diese Sekundärmärkte selbst, durch Dritte oder aber gar nicht bedienen will - tatsächlich im Sinne einer optimalen Erzeugung, Bereitstellung, Verbreitung und Nutzung geschützter Werke effizient ist.

Der technische wie der rechtliche Wandel zu neuen Geschäftsmodellen wird in der Verwertung urheberrechtlich geschützter Inhalte (des sog. „content“) führen. Das Urheberrecht an sich ist den einzelnen Geschäftsmodellen gegenüber jedoch zu recht grundsätzlich neutral, soll doch keine bestimmte Marktentwicklung präjudiziert werden. Ob etwa ein bestimmter Inhalt pro Nutzung (pay-per-view bzw. pay-on-demand) oder im Rahmen einer

pauschalen Abonnementsgebühr abgerechnet wird, darüber enthält das Urheberrecht ebenso wenig bindende Vorgaben wie darüber, ob man durch das Verschenken einer Basisleistung möglichst rasch ein möglichst großes Kundensegment an sich binden will oder nicht. Auch das Konzept der open-source ist urheberrechtlich an sich kein Problem, sofern darunter nicht verstanden wird, dass jeglicher Inhalt schutzrechtsfrei sein müsse oder dass umgekehrt kein Inhalt schutzrechtsfrei sein dürfe. Die wirklich interessantere Frage geht vielmehr dahin, wie das Recht hier überhaupt steuernde Anreize zu setzen vermag. Allerdings steht eine ökonomische Wirkungs- und Folgenabschätzungsforschung hier erst ganz am Anfang. Ohnehin legt es das gewandelte Verständnis der Staatsaufgaben im Sinne einer Infrastrukturverantwortung nahe, dass auch im Bereich des Urheberrechts künftig weniger allzu differenzierende Einzelfallregelungen getroffen als vielmehr ein allgemeinerer gesetzlicher Rahmen bereit gestellt wird. Denn gegen ein allzu ins Einzelne gehendes Tätigwerden des Gesetzgebers spricht bereits die Geschwindigkeit, mit der sich der technologische Wandel vollzieht, und dem selbst eine funktionierende Gesetzgebung schon jetzt allenfalls mit Mühe nachkommen kann.

Nicht absehbar ist im weiteren, welche wirtschaftlichen Rückwirkungen die für elektronische Publikationen praktizierten Geschäftsmodelle im Übergang und in der Parallelität von analoger und digitaler Verwertung künftig haben. Sicherlich werden wir noch eine Weile mit Widersprüchen zu leben haben. Bei der Lösung solcher Widersprüche hilft wohl nur das begrenzte Experiment. Dabei muss der Erfahrungsgewinn nicht einseitig bei den Nutzern liegen; erhält vielmehr der Rechteinhaber im Gegensatz entsprechende Nutzungs- (nicht Nutzer-) daten, so mag eine derartige experimentelle Vereinbarung durchaus zu einem beiderseitigen Gewinn führen.

Wenig Beachtung hat bislang die weitere Frage nach der Verbindung von Geschäfts- und Finanzierungsmodellen gefunden. Gerade aufgrund der Öffnung von Teilen der Verwaltung für den Wettbewerb - sei es angesichts der Privatisierung, sei es wegen des knapper werdenden Geldes - lastet ein erheblicher Druck insbesondere auf öffentlichen Forschungseinrichtungen und Bibliotheken, eigene Mehrwertleistungen zu vermarkten. Das ist für die Einnahmenseite zwar erfreulich, führt im Rahmen der Nutzung fremder Angebote jedoch zugleich zu erhöhten Zahlungen. Ob es wirtschaftspolitisch Sinn macht, einen derartigen Wettlauf zu initiieren und ob dabei tatsächlich diejenige Institution überleben soll, die die Nase „vorne“ hat, erscheint angesichts des weitgehend noch immer öffentlichen Versorgungsauftrages insbesondere von wissenschaftlichen Bibliotheken zumindest zweifelhaft. Helfen mögen immerhin Konsortialverträge, in denen sich mehrere Bibliotheken zusammen tun, um insbesondere marktmächtigen Anbietern wissenschaftlicher Fachzeitschriften ein hinreichendes Verhandlungsgewicht entgegen setzen zu können. Die kartellrechtlichen Implikationen, die sich dabei ergeben, sind bislang jedoch noch kaum untersucht. Und schließlich gerät, wer nicht über seine Mutterorganisation an einem solchen Konsortium teilhaben kann, allzu leicht als “information have-not“ ins Hintertreffen. Ungeklärt ist auch, inwieweit die ökonomischen Rahmenbedingungen urheberrechtlich geschützter Gegenstände aus dem Unterhaltungsbereich mit denen aus dem Bildungs- und Informationsbereich vergleichbar sind und sich Erfahrungen des einen Sektors auf die jeweils anderen Sektoren übertragen lassen.

Immerhin: Die Praxis zeigt, dass der Umgang mit den elektronischen Medien die Beteiligten zunehmend zu Kooperations- anstatt zu Konfrontationsmodellen veranlasst. Das erscheint letztlich auch sinnvoll. Gemeinsam ist

man stärker bzw. haben die bestehenden „player“ unterschiedliche Fähigkeiten und Ressourcen, die sich besser ergänzen als dass sich mit ihnen ein unnötiger Konkurrenzkampf ausfechten ließe. Urheber werden weiterhin die primäre Quelle für die Schaffung des Rohstoffs „content“ sein. Dass die Vernetzung die Mitteilungsmöglichkeiten von Autoren um die private e-mail-Kommunikation und um Pre-Print-Server erweitert, tut der Rolle der Produzenten nicht notwendig Abbruch. Diese werden ihre Stärke auch weiterhin in der Finanzierung von Neuschöpfungen, der Bestandspflege und dem Anbieten elektronischer Mehrwertdienste entfalten können. Außerdem bringen sie angesichts ihrer eingeführten Markenzeichen erheblich bessere Ausgangsbedingungen für kommerziell erfolgreiche Plattformen zur Vermarktung der Inhalte mit. Sie oder auch Dritte vermögen über Portale erheblich größere Ressourcen zu mobilisieren als dies den meisten der Urhebern und selbst kleineren Produzenten möglich ist. Verwertungsgesellschaften schließlich verfügen über einen schon jetzt umfassenden Bestand von Werk- und Nutzungsdaten sowie über eine Infrastruktur, die nicht nur für eine kollektive, sondern auch für eine zentralisierte Rechtswahrnehmung bestens geeignet erscheint.

In der Übergangsphase von Print zu Digital wird es sicherlich zu einer Reihe von Verwerfungen kommen. Auch Prozesse der Vermachtung und damit der partiellen Außerkraftsetzung von Marktmechanismen sind nicht auszuschließen. Dem wird man gegebenenfalls durch eine Anpassung der rechtlichen Rahmenbedingungen begegnen müssen und sicherlich auch können. Einstweilen bleiben die Beteiligten jedoch aufgerufen, den weiten

rechtlichen Rahmen zur optimalen Produktion, Bereitstellung und Nutzbarmachung urheberrechtlich geschützter Werke und Leistungen in digitaler Form zu nutzen. Geiz und Furcht jedenfalls sind - vor allem in Kombination - schlechte Ausgangspositionen für die Zukunft. Sie vermögen in der Tat Sand in das Getriebe unserer elektronischen Welt zu streuen. Dem sollten Gesetzgeber und Gerichte, aber vor allem die Beteiligten selbst, gleichermaßen nach Kräften entgegen wirken.

Prof. Dr. Thomas Dreier, M.C.J. (New York University), ist Inhaber des Lehrstuhls für Bürgerliches, Handels-, Gesellschafts- und Wirtschaftsrecht in Verbindung mit Rechtsfragen in der Informationsgesellschaft sowie Leiter des Instituts für Informationsrecht der Universität Karlsruhe. Schwerpunkt seiner Forschungstätigkeit ist das Recht der Informationsgesellschaft. Zuvor war er 15 Jahre am Münchner Max-Planck-Institut für ausländisches und internationales Patent-, Urheber- und Wettbewerbsrecht. Prof. Dreier ist Vizepräsident der internationalen Urheberrechtsgesellschaft ALAI und Mitherausgeber der Zeitschrift „Computer und Recht International“. 1997 hat Prof. Dreier im Auftrag der Friedrich-Ebert-Stiftung ein Gutachten zum Thema „Urheberrecht und digitale Werkverwertung – Die aktuelle Lage des Urheberrechts im Zeitalter von Internet und Multimedia“ verfasst (<http://www.fes.de/fulltext/stabs-abteilung/00391toc.htm>) sowie für das ECUP-Projekt der EU im Jahr 2001 die Studie „Towards Consensus on the lectronic Use of Publications in Libraries – strategy issues and ecommendations“ (<http://gdz.sub.uni-goettingen.de/tecup/towacons.pdf>).

Electronic Commerce und Verbraucherschutz in Europa*

Michael Lehmann

Schiller (Die Braut von Messina):

„Das Gesetz ist für die Schwachen da“

Adam Smith (Der Wohlstand der Nationen):

„Der Verbrauch allein ist Ziel und Zweck jeder Produktion; daher sollte man die Interessen des Produzenten eigentlich nur soweit beachten, wie es erforderlich sein mag, um das Wohl des Konsumenten zu fördern. Diese Maxime leuchtet ohne weiteres ein, so dass es töricht wäre, sie noch beweisen zu wollen. In einer staatswirtschaftlichen Wirtschaftsordnung aber wird das Wohl des Verbrauchers beinahe ständig dem Interesse des Produzenten geopfert, und man betrachtet offenbar die Produktion und nicht den Konsum als letztes Ziel oder Objekt allen Wirtschaftens und Handelns.“

Der nachfolgende Beitrag stellt den Inhalt der Richtlinie zum Electronic Commerce dar, wobei er einer Einordnung in den Zusammenhang mit anderen einschlägigen Rechtsakten vornimmt, und kritisiert die für den elektronischen Geschäftsverkehr vorgesehenen Regelungen vor allem unter dem Gesichtspunkt des Verbraucherschutzes.

1. Verbraucherschutz und IPR in Europa

Blickt man angesichts der ständig fortschreitenden Globalisierung und Internationalisierung der Märkte zum Schutze der Verbraucher in das Europäische Recht, findet sich in Art. 5 Abs. 2 des Römischen EWG-Übereinkommens „über das auf vertragliche Schuldverhältnisse anzuwendende Recht“ vom 14. Juni 1980 und daraus resultierend, inhaltlich gleichlautend z.B. in Art. 29 des deutschen EGBGB vom 21.9.1994 eine zentrale Schutzbestimmung: Die „zwingenden Be-

stimmungen des Rechts des Staates“, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat, müssen für alle „Verbraucherverträge“ berücksichtigt werden, „wenn dem Vertragsschluss ein ausdrückliches Angebot oder eine Werbung in diesem Staat vorausgegangen ist und wenn der Verbraucher in diesem Staat die zum Abschluss des Vertrages erforderlichen Rechtshandlungen vorgenommen hat“. Diese Voraussetzungen werden in der Regel bei jedem Rechtsgeschäft im Netz eines Verbrauchers im Rahmen des Electronic Commerce erfüllt sein, der etwa zu Hause an seinem Computer sitzend eine Bestellung, also einen Antrag bzw. eine Annahmeerklärung abgibt. Dann gilt für ihn z.B. aus deutscher Sicht das AGB-Gesetz, das Haustür-Widerrufgesetz, das Verbraucher-Kreditgesetz und, für Pauschalreisen, die §§ 651a ff. BGB (Reisevertrag), aus österreichischer Sicht z.B. das Konsumentenschutzgesetz vom 8.3.1979. So betrachtet könnte man meinen, dass der Electronic Commerce für den Europäischen Verbraucher keine besondere Gefahr darstellt und dass ein rechtspolitischer Handlungsbedarf zur Verbesserung des Europäischen Verbraucherschutzes¹ zu verneinen ist. Die Kommission der EU und dabei nicht nur die DG

¹ Vgl. dazu allgemein Krämer, L., EWG-Verbraucherrecht, 1985 passim; Reich, N., Europäisches Verbraucherschutzrecht: Binnenmarkt und Verbraucherinteresse, 2. Aufl. 1993, passim; Drexl, J., Die wirtschaftliche Selbstbestimmung des Verbrauchers, 1998, S. 43 ff.; s. auch v. Hippel, E., Verbraucherschutz, 3. Aufl. 1986, passim; Pützhoven, A., Harmonisierung des europäischen Verbraucherschutzrechts, EWS 1999, 447 ff.; speziell zum „Verbraucherschutz im Netz“, vgl. Drexl, J., in Lehmann, M. (Hrsg.), Rechtsgeschäfte im Netz - Electronic Commerce, 1999, S. 75 ff.; Hoeren/Oberscheidt, Verbraucherschutz im Internet, VuR 1999, 371 ff.; Ernst, S., Verbraucherschutzrechtliche Aspekte des EU-Richtlinienvorschlags zum Electronic Commerce, VuR 1999, 397 ff.; vgl. auch die Entschließung des Rates vom 19.1.99 über die „Verbraucherdimension der Informationsgesellschaft, ABl. EG C 23/1 vom 28.1.99.

XXIV - Verbraucherschutz - sondern auch die DG XV - Binnenmarkt, sieht dies aber anders.

