

Gemeinsamer Standpunkt

Datenschutz und Urheberrechts-Management

angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000 in Rethymnon/Kreta

- Übersetzung -

Das Urheberrecht und das Recht auf Datenschutz sind schon immer als aus den gleichen Wurzeln stammend betrachtet worden. Warren und Brandeis haben sich, als sie die Grundlagen des „Rechts auf Privatheit“¹ des Einzelnen legten, auf die allgemeinen Gesetze zum Schutz geistigen Eigentums bezogen. Trotzdem scheinen im Rahmen des elektronischen Geschäftsverkehrs über das Internet Urheberrecht und Datenschutz zu kollidieren.

Während in der analogen „Offline-Welt“ Urheberrechtsgesetze Ausnahmen für die private (nicht-kommerzielle) Nutzung enthielten, umfasst das Urheberrecht in der digitalen (Online-) Welt jede Handlung der temporären Reproduktion und der Übermittlung in den Arbeitsspeicher eines Computers zum Zwecke des Lesens, Zuhörens oder Betrachtens². Der Autor eines digitalen Werks (einschließlich Software und Datenbanken) hat das Recht, dies zu verbieten oder für jede solche Nutzung eine Gebühr zu erheben.

Das praktische Problem mag teilweise der Tatsache zuzurechnen sein, dass es bisher keine verlässlichen datenschutzfreundlichen Zahlungsmittel im Internet gibt. Wenn anonyme Zahlungsmethoden angeboten würden, könnten digitale Werke zum Download oder zur Nutzung gegen sofortige Bezahlung zur Verfügung gestellt werden.

Für den legitimen Zweck des Schutzes des geistigen Eigentums im Cyberspace und zur Abwehr von Software-Piraterie werden Technologien wie Roboter („web spiders“) geschützte Objekte oder digitale Werke identifizieren, die Nachrichten an zentrale Server mit der Aufforderung zur Erteilung der Zugriffserlaubnis oder zur Bezahlung zu zentralen Servern schicken, wenn sie genutzt oder kopiert werden. Elektronische Copyright-Management-Systeme (ECMS), die zur allgegenwärtigen Überwachung von Nutzern digitaler Werke führen könnten, werden entwickelt und angeboten. Einige ECMS überwachen jede einzelne Handlung des Lesens, Anhörens und Betrachtens im Internet durch individuelle Nutzer, wobei hoch sensible Informationen über die Betroffenen gesammelt werden³.

¹ Warren/Brandeis, Harvard Law Review Vol. IV (1890), 193, 204

² Bygrave/Koelman, Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems, 1998
<http://www.ivir.nl/publications/koelman/privreportdef.pdf>

³ Für eine detaillierte Analyse der verfügbaren Technologien siehe Greenleaf, „IP Phone Home“, ECMS, c-Tech, and Protecting Privacy Against Surveillance by Digital Works, Proceedings of the 21

ECMS werden weniger von individuellen Inhabern von Urheberrechten, sondern mehr von großen Verlagshäusern und Vermittlern (Vertretern der Rechteinhaber) verwendet, die ein starkes Interesse an der Überwachung des Nutzerverhaltens für Zwecke haben, die nichts mit dem Urheberrechtsschutz zu tun haben (z. B. Direktwerbung). Im Gegensatz dazu speichert in der analogen Welt niemand personenbezogene Daten darüber, wer welches Buch wie oft liest. Hier stehen nicht nur der Datenschutz, sondern auch das Recht auf Informationsfreiheit und freie Meinungsäußerung auf dem Spiel.

Zunehmend wird „Rights Management Information“ (RMI) für Zwecke des Urheberrechtsschutzes genutzt. Dazu gehören digitale Wasserzeichen oder andere Techniken, die einen Urheberrechtsgegenstand identifizieren. Diese Information ist durch Bestimmungen des WIPO-Vertrags über Urheberrechte von 1996, die auf die Abwehr der Umgehung von Urheberrechtsschutzmaßnahmen abzielen, geschützt. Allerdings können Rechte-Management-Informationen selbst personenbezogene Daten enthalten, z. B. wenn sie die Identität des Nutzers/Käufers oder die Bedingung einer personalisierten Lizenz enthalten. Daher können sie zur Erhebung und Verbreitung persönlich identifizierender Informationen über die Online-Aktivitäten eines Einzelnen genutzt werden.

