

Dr. Alexander Dix
Landesbeauftragter für den Datenschutz
und für das Recht auf Akteneinsicht
Brandenburg

Digitales Urheberrechts-Management (DRM) und Datenschutz

Statement bei der Konferenz

II. Digital Rights Management 2002

30. Januar 2002

Berlin

Urheberrecht und Datenschutz stehen heute in einem Spannungsverhältnis, das mit den Stichworten „Digital Rights Management“ oder „Electronic Copyright Management Systems“ beschrieben wird. Bevor ich dieses Spannungsverhältnis näher beleuchte, sei daran erinnert, dass Urheberrecht und Persönlichkeitsschutz („privacy“) in der amerikanischen Rechtstradition anfangs gemeinsame Wurzeln hatten. Samuel Warren und Louis Brandeis entwickelten im Dezember 1890 in ihrem einflussreichen Aufsatz im Harvard Law Review das Konzept des „Right to Privacy“ in wesentlicher Analogie zum Urheberrecht.

Im Juni 2000 wurden Pläne von Sony bekannt, es wolle mit einem eigenen Digital Locker Service Kunden den Zugang zu Musik- und anderen Multimedia-Dateien über das Internet ermöglichen. Der Dienst sollte die Kunden mit digitalen Archiven verbinden, die Musik, Videos, Filme und Spiele zum Abruf von überall bereit halten. *„By separating the media from the medium, Digital Locker aims to be your ubiquitous, networked Personal Digital Living Room.“*

In der Datenschutzerklärung der Website von de.mp3.com klingt das so:

„Wenn du zum ersten Mal unsere Site besuchst, bittet MP3.com dich zunächst um einige Angaben zu deiner Person. So fragen wir dich beispielsweise nach deinem Namen, deiner E-Mail-Adresse, deiner Postleitzahl, deinem Heimatland, deiner bevorzugten Sprache, deinem Geschlecht und nach bestimmten Informationen über dein Alter (wie z.B. ob du über 21 Jahre alt bist). Je mehr Daten du uns zur

Verfügung stellst (und je genauer diese sind), umso angenehmer können wir deinen Aufenthalt auf unserer Site gestalten und genau auf deine Belange eingehen."

In der offline-Welt, etwa dem Buch- oder Plattengeschäft um die Ecke, konnte ich schon immer stöbern oder Bücher und CDs kaufen, ohne meinen Namen und meine Anschrift anzugeben, wenn das Produkt vorrätig ist und ich es sofort bezahle (anders bei Bestellungen).

Aber schon vor dem Start des Internet – also noch in der offline-Welt – gab es erste Anzeichen für mögliche Reibungsflächen zwischen dem Urheberrechtsschutz und dem Schutz der Privatsphäre. Das wurde deutlich in der Rechtsprechung des Bundesgerichtshofs zu Privatkopien in den Urteilen von 1964 (Pflicht zur Vorlage von Personalausweisen in Elektronikläden/GEMA) und 1983 (Identifikationspflicht in Kopierläden). Damit begrenzte der Bundesgerichtshof das Recht der Urheber, die private Vervielfältigung und Verwendung von geschützten Werken unbegrenzt zu kontrollieren – ausdrücklich unter Berufung auf den Schutz der Privatsphäre, genauer der Unverletzlichkeit der Wohnung.

„Soll die Namensübermittlung (von Käufern an die GEMA) überhaupt einen ... Sinn haben, so kann dies nur der sein, dass die Kl. (GEMA) aufgrund ihrer Kenntnis von Namen und Anschriften der Geräteerwerber in deren persönlicher häuslicher Sphäre Kontrollmaßnahmen durchführen und auf diese Weise etwaige Rechtsverletzungen ahnden will. Da die Art der Verwendung der Geräte (Tonbandgeräte) nur an Ort und Stelle festgestellt werden könnte und die Kl. bereits ... angekündigt hat, die erforderlichen Feststellungen auf Mitteilungen von Wohnungsnachbarn, Portiers usw. hin zu veranlassen, würde hierdurch die Gefahr unangemessener Eingriffe in die Unverletzlichkeit des häuslichen Bereichs heraufbeschworen (Art. 13 GG).“¹

Mit dem Durchbruch des Internets, das zunehmend zu einem Massenmedium wird, muss die Frage nach der Durchsetzbarkeit des Urheberrechtsschutzes völlig neu gestellt werden. Da es im Internet bisher keinen Kopierschutz gibt, lassen sich die Ergebnisse künstlerischer oder wissenschaftlicher Arbeit, die ins Netz eingestellt

¹ BGH Ur. v. 25.5.1964, GRUR 1965/2, 104

worden sind, weltweit beliebig oft in Kopien verwandeln, die in ihrem digitalen Format vom Original nicht zu unterscheiden sind.