2. Die neuen Europäischen Rechtsquellen für den electronic commerce

Die Kommission der hat sich in Abstimmung mit dem Europäischen Parlament in letzter Zeit besonders intensiv um die Ausgestaltung eines adäquaten rechtlichen Rahmens für den elektronischen Geschäftsverkehr² im europäischen Binnenmarkt bemüht und bereits zahlreiche Richtlinien bzw. Richtlinienvorschläge der Öffentlichkeit unterbreitet. Als europäische Rechtsquellen für den elektronischen Geschäftsverkehr können hier insbesondere benannt werden: die Fernabsatzrichtlinie³,

² Vgl. dazu aus wirtschaftsrechtlicher Sicht Widmer/Bähler, Rechtsfragen beim Electronic Commerce, Zürich 1997 (zum Schweizer Recht); Lehmann, M. (Hrsg.), Rechtsgeschäfte im Netz - Electronic Commerce, Stuttgart 1998; Loewenheim/Koch (Hrsg.), Praxis des Online-Rechts, Weinheim 1998; Hoeren/Sieber (Hrsg.), Multimedia-Recht, München 1999, jeweils passim.

³ ABl. L 144, S. 19 ff., vom 4.6.1997; vgl. dazu Hoffmann, D., Die Europäische Fernabsatzrichtlinie, in Lehmann (Hrsg.), a.a.O. Fn. 1, S. 61 ff.; Drexler, J., Verbraucherschutz im Netz, in Lehmann (Hrsg.), a.a.O. Fn. 1, S. 76 ff.; vgl. auch den Referentenentwurf eines deutschen Fernabsatzgesetzes vom 14.1.00, in der Fassung der Beschlussempfehlung des Rechtsausschusses v. 12.04.00, BT-Drucks. 14/3195, welcher u.a. insbesondere auch einen neuen 29a EGBGB vorschlägt, der 12 AGBG überflüssig werden lässt:

„Artikel 29a

Verbraucherschutz für Sondergebiete

(1) Unterliegt ein Vertrag aufgrund einer Rechtswahl nicht dem Recht eines Mitgliedstaats der Europäischen Union oder eines anderen Vertragsstaats des Abkommens über den Europäischen Wirtschaftsraum, so sind die Vorschriften des AGB-Gesetzes, des Fernabsatzgesetzes, des Fernunterrichtsschutzgesetzes und des Teilzeit-Wohnrechtgesetzes gleichwohl anzuwenden, wenn der Vertrag einen engen Zusammenhang mit dem Gebiet eines oder mehrerer Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Europäischen Wirtschaftsraumes aufweist. Ein enger Zusammenhang ist insbesondere anzunehmen, wenn

- (1) der Vertrag aufgrund eines öffentlichen Angebots, einer öffentlichen Werbung oder einer ähnlichen geschäftlichen Tätigkeit zustandekommt, die in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum entfaltet wird, und
- (2) der andere Teil bei Abgabe seiner auf den Vertragsschluss gerichteten Erklärung in einem Mitgliedstaat der Europäischen

Richtlinie 97/7/EG vom 20.5.1997, welche Verbraucherverträge betrifft, die unter Einsatz von „Fernkommunikationstechniken“ abgeschlossen werden; die Richtlinie 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Richtlinie⁴); die Datenbank-Schutzrichtlinie 96/9/EG vom 11.3.1996 über den Urheber- und sui generis-rechtlichen Schutz von Datenbanken⁵, welche vor allem für die multimedialen Inhalte („content“) im Netz, z.B. im www, sowie für alle on demand-Services⁶ Bedeutung erlangt.

Von den zur öffentlichen und parlamentarischen Diskussion vorgestellten Entwürfen sind insbesondere zu erwähnen der geänderte Vorschlag für eine Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft⁷ vom 21.05.1999, der nicht nur

Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum seinen Wohnsitz oder gewöhnlichen Aufenthalt hat. ...“

Mittelbar kann auch Bedeutung erlangen der Vorschlag für eine Richtlinie über den Fernabsatz von Finanzdienstleistungen an Verbraucher vom 14.10.1998, KOM(1998)468 endg. sowie die bereits erlassene Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates vom 25. Mai 1999 zu bestimmten Aspekten des Verbrauchsgüterkaufs und der Garantien für Verbrauchsgüter, ABl. L 171/12 vom 7.7.1999; vgl. dazu Lehmann, M., Informationsverantwortung und Gewährleistung für Werbeangaben beim Verbrauchsgüterkauf, JZ 2000, ... (in Erscheinung).

⁴ ABl. L 281, S. 31 ff. vom 23.11.1995.

⁵ ABl. L 77, S. 20 ff. vom 27.3.1996; vgl. dazu Lehmann, M., Die Europäische Datenbankrichtlinie und Multimedia, in Lehmann (Hrsg.), Internet- und Multimediarecht (Cyberlaw), 1997, S. 67 ff.; ders., The European Database Directive and its Implementation into German Law, 29 IIC 776 ff. (1998).

⁶ Vgl. etwa Ostermaier, C., Video on demand und Urheberrecht, 1997, S. 63 ff.; ders., CR 1998, 539 ff.

⁷ KOM(99) 250 endg., vom 21.05.1999; zum ursprünglichen Entwurf vgl. Reinbothe, J., Der EU-Richtlinienentwurf zum Urheberrecht und zu den Leistungsschutzrechten in der Informationsgesellschaft, ZUM 1998, 429 ff.; Flehsig, N.P., EU-Harmonisierung des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ZUM 1998, 139 ff.; ders., Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft, CR 1998, 225 ff.; Lehmann, M., Electronic Commerce und Urheberrecht, a.a.O. Fn. 1, S. 105 ff.; Dreier, Th., Adjustment of Copyright Law to the Requirements of the Information Society, 29 IIC 623 ff. (1998).

den WIPO Copyright Treaty und den WIPO Performances and Phonograms Treaty vom 20.12.1996 in europäisches Recht überführen⁸, sondern auch alle urheberrechtlichen Bits and Bytes im Netz wirklich handelbar und verkehrsfähig werden lassen will. Weiter zu erwähnen ist in diesem Zusammenhang auch die Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen⁹, welche die Halbherzigkeiten des deutschen Signaturgesetzes als Teil des Informations- und Kommunikationsdienstegesetzes¹⁰ (Multimediasgesetz) vom 22.7.1997 überwinden und unter bestimmten Voraussetzungen elektronische Unterschriften einer handschriftlichen Unterschrift gemäß § 126 Abs. 1 BGB gleichstellen wird. Außerdem ist der Geänderte Vorschlag für eine Entscheidung des Europäischen Parlaments und des Rates über die Annahme eines mehrjährigen Aktionsplanes der Gemeinschaft zur Förderung einer sicheren Nutzung des Internet¹¹ einschlägig, genauso wie die Mitteilung der Kommission über die Verwaltung des Internet (Internet Governance), die technische Verwaltung von Namen und Adressen im Internet¹² und die Gemeinsame Erklärung der EU und der USA über den Electronic Commerce vom Washingtoner Gipfeltreffen am 5. Dezember 1997¹³.

Zu alledem nunmehr hinzugekommen ist die Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt vom

8.6.2000¹⁴; eine politische Einigung war bereits im Ministerrat am 7.12.99 erarbeitet worden. Weiter erwähnt werden muss der neue Vorschlag einer Verordnung über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen¹⁵, der in Art. 16 vorsieht, dass der Verbraucher immer auch an seinem Wohnsitz Klage erheben kann und zwar auch dann, wenn diese sich gegen einen ausländischen, europäischen Lieferanten richtet.

3. Elektronischer Geschäftsverkehr im Binnenmarkt - Die Richtlinie im Überblick

Die Richtlinie behandelt nicht nur die Neuregelung der Verantwortlichkeit im Netz, sondern möchte auch viele sonstige aktuelle Rechtsfragen in horizontaler Hinsicht in Europa einheitlich regeln; einige besonders wichtige Wertungsansätze sollen hier zunächst hervorgehoben und sodann kritisch gewürdigt werden, welche den „Geist“ und die Intention

⁸ Vgl. dazu auch den Diskussionsentwurf eines Fünften Gesetzes zur Änderung des Urheberrechtsgesetzes vom 7. Juli 1998 (BMJ: 3600/13-5300/98) und den Vorschlag der Kommission vom 27.4.1998 (98/C165/08) KOM(1998)249 endg.

⁹ Richtlinie 1999/93/EG v. 13.12.1999, ABl. EG Nr. L 13/12 ff. s. dazu Kilian, BB 2000, 733 ff.

¹⁰ BGBl. I 1869 ff., vom 28. Juli 1997.

¹¹ Vom 10.9.1998, KOM(1998)518 endg.; vgl. nun den Gemeinsamen Standpunkt (EG) Nr. 56/98 vom 24.9.1998, ABl. C 360, S. 83 ff.

¹² Vom 29.7.1998, KOM(1998)476 endg.

¹³ Vgl. <http://europa.eu.int/eu/comm/dg01/ele/rst.htm>

¹⁴ Richtlinie 2000/31/EG, ABl. EG Nr. L 178, v. 17.7.2000 abgedruckt in EuZW, Heft 17, 2000, S. 526; zum Vorläufer, dem geänderten Vorschlag der Kommission vgl. KOM(1999)427 endg.; vgl. auch den konsolidierten Entwurf des Generalsekretariats des Ministerrats vom 13. August 1999; der ursprüngliche Text ist abrufbar unter <http://www.online-law.de>; vgl. dazu Maennel, F., Der Multimedia-Rechtsrahmen der europäischen Union: Ein Überblick, in Lehmann (Hrsg.), a.a.O. Fn. 1, S. 32 ff.; Lehmann, Rechtsgeschäfte und Verantwortlichkeit im Netz, ZUM 1999, 180 ff.; Waldenberger, A., Electronic Commerce: der Richtlinienvorschlag der EG-Kommission, EuZW 99, 296 ff.; Tettenborn, A., Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr, K & R 99, 252 ff.; Hoeren, Th., Vorschlag für eine EU-Richtlinie über E-Commerce. Eine erste kritische Analyse, MMR 99, 192 ff.; Landfermann, H.-G., Der Richtlinienvorschlag „Elektronischer Geschäftsverkehr“ - Ziele und Probleme, ZUM 1999, 795 ff.; Spindler, G., Der neue Vorschlag einer E-Commerce-Richtlinie, ZUM 1999, 775 ff.

Eng damit zusammenhängt auch der Verordnungsentwurf des Rates über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen vom 14.07.1999, KOM(1999)348 endg.

¹⁵ Vom 14.07.1999, KOM(1999) 348 endg.; vgl. dazu Schwab, EuZW 1999, 737; vgl. dazu allgemein Junker, A., Internationales Vertragsrecht im Internet. Im Blickpunkt: Internationale Zuständigkeit und anwendbares Recht, RIW 1999, 809 ff.

nen der Richtlinie besonders klar zu erhellen vermögen.

Art. 1 bis 3 definieren den Anwendungsbereich dieser Richtlinie, geben umfangreiche Begriffsbestimmungen, z.B. für die Definition der „kommerziellen Kommunikation“, also jede Wirtschaftswerbung im weitesten Sinn, einschließlich Product Placement, Sponsoring, Public Relation-Aktivitäten, und schreiben in Art. 3 Abs. 1 und 2 den Grundsatz des Ursprungslandsprinzips fest, welcher durch Art. 3 Abs. 3 i.V.m. dem Anhang, also insbesondere für das Urheberrecht, die verwandten Schutzrechte, die Topographien und den Datenbankschutz sowie alle sonstigen gewerblichen Schutzrechte wieder dergestalt gelockert wird, dass für diese das althergebrachte Territorialitätsprinzip erhalten bleibt. Dies gilt allerdings nicht für das Marken- und Wettbewerbsrecht. Dieses Herkunfts- bzw. Ursprungslandprinzip, welche z.B. auch in der Kabel- und Satellitenrichtlinie¹⁶ niedergelegt worden ist, setzt allerdings schon das Bestehen eines einigermaßen gleichmäßigen Rechtsniveaus in der EU voraus; andernfalls ist geradezu ein Wettbewerb um die niedrigste Eingriffsschwelle, ein „race to the bottom“, vorprogrammiert. Für den Verbraucherschutz ist dies angesichts von Art. 95 Abs. 3 EV (früher Art. 100a: „hohes Schutzniveau“) sehr abträglich, weil er sich auf sein gewohntes heimatisches Schutzniveau, in Deutschland z.B. gegen irreführende Werbeangaben gemäß §§ 3 und 1 UWG, nicht mehr verlassen kann.

Deswegen sollte im Netz auch nicht z.B. für Pornographieverbote das besonders niedrige Niveau einiger skandinavischer Länder den EU-Maßstab setzen, genauso wenig wie für die Beurteilung von Schmähkritik und von Verletzungen des Allgemeinen Persönlichkeitsrechts das englische Recht, dem z.B. eine

Caroline von Monaco-Rechtsprechung¹⁷ nach deutschem Vorbild völlig fremd ist. Gerade weil das Internet, z.B. für Schmähkritik¹⁸, besonders weitreichende Möglichkeiten eröffnet, sollten besonders niedrige nationale Schutzstandards für die EU nicht entscheidungserheblich werden. Deshalb ist für den Electronic Commerce das Herkunftslandprinzip prinzipiell ungeeignet; es führt nur zu einer Rechtsharmonisierung auf dem kleinsten gemeinsamen Nenner und somit zu einer Art Wirtschaftsrechtsdumping. Demgegenüber vorzugswürdig erscheint ein modifiziertes Wirkungsstatut, was wir aus dem Kartell- und Wettbewerbsrecht kennen.