Versuche, solche Informationen zu löschen oder Roboter („web spiders“) an der Suche nach solchen Informationen sogar für Zwecke der Direktwerbung zu verhindern, könnten als eine illegale Umgehung von Urheberrechtstechnologien angesehen werden.

Die Überwachung des „Weges“ digitaler Werke kann zum Entstehen eines personenbeziehbaren Nutzerprofils führen. Die Verhinderung des Zugriffs auf urheberrechtlich geschützte Objekte insgesamt, z. B. durch die Nutzung von Verschlüsselung, könnte aus Sicht des Datenschutzes vorzuziehen sein, solange dies nicht im Gegenzug zu einer Registrierung des Nutzerverhaltens führt. Nationale Systeme zur Verhinderung der Veröffentlichung illegaler Inhalte werden beraten, die dem Durchsuchungs- und Beschlagnahme-Modell an Landesgrenzen nachgebildet sind und die nicht nur zur Verhinderung der Verletzung von Urheberrechten verwendet werden könnten, sondern auch zum Auffinden von Material im Cyberspace, das unter dem anwendbaren nationalen Recht illegal ist. Allerdings könnte dies zu einer Aushöhlung des Telekommunikationsgeheimnisses führen und dürfte wegen der Architektur des Internet wenig effektiv sein.

Um einen gerechten Ausgleich zwischen dem Datenschutz der Nutzer und den Rechten der Urheber zu erreichen, ruft die Arbeitsgruppe Planer, Produzenten und Anbieter von ECMS auf,

- a) elektronische Copyright-Management-Systeme zu entwickeln, zu produzieren und anzubieten, die keine personenbezogenen Daten erheben und die anonyme oder pseudonyme Transaktionen erlauben. Die Arbeitsgruppe unterstreicht in diesem Zusammenhang die Ansicht, dass die Nutzer generell die Möglichkeit haben sollten, auf das Internet ohne Preisgabe ihrer Identität zuzugreifen, sofern personenbezogene Daten nicht für die Erbringung eines bestimmten Dienstes erforderlich sind⁴. Unter bestimmten Bedingungen kann die Nutzung von Pseudonymen die Privatsphäre der Nutzer und zugleich die ökonomischen Interessen der Inhaber von Urheberrechten schützen: Digitale Wasserzeichen könnten Transaktions-Codes enthalten, durch die einzelne Kopien nummeriert und diese Nummern mit Angaben über die einzelnen Nutzer in eine sichere Datenbank verbunden werden, die z. B. von einem vertrauenswürdigen Dritten betrieben wird. Diese Verbindung sollte nur zum Zwecke des Schutzes von Urheberrechten z. B. aufgrund eines Gerichtsbeschlusses zugänglich gemacht werden;

International Conference on Privacy and Personal Data Protection, Hong Kong 1999,

http://www2.austlii.edu.au/~graham/publications/ip_privacy/

⁴ Bericht und Empfehlungen zu Datenschutz und Privatsphäre im Internet („Budapest-Berlin-Memorandum“) vom 19.11.1996, Empfehlungen 6 und 9; http://www.datenschutz-berlin.de/attachments/137/bbmen_de.pdf

b) die Nutzer über die Verarbeitung personenbezogener Daten (einschließlich Pseudonyme) durch digitale Werke zu informieren und für die größtmögliche Transparenz beim Betrieb der Copyright-Management-Systeme zu sorgen. Die Arbeitsgruppe unterstützt die Empfehlung 1/99 der Europäischen Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware⁵. Dies gilt auch für die Verarbeitung personenbezogener Daten durch digitale Werke.

Filter- und Überwachungstechniken zur Überwachung von Inhalten gefährden den Datenschutz und das Telekommunikationsgeheimnis. Die Arbeitsgruppe hält sie daher für die Abwehr der Verletzung von Urheberrechten nicht für angemessen.

Der datenschutzfreundliche Schutz des geistigen Eigentums ist unverzichtbar für die Entwicklung des globalen elektronischen Geschäftsverkehrs. Daher sind sowohl eine internationale Regelung im Rahmen der WIPO wie auch Standardisierungsmaßnahmen notwendig, um die Probleme des grenzübergreifenden Schutzes von Urheberrechten unter Nutzung datenschutzfreundlicher Technologien zu lösen.

⁵ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp17de.pdf