Ich will in diesem Zusammenhang nicht auf die Grundsatzfrage eingehen, welche Existenzberechtigung das Urheberrecht im Cyberspace überhaupt noch hat. Lawrence Lessig hat bekanntlich vor einer „Ideologie des totalen Eigentums“ gewarnt, die in einer extremistischen Auslegung des „geistigen Eigentums“ zum Ausdruck komme und die Innovationsfähigkeit des Internets gefährde. Von Ian Clarke, dem Gründer der Tauschbörse Freenet, stammt der Satz: „Copyright and freedom of speech cannot coexist. One of them has to go.“

Ich gehe bei meinen folgenden Überlegungen von der These aus, dass das Urheberrecht auch im Zeitalter des Internets seine Berechtigung behält, allerdings nur dann eine realistische Durchsetzungschance hat, wenn Modelle und Techniken zu seiner datenschutzfreundlichen Realisierung entwickelt und umgesetzt werden kann.

Ein Digital Rights Management-Konzept, das auf die lückenlose Registrierung des Nutzerverhaltens abzielt oder sie bewirkt, stößt dagegen jedenfalls in Europa an rechtliche Grenzen und es wird auch wirtschaftlich keinen Erfolg haben. Letzteres ist eine Prognose, ersteres lässt sich bereits heute belegen.

Die Europäischen Urheberrechtsrichtlinie vom 22. Mai 2001 regelt an zwei Stellen den Schutz von technischen Vorkehrungen und Informationen zum Urheberrechtsschutz.

Zum einen müssen die Mitgliedstaaten einen angemessenen Rechtsschutz gegen die Umgehung von wirksamen technischen Maßnahmen zum Schutz des Urheberrechts vorsehen (Art. 6 Abs.1). Damit sind in erster Linie Formen der Zugangskontrolle oder Schutzmechanismen wie Verschlüsselung, Verzerrung oder Umwandlung des geschützten Werks gemeint. Nicht ganz klar ist allerdings, ob auch technische Verfahren zur Registrierung des Nutzerverhaltens darunter fallen. Die weite Definition der „technischen Schutzmaßnahmen“ legt diese Vermutung nahe. Man wird hier aber danach differenzieren müssen, welchem Zweck die technische

Maßnahme primär gilt: Soll sie in erster Linie die Durchsetzung der Urheberrechte ermöglichen, dann müssten die Mitgliedstaaten dagegen für angemessenen Rechtsschutz sorgen. Dient die technische Vorkehrung dagegen in erster Linie anderen Zielen wie etwa dem Direktmarketing und ist der Schutz vor Urheberrechtsverletzungen nur ein sekundärer Effekt, so muss es möglich sein, solche Mechanismen abzuschalten. Das gilt insbesondere für das Setzen von Cookies, die auf der Festplatte des Nutzers abgelegt werden. Hier muss der Nutzer auch nach der Umsetzung der Urheberrechtsrichtlinie die Möglichkeit behalten, Cookies auf einfachem Wege abzulehnen oder zu löschen.

Es ist bemerkenswert, dass die Vereinigten Staaten, die in anderem Zusammenhang (beim transatlantischen Datenexport aus der Europäischen Union) wegen ihres zu geringen Datenschutzniveaus gescholten worden sind und sich erst nach langwierigen Verhandlungen mit der EU-Kommission zum „Safe-harbor“-Kompromiss bereit gefunden haben, in diesem Punkt ein explizit datenschutzfreundlicheres Urheberrecht haben als die Europäische Union. Der Digital Millennium Copyright Act (DMCA) lässt ausdrücklich das Abschalten von solchen Schutzmechanismen und Zugangskontrollsystemen zu, die Daten über die Online-Aktivitäten der Nutzer sammeln oder verbreiten, ohne darüber deutlich aufzuklären und dem Nutzer eine opt-out-Option zu eröffnen, wenn die Abschaltung des Kontrollsystems ausschließlich die Sammlung und Verbreitung von Nutzerdaten verhindern soll. Man mag sich allerdings fragen, ob diese amerikanische Vorschrift in der Praxis große Bedeutung hat, denn sie setzt einen kundigen Nutzer voraus, der trotz fehlender Hinweise des Anbieters/Urhebers erkennt, dass ein solches datensammelndes Schutzsystem in Aktion ist.