In den Art. 4 und 5 werden die Zulassungs- und Lizenzfreiheit für alle Dienstleister rund um das Netz, sowie bestimmte allgemeine Informationspflichten geregelt, welche der Erhöhung der Transparenz der am Electronic Commerce beteiligten Unternehmen dienen sollen; insofern ergeben sich gewisse Parallelen zur Fernabsatzrichtlinie¹⁹, die ursprünglich nicht für den Electronic Commerce, sondern primär für den Verbraucherschutz beim Versandhandel geschaffen worden ist, aber zweifelsohne für ersteres Geschäftsfeld gleichermaßen Anwendung findet. Vor allem die Widerspruchsfrist von sieben Werktagen des Art. 6 dieser Richtlinie wird hier für die Praxis relevant werden sowie der Vorschlag eines neuen § 29a EGBGB im Referentenentwurf eines deutschen Fernabsatzgesetzes (Verbraucherschutz für die Sondergebiete: AGB-Gesetz, Fernabsatzgesetz, Fernunterrichtschutzgesetz und Teilzeit-Wohnrechtgesetz);

¹⁶ Vgl. dazu ausführlich Dreier, Th., Kabelweiterleitung und Urheberrecht, München 1991, 13 ff.; ders., in Quellen des Urheberrechts, Europäisches Gemeinschaftsrecht II-3, 1994; ders., ZUM 1995, 458 ff.

¹⁷ Vgl. BGH vom 19.12.1995, NJW 1996, 1128; Steffen, E., Schmerzensgeld bei Persönlichkeitsverletzungen durch Medien, NJW 1997, 10 ff.; Prinz, M., Geldentschädigung bei Persönlichkeitsverletzungen durch Medien, NJW 1996, 953 ff. Die Richtlinie erlaubt für das Allgemeine Persönlichkeitsrecht nationale Ausnahme-Maßnahmen; dies ist zu begrüßen.

¹⁸ LG München vom 17. Oktober 1996, CR 1997, 155 f. - Schmähkritik via Internet; siehe auch OLG Nürnberg, CR 1998, 686 ff.

¹⁹ Vgl. oben, Fn. 3.

hier fehlt allerdings das Reiserecht gemäß $\square\square$ §§ 651a ff. BGB.

In den Art. 6 bis 8 werden einige Grundsätze für die Werbung im Netz niedergelegt, welche entsprechend einer anderen Initiative der EU-Kommission mit „kommerzieller Kommunikation“²⁰ benannt worden sind. Gemäß Art. 7 müssen nicht angeforderte kommerzielle Kommunikationen bei Eingang beim Nutzer klar und unzweideutig als solche erkennbar sein, was zu einer Aufhebung des bisherigen nationalen Verbots von unerbetenen Werbe-e-mails führen könnte; der deutschen Rechtsprechung zu \square 1 UWG²¹ ist aber der Vorzug zu geben, denn jedem Verbraucher steht zunächst einmal das Recht „to be let alone“ auch gegenüber der Werbung zu, so dass er prinzipiell sich nicht gegen Werbung zur Wehr setzen muss, sondern der Werbende grundsätzlich zu erkennen geben muss, dass es sich bei diesen Kommunikationsbemühungen um Werbung handelt (Transparenzgebot) und sodann auf einfache Art und Weise deren Unterlassung und Beseitigung ermöglichen muss²². Wegen der extrem hohen Nachahmungsgefahr und des besonders hohen Grads der Belästigung durch unerbetene Werbe-e-mails sollte daher dem Werbenden zugemutet werden, zunächst beim potentiellen Werbeadressaten per e-mail anzufragen²³, ob er überhaupt auf diese

Art und Weise umworben werden möchte; und dann muss gelten: *qui tacet consentire non videtur*. Dies ist wegen der besonderen Kostengünstigkeit im Netz jedem Werbenden zuzumuten und dies verlangt auch die angemessene Achtung des Persönlichkeitsrechts jedes Nachfragers²⁴. Im Hinblick auf die ausdrückliche Ausnahme im Anhang für „nicht angeforderte kommerzielle Kommunikation mittels elektronischer Post“ kann diese deutsche Rechtsauffassung auch weiterhin aufrechterhalten werden.

Akzeptabel, weil nunmehr nicht mehr mit vier Willenserklärungen, wie dies ursprünglich die DG XXIV wollte, unnötig verkomplizierend, erscheint auch die Regelung des Vertragsabschlusses im Netz gemäß Art. 9 ff. der Richtlinie. Danach sollen nur zwei Willenserklärungen im Sinne der $\square\square$ §§ 145, 147 BGB zu einem Vertragsabschluss führen, eine Bestellung des Verbrauchers und eine Bestätigung des Anbieters. Gemäß Art. 11 wird dabei offen gelassen, ob die Anpreisungen einer Ware oder Dienstleistung im Netz als *invitatio ad offerendum*, oder, offenbar dem spanischen Modell folgend, schon als Antrag i.S.d. \square § 145 BGB zu bewerten ist. Durch z.B. „das Anklicken eines Symbols“ kann dieser Antrag gemäß \square § 147 BGB angenommen werden; der Vertrag gilt aber erst dann als geschlossen, wenn der Nutzer vom Diensteanbieter auf elektronischem Wege die Bestätigung des Zugangs seiner Annahme beim Diensteanbieter erhalten hat oder diese Bestätigung beim Anbieter abrufen kann. Erleichtert wird dieses Verfahren durch eine juristische Fiktion, die dem deutschen \square § 151 Satz 1 BGB nahe kommt, denn die erwähnte Empfangsbestätigung gilt als beim Verbraucher eingegangen,

²⁰ Vgl. dazu das Folgedokument zum Grünbuch über die kommerzielle Kommunikation im Binnenmarkt, CAB 15/0012/98 - DE, sowie *commercial communications: Commission agrees measures to ensure single market and protect public interests* vom 4. März 1998.

²¹ Beginnend mit dem LG Traunstein vom 14.10.1997, NJW-CoR 1997, 494; siehe auch LG Berlin, NJW-CoR 1998, 431; AG Brakel, NJW-CoR 1998, 431; vgl. die weiteren Hinweise bei Lehmann, a.a.O. Fn. 1, S. 171; Glöckner, J., „Cold Calling“ und europäische Richtlinie zum Fernabsatz, GRUR Int. 2000, 29 ff.

Strittig ist dabei, ob daraus für den einzelnen Verbraucher ein eigener Unterlassungsanspruch resultiert, vgl. ablehnend AG Kiel, NJW-CoR 2000, 49; bejahend Hoeren/Oberscheidt, VuR 1999, 371, 381; Ernst, VuR 1999, 397, 402 jeweils mit weiteren Nachweisen.

²² Vgl. dazu grundlegend BGH, GRUR 1973, 557 - Briefwerbung.

²³ Erfahrungsgemäß reichen Selbstkontrollmechanismen gerade für völlig neue Werbeformen nicht aus, so aber Leupold,

A., Die massenweise Versendung von Werbe-e-mails: Innovatives Direktmarketing oder unzumutbare Belästigung, WRP 1998, 270 ff.; siehe auch Funk, A., CR 1998, 411 ff.

²⁴ Einzelheiten vgl. dazu bei Lehmann, in FS Hubmann 1985, S. 255 ff.; Freund, S., Der persönlichkeitsrechtliche Schutz des Werbeadressaten, BB 1986, 409 ff.; Ehlers, W., WRP 1983, 187 ff.

„wenn die Partei, für die sie bestimmt ist, sie abrufen kann“. Nunmehr erscheint dieses Verfahren als netztauglich und auch der Anbieter muss nicht Gefahr laufen, dass ihm entgegengehalten wird, seine Bestätigung sei dem Verbraucher nicht zugegangen. Ein Abweichen von dem traditionellen, zweigliedrigen Vertragsabschlussschema, das z.B. sich auch für das Teleshopping bewährt hat, erscheint nicht als zwingend geboten²⁵.

Aus Verbraucherschutzerwägungen gewährt außerdem die Fernabsatzrichtlinie regelmäßig eine Widerrufsfrist von sieben Werktagen - und nach deutschem Fernabsatzgesetz von zwei Wochen -, entsprechend dem bereits in der EU geltenden Haustürwiderrufsrecht²⁶. In der Electronic Commerce-Richtlinie selbst werden in Art. 11 Abs. 2 dem Verbraucher außerdem umfangreiche Korrekturmöglichkeiten eröffnet. Gemäß Art. 10 Abs. 3 müssen die Vertragsbestimmungen und die Allgemeinen Geschäftsbedingungen dem Nutzer „so zur Verfügung gestellt werden, dass er sie speichern und reproduzieren kann“. Außerdem gilt selbstverständlich auch weiterhin § 12 AGB-Gesetz, so dass auch bei einer wirksamen Vereinbarung der Geltung ausländischen Rechts die nationale AGB-Kontrolle nicht ausgeschlossen ist. Die Voraussetzungen dieser Vorschrift werden gerade beim verbrauchergerichteten Electronic Commerce regelmäßig erfüllt sein. Dabei handelt es sich auch um ein europarechtliches Prinzip, denn diese Kontrollvorschrift resultiert aus Art. 6 Abs. 2 der Richtlinie 93/13/EWG vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen. Im Ergebnis wird daher häufig ausländisches Recht durch den „Kontrollfilter“ der nationalen, europäischen AGB-Kontrolle „gereinigt“. Viele Allgemeine Geschäftsbedingungen des

ausländischen Rechts vermögen nämlich erfahrungsgemäß dieser Kontrolle nicht standzuhalten und können daher im konkreten Einzelfall keine Wirkung zu Lasten des europäischen Verbrauchers in der EU entfalten; dies gilt insbesondere für schweizerische und amerikanische Anbieter.

4. Verantwortlichkeit im Netz

Ein weiteres Kernstück dieser Richtlinie sind die Haftungsregelungen der Art. 12-15, welche sowohl strafrechtliche²⁷ als auch zivilrechtliche Relevanz²⁸ beanspruchen; für den Verbraucherschutz können sie freilich nur reflexartige Wirkung entfalten. Ziel dieser Vorschriften ist es insbesondere, die net-service-provider, soweit sie nur als technische Gehilfen den Internet-Verkehr ermöglichen und unterstützen, möglichst weitgehend haftungsfrei zu stellen. Als reine Telekommunikatoren sollen sie nicht verpflichtet werden, sich mit den übermittelten Inhalten näher zu beschäftigen. Insoweit gleicht dieser Ansatz dem deutschen Telekommunikationsgesetz²⁹ und dem Mediendienstestaatsvertrag³⁰. Demgemäß statuiert Art. 15 der Richtlinie, dass den Diensteanbietern keine „allgemeine Verpflichtung“ auferlegt werden darf, „die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen Ausschau zu halten, die auf eine rechts-

²⁷ Zur strafrechtlichen Verantwortlichkeit vgl. Sieber, ZUM 1999, 196 ff.; ders., NJW 1999, 2065 ff.; siehe auch Flechsig/Gabel, CR 1998, 351 ff.

²⁸ Allgemein zur zivilrechtlichen Haftung im Netz vgl. Horen, Th., in Lehmann, a.a.O. Fn. 1, S. 45 ff.; Spindler, G., Die Haftung von Online-Diensteanbietern im Konzern, CR 1998, 745 ff.; ders., ZUM 1996, 533 ff.; Bettinger/Freytag, Privatrechtliche Verantwortlichkeit für links, CR 1998, 545 ff.; s. auch Freytag, S., Urheberrechtliche Haftung im Netz, ZUM 1999, 185 ff.; ders., Haftung im Netz, 1999, passim.

²⁹ Vom 25. Juli 1996, BGBl. I S. 1120, vgl. dazu den Beck'schen Kommentar zum Telekommunikationsgesetz, Büchner ed. al. (Hrsg.), 1997, S. 533 ff.

³⁰ Vgl. dazu ausführlich Freytag, S., a.a.O., Fn. 28.

²⁵ Vgl. auch Taupitz/Kritter, Electronic Commerce – Probleme bei Rechtsgeschäften im Internet, JuS 1999, 839 ff.

²⁶ Vgl. zur Anwendung des Haustürwiderrufsgesetzes im Internet Ruoff, A., NJW-CoR 2000, 38 ff.



widrige Tätigkeit hinweisen“³¹. Gleichmaßen haften reine Durchleitungsdienste, also z. B. Router oder Kommunikationsrelaisstationen gemäß Art. 12 Abs. 2 genauso wenig wie reine Zugangsvermittler zum Internet (access provider, connectivity provider). Art. 12 Abs. 2 korrespondiert dabei mit Art. 5 Abs. 1 des Richtlinienvorschlags zum Urheberrecht in der Informationsgesellschaft³², der bestimmte, primär technische Vervielfältigungshandlungen ausdrücklich nicht als „Vervielfältigung“ i.S.d. Urheberrechts definiert. Ähnlich sieht Art. 13 vor, dass automatische kurzzeitige Zwischenspeicherungen, etwa durch einen proxy-Server (vgl. dazu auch § 5 Abs. 3 Satz 2 TDG),

³¹ Warum ursprünglich davon die caching-services nicht profitieren sollten, blieb auch nach Lektüre der Begründung unklar; aber Art. 15 Abs. 1 spricht nun von Art. 12 bis 14.

³² S. oben Fn. 6, „vorübergehende Vervielfältigungshandlungen, wie vergängliche und begleitende Vervielfältigungen, die einen wesentlichen und integralen Teil eines technischen Verfahrens darstellen, einschließlich solcher, die ein effektives Funktionieren von Übertragungssystemen erleichtern, und deren alleiniger Zweck es ist, eine Nutzung eines Werks oder sonstigen Schutzgegenstands zu ermöglichen und die keine eigenständige wirtschaftliche Bedeutung haben, werden von dem in Artikel 2 bezeichneten Recht ausgenommen.“

grundsätzlich nicht zu einer zivilrechtlichen Haftung führen. Ausgenommen von dieser Privilegierung sind nur Unterlassungsansprüche³³, etwa analog § 1004 BGB oder gemäß § 97 UrhG, die verschuldensunabhängig sind.