Die Richtlinie verpflichtet darüber hinaus die Mitgliedstaaten dazu, einen angemessenen Schutz vor Personen vorzusehen, die zur Verletzung von Urheberrechten beitragen, indem sie elektronische Informationen für die Wahrnehmung der Rechte (Rights Management Information) entfernen oder ändern oder Werke verbreiten, bei denen die Informationen zur Rechtswahrnehmung entfernt oder verändert worden sind (Art.7). Was aber sind Informationen zur Rechtswahrnehmung? Sind das auch Informationen über die Nutzer des Werks, die durch ein Management System permanent gesammelt werden?

Die Legaldefinition (Art. 7 Abs.2) der Richtlinie beschränkt diesen Begriff zunächst auf die vom Rechteinhaber stammenden Informationen, die die urheberrechtlich geschützten Werke und den Urheber identifizieren. Allerdings spricht diese Definition auch von Informationen über die Modalitäten und Bedingungen für die Nutzung der Werke („*terms and conditions of use of the work or other subject-matter, and any numbers and codes that represent such information*“). Neben einer Differenz zwischen der deutschen und der englischen Fassung des Richtlinien textes spricht auch von der Sache her vieles dafür, dass diese Regelung sich nicht auf personenbezogene Informationen der Nutzer bezieht. Gemeint sind offenbar Nutzungsbedingungen, die der Urheber mit dem Werk z.B. durch ein digitales Etikett verbindet.

Andererseits haben die Verfasser der Urheberrechtsrichtlinie durchaus erkannt, dass technische Systeme zur Verwaltung und Durchsetzung von Urheberrechten geeignet sein können (nicht müssen!), das Verhalten von Nutzern zu überwachen. Der Erwägungsgrund 57 spricht davon, dass solche Systeme „je nach Auslegung in der Lage sind, gleichzeitig personenbezogene Daten über die individuelle Nutzung von Schutzgegenständen zu verarbeiten und Online-Aktivitäten nachzuvollziehen.“ Daran knüpft der Erwägungsgrund die eher unverbindlich klingende Aussage, dass die technischen Funktionen dieser Vorrichtungen dem Schutz der Privatsphäre gemäß der EU-Datenschutzrichtlinie 95/46/EG gerecht werden sollten. Etwas klarer sagt die Konkurrenzvorschrift des Art. 9 der Urheberrechtsrichtlinie, dass diese Richtlinie gemeinschaftsrechtliche Regelungen zur Vertraulichkeit, zum Datenschutz und zum Schutz der Privatsphäre unberührt lässt.

Zu diesen Regelungen gehört auch die Richtlinie zum Datenschutz in Telekommunikationsnetzen (früher ISDN-Richtlinie), die gegenwärtig überarbeitet wird. Der Entwurf der Kommission für eine Richtlinie über die Verarbeitung personenbezogener Daten und dem Schutz der Privatsphäre in der elektronischen Kommunikation wird zwar gegenwärtig noch kontrovers zwischen Rat und Europäischem Parlament diskutiert. Im Gegensatz zu den übrigen Teilen des sog. Telecom-Packages ist zu dieser Richtlinie bisher kein gemeinsamer Standpunkt beschlossen worden. Nicht kontrovers ist bei dieser Debatte aber die schon in der

bisher geltenden Telekom-Richtlinie enthaltene Regelung, dass Verkehrsdaten stets unmittelbar nach Ende der Verbindung zu löschen oder zu anonymisieren sind, soweit sie nicht zu Abrechnungszwecken benötigt werden. Für andere Zwecke (z.B. Marketing) oder zur Verwendung beim Angebot von Mehrwertdiensten ist die Zustimmung des betroffenen Nutzers erforderlich, um die Datenverarbeitung zu legitimieren.