Ähnlich kompliziert wie § 5 Abs. 2 TDG³⁴ und die noch detaillierter, aber inhaltlich auch besser ausgearbeiteten amerikanischen Haftungsregeln im „Digital Millenium Copyright Act“³⁵ ist Art. 14, der die Haftung für die Bereithaltung fremder Inhalte in einem Server (sog. hosting, etwa durch einen bulletin board service, bbs) regelt; hier soll eine Haftung nur dann ausgeschlossen sein, wenn dieser Service Provider „keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information“ hat, und er sich, wenn es um Schadensersatzansprüche geht, „auch keiner Tatsachen oder Umstände bewusst“ ist, „aus denen die rechts-

³³ Der deutsche Text sprach ursprünglich missverständlicherweise von „Unterlassungsklage“; gemeint ist „injunctive relief“.

³⁴ Vgl. dazu Lehmann, M., Unvereinbarkeit des § 5 TDG mit Völkerrecht und Europarecht, CR 1998, 232 ff.

³⁵ H.R. 2281, sec. 202, § 512 ff.; vgl. dazu auch Bettinger/Freytag, CR 1998, 552 ff.

widrige Tätigkeit oder Information offensichtlich wird³⁶. Außerdem muss er nachdem er erfahren hat oder ihm bewusst geworden ist, dass die Tätigkeit illegal ist, unverzüglich tätig werden, „um die Information zu entfernen oder den Zugang zu ihr zu sperren“. Dies kann z.B. eine adäquate Reaktion auf eine Abmahnung sein, dass auf seinem Server urheberrechtsverletzendes Material, etwa plagiierte Musikwerke, vorgehalten wird.

Diese weitgehende Haftungsfreistellung ist insoweit verwunderlich, als rechtshistorisch betrachtet bereits schon seit Savigny für neue und insbesondere technisch im wesentlichen vom Betreiber zu beherrschende Gefahren (Eisenbahn, Kfz-Halter, Halter eines Luftfahrzeuges, Betreiber einer Anlage zur Kernspaltung) grundsätzlich eine Gefährdungshaftung, also eine Haftung ohne Verschulden vom deutschen Gesetzgeber eingeführt worden ist³⁷. Auch aus den Erkenntnissen der ökonomischen Analyse des Rechts kann abgeleitet werden, dass Haftungssysteme³⁸ richtige Verhaltensanreize, nicht aber „incentives to moral hazard“ geben sollten. Weiterhin bedürfen die jungen Unternehmen im Netz keiner „Wirtschaftsförderung durch Haftungsprivilegierungen“, sondern allenfalls Rechtssicherheit³⁹; alles andere sollte man getrost dem Markt überlassen. Es ist daher kritisch anzumerken, dass es nur wenig sinnvoll erscheint, dass ein Service Provider eines bbs-Systems im Netz weniger streng haften soll, als jeder Verleger z. B. gemäß § 13 Abs. 5 Nr. 1 Satz 2 UWG; dieser haftet aber z.B. für alle Wettbewerbs- und Urheberrechtsverstöße, die er positiv kannte ohne jede weitere Einschränkung, wie etwa in § 5 Abs. 2 TDG („zumutbar“) oder in Art. 14 („offensichtliche Illegalität“). Der BGH hat

zwar für das Wettbewerbs-⁴⁰ und Urheberrecht⁴¹ eine Haftung Dritter nur dann eingreifen lassen, wenn es sich um grobe, unschwer zu erkennende Verstöße handelt; aber er hat dabei auch immer eine gewisse eigene Prüfungspflicht des potentiellen Störers ausdrücklich anerkannt⁴². Warum diese Prinzipien plötzlich nicht mehr gelten sollen, wenn die gleichen Störerhandlungen in das Netz verlagert werden, ist rechtsdogmatisch nicht nachvollziehbar.

5. Europarechtliche und völkerrechtliche Verpflichtungen

Darüber hinaus müssen derartige neue Haftungsregeln dem Europäischen Recht und den völkerrechtlichen Verpflichtungen entsprechen, welche auf diesem Gebiet, z.B. für das Urheberrecht, Patentrecht und Markenrecht, nicht aber auch das Wettbewerbsrecht, existieren und dies sind die WTO/TRIPS⁴³. Weil die EU neben den Mitgliedstaaten den WTO selbstständig unterzeichnet hat, gehören die TRIPS zum *acquis communautaire*⁴⁴ genauso wie sie für alle Unterzeichnerstaaten völkerrechtliche Verpflichtungen generiert haben.

Gemäß Art. 41 TRIPS müssen die Mitgliedstaaten dieses Vertragswerkes sicherstel-

⁴⁰ BGH, GRUR 1997, 313 - Architektenwettbewerb.

⁴¹ BGH, GRUR 1999, 418 ff. - Möbelklassiker; vgl. dazu Haedicke, M., Lex informatica oder allgemeines Deliktsrecht?, CR 1999, 309 ff.

⁴² Vgl. nur den Leitsatz dieser BGH-Entscheidung, a.a.O. Fn. 38: „Die urheberrechtliche Störerhaftung von Personen, die nicht selbst die rechtswidrige Nutzungshandlungen vorgenommen haben, setzt - wie die wettbewerbsrechtliche Störerhaftung Dritter - die Verletzung von Prüfungspflichten voraus“.

⁴³ Vgl. allgemein Beier/Schricker (eds.), From GATT to TRIPS. The Agreement on Trade Related Aspects of Intellectual Property Rights, München 1996, passim; speziell zum Urheberrecht s. Katzenberger, P., TRIPS und das Urheberrecht, GRUR Int. 1995, 447 ff.; zum § 5 TDG vgl. Lehmann, CR 1998, 234.

⁴⁴ Drexl, J., GRUR Int. 1994, 777 ff.

³⁶ Wobei eine aktive Untersuchungspflicht wiederum wegen Art. 15 Abs. 1 nicht auferlegt werden darf.

³⁷ Vgl. statt vieler Kötz, H., Deliktsrecht, 8. Aufl. 1998, S. 134 ff.

³⁸ Vgl. Lehmann, M., BGB und HGB - eine juristische und ökonomische Analyse, 1983, S. 91 ff.

³⁹ Lehmann, CR 1998, 234.

len, „dass die in diesem Teil⁴⁵ aufgeführten Durchsetzungsverfahren in ihrem Recht vorgegeben werden, um ein wirksames Vorgehen gegen jede Verletzung von unter dieses Übereinkommen fallenden Rechten des geistigen Eigentums... zu ermöglichen“. Es erscheint daher höchst bedenklich, ob die Art. 12 ff. der Richtlinie ganz generell wegen ihrer weitgehenden Haftungsfreistellung dieser grundsätzlichen Verpflichtung noch zu entsprechen vermögen. Speziell schreibt weiter Art. 45 TRIPS für den Schadensersatz vor, „dass der Verletzer dem Rechtsinhaber zum Ausgleich des von diesem wegen einer Verletzung seines Rechts des geistigen Eigentums durch einen Verletzer, der wusste oder *vernünftigerweise hätte wissen müssen*⁴⁶, dass er eine Verletzungshandlung vornahm, erlittenen Schadens angemessen Schadensersatz zu leisten hat“. Diese konkrete Verpflichtung lässt sich mit der in Art. 14 gewählten Formulierung „keiner Tatsachen oder Umstände bewusst, aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wird“ selbst unter Heranziehung aller noch so weitgehenden juristischen Auslegungskunstgriffe nicht vereinbaren, denn Art. 15 Abs. 1 will den hosting-services keine aktive Überwachungs- und Untersuchungspflicht auferlegen. Gerade diese Verpflichtung enthält aber Art. 45 TRIPS, „vernünftigerweise hätte wissen müssen“, vor allem wenn man dies an dem bekannten Fahrlässigkeitsmaßstab des § 122 Abs. 2 BGB misst, der kennen müssen als „infolge von Fahrlässigkeit nicht kannte“ legal definiert. Der Art. 14 der Richtlinie verstößt daher gegen bestehendes Europäisches Recht und die völkerrechtlichen Verpflichtungen der EU und der einzelnen Mitgliedstaaten aus Art. 45 Abs. 1 WTO/TRIPS. Auch eine völkerrechtskonforme, einschränkende Auslegung

und Reduktion, wie bei § 5 TDG⁴⁷, ist hier nicht mehr möglich.

6. Zusammenfassung

So verdienstvoll es ist, dass die Kommission besonders rasch⁴⁸ einen Richtlinienentwurf und nunmehr auch eine definitive Richtlinie zur Regulierung des Electronic Commerce im europäischen Binnenmarkt vorgelegt und verabschiedet hat, so umfangreich ist der dadurch im Detail bedingte wirtschaftsrechtliche Diskussionsbedarf. Unausgewogen erscheint das Herkunftslandprinzip, inkonsequent die Ermöglichung unerbetener Werbung über das Netz, europarechts- und völkerrechtswidrig sind wichtige Teile der Haftungsprivilegierung, insbesondere was den Schutz des gewerblichen und geistigen Eigentums angeht. Dieser Richtlinie kann daher im Zuge der Transformation in die jeweiligen nationalen Rechtsordnungen eine umfangreiche europäische Diskussion vorhergesagt werden. Aus der Sicht des Europäischen Verbraucherschutzes sind allerdings keine allzu großen Schutzdefizite anzumerken und viele seriöse Anbieter im Netz erfüllen schon heute beim Electronic Commerce die kommenden Schutzvorschriften in Europa. Gleichsam als Notbremse ist außerdem in Art. 3 Abs. 4 lit. a der Electronic Commerce-Richtlinie vorgesehen, dass zum „Schutz der Verbraucher, einschließlich des Schutzes von Anlegern“ nationale Ausnahmen vom sog. Binnenmarkt- bzw. Herkunftslandprinzip gemacht werden können, wie dies bereits schon durch die Rechtsprechung des Europäischen Gerichtshofs zu Art. 30 EV (früher Art. 36 EWGV) vorgezeichnet worden ist; im Anhang wird außerdem als Ausnahme vom

⁴⁵ Gemeint ist Teil III der TRIPS, der den Sanktionen gewidmet ist, vgl. dazu Dreier, Th., TRIPS und die Durchsetzung von Rechten des geistigen Eigentums, GRUR Int. 1996, 205 ff.

⁴⁶ Hervorhebung durch den Verf.

⁴⁷ Vgl. Lehmann, CR 1998, 234 f.

⁴⁸ Erste negative Erfahrungen, vgl. SZ vom 29.12.1998, S. 18: „Kaufen per Internet beschert nichts als Frust. Immer mehr Amerikaner wenden sich vom `Cybershopping` ab“, scheinen inzwischen der Vergangenheit anzugehören.

Binnenmarktprinzip des Art. 3 Abs. 1 und 2 der Bereich der „vertraglichen Schuldverhältnisse in bezug auf Verbraucherverträge“ genannt, ohne dass dadurch wirklich Rechtsklarheit geschaffen werden würde.

* *Der Beitrag erschien zunächst in: EuZW, Heft 17/2000, S. 517 – 521. Der Nachdruck erfolge mit Einwilligung des Autors.*

Prof. Dr. Michael Lehmann, Studium der Rechtswissenschaften an der Universität München, diverse Gastprofessuren u.a. an den Universitäten Chicago, Luxemburg, Ferrara, Palermo sowie an der Harvard Law School und der Santa Clara Law School. 1996 Ernennung zum Professor für Bürgerliches Recht, Handels- und Wirtschaftsrecht sowie Urheberrecht und Gewerblicher Rechtsschutz, Universität München. Zudem ist er Professor am Max-Planck-Institut für Ausländisches und Internationales Patent-, Urheber- und Wettbewerbsrecht in München.

An die Ausführungen *Lehmanns* schloss *Pfitzmann* die Frage an, ob es rechtlich zulässig sei, die Nutzung von in Europa erworbenen Content auf die Mitgliedstaaten zu beschränken. *Lehmann* sah keine Verletzung europäischen Rechts, da der Grundsatz des Binnenmarktes und der urheberrechtliche Erschöpfungsgrundsatz nur innerhalb des Binnenmarkts gälten.

Pfitzmann wollte weiterhin wissen, ob man sich technisch gegen solche Beschränkungen, z.B. durch „reverse engineering“ wehren könne. Dies verneinte *Lehmann* mit dem Hinweis, dass trotz globaler Märkte territoriale Schutzrechte bestünden. Alle Patente, alle Marken und alle Urheberrechte endeten unter Berücksichtigung der Informationspflichten der Hersteller gegenüber den Kunden an den jeweiligen Grenzen, es gebe noch keine globalen

Nutzungsbedingungen. *Kristian Köhntopp* merkte kritisch an, dass somit zwar eine Globalisierung für die Hersteller und Firmen bestünde, nicht jedoch für die Kunden. Darauf entgegnete *Lehmann*, dass die Entwicklung rechtlicher Strukturen in globalen Märkten ein langsamer, aber kontinuierlicher Prozess sei.

Erd merkte hinsichtlich des Beispiels der „Regional Codes“ bei DVDs an, dass die künstliche Segmentierung der Märkte rechtlich zwar umgesetzt werden könnte, die Rechtsdurchsetzung jedoch aufgrund der technisch leicht machbaren Umgehung durch Umrüstung oder Kauf von „Regional-Code-Free“ DVD-Playern kaum möglich sei. Die rechtlich zulässige Segmentierung von Märkten werde also faktisch von neuen Märkten aufgehoben. Damit stelle sich die Frage nach der Effektivität des internationalen Urheberrechts. *Lehmann* verwies in seiner Antwort darauf, dass eine solche Entwicklung der Wettbewerb richten müsse und auf diese Weise die Frage der künstlichen Segmentierung entschieden werde. Das Recht könne nur faire Spielregeln für den Markt anbieten. Ein Wechselspiel zwischen Rechtsregeln und Wirtschaftsregeln werde es immer geben.