Zwar regelt die Richtlinie über die Harmonisierungspflicht der Mitgliedstaaten indirekt nur die Datenverarbeitung durch Diensteanbieter (Transporteure im Netz), nicht direkt durch die Anbieter von Inhalten. Die Inhaltsanbieter sind aber wiederum auf die Diensteanbieter angewiesen, weil nur über sie Nutzerdaten bei Herstellung der Verbindung automatisch entstehen

An dieser Stelle sei ein kleiner Exkurs zu den Versuchen von Microsoft gestattet, die Käufer von Windows XP noch nach Zahlung des Kaufpreises zur Identifikation durch eine vorgeschriebene Produktaktivierung zu zwingen: Die Stiftung Warentest hat kürzlich den Microsoft-Kunden in Deutschland empfohlen, die Variante der telefonischen Registrierung der online-Registrierung vorzuziehen, weil die Mitarbeiterinnen im CallCenter durchaus bereit sein, den Aktivierungscode auch demjenigen zu nennen, der hartnäckig genug auf den Schutz seiner Privatsphäre pocht und die Nennung seines Namens ablehnt. Zwar gebührt den Testern der Stiftung Warentest ein Lob dafür, dass sie dieses Schlupfloch für Datenschutzbewusste aufgefunden haben; ich erwarte aber darüber hinaus, dass das Produkt eines faktischen Monopolisten (wie übrigens jedes Produkt !) datenschutzfreundliche Optionen von vornherein anbietet und vom Käufer nicht verlangt, dass er seine Rechte erst in telefonischen Diskussionen durchsetzt.

Dass die geltende Telekommunikationsrichtlinie und auch der Entwurf der Nachfolge-Richtlinie, mit deren Verabschiedung in diesem Jahr zu rechnen ist, direkte Auswirkungen auf unsere Themenstellung heute hat, ergibt sich daraus, dass in den Erwägungsgründen ausdrücklich video-on-demand und andere Dienste (also auch music-on-demand !) in den Geltungsbereich einbezogen werden, bei denen der einzelne Nutzer identifiziert wird.

Die Vorgabe der Datenschutzrichtlinien ist klar: Verkehrs- oder Nutzungsdaten müssen unmittelbar nach Ende gelöscht oder anonymisiert werden, soweit sie nicht für Abrechnungszwecke benötigt werden. Elektronische Kommunikationssysteme, also auch Plattformen zum Abruf von Musikdateien und anderen Inhalten, müssen sich strikt am Grundsatz der Datensparsamkeit orientieren und dürfen nur diejenigen personenbezogenen Daten verarbeiten, die für die Erbringung des Dienstes erforderlich sind (Erwägungsgrund 30 Entwurf der Nachfolge-Richtlinie). Ein Diensteanbieter (Transporteur) im Internet kann also nicht wie ein Portier eingesetzt werden, bei dem die GEMA wie in der BGH-Entscheidung von 1964 Erkundigungen über die Verwendung von Tonbandgeräten in Privatwohnungen einholen wollte (woran der BGH sie mit Recht gehindert hat). Ein *Portal* darf eben kein neugieriger *Portier* sein.

Dem trägt das deutsche Multimedia-Datenschutzrecht auch in seiner novellierten Form Rechnung. Während das mit dem Gesetz über den Elektronischen Geschäftsverkehr geänderte Teledienstedatenschutzgesetz (TDDSG) bereits seit Dezember vergangenen Jahres in Kraft ist, bedarf der 6. Rundfunkänderungsstaatsvertrag, der die entsprechenden Änderungen des Mediendienstestaatsvertrages enthält, noch der Ratifizierung durch die Länder.

Auch nach dem neuen TDDSG dürfen Nutzungsdaten ohne Einwilligung des Nutzers nur verarbeitet werden, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen. Dass sie im übrigen unmittelbar nach Ende der Verbindung zu löschen sind, steht zwar im Gegensatz zur alten Fassung des TDDSG nicht mehr ausdrücklich im neuen Gesetz, es gilt aber nach wie vor. Das neue Bundesdatenschutzgesetz, aus dem sich der Erforderlichkeitsgrundsatz als Grenze der Verarbeitung von Nutzungsdaten ergibt, ist stets ergänzend zum Teledienstedatenschutzgesetz anzuwenden, .

Wichtiger noch als Löschungs- und Zweckbindungsvorschriften ist im modernen Datenschutzrecht der Grundsatz des Systemdatenschutzes, der erstmals im Multimediarecht und jetzt auch im Bundesdatenschutzgesetz 2001 (§ 3a) seinen Niederschlag gefunden hat. Danach haben sich Gestaltung und Auswahl von

Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

Noch deutlicher verpflichtet das Multimediarecht die Anbieter von Tele- und Mediendiensten dazu, den Nutzern die Inanspruchnahme und Bezahlung von Diensten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 4 Abs.6 TDDSG). Nutzungsprofile dürfen nur für Zwecke der Werbung und Marktforschung oder zur bedarfsgerechten Gestaltung des Dienstes erzeugt werden, wenn der Nutzer dem nicht widerspricht ("opt-out", § 6 Abs.3 TDDSG). Daraus ergibt sich, dass Nutzungsprofile für andere Zwecke (z.B. Zwecke des content providers, Durchsetzung von Urheberrechten) vom Diensteanbieter nur mit Einwilligung des Nutzers erstellt werden dürfen ("opt-in").

Insgesamt enthalten diese Regelungen des deutschen Multimediarechts bereits die Grundelemente eines Mediennutzungsgeheimnisses, dessen ausdrückliche Verankerung die Datenschutzbeauftragten des Bundes und der Länder vorgeschlagen haben. Gerade in einer demokratischen Informationsgesellschaft müssen Optionen des spurlosen, anonymen Medienkonsums erhalten bleiben, wenn man den Grundrechten auf informationelle Selbstbestimmung, aber auch der Informationsfreiheit und der freien Meinungsäußerung nicht die Grundlage entziehen will.

Auch die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat in einem Gemeinsamen Standpunkt aus dem Jahr 2000 zu Datenschutz und Urheberrechts-Management betont, dass bestimmte elektronische Copyright-Management-Systeme geeignet sind, den Weg digitaler Werke lückenlos zu überwachen und damit ein umfassendes personenbezogenes Nutzerprofil zu erzeugen. Demgegenüber hat die Arbeitsgruppe die Entwickler und Anwender solcher Systeme aufgefordert, anonyme oder pseudonyme Transaktionsoptionen vorzusehen.

Als eine datenschutzgerechte Möglichkeit, den notwendigen Ausgleich zwischen dem Schutz der Privatsphäre der Nutzer und dem ökonomischen Interesse der Urheber herbeizuführen, hat die Arbeitsgruppe vorgeschlagen, digitale

Wasserzeichen mit Transaktions-Codes zu versehen, durch die einzelne Kopien des Werks nummeriert werden. Diese Codes sollten nur in einer sicheren Datenbank mit personenbezogenen Daten der Nutzer zusammengeführt werden, die von einem vertrauenswürdigen Dritten verwaltet wird. Diese Verknüpfung, also die Aufdeckung des Pseudonyms, sollte nur zu Zwecken des Urheberrechtsschutzes auf richterlichen Beschluss möglich sein.

Ich würde heute noch einen Schritt weiter gehen: Dieses Modell kann auf die gesamte digitale Wertschöpfungskette ausgedehnt werden. In jeder Phase einer elektronischen Transaktion und ihrer Realisierung in der offline-Welt von der Bestellung über die Bezahlung bis hin zur Lieferung lassen sich Pseudonyme in praktikabler Weise zum Schutz der Privatsphäre des Nutzers einsetzen. Das hat auch Konsequenzen für den Urheberrechtsschutz: In dem Maße wie datenschutzfreundliche Zahlverfahren online angeboten werden, wird sich auch das Problem der urheberrechtlichen Vergütung datenschutzgerecht lösen lassen. Aber auch der Händler, der im Netz bestellte "hardware" liefern lassen will, muss die Postanschrift des Nutzers ebenso wenig kennen wie der Paketbote wissen muss, was der Kunde bestellt hat. Entsprechende Versuche eines Zustellverfahrens unter Einsatz von Pseudonymen laufen meines Wissens beim U.S. Postal Service.

Ich komme zurück zum "digitalen Wohnzimmer", wie es uns Sony versprochen hat. Wenn ich mir ein solches Wohnzimmer im Netz mit einem virtuellen Plattenschränk einrichten sollte, dann nur, wenn ich sicher sein kann, dass mir weder Sony noch sonst jemand in diesem Wohnzimmer über die Schulter sieht und überprüft, was ich dort tue. Ich möchte auch sichergestellt wissen, dass nur ich mit meinem persönlichen Schlüssel dieses Wohnzimmer betreten kann.