Marit Köhntopp fragte mit Blick auf technische Sicherungsmechanismen wie „watermarking“, ob die Forschung in Kryptographie und Steganographie durch die Urhebersrichtlinie Einschränkungen zu befürchten habe. *Lehmann* äußerte die Auffassung, dass das Gegenteil der Fall sei, der Wettbewerb der Forschung würde erst richtig angefacht. Es sei nicht so, dass das Urheberrecht immer nur den Produzent, den Copyright-Holder im allgemeinen, berücksichtige, sondern es werde auch dafür gesorgt, dass dem Verbraucher Mindestnutzungsrechte zustünden (z. B. § 69d UrhG), die ihm auch nicht durch vertragliche Regelungen entzogen werden könnten.

Privacy als Schranke des Urheberschutzes

Johann Bizer

1 Einleitung

1.1 Die Bedeutung des Urheberschutzes für den E-Commerce

Im Ranking der typischen Online-Aktivitäten der Internetnutzungen nimmt in Europa das Herunterladen freiverfügbarer Software mit 47 % der Nutzungen eine Spitzenposition ein.¹ Der Aufstellung ist zwar nicht zu entnehmen, in welchem Umfang die Nutzung mit Urheberrechtsverletzungen verbunden ist. Einen gewissen Anhaltspunkt gibt jedoch die niedrige Zahl der Nutzer, die über das Internet Software schließlich auch gekauft haben (9%). Offensichtlich ist schließlich, dass der kostenlose Abruf von Software attraktiver ist als ihre Bezahlung. Für Deutschland liegen die Werte jeweils knapp über dem europäischen Durchschnitt: Während 51 % der Internetnutzer in Deutschland das Herunterladen freiverfügbarer Software favorisieren, haben 11 % nach eigenen Angaben auch Software gekauft.²

Einen weiteren Indikator für die Bedeutung der Verletzung von Urheberrechten im Internet bildet die polizeiliche Kriminalitätsstatistik (PKS). Sie verzeichnet von 1998 auf 1999 bei den privaten Anwendungen einen Zuwachs von 168 % und im gewerblichen Bereich von 333 %. Der starke Anstieg wird vom BKA mit „komplexen Ermittlungsvorgängen mit zahlreichen Einzelfällen“ erläutert, gleichwohl geht das Bundeskriminalamt insgesamt noch

von einem erheblichen Dunkelfeld insbesondere bei Raubkopien aus.³

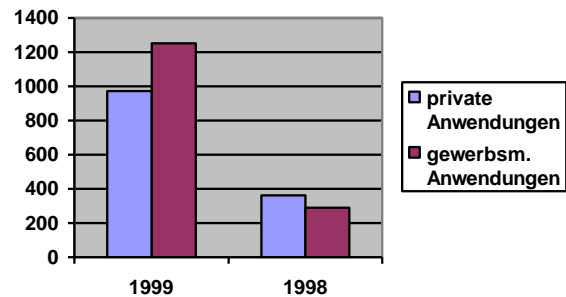


Tabelle 1: PKS 1999: Softwarepiraterie

1.2 Bedeutung des Datenschutzes für den E-Commerce

Von Bedeutung für die Entwicklung des E-Commerce ist aber nicht nur der Urheberrechtsschutz, sondern auch der Schutz personenbezogener Daten im Internet.

Nach einer bereits 1998 durchgeführten repräsentativen Umfrage fühlten sich in Deutschland 74 % durch Datenmissbrauch sehr (29 %) oder mittel (45 %) betroffen.⁴ Diese Einstellung ist keine nationale Besonderheit. Eine jüngere Umfrage unter US-Bürgern vom August 2000 ergibt, dass 84% darüber besorgt sind, wenn Geschäftsleute oder Unbekannte Informationen über sie oder ihre Familie bekommen.⁵

¹ Europäische Kommission, Eurobarometer Nr. 53, Oktober 2000, S. 85. Umfragen erfolgten zwischen April-Mai 2000. Gefragt wurden Internet Nutzer nach ihren Aktivitäten innerhalb der letzten drei Monate von zu Hause aus. Die Untersuchung ist verfügbar unter

<<http://europa.eu.int/comm/dg20/epo/>>.

² Annex B.79 (Tabelle 7.2).

³ Bundeskriminalamt, Polizeiliche Kriminalstatistik 1999, Wiesbaden 2000, Kap. 3.21 Computerkriminalität <http://www.bka.de/pks/pks1999/p_3_21-3_21.html>.

⁴ Opaschowski, Quo vadis, Datenschutz? DuD 1998, 57.

⁵ 59 % very bzw. 25 % somewhat concerned. The Pew Internet & American Life Project, Trust and privacy online. Why Americans want to rewrite the rules, August 2000, pg 25 Question 3.

Umfragen ergeben einen direkten Zusammenhang zwischen Datenschutz und dem Kaufverhalten der Nutzer im Internet. Nach einer länderübergreifenden Untersuchung aus dem Jahr 1999 im Auftrag der IBM haben 57 % der Nutzer in den USA, 41 % in Großbritannien und 56 % in Deutschland angegeben, dass sie wegen fehlender Sicherheit über die Verwendung ihrer Daten auf die Nutzung oder den Kauf eines Online-Angebots verzichtet haben.⁶ Dass dieses Ergebnis keine Eintagsfliege ist, beweist eine jüngere Umfrage der Mannheimer Forschungsgruppe Wahlen im Auftrag des Bundesverbandes der Banken vom Oktober 2000, wonach 62 % der Internetnutzer in Deutschland erklärten, sie hätten im Internet noch nicht online bestellt oder gekauft, weil ihrer Meinung nach der Datenschutz unzureichend gewährleistet sei. Neuere Zahlen bestätigen auch für die USA diesen Trend: So wollen einer Umfrage aus dem Jahr 2000 zu Folge 86 % der Internetnutzer, in die Nutzung ihrer Daten vorher einwilligen („option“). Immerhin 54 % halten die Bildung personenbezogener Nutzerprofile („web-tracking“) für schädlich.⁷

Dass der Datenschutz ein wesentlicher Akzeptanzfaktor für die Entwicklung des E-Commerce ist, kann demnach zu den gesicherten Aussagen zählen.

2 Zielkonflikt zwischen Urheberschutz und Datenschutz

Obwohl Urheberschutz und Datenschutz als geistige und persönliche Selbstbestimmungsrechte über Wurzeln im allgemeinen Persönlichkeitsrechts verfügen, stehen sie in einem gewissen Zielkonflikt zueinander. Das Recht, seine geistige Leistung wirtschaftlich zu ver-

werten, ordnet die Rechtsprechung des BVerfG dem Schutzbereich des Eigentum nach Art. 14 Abs. 1 GG zu,⁸ dessen wirtschaftliche Verwertungsmöglichkeiten jedoch in einem „inneren Zusammenhang“ mit dem Schutz der geistig-persönlichen Rechte des Urhebers aus dem allgemeinen Persönlichkeitsrecht stehen.⁹ Als Bestimmungsbefugnis über die Verwendung und Verwertung des geistigen Eigentums ergibt sich die Parallele zum informationellen Selbstbestimmungsrecht, das abgeleitet und konkretisiert aus dem allgemeinen Persönlichkeitsrecht die Befugnis des Einzelnen schützt, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“.¹⁰

Der Zielkonflikt zwischen Urheberschutz und Datenschutz ergibt sich praktisch aus der Entwicklung und Anwendung von informationstechnischen Programmen, mit deren Hilfe zum Schutz wirtschaftlicher Verwertungsinteressen der Nutzer eines Werkes identifiziert und seine Verwertung nachvollzogen wird. Derartige Programme sind unter den Schlagworten des Online-Profiling, des Data Warehousing oder schlichter des Setzen von Cookies bereits seit längerem im Blickwinkel der datenschutzrechtlichen Diskussion.¹¹ Im Kern kollidiert eine Identifizierung des Nutzers mit dessen Interesse, anonym Online-Dienste nutzen zu können.

Der Konflikt lässt sich an Hand der Erwägungsgründe des Gemeinsamen Standpunktes 48/2000 zur Richtlinie „zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte der Informationsge-

⁸ BVerfGE 79, 29 (38 ff.).

⁹ BVerfGE 31, 229, 238, 239.

¹⁰ BVerfGE 65, 1, 42.

¹¹ Bspw. Bizer, Web Cookies – datenschutzrechtlich DuD 1998, 277 ff.; Bizer, TK-Datenschutz im Data Warehouse, DuD 1998, 570 ff.; Wichert, Web-Cookies – Mythos und Wirklichkeit DuD 1998, 273 ff.; Schaar, Cookies – Unterrichtung und Einwilligung, DuD 2000, 275 ff.; Hillenbrand-Beck/-Greb, Datengewinnung im Internet, DuD 7/2001; Köhntopp/Köhntopp CR 2000, 248 ff.

⁶ IBM Multi-National Consumer Privacy Survey, October 1999, pg. 23, 27.

⁷ Pew Internet & American Life Project, August 2000.

sellschaft“ vom 28. September 2000¹² (hier kurz EG-Urheberrichtlinie) nachvollziehen. Erwägungsgrund 54 beschreibt die Notwendigkeit zur Identifizierung von Werken und Urhebern, um die Wahrnehmung der mit dem Werk verbundenen Rechte zu erleichtern. Erwägungsgrund 56 weist darauf hin, dass die Informationssysteme zur Wahrnehmung der Rechte in der Lage sind,

„gleichzeitig personenbezogene Daten über die individuelle Nutzung von Schutzgegenständen zu verarbeiten und Online-Aktivitäten nachzuvollziehen“.

Allerdings regelt die Urheberrichtlinie diese technischen Informationssysteme nicht, denn sie ist auf die Harmonisierung des Rechts innerhalb der EU gerichtet. Sie setzt die Existenz technischer Informationssysteme zum Schutz der Urheberrechte daher lediglich voraus, indem sie bspw. in Art. 6 Abs. 1 einen „angemessenen Rechtsschutz gegen die Umgehung wirksamer technischer Maßnahmen durch eine Person“ vorsieht.

Auf den ersten Blick scheint der Zielkonflikt zwischen Urheberschutz und Datenschutz nur in allgemeinen Formelkompromissen ausgedrückt werden zu können. So heißt es in der Mitteilung der Kommission KOM(2000)890 „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität“ vom 26. Januar 2001 in einer typischen EU-Formulierung in schönstem EU-Deutsch.

„Es bedarf wirksamer, global oder zumindest auf EU-Ebene angeglicher Instrumente sowohl des materiellen Strafrechts als auch des Verfahrensrechts, die die Opfer der Computerkriminalität schützen und es ermöglichen, die Täter zur Verantwortung zu ziehen. Gleichzeitig darf jedoch nicht vergessen werden, dass das Recht auf

Kommunikation, Privatsphäre und Datenschutz sowie auf Informationszugang und -verbreitung in modernen Demokratien grundrechtlich verankert ist. Aus diesem Grund ist es wünschenswert, wirksame Präventivmaßnahmen anwenden zu können, um die Notwendigkeit von Zwangsmaßnahmen zu begrenzen. Etwaige notwendige Legislativmaßnahmen zur Bekämpfung der Computerkriminalität müssen somit beiden Aspekten in geeigneter Weise gerecht werden.“ (S. 15).

Aufgelöst wird der Konflikt zwischen den technischen Informationssystemen zum Schutz der Urheberrechte und dem Schutz personenbezogener Nutzerdaten im Erwägungstext der Urheberrechtsrichtlinie *zu Gunsten des Datenschutzes*. Nach Erwägungsgrund 56 müssen die technischen Funktionen die nach der EG-Datenschutzrichtlinie 95/46/EG geltenden Anforderungen erfüllen. So heißt es in Erwägungsgrund 56:

„(56) Die technischen Funktionen dieser Vorrichtungen sollten dem Schutz der Privatsphäre gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr¹³ gerecht werden.

Und noch deutlicher ergibt sich die Rangfolge aus Art. 9 der Urheberrichtlinie, wonach sie Rechtsvorschriften

insbesondere in folgenden Bereichen unberührt lässt: (...) „Sicherheit, Vertraulichkeit, Datenschutz und den Schutz der Privatsphäre“.

Im Ergebnis bedeutet dies, dass die zum Schutz der Urheberrechte durchgeführte Erhebung und Verarbeitung personenbezogener

¹² Abl.EG C 344 vom 1.12.2000, S. 1.

¹³ Abl.EG L 281 vom 23.11.1995, S. 31.

Daten die wesentlichen Prinzipien des EG-Datenschutzrechts beachten muss. Hierzu gehören insbesondere die Grundsätze

- der Zweckbindung (Art. 6 Abs. 1 b EG-Datenschutzrichtlinie),
- der Erforderlichkeit (Art. 6 Abs. 1 c EG-Datenschutzrichtlinie) und
- der Transparenz der Datenverarbeitung gegenüber dem Betroffenen durch Information und Auskunft (Art. 10 ff. EG-Datenschutzrichtlinie).

Die näheren Umstände des Schutzes der Urheberrechte durch Identifizierung des Nutzers sollen im folgenden in zwei Szenarien verdeutlicht und bewertet werden, nämlich

- dem Fall der von einem Nutzer „gekauften“ Software (Szenario A) und
- dem Fall des Down- bzw. Upload von Software (Szenario B).

Beide Szenarien beschreiben typische Situationen einer Urheberrechtsverletzung: Szenario A im Rahmen einer Vertragsbeziehung zwischen dem Urheber und dem Nutzer und Szenario B im Rahmen der Inanspruchnahme eines Dienstansbieters, über dessen technische Einrichtungen Software aufgespielt (upload) oder heruntergeladen (download) werden kann.

3 Szenario A: „Gekaufte Software“

Dem Szenario liegen Fallgestaltungen zu Grunde, bei denen zwischen dem Nutzer und dem Urheber eine Vertragsbeziehung besteht.

3.1 „Nutzung gegen Geld“

Im Regelfall erwirbt der Nutzer eine Software käuflich. Die Gestaltung der rechtlichen Beziehung wird durch Leistung „Übertragung der Nutzungsrechte“ und die Gegenleistung

„Kaufpreis“ bestimmt. Die datenschutzrechtliche Gestaltung derartiger Fälle wirft wenig Probleme auf: Im Regelfall ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG nur zulässig, soweit sie zur Abwicklung des Vertragsverhältnisses erforderlich ist. Hierbei sind die Nutzungszwecke bereits „bei der Erhebung“ der personenbezogenen Daten festzulegen, § 28 Abs. 1 Satz 2 BDSG. Die Verarbeitung der erhobenen Daten wird durch den Zweck des Vertragsverhältnis bestimmt und beschränkt, so dass eine Verarbeitung und Nutzung der im Rahmen des Vertragsschlusses erhobenen Daten des Nutzers nicht über den konsentierten Zweck der Übertragung der Nutzungsrechte hinausgehen darf.

3.2 „Nutzung gegen Daten“

Problematisch ist für den Nutzer die Fallgestaltung, bei der die Einräumung von Nutzungsrechten nur gegen die Überlassung mehr oder weniger umfassender personenbezogener Daten erfolgt. Derartige Nutzerdaten werden vom Urheber häufig erhoben, um sie zur Vermarktung weiterer eigener Produkte nutzen können oder um sie durch Überlassung an Dritte wirtschaftlich verwerten zu können.

Das Erheben personenbezogener Daten „Nutzung gegen Daten“ erfolgt zumeist über eine Registrierung einer den Nutzer zur Verfügung gestellten Software.¹⁴ Der Nutzer ist nach den Lizenzbestimmungen zur Nutzung nur berechtigt, wenn er über einen „Schlüssel“ bzw. eine „Kennung“ verfügt, die dem Nutzer erst nach Übersendung einer Registrierung unter Angaben mehr oder weniger umfangreicher Daten überlassen wird. Die Qualität der Nutzerdaten gewährleistet der Hersteller, indem die Registrierung zeitlich begrenzt wird und in

¹⁴ Unerheblich ist, ob für Software sofort, später oder gar nicht einen Kaufpreis entrichtet werden muss.

regelmäßigen Abständen aktualisiert werden muss. Zur Registrierung wird der Nutzer durch die Schaltung „störender“ Blinkbilder oder durch das Versprechen, nach einer Registrierung weitere „attraktive“ Features oder Updates in Anspruch nehmen zu können.

Datenschutzrechtlich sind Datenerhebungen „Nutzung gegen Daten“ mindestens unter drei Aspekten zu problematisieren, nämlich

- die Erhebung überflüssiger Daten,
- die scheinbare Einwilligung sowie
- das heimliche Erheben und Verarbeiten von Nutzungsprofilen (Online Profiling).

3.2.1 Erhebung überflüssiger Daten

Problematisch ist der Umfang und die Art der mit einer Registrierung erhobenen Daten, soweit der zur Identifizierung des Nutzers erforderlichen Datensatz aus Name, Vorname und postalische Anschrift bereits bei der Erhebung überschritten wird. Rechtlich ergibt sich die normative Grenze der *Erforderlichkeit* der Datenerhebung aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Die Zweckbestimmung des Nutzungsverhältnisses kann allenfalls eine Erhebung des Datensatzes rechtfertigen, der zur Identifizierung des Nutzers erforderlich ist.

Diese Rechtslage gilt im Wesentlichen auch, wenn es sich um einen ausländischen Anbieter handelt. So findet das deutsche Da-

tenschutzrecht grundsätzlich Anwendung, wenn die erhebende Stelle eine Niederlassung in Deutschland hat oder die Daten im Inland von einer Stelle mit Sitz in einem Drittstaat erhoben werden, d. h. außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraum, § 1 Abs. 5 Satz 1 und 2 BDSG. Deutsches Datenschutzrecht kommt nur dann nicht zur Anwendung, wenn die für die Datenerhebung verantwortliche Stelle ihre Niederlassung in einem Mitgliedstaat der EU oder des EWR hat: In diesem Fall richtet sich die Datenerhebung aber nach dem nationalen Datenschutzrecht des Sitzlandes, das sich aber in Übereinstimmung mit der EG-Datenschutzrichtlinie befinden muss. Ebenso wie das deutsche Datenschutzrecht begrenzt aber auch das europäische Datenschutzrecht die Datenerhebung im Rahmen eines Vertragsverhältnisses auf den Grundsatz der Erforderlichkeit, Art. 7 Abs. 1 b, Art. 6 Abs. 1 b Satz 1, c) EG-Datenschutzrichtlinie 95/46/EG.

Tatsächlich werden im Rahmen der Registrierung von Software häufig Informationen erhoben, die mit dem Zweck der Registrierung in keinem Zusammenhang stehen und deren Erhebung daher rechtswidrig ist. Hierzu zählen bspw. Angaben zum Geschlecht, der Nationalität, zum Alter, die Bildung oder den Beruf des Nutzers.

Eine Übermittlung oder Nutzung bereits erhobener Daten des Nutzers zu Zwecken der Werbung, der Markt- oder Meinungsforschung ist nach Datenschutzrecht nur bei mit bestimmten Angaben listenmäßig zusammengefassten Daten zulässig. Es darf zusätzlich kein Grund zur Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Nutzung oder Übermittlung hat, § 28 Abs. 3 Satz 1 Nr. 3 BDSG. Ein derartiges überwiegendes schutzwürdiges Interesse ist bspw. anzunehmen, wenn die Übermittlung dazu dient, den betroffenen Nutzer via Telefax oder Voice-Mail-Systemen direkt zu anzuspre-



chen. Das überwiegende schutzwürdige Interesse des Nutzers ergibt sich aus Art. 12 Abs. 1 EG-Telekommunikationsdatenschutzrichtlinie 97/66/EG wonach die Verwendung derartiger Systeme „für Zwecke des Direktmarketings“ nur bei vorheriger Einwilligung des Teilnehmers gestattet ist. Die Revision dieser Richtlinie KOM(2000)385 vom 21. Juli 2000 schließt nun in Art. 14 Abs. 1 auch die elektronische Post mit ein. Dasselbe ergibt sich im übrigen aus der bundesdeutschen Rechtsprechung zur Telefonwerbung. Danach ist selbst das formularmäßig erteilte Einverständnis in eine AGB-Klausel, mit der sich ein Kontoinhaber „mit der persönlichen und telefonischen Beratung in Geldangelegenheiten durch die Bank einverstanden“ erklärt, rechtswidrig.¹⁵

Angaben über die Kommunikationsmöglichkeiten des Nutzers wie die Telefon- oder Faxnummer sind zur Identifizierung des Nutzers der Software nicht erforderlich. Eine andere Beurteilung kann sich nur ergeben, wenn die Angabe der Email-Adresse ausschließlich dazu dient, den Nutzer über die Bereitstellung späterer Updates zu informieren. Der Anbieter darf die elektronische Kommunikationsadresse allerdings nur zu diesem einen Zweck verwenden. Als datensparsamere Variante bietet sich an, den Nutzer direkt über die genutzte Software in regelmäßigen Abständen zu einer Online-Aktualisierung seiner Software aufzufordern.

3.2.2 Die scheinbare Einwilligung

Soweit Angaben zur Identifizierung des Nutzers nicht erforderlich sind, kann ihre Angabe nur freiwillig sein. Wohl auch aus diesem Grund differenzieren zahlreiche Softwareanbieter zwischen unbedingten und optionalen Angaben. Auf die Freiwilligkeit seiner Anga-

ben ist der Nutzer nach § 4 Abs. 3 Satz 2 BDSG hinzuweisen.

Freiwillig sind die Angaben allerdings nur, wenn die Nutzungsrechte an der Software auch ohne die Angabe der „optionalen“ Informationen eingeräumt werden. Ausdrücklich ist das Verbot, eine Datenerhebung als Gegenleistung für die Einräumung einer Nutzung in § 3 Abs. 3 Teledienstschutzgesetz (TDDSG) geregelt. Es ergibt sich auch aus § 4 Abs. 1 Satz 1 BDSG, wonach die Einwilligung des Betroffenen nur wirksam ist, wenn „sie auf dessen freier Entscheidung beruht“.

Ferner ist der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen, § 4 Abs. 1 Satz 2 BDSG. Der Softwareanbieter muss folglich dem Nutzer gegenüber transparent machen, zu welchen Zwecken er die optional erhobenen Daten verwenden will. Eine entsprechende Rechtsregel ergibt sich nun aus § 4 Abs. 3 Satz 1 BDSG, wonach die verantwortliche Stelle den Betroffenen über die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung (Nr. 2) und die Kategorien von Empfängern (näher Nr. 3) unterrichten muss. Nur soweit der Nutzer die Verwendungszwecke kennt, kann er in diese auch konkret einwilligen. Eine Verwendung der auf der Grundlage einer solchen Einwilligung erhobenen Daten zu anderen Nutzungszwecken ist unzulässig.

Ein exemplarisches Beispiel für die unzulässige Verknüpfung von Einwilligung und Verwendungszweck ist eine Formulierung in den Nutzungsbedingungen des – von mir im übrigen käuflich erworbenen – Programms Adobe Acrobat 4.0. Im Zuge der Registrierungsprozedur erscheint ein Fenster mit folgendem Inhalt:

„Sie sind damit einverstanden, dass Adobe auf Ihre Kundendaten zugreift, diese speichert und in Ländern mit einer Adobe Vertretung benutzt, einschließlich, aber ohne Beschränkung, den USA.“

¹⁵ BGH NJW 2000, 2677.

Da eine „Ja-Nein“-Option nicht angeboten wird, muss der Nutzer entweder auf eine Registrierung verzichten, auf deren Folgen er aber entgegen § 4 Abs. 1 Satz 2 Zweiter Halbsatz BDSG nicht hingewiesen wird, oder er muss einwilligen, was wiederum gegen das Prinzip der Freiwilligkeit nach § 4 Abs. 1 Satz 1 BDSG verstößt. Darüber hinaus enthält die Klausel weder eine Information über die vorgesehene Zweckbindung noch ist sie mangels Zweckbestimmung eine ausreichende Rechtsgrundlage in eine Datenübermittlung in die USA. Bemerkenswert ist, dass diese Klausel mangels ausreichender Information (notice) und Wahlmöglichkeit (choice) auch gegen die im Wege der Selbstregulierung anerkannten US-amerikanischen Datenschutzstandards der Network Advertising Initiative - NAI verstößt.¹⁶

3.2.3 Online Kontrolle

Neben der direkten Erhebung personenbezogener Daten und ihrer Verwendung zu Zwecken des Marketings und der Werbung sind auch *indirekte* Datenerhebungen im Zusammenhang einer Registrierung im Zielkonflikt zwischen Urheberschutz und Datenschutz von erheblicher Bedeutung. Im Bemühen um die Wahrung von Urheberrechten, aber auch zur späteren Nutzung und Auswertung im eigenen Geschäftsinteresse werden der Online-Abruf von Software, die Online-Registrierung oder eine spätere Online-Aktualisierung zur Erhebung näherer Angaben über den Nutzer verwendet. Die Anbieter bedienen sich hierbei verschiedener Erhebungsstrategien von auf der Festplatte des Nutzers (Client) gesetzten *Cookies*, dem Aufspielen im System des Nutzers *aktiven Programmen* oder unter Ausnutzung voreingestellter Hardware-Kennzeichen, deren

Grunddaten der Anbieter (Server) bei jedem Online-Abruf abfragt und dem Nutzer zuordnet.¹⁷

Datenschutzrechtlich ist eine heimliche Erhebung personenbezogener Daten des Nutzers durch den Dienstanbieter ohne vorherige Unterrichtung des Nutzers nach § 3 Abs. 5 TDDSG/ § 12 Abs. 6 MD-StV unzulässig. Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten bspw. über das Setzen oder Auslesen eines Cookies ist ohne ausdrückliche Einwilligung des Nutzers rechtswidrig.¹⁸ Ausdrücklich regelt § 4 Abs. 4 TDDSG, dass die Verwendung von Nutzungsprofilen nur unter Pseudonym zulässig ist.

3.3 Szenario B: Download – Upload

Im zweiten Szenario geht es um den Schutz der Urheberrechte bei einem Upload oder Download von Dateien. Im ersten Fall spielt der Nutzer in ein Angebot eines Anbieters im Internet Dateien auf, die sich Dritte dann abrufen können. Urheberrechte können hier sowohl mit der Weitergabe als auch mit der Bereitstellung für Dritte verletzt werden. Im zweiten Fall verstößt das Herunterladen aus einem bereitgestellten Angebot durch den Dritten gegen die Rechte des Urhebers. Gemeinsam ist den Fällen dieses Szenarios, dass die Urheberrechte aktiv durch einzelne Nutzer verletzt werden, die Software aufspielen oder abrufen, der Rechtsverstoß effektiv aber vor allem durch die Inanspruchnahme des Anbieters beseitigt und verhindert werden kann, der den Nutzern sein Angebot als Plattform zur Verfügung stellt.

3.3.1 Verantwortlichkeit der Dienstanbieter

¹⁷ Siehe näher Köhntopp/ Köhntopp, CR 2000, 248 ff.; Wichert DuD 1998, 273 ff.; Cornelius, Die Intel Pentium III Prozessor Seriennummer, DuD 1998, 529 ff.

¹⁸ Bizer in: Rossnagel, Recht der Multimediadienste, 2000, § 3 TDDSG, Rdnr. 217.

¹⁶ Siehe näher Schaar, Persönlichkeitsprofile im Internet, DuD 7/2001.

Bei einer Verletzung seiner Urheberrechte verfügt der Berechtigte über ein zivilrechtliches Instrumentarium, um die weitere Verletzung seiner Rechte für die Zukunft zu unterbinden, die weitere Verbreitung der rechtswidrig bereitgestellten Software oder Inhalte zukünftig zu verhindern und seinen Schaden bei dem Schädiger zu liquidieren. Im Mittelpunkt der Rechtsprechung zum Internetrecht steht vor allem die Frage, ob und unter welchen Voraussetzungen unter Anwendung des § 5 TDG/ MD-StV gegen die Internetprovider vorgegangen werden kann, die die für Bereitstellung und Abruf der Inhalte erforderliche Infrastruktur als Service oder Access Provider zur Verfügung stellen.

Einer der umstrittenen Punkte ist die Differenzierung zwischen der Haftung des Anbieters für eigene Inhalte und der für fremde Inhalte, die er entweder nur bereitstellt oder zu denen er den Zugang vermittelt. Entschieden wurde bislang, dass

- der Anbieter eines Einwählknoten nicht verantwortlich ist für die Inhalte, zu denen er den Zugang vermittelt, unabhängig von dem Umstand, ob die Nutzer des Zugangs seine Kunden sind.¹⁹
- sich ein Anbieter durch die Eröffnung eines Zugangs zu Softwarearchiven anderer Anbieter die angebotene Software *nicht* zu eigen, selbst wenn er die Archive täglich spiegelt.²⁰
- sich ein Anbieter einen Inhalt aber zu eigen macht, wenn er bewusst einen Link auf die Downloadseiten eines Dritten setzt, von der aus Software unter Verstoß gegen Urheberrechte geladen werden kann.²¹
- dem Dienstanbieter, der über einen Link einen Zugang auf Seiten eines Dritten eröff-

net, wegen der jederzeitigen Veränderbarkeit dieser Seiten eine ständige Überprüfung, ob auf rechtswidrige Inhalte verwiesen wird, nicht zuzumuten oder von ihm typischerweise auch nicht erwartet wird.²²

„Bei einer Verletzung seiner Urheberrechte verfügt der Berechtigte über ein zivilrechtliches Instrumentarium, um die weitere Verletzung seiner Rechte für die Zukunft zu unterbinden, die weitere Verbreitung der rechtswidrig bereitgestellten Software oder Inhalte zukünftig zu verhindern und seinen Schaden bei dem Schädiger zu liquidieren.“

Ein anderer Diskussionspunkt betrifft die Voraussetzungen, unter denen ein Service Provider für fremde von ihm bereitgestellte Inhalte haftet. § 5 Abs. 2 TDG/MD-StV setzt erstens positive Kenntnis der Inhalte und zweitens eine technisch mögliche und zumutbare Sperrung dieser Inhalte voraus. Nach der Rechtsprechung muss

- der Dienstanbieter nach § 5 Abs. 2 TDG nur Kenntnis der Inhalte, nicht aber ihrer Rechtswidrigkeit haben, allerdings genügt bedingter Vorsatz.²³ der Dienstanbieter sich die Kenntnis sogenannter „Scouts“ zurechnen lassen, die er zur Kontrolle der Inhalte beispielsweise auf erkennbare Copyright-Vermerke einsetzt²⁴ und

¹⁹ LG München I vom 17.11.1999, CR 2000, 117, 119 = DuD 2000, 365 – Compuserve.

²⁰ OLG München I, Urteil vom 30.3.2000, CR 8/2000, 542-Simtel.

²¹ LG München I vom 25.5.2000, MMR 9/2000, 565 (566) – FTP-Explorer

²² LG Lübeck vom 24.11.1998, MMR 1999, 686 = DuD 2000, 368 – Hyperlinks.

²³ LG München I, Urteil vom 30.3.2000, DuD 6/2000, 362 – MIDI/AOL, DuD 6/2000 = CR 8/2000, 389 = MMR 7/2000, 431 m. Anmk. Hoffmann.

²⁴ LG München I, Urteil vom 30.3.2000, DuD 6/2000, 362 – MIDI/AOL.

- haftet der rechtswidrig Inhalte bereithaltende Dienstanbieter nach Kenntnis einer ersten auch für weitere Rechtsverletzungen, selbst wenn er diese nicht kennt.²⁵

Die Regelung über das Tatbestandsmerkmal der Kenntnis wird der deutsche Gesetzgeber wegen Art. 14 der E-Commerce Richtlinie 2000/31/EG vom 8. Juni 2000 modifizieren: Die Haftungsprivilegierung des Dienstanbieters greift nur ein, wenn der Dienstanbieter „keine Kenntnis von der rechtswidrigen Handlung“ hat, mit der Urheberrechte verletzt werden.²⁶ Schadensersatzansprüche soll der Dienstanbieter nur entgegenreten können, wenn ihm „keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird“. Umgekehrt formuliert, wird der Dienstanbieter bei einer grob fahrlässigen Unkenntnis der Verletzungshandlungen nicht von Schadensersatzansprüchen frei.

- Der Anbieter muss „nicht jeden nur denkbaren Aufwand betreiben, um die Nutzung rechtswidriger Inhalte zu vermeiden, sondern [es müssen] die Bedeutung des Einzelfalls und der erforderliche technische und wirtschaftliche Aufwand sowie die Auswirkungen auf andere Teile des Dienstes und andere Nutzer im Verhältnis zueinander gesehen werden“.²⁷
- Schließlich sind Maßnahmen zur Verhinderung des Zugangs auf fremde Inhalte unzumutbar, „wenn sie einen erheblichen Aufwand erfordern, ihre Wirksamkeit jedoch durch einen Zugriff auf entsprechende Informationsangebote über andere Netzverbindungen mit einem vergleichsweise geringen Aufwand umgangen werden kann.“

²⁵ LG München I, Urteil vom 30.3.2000, DuD 6/2000, 362 – MIDI/AOL.

²⁶ Art. 1 Entwurf-Elektronisches Geschäftsverkehrsgesetz, § 11 Abs. 1 Nr. 1 E-TDG.

²⁷ OLG München, Urteil vom 30.2.2000, CR 2000, 541 (542) – Simtel.

So ist die Grenze einer zumutbaren technischen Sperrung überschritten, wenn der Anbieter bei einer täglichen Spiegelung von einem Quellserver die streitgegenständliche Datei „einzeln herausfiltern müsste“.²⁸

- Bereits die Gesetzesbegründung stellt heraus, dass eine Einstellung eines ganzen Dienstes nicht wegen einzelner rechtswidriger Inhalte Dritter erfolgen dürfe (BT-Drs. 13/7385, S. 20).

Für die Praxis ist jedoch entscheidend, dass der Geschädigte oder ein Dritter den Dienstanbieter über den Verstoß gegen Urheberrechte lediglich in Kenntnis setzen muss, um ihn zu einer Sperrung und damit der Unterbindung weiterer Rechtsverstöße anzuhalten.²⁹

3.3.2 Identifizierung des Anbieters

Voraussetzung einer erfolgreichen Unterbindung von Urheberverstößen ist die Identifizierung des Anbieters, auf dessen technischer Plattform Nutzer durch Down- oder Uploads die Urheberrechte verletzt werden. Das Interesse der Inhaber der Urheberrechte besteht bei wirtschaftlicher Betrachtungsweise vor allem darin, Verletzungshandlungen zukünftig wirksam zu unterbinden. Demgegenüber ist das Interesse vergangene Verletzungshandlungen im Wege von Schadensersatzforderungen gegenüber einzelnen Nutzern zu liquidieren von wirtschaftlich nachrangiger Bedeutung, zumal der Geschädigte regelmäßig mit gewissen Schwierigkeiten zu kämpfen haben wird, den Umfang der rechtswidrigen Nutzungen und seine wirtschaftlichen Auswirkungen zu beweisen.

Die zentrale Regelung für die Identifizierung des Anbieters ist § 6 TDG bzw. § 6

²⁸ OLG München, Urteil vom 30.2.2000, CR 2000, 541 (542) – Simtel.

²⁹ Vgl. auch § 5 Abs. 4 TDG sowie § 18 Abs. 3 MD-StV.

Abs. 1 MD-StV. Danach haben Anbieter für ihre geschäftsmäßigen Angebote „Name und Anschrift“ anzugeben. Auf diese Weise soll den Nutzern eine wirksame Verfolgung ihrer Rechte ermöglicht werden.³⁰ Allerdings ist der Verstoß gegen die Verpflichtung der Anbieterkennzeichnung im Unterschied zum MD-StV nicht bußgeldbewehrt. Untersuchungen der Arbeitsgemeinschaft der Verbraucherverbände haben auf erhebliche Defizite bei der Umsetzung der Anbieterkennzeichnung aufmerksam gemacht.³¹

Mittlerweile setzt sich die Verpflichtung der Dienstanbieter im Internet, ihre Angebote zu kennzeichnen auch europaweit durch. Art. 5 Abs. 1 a E-Commerce-Richtlinie 2000/31/EG verpflichtet die Mitgliedstaaten in ihrem nationalen Recht sicherzustellen, dass die Anbieter den Nutzern des Dienstes und den zuständigen Behörden

a) den Namen des Dienstanbieters

b) die geographische Anschrift, unter der der Dienstanbieter niedergelassen ist, leicht, unmittelbar und ständig verfügbar zu machen.

Diese Regelung ist nun fast wörtlich in dem Entwurf zur Änderung des § 6 TDG übernommen worden. Darüber hinaus soll nach § 12 E-TDG in Zukunft der Verstoß gegen die Verpflichtung zur Anbieterkennzeichnung bußgeldbewehrt sein.

Die Anbieterkennzeichnung weist Parallelen zu einer ähnlichen Regelung im Zusammenhang mit dem Abschluss von Fernabsatzverträgen auf. Die bundesgesetzliche Regelung des Fernabsatzgesetzes (FernAbsG)³² beruht auf europäischen Verbraucherrecht, nämlich

der EG Fernabsatzrichtlinie 97/7/EG.³³ Nach § 2 FernAbsG muss dem Verbraucher beim Einsatz von Fernkommunikationsmitteln, zu denen nach § 1 Abs. 2 FernAbsG auch Tele- und Mediendienste gehören, „die Identität des Unternehmers für den Verbraucher eindeutig erkennbar sein“. Darüber hinaus muss der Unternehmer nach § 1 Abs. 2 „rechtzeitig vor Abschluss eines Fernabsatzvertrages“ den Verbraucher

„in einer dem eingesetzten Fernkommunikationsmittel entsprechenden Weise klar und verständlich informieren über

1. seine Identität und Anschrift.

Eine nach ihrer Funktion vergleichbare Regelung besteht im übrigen auch im Datenschutzrecht. Nach § 4 Abs. 3 Satz 1 BDSG ist der Betroffene, wenn Daten bei ihm erhoben werden, über die „Identität der verantwortlichen Stelle“ zu unterrichten.

Die Regelung der Anbieterkennzeichnung ist von überragenden Bedeutung für die Internetkommunikation, weil sie die Durchsetzung von Rechtsansprüchen ermöglicht und damit letztlich zur Vertrauensbildung gegenüber den Nutzern im Internet beiträgt. Die Identifizierung des Anbieters gewährleistet aber nicht nur den Verbraucherschutz, sondern die Sanktionierung von Wettbewerbsverstößen zwischen den Anbietern. Ohne Anbieterkennzeichnung könnten die Betroffenen im übrigen auch ihre datenschutzrechtlichen Auskunftsansprüche nicht wirksam durchsetzen.

Gerade wegen ihrer Bedeutung für verschiedene Anwendungszusammenhänge ist die Anbieterkennzeichnung ein geeignetes Anwendungsfeld für eine Selbstregulierung durch die Wirtschafts- und Verbraucherverbände.³⁴ Jedoch muss die Befolgung der Vorschriften

³⁰ Bizer/Trosch, Die Anbieterkennzeichnung im Internet, DuD 1999, 621 ff.; Siehe auch Brönnecke, § 6 TDG in: Rossnagel, Multimediarecht 1999.

³¹ Wolters, Einkauf via Internet: Anbieterkennzeichnung, DuD 1999, 633 ff.; Bundesregierung, DuD 1999, 656.

³² Art. 1 des Gesetzes über Fernabsatzverträge vom 27. Juni 2000., BGBl. I S. 896.

³³ vom 20. Mai 1997, Abl. EG L 24/1 vom 30.1.1999.

³⁴ Brönnecke, Nationaler Dialog: Anbieterkennzeichnung, DuD 1999, 638; Bizer, Bereitschaft zur Selbstregulierung, DuD 1999, 618; Pernice, Anbieterkennzeichnung für Werbung im Internet, DuD 1999, 635 ff.

über die Anbieterkennzeichnung von wirksamen Durchsetzungsmechanismen begleitet werden. Völlig unterschätzt werden insbesondere die Möglichkeiten, die rechtsgemäße Implementierung und Gestaltung der Anbieterkennzeichnung bereits bei der Gestaltung von Webseiten durch geeignete Werkzeuge technisch zu unterstützen.³⁵

3.4 Identifizierung des Nutzers

Die Identifizierung des Anbieters ist gegenüber einer Identifizierung des Nutzers das mildere und vor allem auch wirksamere Mittel zur Wahrung der Urheberrechte – zumal das Datenschutzrecht der Vorstellung einer umfassenden Identifizierung zur Wahrung von Urheberrechten mit einer Reihe von Rechtsregeln deutliche Schranken setzt.

3.4.1 Datenvermeidung und Datensparsamkeit

und Datensparsamkeit haben die Anbieter im Internet „die technische Gestaltung und Auswahl“ ihrer Dienste an dem Ziel auszurichten

„keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen“ (§ 3 Abs. 4 TDDSG).

Eine entsprechende Regelung gilt nach § 12 Abs. 5 MD-StV für Mediendienste sowie nach § 47 Abs. 5 Rf-StV für den Rundfunk. Einzelne Regelungen des TDDSG/MD-StV präzisieren und konkretisieren diese Zielvorgabe.³⁶ Unausweichlich steht die Einrichtung technischer Informationssysteme, mit denen zum Schutz der Urheberrechte personenbezogene

Nutzerdaten erhoben werden sollen³⁷, im Widerspruch mit dem Grundsatz der Datenvermeidung. Die Diensteanbieter müssen sich folglich zum Schutz der Urheberrechte um datenschutzgerechte Lösungswege bemühen, personenbezogene Daten nicht erhoben werden müssen oder zumindest ihre Verarbeitung begrenzt werden kann. Gegenüber umfassenden Erhebungsstrategien verspricht die wirksame Implementierung der Anbieterkennzeichnung bei Telediensteanbieter im Internet einen geringeren Aufwand bei höherem Nutzen.

Das Prinzip der Datensparsamkeit gilt mittlerweile auch in anderen Rechtsbereichen. Nach § 3 Abs. 4 TDSV haben sich Diensteanbieter geschäftsmäßiger Telekommunikation

an dem Ziel der Datenvermeidung und Datensparsamkeit auszurichten.

Das Prinzip der datenvermeidenden Technikgestaltung hat über das Datenschutzrecht für Tele-/Mediendienste nun auch Eingang in das Allgemeine Datenschutzrecht gefunden. Neben einigen Landesdatenschutzgesetzen gilt es über nach § 3 a Satz 1 BDSG 2001 nun auch für das allgemeine Datenschutzrecht:

„Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.“

³⁵ Grimm, Technische Umsetzung der Anbieterkennzeichnung, DuD 1999, 628 ff.

³⁶ Siehe näher Bizer in: Rossnagel, Recht der Multi-Mediadienste, § 3 TDDG, Rdnr. 150 ff.

³⁷ Siehe oben Erwägungsgrund 56 der Urheberrechtsrichtlinie.



3.4.2 Anonyme und pseudonyme Nutzung

Der zweite datenschutzrechtliche Grundsatz, mit dem personenbezogene Informationssysteme zum Schutz der Urheberrechte in Konflikt geraten, ist die Regelung des § 4 Abs. 1 TDDSG, wonach der Diensteanbieter

„dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.“

Entsprechende Regelungen gelten nach § 13 Abs. 1 MD-StV für Mediendienste sowie nach § 47 a Rdf-StV für den Rundfunk. Nach diesen Regelungen soll die anonyme/pseudonyme Inanspruchnahme eines Internetangebots die Regel, eine personenbezogene Inanspruchnahme jedoch die Ausnahme sein soll. Grenze dieser Verpflichtung bildet neben der technischen Möglichkeit die wirtschaftliche Zumutbarkeit, bei der neben dem Durchschnitt brachentypischer Anbieter auch das Gewicht der anonymen Nutzung zugrunde zu legen ist.³⁸

Derzeit bieten die meisten Angebote im Internet zum Down- und Upload von Software ihre Dienste kostenlos und ohne eine persönliche Registrierung der Nutzer an. Nach dem

³⁸ Schaar/Schulz in: Rossnagel, § 4 TDDSG, Rdnr. 54a; Schmitz, P., TDDSG und das Recht auf informationelle Selbstbestimmung, München 2000, S. 118 f.

derzeit weitverbreiteten Finanzierungsmodell über Einnahmen für Webbanner würde eine personenbezogene Registrierung dieses Geschäftsmodell durch sinkende Zugriffszahlen gefährden. Vor diesem Hintergrund liegt eine personenbezogene Registrierung der Nutzer zwar möglicherweise im Interesse der Urheber, nicht aber der Diensteanbieter im Internet und angesichts der hohen Wertschätzung des Datenschutzes bei den Nutzern auch nicht in deren Interesse. Auch unter diesem Gesichtspunkt erweist sich eine wirksamere Durchsetzung der Anbieterkennzeichnung als der wirksamere Weg zum Schutz der Urheberrechte.

3.4.3 Löschungspflicht von Nutzungsdaten

Die Konkretisierung der „weichen“ Zielvorgabe datensparsamer Technikgestaltung erfolgt bspw. durch die restriktiven Regelungen über die Löschungspflicht personenbezogener Nutzungsdaten.³⁹ Nach § 6 Abs. 2 Nr. 1 TDDSG sind diese Daten

frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen.

Eine Ausnahme von der Löschungspflicht ist lediglich zulässig, soweit die Nutzungsdaten zur Abrechnung der Teledienste benötigt werden. Da im Regelfall die Angebote dieser Fallgruppe von Urheberrechtsverletzungen durch Down- oder Upload im Internet kostenlos sind, spielt diese Ausnahme derzeit keine praktische Rolle.

Sollten derartige Internetangebote kostenpflichtig sein, ist eine Verarbeitung der Nutzungsdaten gleichwohl nur in engen Grenzen zulässig. Die Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind, § 6 Abs. 2 Nr. 2

³⁹ Bizer in: Rossnagel, Recht der Multimediendienste, TDDSG, § 3, Rdnr. 165 ff.

TDDSG. „Nutzerbezogene Abrechnungsdaten“ dürfen darüber hinaus nur auf Verlangen des Nutzers „für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote gespeichert werden“ und sind spätestens 80 Tage nach Versendung des Einzelnachweises zu löschen, es sei denn, die Entgeltforderung wird innerhalb dieser Frist bestritten oder trotz Zahlungsaufforderung nicht beglichen. Entsprechende Regelungen enthalten MD-StV und Rdf-StV.

3.4.4 Missbrauchsbekämpfung im TDDSG

Mit der im Zusammenhang mit dem Elektronischen Geschäftsverkehrsgesetz geplanten Novellierung des TDDSG ist zum einen beabsichtigt, die höchstzulässige Speicherfrist der Nutzungsdaten von bisher 80 Tagen auf 6 Monate nach Rechnungsversand zu erweitern. Zum anderen findet sich im Entwurf des TDDSG eine gesonderte Missbrauchsklausel (§ 6 Abs. 8 E-TDDSG), die eine Verarbeitung von Nutzungsdaten über die Löschungspflichten hinaus ermöglicht. Für den Diensteanbieter sind Anhaltspunkte Voraussetzung, dass „seine Dienste“ von bestimmten Nutzern „missbräuchlich in Anspruch genommen werden“. Die aufgrund der geplanten Bestimmung erhobenen Daten sollen zur Aufklärung des Missbrauchs – zum anderen aber auch zur Rechtsverfolgung verwendet werden können.

(8) Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern missbräuchlich in Anspruch genommen werden, so darf der Diensteanbieter die personenbezogenen Daten dieser Nutzer zur Wahrung überwiegender Interessen des Diensteanbieters an der Aufklärung des Missbrauchs und der Rechtsverfolgung über das Ende des Nutzungsvorgangs sowie die in Absatz 7 ge-

nannte Speicherfrist hinaus verarbeiten, nutzen und an Dritte übermitteln, soweit dies hierfür erforderlich ist.

Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn Anhaltspunkte für eine missbräuchliche Inanspruchnahme nicht mehr vorliegen oder sie für die in Satz 1 genannten Zwecke nicht mehr benötigt werden.

Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.“.

Allerdings wirft die Auslegung des Begriffs der „missbräuchlichen“ Nutzung Auslegungsprobleme auf. Mit Rücksicht auf den Wortlaut der Bestimmung liegt dieser Tatbestand vor, wenn ein Nutzer den Teledienst entgegen den Nutzungsbestimmungen seines Anbieters verletzt. Inwieweit die missbräuchliche Nutzung sich auch auf den Schutz der Rechte Dritter erstreckt, ist durch Ausgestaltung der Nutzungsbedingungen zu regeln. Eine grundsätzliche Verpflichtung des Diensteanbieters (service providers), über seine Nutzungsbedingungen die Nutzer zur Wahrung der Urheberrechte Dritter anzuhalten, besteht nicht. Der Diensteanbieter ist lediglich nach § 5 Abs. 2 TDG mit eigener positiver Kenntnis von derartigen Umständen bei gegebener Zumutbarkeit und technischer Möglichkeit zur Sperrung verantwortlich.

Schließlich ist zu berücksichtigen, dass der Diensteanbieter die Nutzungsdaten nur zur Wahrung seiner eigenen überwiegenden Interessen („des Diensteanbieters“) verwenden darf, nicht aber zur Wahrung der Interessen Dritter.

Als Zwischenergebnis ergibt sich, dass das derzeit geltende Datenschutzrecht eine Verwendung personenbezogener Daten über die Nutzung einzelner Internetdiensten für Zwecke ihrer Identifizierung bei Urheberrechtsverstößen nicht ermöglicht.

4 Drei Thesen

1. Datenschutz ist ein Akzeptanzfaktor, ohne den sich der E-Commerce nicht entwickeln kann. Es ist daher folgerichtig, dass die Urheberrichtlinie der EU für die Gestaltung technischer Informationssysteme zum Schutz der Urheber auf die datenschutzrechtlichen Anforderungen des europäischen Rechts verweist.

2. Der Schutz des Urheberrechts ist nicht durch eine zunehmende Speicherung von Nutzungsdaten, wohl aber über eine konsequente Durchsetzung der Anbieterkennzeichnung zu gewährleisten. Mit Hilfe der Anbieterkennzeichnung können Dienstanbieter zum Down- und Upload von Software zur Gewährleistung ihrer Verantwortlichkeit angehalten werden können.

3. Strategien der Nutzeridentifizierung zum Schutz der Urheber unterlaufen die Vertrauensbasis der Internetkommunikation und werden mittelfristig die Entwicklung des E-Commerce stärker schädigen als die Restmenge an Urheberrechtsverletzungen, die trotz einer effektiven Implementierung der Anbieterkennzeichnung hingenommen werden muss.

Dr. jur. Johann Bizer ist Wissenschaftlicher Assistent am Institut für öffentliches Recht an der Universität Frankfurt/Main. Im Mittelpunkt seiner wissenschaftlichen Arbeiten stehen Untersuchungen zur Gewährleistung der Vertraulichkeit, der Beweissicherheit und des Datenschutzes in elektronischen Netzen und in diesem Zusammenhang auch Rechtsfragen der Kryptographie. Darüber hinaus ist er (Mit)-

Herausgeber der Fachzeitschrift „Datenschutz und Datensicherheit“ (<http://www.dud.de>).

Kristian Köhntopp schilderte im Anschluss an den Vortrag von *Bizer* seine praktische Erfahrung mit der Löschung von Logfile-Daten im Rahmen einer Rechnungsstellung. Hier bestehe ein Konflikt zwischen den gesetzlichen Vorgaben zur Löschung von Daten einerseits und den Anforderungen des Finanzamts andererseits, nach dessen Auffassung die Rechnungsdaten über Jahre aufgehoben werden müssten. *Bizer* erwiderte, die Löschungspflicht sei klar geregelt, daher müsse es eine ausdrückliche Rechtsgrundlage geben, die eine Ausnahme von dieser Pflicht konstituiere. Eine solche gebe es in der Abgabenordnung aber nicht. *Mayer* wies in diesem Zusammenhang darauf hin, dass diskutiert werde, ob Logfile-Daten im hinreichenden Maße personenbezogene Daten seien.

Zerdick bestätigte die Feststellung von *Bizer*, Datenschutz sei ein wesentlicher Akzeptanzfaktor, wies aber auf die generelle Problematik von Umfragen hin. Dem stimmte *Bizer* prinzipiell zu. Man müsse die Umfragen relativ betrachten, weil die Nutzer aufgrund des vom Internet geweckten natürlichen Spieltriebs sich häufig auch entgegen ihrer Aussagen verhielten und Daten preisgäben. Ferner sah *Zerdick* die Problematik weniger in der Löschung von Daten, sondern in der Frage, wie man den Missbrauch von Daten sanktionieren könne.

Implementierungsmöglichkeiten für Urheberschutz in offenen Portalen

Horst Henn



Dr.-Ing. Horst Henn studierte Datenverarbeitung an der Universität Stuttgart und promovierte anschließend im Fach Nachrichtentechnik ebenfalls an der Universität Stuttgart. Von 1970 bis 1975 war er als Wissenschaftlicher Assistent am Institut für Nachrichtentechnik auf dem Gebiet der Halbleiterspeicher, supraleitender Speicher sowie fehlertoleranter Systeme tätig. 1975 trat er in das Entwicklungslabor der IBM Deutschland ein und entwickelte vorwiegend grafische Programme für die Entwicklung von /370 Systemen und der 801 RISC Maschine in IBM Research, Yorktown Heights, USA.. Danach war er Leiter von Projekten zur Entwicklung neuer Produkte speziell auf den Gebieten verteilte Mikroprozessorsysteme, Kommunikationssysteme, CMOS Design, /390 Sysplex Design und Grafische Systeme sowie Unterschriftenerkennung mit neuronalen Netzen für Banken. Seit 1975 ist er auf dem Gebiet Pervasive Computing zunächst als Leiter der

IBM Smartcard Entwicklung tätig und dabei speziell an der Definition von Standards im Smartcard Umfeld wie PC/SC, OpenCard Framework (OCF), Java Card und G8 Gesundheitskarte engagiert. Zur Zeit arbeitet er als Lead Consultant sowohl mit Kunden als auch mit Entwicklungs- und Serviceteams an der Implementierung neuartiger Systeme und Geschäftsmodellen basierend auf Pervasive Computing Portalen und deren wirtschaftlichen (Zahlungsverfahren) und gesellschaftlichen Auswirkungen (Datenschutz). In letzter Zeit wurde speziell die Entwicklung eines multimodalen Portals (PC, PDA, WAP, Sprache) in Kooperation mit der Deutschen Bank sowie die Entwicklung des offenen WebSphere Portal Servers der IBM vorangetrieben. Er ist Koautor des Buches: „Pervasive Computing, das 2001 bei Addison Wesley erschien.

